European Commission

Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector

FINAL REPORT
A study prepared for the European Commission
DG Communications Networks, Content & Technology by:

Deloitte.

Digital Single Market

This study was carried out for the European Commission by

Deloitte.

Internal identification
Contract number: 30-CE-0791921/00-66
SMART 2016/0080

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Copyright © 2017 – European Union. All rights reserved. Certain parts are licensed under conditions to the EU.
Reproduction is authorised provided the source is acknowledged.

Table of Contents

i

0 Executive Summary 15

1 Introduction 25

1.1 Objectives of this study 25

1.2 Scope of the Study 25

1.3 Structure of this Report 27

2 Methodology 29

2.1 Introduction and overview 29

2.2 The European Commission's public consultation 31

2.3 Online surveys conducted during the study 33

2.4 Interviews with different stakeholders 39

3 Background to the initiative 42

3.1 Introduction 42

3.2 The relevance of the ePD 42

3.3 The content of the ePD 46

3.4 Relationship with other pieces of legislation 50

3.5 The market covered by the ePD 56

Task 1: REFIT exercise (transposition check and evaluation) 68

4 Transposition Check 69

4.1 Introduction 69

4.2 Main findings of the 2015 Study on the ePrivacy Directive 70

4.3 Transposition Check in the 28 Member States 71

5 Answers to the evaluation questions 89

5.1 Introduction 89

5.2 Evaluation questions 90

5.3 Overview of findings 93

5.4 Scope of application and definitions (Articles 1, 2 and 3) 94

5.5 Obligations for service providers on the security of processing and notification of personal data breaches (Article 4) 111

5.6 Confidentiality of electronic communications (Article 5.1 and 5.2) 124

5.7 Confidentiality of information stored on the users' terminal equipment (Article 5.3) 134

5.8 Specific rules on traffic and location data (Articles 6 and 9) 147

5.9 Itemised billing of invoices (Article 7) 155

5.10 Presentation and restriction of calling and connected line (Articles 8 and 10) 159

5.11 Automatic call forwarding (Article 11) 165

5.12 Directories of subscribers (Article 12) 169

5.13 Unsolicited marketing communications sent and received through the Internet (Article 13) 174

5.14 Development and free circulation of electronic communication equipment and services (Article 14) 185

5.15 Enforcement (Article 15a) 189

6 Conclusions on the REFIT evaluation of the ePD 200

6.1 Effectiveness 200

6.2 Efficiency 207

6.3 Relevance 219

6.4 Coherence 223

6.5 EU added value 226

Task 2: Assessment of Options 229

7 Problem assessment 230

7.1 Introduction 230

7.2 Assessment of the Causes 231

7.3 Assessment of the Problems 239

7.4 Assessment of the Effects 259

7.5 The likely development of the problems without policy action (baseline scenario) 262

8 Policy Objectives and Policy Options 264

8.1 Policy objectives 264

8.2 Policy options 265

Objective 3: Simplifying the legal framework and adapting it to the new legal, market and technological reality 266

Objective 3: *Simplifying the legal framework and adapting it to the new legal, market and technological reality* 267

Objective 3: *Simplifying the legal framework and adapting it to the new legal, market and technological reality* 268

1. All the measures under No 1, 2, 3 and 4 of Option 3. 269

2. Explicitly prohibit the practice of denying access to a website or an online service in case users do not provide consent to tracking (so-called cookie-wall). 269

3. All the measures under No 5, 6 and 7 of Option 3. 269

4. Under this option, the Commission would repeal the provision allowing direct marketers to send communications to subscribers and users when they have received their contact details in the context of a previous business relationship 269

5. Measures under No 8 - 12 of Option 3. 269

6. Commission's implementing powers for deciding on the correct application of the ePD instrument where there is an issue of consistency or coherence with EU law. 269

7. Repeal the provisions on calling line identification and directories of subscribers. 269

9 Assessment of the Impacts of the Options 271

9.1 Introduction 271

9.2 Baseline scenario: No policy change 273

9.3 Policy Option 1: Non-legislative ("soft law") measures 286

9.4 Policy Option 2: Limited reinforcement of privacy/confidentiality and simplification 305

9.5 Policy Option 3: Measured reinforcement of privacy/confidentiality and simplification 326

9.6 Policy Option 4: Far reaching reinforcement of privacy/confidentiality and simplification 374

9.7 Policy Option 5: Repeal of the ePD 400

9.8 Comparison of policy options 412

Table of Figures

Figure 1Problem tree 22

Figure 2 - Overview of the different phases and data collection activities 29

Figure 3 – General service offerings by business survey respondents (total n° of responses = 37) .. 34

Figure 4 – Specific types of services by business survey respondents (total n° of responses = 37) .. 36

Figure 5: Digital Market (shares per region) 43

Figure 6 – Intervention logic 49

Figure 7 – Expected breakdown of profiles of primaries (in 2020) 58

Figure 8 – OTT market size and growth by region (in 2020) 58

Figure 9 – Share of third-party tracking tools by the major 6 advertisement networks on websites in selected European markets 62

Figure 10 – Share of third-party tracking tools originating from the four major companies found on major news websites 63

Figure 11 – OBA revenue in the US market (2005-2015, in billion USD) 65

Figure 12 – OBA revenue concentration in the US market (2005-2015, in billion USD) 66

Figure 13 – Share of OBA revenue per type of advertisement in the US market (2014 & 2015) 66

Figure 14 – Usage patterns of citizens regarding different types of telecom services 106

Figure 15 – Aggregated notification and response costs for businesses in selected EU MS between 01/2015 and 03/2016 (in EUR Mio.) 117

Figure 16 – Coherence of security requirements of ePD with other legal instruments 123

Figure 17 – Consumers' assumptions concerning the scope of legislation regarding electronic communication 127

Figure 18 – Importance of confidentiality and security of electronic communication services for consumers 130

Figure 19 – Consumers' preferences with regard to the timing of websites asking for permission to access information or store tools 137

Figure 20 – Users' action to ensure confidentiality of the information stored in their terminal equipment 143

Figure 21 – Users' action to ensure confidentiality of the information stored in their terminal equipment 144

Figure 22 – Consumers' agreement with potential privacy enhancing measures by service providers 144

Figure 23 – Consumers' assessment regarding the encryption of messages 164

Figure 24 – Consumers' assessment of the amount of unsolicited calls 175

Figure 25 – Consumers' preferences regarding the identification of commercial calls 184

Figure 26 – Public Consultation's results regarding fragmentation of enforcement of the ePD 192

Figure 27 – Public Consultation's results regarding confusion in relation to the enforcement of the ePD 193

Figure 28 – Main cost factors for competent authorities in relation to the ePD 197

Figure 29 – Achievement of the specific objectives of the ePD 206

Figure 30 – Number of businesses affected by the ePD per year (2002-2016) 214

Figure 31 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (2002-2016) 215

Figure 32 – Compliance costs of businesses affected by the ePD per year (2002-2016) 215

Figure 33 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (2002-2016) 216

Figure 34 – Average compliance costs of per business affected by the ePD per year (2002-2016) . 216

Figure 35 – Costs from administrative burden of businesses affected by the ePD per year (2002-2016) 217

Figure 36 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (2002-2016) 217

Figure 37 – Average costs from administrative burden per business affected by the ePD per year (2002-2016) 218

Figure 38 – Number of citizens affected by communication services per year (2002-2016) 221

Figure 39 - Problem tree 230

Figure 40 – Usage patterns of citizens regarding different types of telecom services 242

Figure 41 – Consumers' assessment of the amount of unsolicited calls 245

Figure 42 – Number of businesses affected by the ePD per year (2002-2016) 254

Figure 43 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (2002-2016) 254

Figure 44 – Compliance costs of businesses affected by the ePD per year (2002-2016) 255

Figure 45 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (2002-2016) 256

Figure 46 – Average compliance costs of per business affected by the ePD per year (2002-2016) . 256

Figure 47 – Costs from administrative burden of businesses affected by the ePD per year (2002-2016) 257

Figure 48 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (2002-2016) 257

Figure 49 – Average costs from administrative burden per business affected by the ePD per year (2002-2016) 258

Figure 50 – Objectives tree 265

Figure 51 – Number of businesses affected by the ePD per year (baseline scenario, 2016-2030) ... 276

Figure 52 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (baseline scenario, 2016-2030) ... 277

Figure 53 – Compliance costs of businesses affected by the ePD per year (baseline scenario, 2016-2030) ... 277

Figure 54 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (baseline scenario, 2016-2030) ... 278

Figure 55 – Average compliance costs of per business affected by the ePD per year (baseline scenario, 2016-2030) ... 278

Figure 56 – Costs from administrative burden of businesses affected by the ePD per year (baseline scenario, 2016-2030) ... 279

Figure 57 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (baseline scenario, 2016-2030) ... 279

Figure 58 – Average costs from administrative burden per business affected by the ePD per year (baseline scenario, 2016-2030) ... 280

Figure 59 – Estimated developments relating to the use of messaging services ... 282

Figure 60 – Number of citizens affected by communication services per year (baseline scenario, 2016-2030) ... 285

Figure 61 – Number of businesses affected by the ePD per year (policy option 1, 2016-2030) ... 293

Figure 62 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 1, 2016-2030) ... 294

Figure 63 – Compliance costs of businesses affected by the ePD per year (policy option 1, 2016-2030) ... 294

Figure 64 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 1, 2016-2030) ... 295

Figure 65 – Average compliance costs of per business affected by the ePD per year (policy option 1, 2016-2030) ... 295

Figure 66 – Costs from administrative burden of businesses affected by the ePD per year (policy option 1, 2016-2030) ... 296

Figure 67 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 1, 2016-2030) ... 296

Figure 68 – Average costs from administrative burden per business affected by the ePD per year (policy option 1, 2016-2030) ... 297

Figure 69 – Number of businesses affected by the ePD per year (policy option 2, 2016-2030) ... 314

Figure 70 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 2, 2016-2030) ... 315

Figure 71 – Compliance costs of businesses affected by the ePD per year (policy option 2, 2016-2030) ... 315

Figure 72 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 2, 2016-2030) 316

Figure 73 – Average compliance costs of per business affected by the ePD per year (policy option 2, 2016-2030) 316

Figure 74 – Costs from administrative burden of businesses affected by the ePD per year (policy option 2, 2016-2030) 317

Figure 75 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 2, 2016-2030) 317

Figure 76 – Average costs from administrative burden per business affected by the ePD per year (policy option 2, 2016-2030) 318

Figure 77 – Number of businesses affected by the ePD per year (policy option 3, "Browser solution" 2016-2030) 341

Figure 78 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Browser solution" 2016-2030) 342

Figure 79 – Compliance costs of businesses affected by the ePD per year (policy option 3, "Browser solution" 2016-2030) 342

Figure 80 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Browser solution" 2016-2030) 343

Figure 81 – Average compliance costs of per business affected by the ePD per year (policy option 3, "Browser solution" 2016-2030) 343

Figure 82 – Costs from administrative burden of businesses affected by the ePD per year (policy option 3, "Browser solution" 2016-2030) 344

Figure 83 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Browser solution" 2016-2030) 344

Figure 84 – Average costs from administrative burden per business affected by the ePD per year (policy option 3, "Browser solution" 2016-2030) 345

Figure 85 – Number of businesses affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030) 349

Figure 86 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030) 350

Figure 87 – Compliance costs of businesses affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030) 350

Figure 88 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030) 351

Figure 89 – Average compliance costs of per business affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030) 351

Figure 90 – Costs from administrative burden of businesses affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030) 352

Figure 91 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, “Tracking companies solution” 2016-2030) 352

Figure 92 – Average costs from administrative burden per business affected by the ePD per year (policy option 3, “Tracking companies solution” 2016-2030) 353

Figure 93 – Number of businesses affected by the ePD per year (policy option 3, “Publishers solution” 2016-2030) 357

Figure 94 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, “Publishers solution” 2016-2030) 358

Figure 95 – Compliance costs of businesses affected by the ePD per year (policy option 3, “Publishers solution” 2016-2030) 358

Figure 96 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, “Publishers solution” 2016-2030) 359

Figure 97 – Average compliance costs of per business affected by the ePD per year (policy option 3, “Publishers solution” 2016-2030) 359

Figure 98 – Costs from administrative burden of businesses affected by the ePD per year (policy option 3, “Publishers solution” 2016-2030) 360

Figure 99 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, “Publishers solution” 2016-2030) 360

Figure 100 – Average costs from administrative burden per business affected by the ePD per year (policy option 3, “Publishers solution” 2016-2030) 361

Figure 101 – Number of businesses affected by the ePD per year (policy option 4, 2016-2030) 390

Figure 102 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 4, 2016-2030) 391

Figure 103 – Compliance costs of businesses affected by the ePD per year (policy option 4, 2016-2030) 391

Figure 104 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 4, 2016-2030) 392

Figure 105 – Average compliance costs of per business affected by the ePD per year (policy option 4, 2016-2030) 392

Figure 106 – Costs from administrative burden of businesses affected by the ePD per year (policy option 4, 2016-2030) 393

Figure 107 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 4, 2016-2030) 393

Figure 108 – Average costs from administrative burden per business affected by the ePD per year (policy option 4, 2016-2030) 394

Figure 109 – Overall number of businesses affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 418

Figure 110 –Number of micro-enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 419

Figure 111 –Number of SMEs affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 419

Figure 112 –Number of large enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 420

Figure 113 –Number of foreign controlled enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 420

Figure 114 – Compliance costs for all businesses affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 421

Figure 115 – Compliance costs for micro-enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 422

Figure 116 – Compliance costs for SMEs affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 422

Figure 117 – Compliance costs for large enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 423

Figure 118 – Compliance costs for foreign controlled enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 423

Figure 119 –Average compliance costs for all businesses affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 424

Figure 120 – Costs from administrative burden for all businesses affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 425

Figure 121 – Costs from administrative burden for micro-enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 425

Figure 122 – Costs from administrative burden for SMEs affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 426

Figure 123 – Costs from administrative burden for large enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 426

Figure 124 –Costs from administrative burden for foreign controlled enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 427

Figure 125 –Average costs from administrative burden for all businesses affected by the ePD per year under each policy option and the baseline scenario (2016-2030) 427

Table of Tables

Table 1 – Specific objectives of the study 25

Table 2 – Responses to the public consultation by type of stakeholder group 31

Table 3 – Responses to the public consultation by country 32

Table 4 – Type of body the respondents represent (total n° of responses = 34) 33

Table 5 – Number of responses received per Member State (total n° of responses = 34) 34

Table 6 – Cross-tabulation of general and specific types of services reported by business survey respondents (total n° of responses = 37) 37

Table 7 – Ownership structure and associated specific types of services of business survey (total n° of responses = 37) 38

Table 8 – Number of Interviews Performed per type of stakeholders 39

Table 9 – The main legal instruments of the Electronic Communications Package 52

Table 10 – Annual enterprise statistics for the EU telecommunications sector 56

Table 11 – Links between operational objectives and the different articles 90

Table 12 – Our understanding of the evaluation criteria 90

Table 13 – Evaluation questions (incl. status quo) 92

Table 14 – Findings / trends regarding the achievement of the evaluation criteria 93

Table 15 – Initial overview of the scope in relation to the types of services covered per provision 96

Table 16 – The coverage of OTTs within the scope of national implementing legislation 99

Table 17 – Businesses' assessment of the scope of the ePD (total n° of responses = 29) 102

Table 18 – Definitions provided in Article 2 of the ePD 103

Table 19 – Coherence of Articles 1, 2 and 3 with the GDPR and the Electronic Communications package 108

Table 20 – Extent to which respondents encountered problems in relation to the rules on security of processing, per stakeholder group. 112

Table 21 – Reported incidents of personal data breaches in selected EU Member States 113

Table 22 – Coherence of Article 4 with the GDPR, the Electronic Communications package and the RED 121

Table 23 – Extent to which respondents encountered problems in relation to the rules on confidentiality of communications, per stakeholder group 125

Table 24 – Extent to which respondents see an added value in the rules on confidentiality of communications, per stakeholder group 129

Table 25 – Coherence of Article 5(1) and (2) with the GDPR, the Electronic Communications package and the Radio Equipment Directive 131

Table 26 – Necessity of EU rules to ensure an equivalent level of protection (full protection) across the EU regarding the right to privacy and confidentiality 132

Table 27 – Respondents' agreement with the EU added value of rules regarding increasing and harmonising confidentiality 133

Table 28 – Respondents' agreement with the EU added value of rules regarding confidentiality 134

Table 29 – Coherence of Article 5(3) with the GDPR, the Electronic Communications package and the RED 146

Table 30 – Extent to which respondents encountered problems in relation to the rules on traffic and other location data, per stakeholder group 149

Table 31 – Competent authorities' assessment of the functioning of Articles 6 and 9 149

Table 32 – Coherence of Articles 6 and 9 with the GDPR 154

Table 33 – Extent to which respondents encountered problems in relation to the rules on itemised billing, per stakeholder group 156

Table 34 – Extent to which respondents see an added value in the rules on itemised billing, per stakeholder group 157

Table 35 – Extent to which respondents encountered problems in relation to the rules on control over calling line identification, per stakeholder group 160

Table 36 – Challenges reported in the context of Article 8 (total n° of responses = 28) 160

Table 37 – Extent to which respondents see an added value in the rules on control over calling line identification, per stakeholder group 163

Table 38 – Extent to which respondents encountered problems in relation to the rules on automatic call forwarding, per stakeholder group 166

Table 39 – Extent to which respondents see an added value in the rules on automatic call forwarding, per stakeholder group 168

Table 40 – Extent to which respondents encountered problems in relation to the rules on directories of subscribers, per stakeholder group 170

Table 41 – Challenges reported in the context of Article 12 (total n° of responses = 28) 171

Table 42 – Extent to which respondents see an added value in the rules on directories of subscribers, per stakeholder group 173

Table 43 – Extent to which respondents encountered problems in relation to the rules on unsolicited marketing communications, per stakeholder group 175

Table 44 – Complaints by citizens concerning Article 13 by Member State and year 176

Table 45 – Opt-in and opt-out regimes per Member State 177

Table 46 – Extent to which respondents see an added value in the rules on unsolicited marketing communications, per stakeholder group 183

Table 47 – Responses of different stakeholder groups regarding the coherence of Art. 13(1) and 13(3) 184

Table 48 – Coherence of Article 14 with the GDPR, the Electronic Communications package and the RED 187

Table 49 – Necessity of EU rules to ensure the objective of free movement of electronic communication terminal equipment and services in the EU 188

Table 50 –Competent national authorities to enforce the ePrivacy Directive implementing provisions (Articles 5, 6, 9 & 13) 190

Table 51 – Number of FTEs working with tasks related to the ePD in the authorities 195
Table 52 – Comparison of the time consumed for the different tasks 196
Table 53 – Coherence of Article 15a with the GDPR and the Electronic Communications package. 198
Table 54 – Main findings in relation to the operational objectives 201
Table 55 – Challenges hindering the success of the ePD (total n° of responses = 28) 205
Table 56 – Main findings in relation to the efficiency of the provisions 207
Table 57 – Key quantitative data estimated in relation to the REFIT exercise (2002-2016) 213
Table 58 – Key quantitative data estimated in relation to the REFIT exercise (2002-2016) 219
Table 59 – Main findings in relation to the relevance of the provisions 222
Table 60 – Main findings in relation to the coherence of the provisions 223
Table 61 – Main findings in relation to the EU added value of the provisions 227
Table 62 – Overview of the scope in relation to the types of services covered per provision 231
Table 63 – Opt-in and opt-out regimes per Member State 236
Table 64 – Number of citizens potentially affected based on the usage rates of relevant services ... 241
Table 65 – The coverage of OTTs within the scope of national implementing legislation 243
Table 66 – Number of citizens potentially affected based on the usage rates of relevant services ... 244
Table 67 – Complaints by citizens concerning Article 13 by Member State and year 246
Table 68 – Main findings in relation to the costs for businesses generated by the individual provisions 248
Table 69 – Key quantitative data estimated in relation to the REFIT exercise (2002-2016) 252
Table 70 – Key quantitative data estimated in relation to the REFIT exercise (2002-2016) 259
Table 71 –Policy Options suggested by the European Commission 266
Table 72 – Qualitative rating of the impacts of the baseline scenario 273
Table 73 – Key quantitative data estimated in relation to the baseline scenario (2016-2030) 275
Table 74 – Key quantitative data estimated in relation to the baseline scenario (overall 2016-2030) 281
Table 75 – Qualitative rating of the impacts of Policy Option 1 286
Table 76 – Qualitative classification of the impacts of policy option 1 on costs for businesses 288
Table 77 – Key quantitative data estimated in relation to policy option 1 (2016-2030) 291
Table 78 – Key quantitative data estimated in relation to policy option 1 (overall 2016-2030) 298
Table 79 – Qualitative classification of the impacts of policy option 1 on costs for public administrations 299
Table 80 – Qualitative rating of the impacts of Policy Option 2 305
Table 81 – Qualitative classification of the impacts of policy option 2 on costs for businesses 308
Table 82 – Key quantitative data estimated in relation to policy option 2 (2016-2030) 312

Table 83 – Key quantitative data estimated in relation to policy option 2 (overall 2016-2030) 319

Table 84 – Qualitative classification of the impacts of policy option 2 on costs for public administrations 320

Table 85 – Qualitative rating of the impacts of Policy Option 3 326

Table 86 – Qualitative classification of the impacts of policy option 3 on costs for businesses 329

Table 87 – Key quantitative data estimated in relation to policy option 3 ("browser solution", 2016-2030) 339

Table 88 – Key quantitative data estimated in relation to policy option 3 ("browser solution", overall 2016-2030) 346

Table 89 – Key quantitative data estimated in relation to policy option 3 ("tracking companies solution", 2016-2030) 347

Table 90 – Key quantitative data estimated in relation to policy option 3 ("tracking companies solution"), overall 2016-2030) 354

Table 91 – Key quantitative data estimated in relation to policy option 3 ("publishers solution"), 2016-2030) 355

Table 92 – Key quantitative data estimated in relation to policy option 3 ("publishers solution"), overall 2016-2030) 362

Table 93 – Qualitative classification of the impacts of policy option 3 on costs for public administrations 364

Table 94 – Opt-in and opt-out regimes per Member State 371

Table 95 – Qualitative rating of the impacts of Policy Option 4 375

Table 96 – Qualitative classification of the impacts of policy option 4 on costs for businesses 377

Table 97 – Key quantitative data estimated in relation to policy option 4 (2016-2030) 388

Table 98 – Key quantitative data estimated in relation to policy option 4 (overall 2016-2030) 395

Table 99 – Qualitative classification of the impacts of policy option 4 on costs for public administrations 397

Table 100 – Qualitative rating of the impacts of Policy Option 5 400

Table 101 – Qualitative classification of the impacts of policy option 5 on costs for businesses 403

Table 102 – Key quantitative data estimated in relation to policy option 5 (2016-2030) 405

Table 103 – Key quantitative data estimated in relation to policy option 5 (overall 2016-2030) 407

Table 104 – Qualitative classification of the impacts of policy option 5 on costs for public administrations 408

Table 105 – Qualitative rating of the impacts of the policy options 413

Table 106 – Key figures of the quantitative assessments concerning businesses (absolute values) 415

Table 107 – Key figures of the quantitative assessments concerning businesses (absolute changes) 416

Table 108 – Key figures of the quantitative assessments concerning businesses (relative changes) 416

Table 109 – Key figures of the quantitative assessments concerning citizens (absolute values) 428

Table 110 – Key figures of the quantitative assessments concerning citizens (absolute changes) ... 428

Table 111 – Key figures of the quantitative assessments concerning citizens (relative changes) 429

0 Executive Summary

Introduction

The study "Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector" was conducted to support the Commission in gathering the evidence base needed to evaluate Directive 2002/58/EC on privacy and electronic communications[1],(hereafter "ePD"), and to assist the Commission in assessing a number of policy options, notably from an economic perspective. The study was performed with a view to collect fact and figures, as well as other relevant information, to be used by the Commission in the Regulatory Fitness and Performance Programme[2] (hereafter "REFIT) evaluation of the ePD and in the work of assessing the policy options that could lead to a possible legislative revision.

Context

The ePD forms part of the Regulatory Framework for Electronic Communications, first adopted in 2002, amended in 2009 and 2013. The ePD regulates the processing of personal data and the protection of privacy in the electronic communications sector, and has implemented into national laws in all EU Member States. The scope of the rules set out in the ePD is limited to services that qualify as an "electronic communications service".

Specifically, the ePD lays down rules on (1) security obligations by electronic communication services providers (Article 4); (2) confidentiality of electronic communications and related traffic data (Article 5(1); (3) confidentiality of electronic communication terminal equipment (Article 5(3)); (4) the processing of traffic data and location data (Article 6 and 9); and (5) the sending of unsolicited communications (Article 13(1)). The ePD also regulates issues such as itemised billing (Article 7), presentation and restriction of calling and connected line identification (Article 8) and related exceptions (Article 10), automatic call forwarding (Article 11), directories of subscribers (Article 12), and technical features and standardisation (Article 14). It also specifies the circumstances and conditions under which Member States may adopt legislative measures to restrict the scope of certain rights and obligations provided for under the ePD (Article 15), and the rules concerning implementation and enforcement (Article 15a).

The Data Protection Directive 95/46/EC[3] (hereafter "Personal Data Protection Directive") and the ePD are complementary since they both apply to the electronic communications sector, even though their respective scopes differ. The Personal Data Protection Directive applies to all sectors, including the electronic communications sector, provided that the subject matter in question is not regulated by the *lex specialis* laid down by the ePD. The general rule is that where provisions overlap, the ePD (i.e. *lex*

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002.
[2] COM(2012) 746 final http://ec.europa.eu/smart-regulation/better_regulation/documents/com_2013_en.pdf
[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 , 23/11/1995

specialis) overrides the Personal Data Protection Directive (i.e. *lex generalis*). In other words, where no specific rules exist in the ePD, the Personal Data Protection Directive will apply by

However, the study should be seen in light of the recent adoption of the General Data Protection Regulation (hereafter ”GDPR”), set to enter into force in May 2018, which has resulted in the relevance of several provisions of the ePD to be questioned. As the Personal Data Protection Directive will be repealed and replaced by the GDPR, it is crucial to ensure consistency and coherency between the ePD rules and the GDPR.

In the 2015 European Commission Communication on a Digital Single Market Strategy for Europe (hereafter “DSM Communication”), the review of the ePD was highlighted as one of the priorities under the roadmap for completing the Digital Single Market. Importantly, the DSM Communication stressed that the ePD review should aim to ensure a high level of protection for data subjects and a level playing field for all market players.

Finally, this study, is part of a wider reform of the EU’s telecoms policy (aimed at facilitating increased access to fast broadband across the EU, as well as smoothing out differences in regulation faced by telecoms groups and their internet competitors).

About the study

This study is divided into two main tasks, (1) the Regulatory Fitness and Performance Programme4 (hereafter “REFIT) exercise, which is retrospective (i.e. from 2002 to 2016), and (2) the assessment of policy options, which is prospective (i.e. from 2016 and 2030).

Concretely, the REFIT part consists of a transposition check covering all EU Member States and the evaluation. The objectives of this first task was to gather evidence on the transposition and implementation of the ePD of certain provisions[5], and to evaluate the performance of the entire ePD in the light of the Better Regulation Guidelines[6] evaluation criteria.

Regarding the second task, the assessment of policy options, the objectives were to identify the relevant problems to be addressed, building on Task 1, and to assess and compare the policy options (defined in close interaction with the European Commission Project Team), providing the necessary quantitative and qualitative empirical evidence and quantifying, to the extent possible, costs and benefits.

For the prospective part, the key questions addressed include, but were not limited to, the following:

- What is the problem and why is it a problem?
- What are their economic, social and environmental impacts and who will be affected?
- How do the different options compare in terms of their effectiveness and efficiency (benefits and costs)?[7]

With regard to the assessment of the impacts of the policy options, the study covers the following assessment criteria:

- Economic impacts:
  - Impacts on costs for businesses (incl. SMEs and micro-enterprises);

[4] COM(2012) 746 final http://ec.europa.eu/smart-regulation/better_regulation/documents/com_2013_en.pdf
[5] Article 1, Article 2, Article 3, Article 4, Article 7, Article 8, Article 10, Article 11 and Article 12.
[6] European Commission, Better Regulation Guidelines, 19 May 2015, SWD(2015) 111 final (http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm).
[7] European Commission, Better Regulation Guidelines, 19 May 2015, SWD(2015) 111 final (http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm).

- Impacts on costs for public authorities;
- Other economic impacts (incl. impacts on competition, opportunity costs, and Online Behavioural Advertising (OBA) markets;

- Effectiveness in reaching the policy objectives; and
- Social impacts (incl. impacts on employment and labour markets).

The following sources form the body of evidence for this study:

- Desk research, including:
  - Literature;
  - Statistics;
  - Transposition check;
  - An analysis of the European Commission's public consultation[8];
  - The results of the Flash Eurobarometer 443 on e-Privacy;[9]
  - Other types of documents provided by the Commission, including the minutes of two workshops that were held by the Commission in spring 2016;[10]
- Legal analyses in relation to the coherence of the ePD with other instruments;
- An analysis of the online surveys organised by our project team with businesses and competent authorities; and
- Inputs received based on interviews carried out by members of the project team.

The data collected underwent a horizontal data analysis and triangulation. For the approach on the economic and quantitative data please see Annex A.

REFIT Exercise - retrospective part

Main findings

The **REFIT exercise included a transposition check** to monitor national laws by conducting an in-depth analysis of the national implementation of the following nine (9) ePD provisions: 1-4, 7-8, 10 - 12. The analysis sought to assess the information gathered, identify and discuss common trends among EU Member States, including deviations from the letter and the spirit of the ePD, national specificities or overlaps, and, in general, diverging transpositions. To this end, the following modes of transposition were considered:

- **Literal transposition**: meaning that the specific article was incorporated in the national legislation word-by-word or with a semantic equivalence to the formulation of the ePD;
- **Full transposition** without material differences: meaning that the provision was not literally incorporated in national legislation but that the requirements and objectives of the ePD have been fully transposed in local law;
- **Partial transposition**: meaning that the scope of the article was narrowed in national legislation, with the provisions of the ePD not being fully covered;
- **Full transposition but with a broader scope**: meaning that the provision was fully transposed but that national legislation provides additional details or requirements;
- **No transposition**: meaning that the requirements and objectives of the provision were not transposed in national legislations by any means.

[8] See: https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive. Our analysis focuses on key closed questions dealing with the evaluation of the current legal framework. The aspects relating to potential future changes (policy options) have only been taken into account to a limited extent.
[9] Survey requested by the European Commission, Directorate-General for Directorate General Digital Single Market and coordinated by the Directorate-General for Communication, carried out by TNS Political & Social. For this report we used the preliminary raw data.
[10] One of the workshops involved national competent authorities for the ePD, while the other workshop gathered various stakeholders from the industry, civil society and consumer associations.

The **main conclusions of the transposition check** at the Member State level[11] include

- Overall, Member States have relied on the formulation provided by the ePD, notwithstanding the many deviations that occur in terms of form, specific local requirements, and applicable procedures. Cases of semantic equivalence are very common across the various forms of transposition.
- With the exception of a number of areas such as itemised billing or the mechanisms for handling nuisance calls, the provisions of the ePD have been almost entirely transposed across Member States. Although national approaches vary considerably in terms of procedure and requirements, it is possible to discern a common level of protection of users and subscribers across all Member States, evidence that the ePD has been instrumental in providing a minimum, harmonised background.
- The question of whether Over-The-Top (OTT) service providers and private networks are subject to the requirements of the ePD and the corresponding national implementing acts has not been uniformly addressed in the transposition of the ePD. Member States vary considerably in their approach to this topic. Therefore, the role and importance of case law and administrative decisions in each Member State therefore cannot be overstated.
- While no national implementing law explicitly refers to the inclusion of OTT services and private networks, a number of cases have arisen where administrative decisions, taking into account the functional equivalence between services traditionally covered by the ePD and these new forms of communication, ruled that the national law also applied to at least a part of these services. VoIP services seem to be particularly in scope in those Member States where this extensive interpretation was adopted. This represents a deviation in the transposition of the ePD, which was not originally intended to cover these types of services. In other Member States, we have found that there is a lively but ultimately inconclusive debate on whether such services should be covered by the ePD or the corresponding national acts.
- Based on the uneven transposition of the ePD, is it possible to conclude that the current situation obscures the level of legal certainty by obliging operators and users to consult secondary sources of law, some of which might not always be readily accessible or drafted with the principal concern of clarity. More importantly, the current status quo provides for appreciable differences in legal treatment across Member States, creating an uneven playing field for operators and a potential obstacle to the goals set out by the ePD.
- The ePD was transposed by means of a great variety of legal instruments. While some Member States adopted specific legal acts designed solely for the transposition, others incorporated the provisions of ePD in existing laws, and occasionally into their omnibus telecommunications regulations. While this still represents transposition, there were cases in which the specific references to the protection of privacy and confidentiality in the ePD did not immediately result from the implementing act.

The evaluation was conducted in line with the *Better Regulation Guidelines*[12], with the analysis covering the following five evaluation criteria: These evaluation criteria include:

- Effectiveness;
- Efficiency;
- Relevance;
- Coherence; and
- EU added value.

[11] For the conclusions on the transposition check per article, please refer to chapter 4
[12] European Commission, Better Regulation Guidelines, 19 May 2015, SWD(2015) 111 final (http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm).

In terms of the key findings, the overview table below illustrates the achievement of the evaluation criteria in relation to each Article. The following colour coding indicates identified trends regarding the extent to which an evaluation criterion seems to be achieved based on the information available:

- Achieved / tends to be achieved;
- Partially achieved or not achieved; and
- Insufficient information to assess or criterion not relevant.

Table - Findings / trends regarding the achievement of the evaluation criteria

Topic	Effectiveness	Efficiency	Relevance	Coherence	EU added value
Scope of application and definitions (Article 1, 2 and 3)					
Security of processing (Article 4)					
Security of communications (Article 5.1 and 5.2)					
Confidentiality of information stored on users' terminal equipment (Article 5.3)					
Traffic data and other location data (Article 6 and 9)					
Itemised billing (Article 7)					
Presentation and restriction of calling and connected line identification (Articles 8 and 10)					
Automatic call forwarding (Article 11)					
Directories of subscribers (Article 12)					
Unsolicited communications (Article 13)					
Development and free circulation of electronic communication equipment and services (Article 14)					
Implementation and enforcement (Article 15a)					

Source: Deloitte.

Effectiveness - While the ePD has contributed to enable more trust and confidence in the market, its effectiveness has not been fully achieved. Although some of the provisions seem to function quite well, several challenges could be identified at the level of the operational objectives. In addition to the challenges identified in relation to the individual provisions and/or operational objectives, a number of horizontal challenges were identified, related to the complexity of the rules. Such challenges lead to difficulties in relation to the achievement of the specific and general objectives.

Efficiency - The analysis focussed on the regulatory burden, complexity, and costs which form an integral part of the assessment of the efficiency of the ePD. The available information points towards a limited efficiency of the ePD in relation to both businesses and citizens.

Across the board, stakeholders highlighted the fragmented implementation of the ePD at the national level and subsequent complexity as an issue and an important source of cost. Businesses, for instance, were not able to leverage existing legislative requirements and obligations for the business model but need to adapt. Some Member States transposed the ePD in a more restrictive manner than provided by the ePD (as well as compared to other Member States). Business associations pointed

out that the costs related to the ePD are disproportionate. For instance, the costs related to the cookie provision are not seen as justified since the provision failed to accomplish its purpose. From the perspective of the telecom sector, the ePD legislation has disproportionate implementation costs due to the fact that different actors providing the same services are subject to different rules.

Relevance – The specific objectives and the overall relevance of the ePD were confirmed by the stakeholders. In principle, the ePD is still relevant with a view to both achieving the DSM and strengthening the right to the protection of confidentiality of communications and personal data. This supported the relevance of its specific objectives; "to ensure that the right to privacy and confidentiality with respect to the processing of personal data in the electronic communications sector is respected" and "to ensure the free movement of personal data in the internal market". However, although its objectives are still relevant, its scope is not fully in line with society's needs. For instance, technological developments have altered how citizens communicate, for instance via channels provided by OTT service providers, which are currently not in scope of the ePD. Hence, for a significant part of electronic communications, EU citizens are not enjoying the same levels of confidentiality and data protection as they do while using traditional means of communications. On this basis, not all the operational objectives appear to be fully relevant.

Coherence - The analysis focused on the coherence of the ePD with the GDPR, the Electronic Communications Package, the RED as well as the EU's aim to achieve the DSM. On this basis, the ePD does not seem to be fully coherent with the relevant instruments. Notably, while the ePD is largely coherent with the Electronic Communications Package and the Radio Equipment Directive (RED), there are potential challenges in relation to the GDPR and the DSM.

The ePD is to be considered as a *lex specialis* in relation to the GDPR since it provides more specific rules for the electronic communications sector. However, the findings points to some potential challenges in relation to a number of specific provisions. These include the following articles:

- **Services concerned (Article 3)**: There may be a lack of clarity as to whether the ePD or the GDPR applies, based on the distinction of "public or publicly available electronic communications services";
- **Notification of personal data breaches (Article 4.3 and 4.4)**: The procedures for personal data breaches vary considerably. Thus, the same business may need to follow different procedures in case it offers electronic communications and other services;
- **Confidentiality of the Communications (Article 5.3)**: From the interplay between the provisions in the ePD and the GDPR, it is not clear what level of information has to be provided to a subscriber who is not a natural person; and
- **Implementation and Enforcement (Article 15a)**: There are differences as concerns the application of fines and sanctions for the breach of provisions related to the processing of personal data and as for the competent authorities.

While in general terms, the objectives of the ePD are coherent with the goal to establish the DSM, including to create the right conditions and level playing field for advanced digital networks and innovative services, built *"on reliable, trustworthy, high-speed, affordable networks and services that safeguard consumers' fundamental rights to privacy and personal data protection while also encouraging innovation".*[13] However, it represents a potential challenge to the aims of the DSM that

[13] Communication COM(2015) 192 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, p. 9 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN.

the scope of the ePD is limited to public or publicly available electronic communication services. In fact, the European regulatory landscape with regard to the online environment still operates on the basis of the distinction between three differently regulated legal bases:

- Information society services (E-Commerce Directive);
- Electronic communications services (Telecoms package); and
- Audio-visual media services (Audio-visual Media Service Directive).[14]

Finally, as regards the individual provisions of the ePD, coherence was been confirmed for most of them, while issues exist in relation to Article 4 and Articles 6 and 9.

EU added value - The EU added value of harmonised rules on privacy and confidentiality can be confirmed. It was already recognised at the time of the adoption of Directive 95/46/EC and the ePD itself that there is a need to address data protection, including in the electronic communications sector, at the EU level. It was argued that the establishment of the internal market, as well as the introduction of new telecommunications networks would necessarily lead to a substantial increase in cross-border flows of personal data. A potential difference in levels of protection was expected to constitute a barrier to the functioning of the internal market, as data exchanges may be hindered[15]

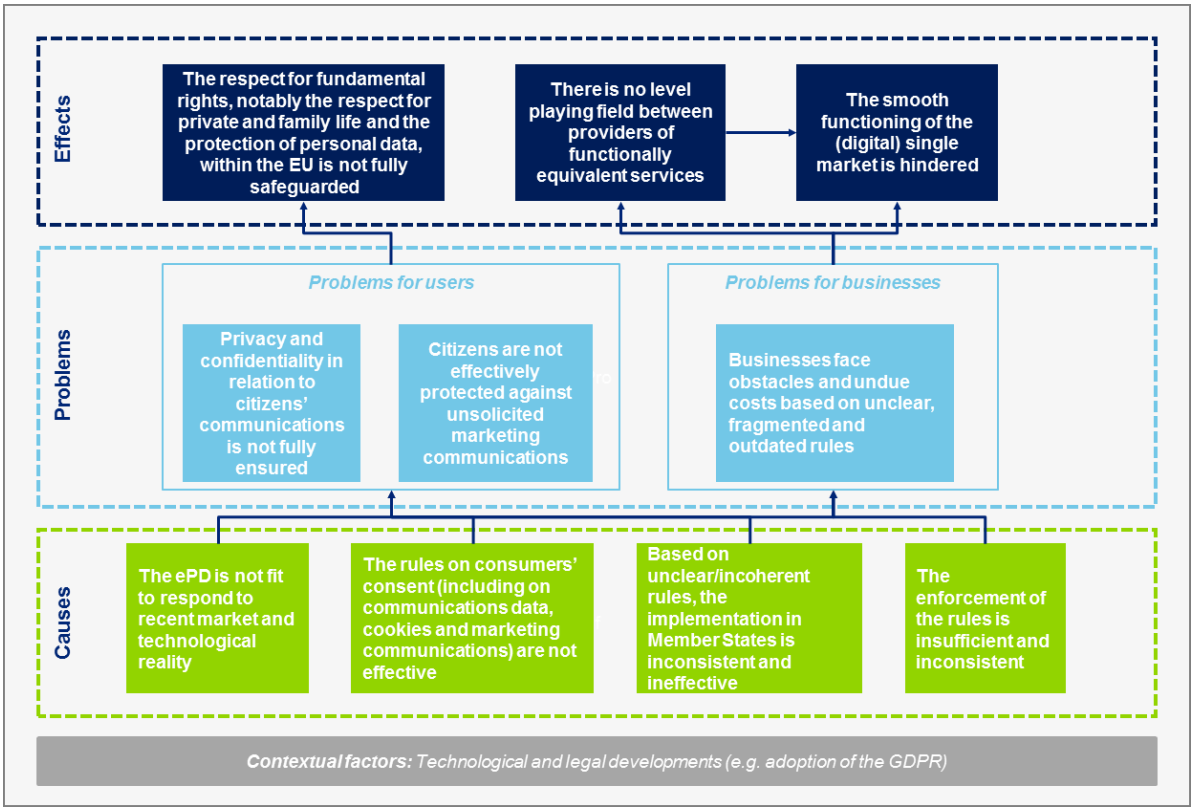
This assessment is still valid today, as pointed out in the recent Impact Assessment on the GDPR. The EU is best placed to ensure an effective and consistent protection for individuals, in particular when personal data is transferred across borders, as common standards are required for this purpose.[16]

Assessment of options - prospective part

The starting point of the impact assessment consists of an assessment of the current problems. This takes into account an identification and analysis of the problems, their causes and their effects / impacts, taking into account how different stakeholder groups are affected. Our understanding of the problems covered by the present assignment, their causes and effects is presented below by means of a problem tree, which should be read from the bottom to the top.

[14] Sandfeld Jakobsen, S. (2014). *EU Internet law in the era of convergence: the interplay with EU telecoms and media law*. In. Savin, A. & Trzaskowski, J. (eds.) (2014). Research Handbook on EU Internet Law, Cheltenham, UK: Edward Elgar, p. 60.
[15] Recitals (5), (6), (7), and (8) of Directive 95/46/EC; Recital (8) of the ePD.
[16] Impact Assessment Accompanying the document "Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 10 final, p. 37.

Figure 1Problem tree



Source: Deloitte

Five policy options were prepared and proposed by the European Commission, which were the basis of the assessment of options as a part of this study. These policy options can be summarised as follows:

Policy Option 1: Non-legislative ("soft law") measures

Under this option, the Commission proposes to make extensive use of its implementing powers and use soft policy instruments in order to improve the protection of the users (i.e. EU citizens). While the specific contents of the individual measures cannot be delineated with precision at this stage, possible actions could include, but are not limited to, increased use of interpretative communications, support EU-wide self-regulatory initiatives, awareness-raising initiatives and support MS cooperation.

Policy Option 2: Limited reinforcement of privacy/confidentiality and simplification

Under this option the Commission would propose minimum changes to the current Directive with a view to adjust privacy and confidentiality provisions and to improve harmonisation and simplification of the current rules. Proposed actions under this policy option include an extension of the scope of the ePD to OTTs providing communications functions, such as webmail, Internet messaging, VoIP, as well as a clarification that the ePD applies to publicly available communications networks, such as in particular commercial Wi-Fi networks in stores, hospitals, airports, etc.

Policy Option 3: Measured reinforcement of privacy/confidentiality and simplification

Under this option, the Commission would propose a new ePrivacy instrument, complementing and particularising the GDPR, including selective measures to reinforce privacy/confidentiality and harmonisation/simplification.

- ***Policy Option 4: Far reaching reinforcement of privacy/confidentiality and simplification***

Under this option, the Commission would propose a new ePrivacy legal instrument, such as a new ePrivacy Regulation, with significant reinforcement and harmonisation/simplification, more far reaching measures enhancing the protection of privacy/confidentiality and guaranteeing greater simplification/harmonisation.

- ***Policy Option 5: Repeal of the ePD***

Under this option, the Commission would propose the repeal of the ePD. In this scenario, the GDPR provides for reinforced rights of individuals and the obligations of data controllers, which are in keeping with the challenges of the digital age. The GDPR would guarantee more effective enforcement in view of the reinforced powers conferred on data protection authorities.

As for the **final impact assessment**, the assessment of the impacts of the options included the following types of impacts[17], as per agreement with the Commission:

- Economic impacts[18];
- Effectiveness in reaching the policy objectives; and
- Social impacts.

The assessment of the **economic impacts** vis-à-vis the baseline scenario, included the compliance costs, as well as the costs from administrative burden for businesses (of different size classes, incl. SMEs and micro-enterprises) were assessed, as well as the costs for public administrations

The assessment of the **effectiveness** is related to the contributions of the policy options to effectively achieve the policy objectives. This assessment focused on the specific policy objectives:[19]

- To ensure effective confidentiality and security of communications;
- To ensure that citizens are effectively protected against unsolicited marketing communications; and
- To simplify the legal framework and adapt it to the new legal, market and technological reality

The assessment of the **societal impacts,** in line with the Better Regulation Guidelines, focused on impacts on employment and labour markets. Issues such as effects on income, its distribution and social inclusion have been excluded from the analysis.

Based on a qualitative rating, **Policy Option 3 with the Browser solution is the best performing policy option**. It achieves cost savings for businesses and entails very low costs for public administration. This option would have positive impacts on competition, notably based on the extension of the scope to OTTs. At the same time, some stakeholders would incur opportunity costs (OTTs and other businesses based on changes envisaged with respect to Article 13). The impact on

[17] This means that the European Commission has confirmed that legal impacts of the policy options (incl. on the coherence, as well as on Fundamental Rights) are excluded from the scope of the assessment. This is also valid for the assessment of the proportionality of the policy options.
[18] The assessment of the impacts is focused on the assessment of the economic impacts as this was prioritised by the European Commission.
[19] Specific objectives relate to the specific domain and set out what the Commission wants to achieve with the intervention in detail. General objectives refer to Treaty-based goals and constitute a link with the existing policy-setting.

SMEs would be mixed. In addition, this policy option achieves the best rating when it comes to the achievement of the objectives. It does not entail any significant social impacts.

We note that policy option 5 also scores well, especially because it would entail the highest cost savings for businesses. However, it does not reach 2 of the three policy objectives studied.

1 Introduction

1.1 Objectives of this study

The purpose of this study is twofold:

- To support the Commission in gathering the evidence base needed to evaluate the ePD; and
- To assist the Commission in assessing potential policy options to amend the Directive.

The assignment therefore includes a retrospective part, i.e. the evaluation of the current rules, as well as a prospective part, i.e. the assessment of potential policy options to amend the current legal framework.

In terms of the evidence gathering, emphasis was put on the quantitative aspects, including a strong economic component, including cost-benefit and cost-effectiveness analysis, using robust research and analysis methods, to the extent possible.

In light of these considerations and based on the Tasks stipulated in the Terms of Reference (ToR), the study has the following specific objectives:

Table 1 – Specific objectives of the study

Task	Objectives of task
Task 1: *REFIT exercise* (retrospective part)	• To gather evidence on the transposition and implementation of the ePD of certain provisions[20]; • To evaluate the performance of the entire Directive in the light of the Better Regulation[21] evaluation criteria;
Task 2: *Assessment of Options* (prospective part)	• Building on Task 1, to identify the relevant problems to be addressed; • To assess and compare the preliminary policy options provided by the Commission, providing the necessary quantitative and qualitative empirical evidence and quantifying as far as possible costs and benefits. The final options retained in the impact assessment may to a certain extent differ than the initially designed ones.

Source: Deloitte

1.2 Scope of the Study

As outlined above, the study will include two main tasks, reflecting a retrospective and a prospective part.

[20] Article 1, Article 2, Article 3, Article 4, Article 7, Article 8, Article 10, Article 11 and Article 12.
[21] European Commission, Better Regulation Guidelines, 19 May 2015, SWD(2015) 111 final (http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm).

In relation to the **retrospective part**, we will cover in line with the ToR and the *Better Regulation Guidelines*[22] the following five evaluation criteria:

- Effectiveness;
- Efficiency;
- Relevance;
- Coherence; and
- EU-added value.

As concerns the **prospective part**, we base our approach on the Commission's guidelines on impact assessment as contained in the *Better Regulation Guidelines*[23]. We note that these include seven questions, which normally need to be treated as part of an impact assessment:

- **What is the problem and why is it a problem?**
- Why should the EU act?
- What should be achieved?
- What are the various options to achieve the objectives?
- **What are their economic, social and environmental impacts and who will be affected?**
- **How do the different options compare in terms of their effectiveness and efficiency (benefits and costs)?**
- How will monitoring and subsequent retrospective evaluation be organised?

While it is important to keep all these aspects in line in order not to miss any important aspects, this study focuses on the **bold** questions in line with the ToR.

With regard to the assessment of the impacts of the policy options, the study covers the following assessment criteria:

- Economic impacts:
  - Impacts on costs for businesses (incl. SMEs and micro-enterprises);
  - Impacts on costs for public authorities;
  - Other economic impacts (incl. impacts on competition, opportunity costs, and Online Behavioural Advertising (OBA)[24] markets;
- Effectiveness in reaching the policy objectives; and
- Social impacts (incl. impacts on employment and labour markets).

The **thematic scope** of the study covers the entirety of the ePD.

In the context of the **transposition check**, it has been taken into account that the Commission concluded a *Study on the ePD concerning the assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation* in February 2015 (the "2015 Study"). The 2015 study did not deal with the entire ePD, but focused on the five following articles:

- Articles 1 and 3 on the scope;
- Article 5 on confidentiality;
- Article 5(3) on confidentiality of terminal equipment;
- Articles 6 and 9 on traffic and location; and

[22] European Commission, Better Regulation Guidelines, 19 May 2015, SWD(2015) 111 final (http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm).
[23] European Commission, Better Regulation Guidelines, 19 May 2015, SWD(2015) 111 final (http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm).
[24] See: https://ec.europa.eu/digital-single-market/en/glossary#o.

- Article 13 on unsolicited communications.[25]

The present study builds upon the insights of the 2015 study in order to support the Commission in the evaluation of the ePD. Therefore, for the purpose of the transposition check, the assignment focuses on the articles that were not covered in the 2015 study.

However, for the **evaluation** in the light of the Better Regulation principles and impact assessment, the entire ePD was considered. In addition to the ePD itself, adjacent legal and policy instruments are also covered, for example as part of the analysis of the relevance and coherence criteria. In this regard, the GDPR and the Electronic Communications Package part of which is the ePD, are particularly important[26].

As far as the **geographic scope** is concerned, the aim was to provide a holistic view of the national implementation of the provisions listed above.

The **timeframe** covered by retrospective part was the time since the adoption of the current Directive (which repealed the 97/66 Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector) until today, i.e. from 2002 to 2016. For the prospective part we cover the years between 2016 and 2030.

1.3 Structure of this Report

The structure of the draft Final Study Report contains the following elements:

- *Horizontal aspects:*
  - *Chapter 2:* Brief outline of the methodology and the evidence based used for this report;
  - *Chapter 3:* Brief analysis of the policy context of the ePD, incl. its relevance, content, and relationship with other EU legal instruments, as well as the market covered;
- *Task 1: REFIT exercise:*
  - *Chapter 4:* Findings of the transposition check;
  - *Chapter 5:* Answers to the evaluation questions in relation to each of the substantial provisions of the ePD;
  - *Chapter 6:* Conclusions for the entire ePD;
- *Task 2: Assessment of the options:*
  - *Chapter 7:* Problem assessment;
  - *Chapter 8:* Policy objectives and policy options (as defined by the European Commission in interaction with the Deloitte project team); and
  - *Chapter 9:* Assessment of the impacts and comparison of the Policy Options vis-à-vis the baseline scenario.

In addition to these Chapters, the report contains the following Annexes:

- Annex A: Economic Analysis;
- Annex B: Horizontal analysis of the interviews carried out;
- Annex C: Analysis of Deloitte's online surveys;

[25] European Commission, ePD Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, 2015, (https://ec.europa.eu/digital-single-market/news/ePD-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data).
[26] More details on the EU Regulatory Framework for electronic communications can be found at: https://ec.europa.eu/digital-single-market/en/telecoms-rules.

- Annex D: Other information sources;
- Annex E: Detailed transposition check of individual provisions; and
- Annex F: Detailed tables relating to the coherence of the ePD with other relevant instruments.

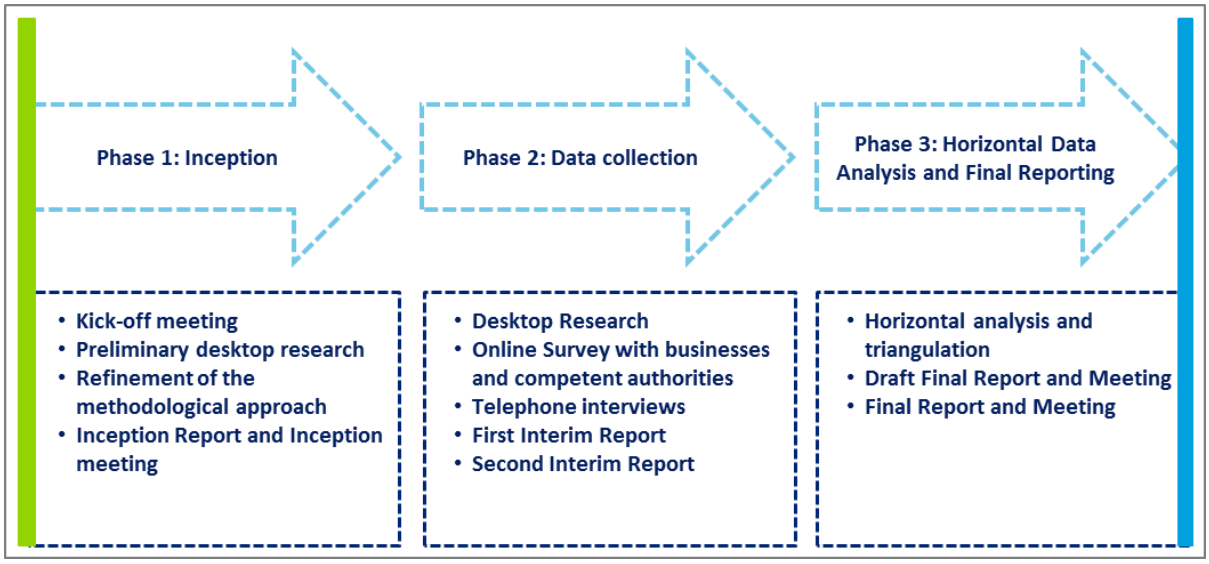
2 Methodology

In this section, we present an overview of our methodological approach and data collection activities. We also provide an overview of the available evidence used in the analysis of our findings outlined in this report.

2.1 Introduction and overview

As presented in Figure 1, the assignment is structured around three main phases. Relevant data was collected through the implementation of the methods foreseen in Phase 2 of the assignment.

Figure 2 - Overview of the different phases and data collection activities



Source: Deloitte

The **transposition check** was carried out with the help of a network of legal/privacy experts in the Member States, who all received a common template to facilitate the data collection and analysis. As noted in section 1.2, this study builds upon the insights of the 2015 Study in order to support the Commission in the evaluation of the ePD. Regarding the transposition check, the assignment, therefore, focuses on the articles that were not covered in the 2015 study.[27]

Both the **REFIT** exercise, i.e. the evaluation of the ePD, as well as the **Impact Assessment** are based on the following methodological elements:

- Desk research, including:
  - Literature;

[27] As mentioned above, the 2015 Study focused on the following articles: Articles 1 and 3 on the scope; Article 5 on confidentiality; Article 5(3) on confidentiality of terminal equipment; Articles 6 and 9 on traffic and location; and Article 13 on unsolicited communications.

- Statistics;
- Transposition check;
- An analysis of the European Commission's public consultation on the ePD[28];
- The results of the Flash Eurobarometer 443 on e-Privacy;[29]
- Other types of documents provided by the Commission, including the minutes of two workshops that were held by the Commission in spring 2016;[30]

- Legal analyses in relation to the coherence of the ePD with other instruments;
- An analysis of the online surveys organised by our project team with businesses and competent authorities; and
- Inputs received based on interviews carried out by members of the project team.

Limitations in relation to data relating to costs associated with the ePD

We made use of various channels to gather data on the costs associated with the implementation of the ePD, including in particular desk research (e.g. journal articles and the EC's public consultation), as well as two online surveys addressed to businesses and competent national authorities and interviews with selected stakeholders from the public and private sector. Both the online survey and interview guides included specific questions asking for (estimates of) the costs associated with the ePD. However, the feedback received as part of the interviews shows that it is extremely difficult for the stakeholders to provide concrete numbers or estimates.

According to **businesses**, this is mainly due to the following reasons:

- It is difficult to impossible for businesses to separate the costs caused by the ePD from other types of costs. The ePD is not the only source of costs for businesses as they have to implement technical measures under several legislative instruments, incl. general data protection legislation or consumer protection measures. From a business perspective, there is no reason to separate these costs based on the specific legal instrument they stem from.
- Estimates of costs require extensive internal work on the side of the businesses within and across organisational departments (e.g. litigation, compliance department, marketing department...). Hence, providing estimates on costs stemming from or related to the ePD is regarded as a "cost" in itself.
- The biggest part of the costs related to the implementation of the ePD incurred 10 years ago when the ePD was introduced. However, it was hard for the majority of business involved in this study to quantify this "one off" cost for the reasons explained above.
- An important part of the costs are opportunity costs, e.g. the opportunities providers of public telecommunications services or operators of public electronic communications networks are prevented from pursuing because of the ePD, unlike other over-the-top (OTT)[31] providers.

[28] See: https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive. Our analysis focuses on key closed questions dealing with the evaluation of the current legal framework. The aspects relating to potential future changes (policy options) have only been taken into account to a limited extent.
[29] Survey requested by the European Commission, Directorate-General Digital Single Market and coordinated by the Directorate-General for Communication, carried out by TNS Political & Social. For this report we used the preliminary raw data of the survey.
[30] One of the workshops involved national competent authorities for the ePD, while a second workshop gathered various stakeholders from the industry, civil society and consumer associations.
[31] (Over The Top) is a generic term commonly used to refer to the delivery of audio, video, and other media over the Internet without the involvement of a multiple-system operator in the control or distribution of the content. The term over-the-top (OTT)

On this basis, businesses indicated that it would be a considerable effort to calculate these opportunity costs or come up with estimates.

It was also difficult for **competent authorities** to provide estimates on costs, for similar reasons. Interviewees from competent authorities explained, for example, that it is not possible to separate costs relating to the ePD from costs relating to general data protection legislation, as both (privacy in general and e-privacy in particular) subject matter areas are usually dealt with in the same working groups/responsible teams. In addition, there are often different departments or authorities involved for different aspects of these regulations and, therefore, the effort required to collect the relevant information from all the departments or authorities concerned would be particularly high.

In spite of these challenges, a number of stakeholders did provide input on costs related to the ePD. While it is hard to qualify such information as representative enough for the purposes of this study, we leveraged all quantitative data we received throughout the data collection phase exhaustively. All quantitative input received by the stakeholders served as basis for the design of our assumptions to provide the economic calculations contained in this study and supported our analyses by means of examples throughout the report.

Below, we indicate the basic stakeholder categories of the European Commission's public consultation, of the online survey we carried out with competent authorities, businesses, and business associations as part of this project, as well as our selected interviews with different stakeholders.

2.2 The European Commission's public consultation

As concerns the replies to the public consultation, overall, 421 responses were submitted. A breakdown of the types of respondents that contributed to the consultation is presented in Table 2.

Table 2 – Responses to the public consultation by type of stakeholder group

Group of stakeholders	Specification	Number of responses	Share of responses
Citizens: 195 in total (46%)	Citizen	162	38%
	Consumer association or user association	11	3%
	Civil society association (e.g. NGO in the field of fundamental rights)	22	5%
Industry: 186 in total (44%)	Electronic communications network provider or provider of electronic communication services (e.g. a telecom operator)	25	6%
	Association/umbrella organisation of electronic communications network providers or providers of electronic communication services	15	4%
	Association/umbrella organisation/ trade association (other than associations of electronic communication service provider/network providers)	82	19%
	Internet content provider (e.g. publishers, providers of digital platforms and service aggregators, broadcasters, advertisers, ad network providers)	30	7%

is commonly used to refer to online services which could substitute to some degree for traditional media and telecom services. Definition provided in the study of the European Parliament, Directorate-General for internal policies, policy department A: Economic and Scientific Policy, Over-the-Top (OTTs) players: Market dynamics and policy challenges, dd..December 2015, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf.

Group of stakeholders	Specification	Number of responses	Share of responses
	Other industry sector	34	8%
Public bodies 40 in total (10%)	Government authority	15	4%
	Competent Authority to enforce (part of) the ePD	15	4%
	Other public bodies and institutions	10	2%
Total		**421**	**100%**

Source: European Commission.

As it can be seen above, almost half of the responses (46%) were submitted by citizens or organisations representing citizens' interests. A similar share (44%) was submitted by industry actors. Public bodies were responsible for the remaining 10% of the replies received.

At least one response was received by stakeholders from each Member State. Most responses were submitted by stakeholders from Germany (26%), followed by the United Kingdom (14%) and Belgium (10%). A detailed breakdown is presented in the following table. It can be noted that around 7% of the responses were submitted from stakeholders from outside the EU.

Table 3 – Responses to the public consultation by country

Member State / country	Number of responses	Share of responses
Austria	20	4.8%
Belgium	42	10.0%
Bulgaria	3	0.7%
Croatia	2	0.5%
Cyprus	2	0.5%
Czech Republic	6	1.4%
Denmark	7	1.7%
Estonia	1	0.2%
Finland	12	2.9%
France	30	7.1%
Germany	109	25.9%
Greece	3	0.7%
Hungary	2	0.5%
Ireland	8	1.9%
Italy	12	2.9%
Latvia	1	0.2%
Lithuania	1	0.2%
Luxembourg	1	0.2%
Netherlands	20	4.8%
Poland	9	2.1%
Portugal	6	1.4%
Romania	1	0.2%
Slovakia	2	0.5%

Member State / country	Number of responses	Share of responses
Slovenia	1	0.2%
Spain	15	3.6%
Sweden	15	3.6%
United Kingdom	60	14.3%
Other	30	7.1%
Total	**421**	**100%**

Source: European Commission.

We have used the input from the public consultation for both Tasks 1 (REFIT exercise) and 2 (Assessment of the options).

2.3 Online surveys conducted during the study

In addition to the public consultation on the ePD launched by the EC, Deloitte prepared two online surveys in order to collect additional information and stakeholders views on the Directive, looking in particular for precise quantitative elements, practical costs and benefits that business and competent authorities have likely experienced while implementing the ePD. Whilst the online surveys dedicated to this study were kept distinct from the EC's public consultation, they at the same time complemented the latter. The stakeholder communities targeted by the specific study surveys we conducted during this study are indicated below.

2.3.1 Online survey with competent authorities

The on-line survey with competent authorities was **completed by a total of 34 respondents**, representing **primarily data protection authorities (50%)** followed by regulatory authorities[32] (35%) and to a smaller degree consumer protection authorities (9%) as well as ministries (6%) in most of the Member States. Furthermore, **nearly all of the respondents (33 out of 34) represented national authorities**, except one representing the local level.

Table 4 – Type of body the respondents represent (total n° of responses = 34)

Answer Options	Share of responses
Ministry	6%
Data protection authority	50%
Regulatory authority (Telecom)	35%
Consumer protection authority	9%
Other (please specify)	0%

Source: Information provided by competent authorities of the EU Member States, tabulation by Deloitte.

The sample included **respondents from 24 Member States**. Normally, up to one or two institutions from each Member State took part in this survey. **Slovakia** was the only Member State from which

[32] These are usually national authorities which are in charge of the implementation and/or supervision of the national regulations having transposed the ePD in their country.

four responses were received, whereas **Cyprus, the Czech Republic, Italy and Malta are not represented**.

Table 5 – Number of responses received per Member State (total n° of responses = 34)

Member States	Number of responding competent authorities
Slovakia	4
Bulgaria, Croatia, Finland, Hungary, The Netherlands, Portugal, United Kingdom	*2*
Austria, Belgium, Estonia, France, Germany, Greece, Ireland, Latvia, Lithuania, Luxembourg, Poland, Romania, Slovenia, Spain, Sweden	*1*
Cyprus, Czech Republic, Italy, Malta	*0*

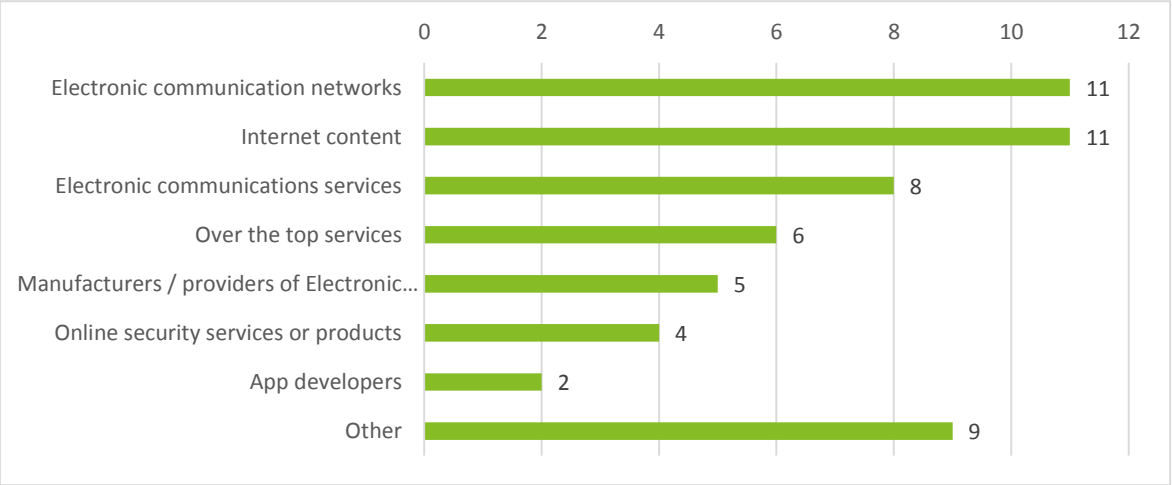
Source: Information provided by competent authorities of the EU Member States, tabulation by Deloitte.

2.3.2 Online survey with businesses

The invitation to our online survey with businesses was disseminated to 89 business associations across the EU.

In total, 37[33] businesses contributed to the survey, a **majority offering either electronic communication services or networks** (19 respondents combined).[34] Out of these 37 enterprises, 20 fall in the threshold of SMEs as defined in EU legislation (see details below)[35]. Almost one third of the responding companies are offering internet content services and 6 represent OTT service providers. While singular responses grouped in the "other" response category indicate business activities as diverse as eCommerce, financial services or privacy software solutions, at least 4 respondents work in the field of advertisement or marketing.

Figure 3 – General service offerings by business survey respondents (total n° of responses = 37)



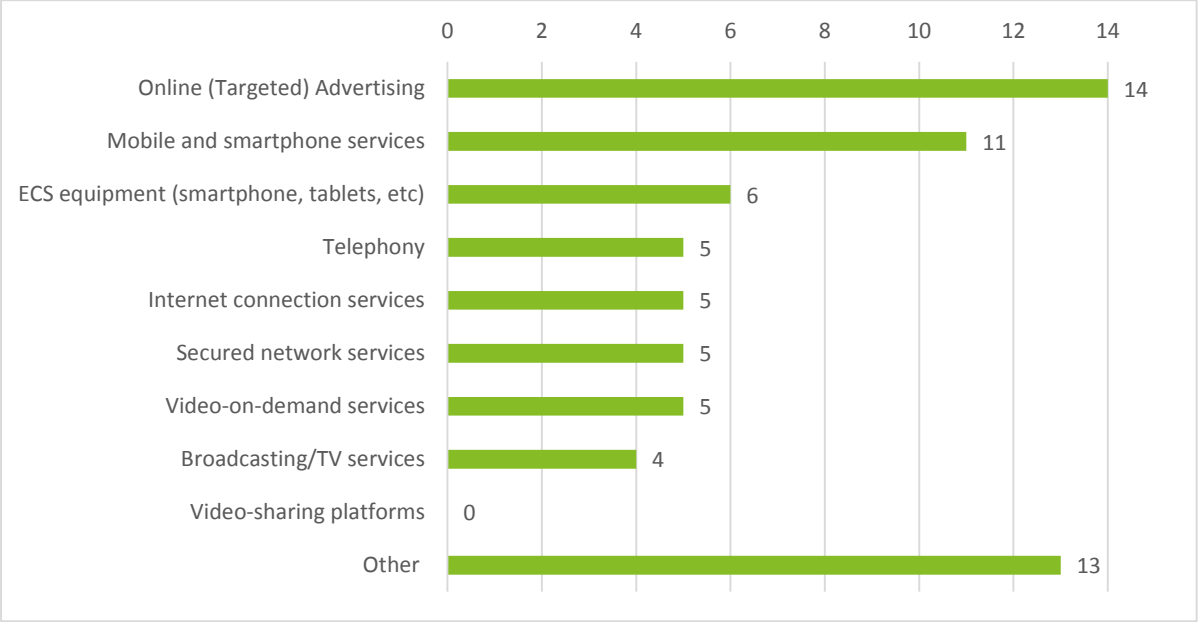
[33] The online survey included the option for businesses to skip individual questions in case they were not able nor inclined to answer. Therefore, the total number of responses may vary from one question to the next, remaining below the total number of 37 respondents in most instances.
[34] Respondents were able to indicate more than one answer to this question, accounting for companies operating in different sectors.
[35] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422).

Source: Responses to the online survey by businesses, presentation of data by Deloitte.

With regard to **specific services offered by the responding firms**[36], most of the participating businesses indicated that they are (amongst other aspects) active in advertisement activities: 14 out of 37 respondents offer online (targeted) advertisement services. Nevertheless, the large share of ECS service and network companies is reflected in significant shares offering mobile and smartphone services (11 of 37 respondents), or Telephony and internet connection services (5 out of 37 for each). Another 6 respondents also offer ECS equipment such as smartphones and tablet devices. Furthermore, response in the "other" category indicated business activities in the field of data analytics and eCommerce (2 out of 37 respectively); yet its large share is mostly grounded in companies offering multichannel advertisement and marketing campaigns (5 out of 37 respondents).

[36] Respondents were able to indicate more than one answer to this question, accounting for companies operating in different sectors.

Figure 4 – Specific types of services by business survey respondents (total n° of responses = 37)



Source: Responses to the online survey by businesses, presentation of data by Deloitte.

Table 6 on the following page helps to understand clustering of services into different business models apparently affected by the ePD:

- Classical **ECS networks and service providers** display a focus on mobile, telephony and internet connection services although some others also offer video-on-demand and broadcasting services. None or hardly any are active in modern online services like video platforms or online (targeted) advertising.
- This is different for **OTT services** and **internet content services**, reporting a much higher activity in the areas of online advertisement services among other services such as those related to smartphones, video-on-demand or broadcasting.

Providers of online security services as well as **manufacturers of ECS equipment** on the other hand are much more active in the segments for equipment and secured network services.

Table 6 – Cross-tabulation of general and specific types of services reported by business survey respondents (total n° of responses = 37)

	Specific Services								
General Service	**Mobile and smartphone services**	**Telephony**	**Internet connection services**	**Secured network services**	**Online (Targeted) Advertising**	**Video-on-demand services**	**ECS equipment**	**Video-sharing platforms**	**Broadcasting / TV services**
Electronic communication networks	7	5	4	3	0	4	3	0	3
Electronic communications services	3	3	4	3	1	3	3	0	3
Over the top services	2	1	1	1	4	1	2	0	2
App developers	2	1	0	1	0	1	1	0	1
Internet content	3	0	0	0	9	1	0	0	1
Online security services or products	2	2	2	3	0	1	4	0	2
Manufacturers / providers of ECS equipment	1	0	1	1	0	0	3	0	0
Other	1	1	0	1	2	1	1	0	1

Source: Responses to the online survey by businesses, tabulation by Deloitte.

Of the 37 business entities that took part in the study's online survey, the vast majority (i.e. 30 companies) are privately held as opposed to a very small minority being publicly held (only 7). The former display a wider array of services offered than the latter, as Table 7 illustrates. **Publicly held companies** indicated types of services mostly in the field of mobile and smartphone services, followed by internet connection and video-on-demand services. The categories of services most often reported by **privately held businesses** included online (targeted) advertisement with 13 out of 30 respondents, mobile and smartphone services with 8 respondents and services concerning ECS equipment.

Table 7 – Ownership structure and associated specific types of services of business survey (total n° of responses = 37)

	Ownership structure	
What specific services does your business offer?	**Privately held**	**Publicly held**
Mobile and smartphone services	8	3
Telephony	4	1
Internet connection services	3	2
Secured network services	4	1
Online (Targeted) Advertising	13	1
Video-on-demand services	3	2
ECS equipment (smartphone, tablets, etc.)	6	0
Video-sharing platforms	0	0
Broadcasting/TV services	3	1

Source: Responses to the online survey by businesses, tabulation by Deloitte.

Concerning their types of **business activities**, companies were asked to indicate all forms of customer interactions they are engaged in. A vast majority of 33 out of 37 businesses reported activities in *business-to-business* (B2B) and 24 in *business-to-consumer* (B2C) transactions. Only 4 respondents indicated activities in *research and development* (R&D).

With regard to **geographic origin**, the largest single group of 10 respondents (out of 36) report their primary established business to be located in Germany. In addition, 5 respondents indicate registered offices in France, 4 in Austria, 3 in Belgium or Denmark and 2 in the United Kingdom. Singular responses are received from companies with offices in Ireland, Portugal, The Netherlands and Romania. Three additional survey responses were received from U.S. firms operating in the European Single Market.

A large share, or 15 of 36 responding businesses reported **cross-border operations** on a global level, while 5 indicate activities in "a few countries outside the EU". Looking more closely at the European Single Market, only one respondent indicates activities in the whole EU, while 4 are active

in more than 14 Member States and another 14 respondents in 2 to 14 EU Members States. Finally 6 businesses only report activities in their respective country of establishment.[37]

With regard to **business size**, a relative majority of 16 out of 36 respondents in the sample represent larger companies with more than 250 employees. The other 20 respondents represented **SMEs** according to their workforce: 8 companies constitute medium sized enterprises with 50 to 249 employees. Another fourth of respondents (9 businesses) represent small enterprises with a workforce of 10 to 49, whereas only 3 respondents are micro-enterprises with less than 10 employees.

In line with these figures, around 18 companies report an **annual turnover** larger than EUR 50mio and 15 indicate a **balance sheet total** larger than EUR 43million for the previous financial year. Amongst, another 4 respondents, each report a value between EUR 10 million and EUR 50 million or EUR 10 million to EUR 43 million respectively. In the ranges defined for SMEs by the European Commission, 10 respondents report an annual turnover between EUR 2mio and EUR 10mio and 9 companies indicate a balance sheet total in the same range. Finally, along the official definition for micro-enterprises, 4 businesses had an annual turnover below EUR 2 million and 8 a balance sheet total below that same figure.

Besides this structural information, respondents were also asked to provide a self-assessment on their **awareness of the content of the ePD**. Out of 35 respondents, the vast majority of 25 businesses indicated to be fully aware of the ePD's content, while 5 were at least aware of some of its provisions. Another 5 respondents could only say that they are aware of the Directive's existence.

2.4 Interviews with different stakeholders

We conducted phone interviews with forty-six (46) stakeholders in total. Four different groups of stakeholders were contacted for the purposes of this study:

- Telecoms
- Other businesses
- Competent authorities
- Other stakeholders such as business associations

Table 8 – Number of Interviews Performed per type of stakeholders

Type of Stakeholders	Interviews Performed
Competent Authorities	**20**
Telecom operators	**8**
Other types of businesses	**9**
Other Stakeholders	**9**
Total	**46**

In the following sub-sections we describe the target groups interviewed in more detail.

A summary of the content of the interviews is provided in Annex B.

[37] Multiple answers were possible.

2.4.1 Interviews with businesses

We interviewed different businesses likely to be affected by the ePD such as telecoms, OTTs, banks, e-commerce service providers and business-to-business companies in order to gather their point of view on the impact, relevance, effectiveness, weaknesses and strengths of the ePD. It was found out that the ePD has a varying relevance depending on the group of stakeholders approached. Some of the businesses such as telecoms are directly and the most affected by the ePD as they would fall entirely under its scope. Others such as information society services and business-to-business companies are partially or indirectly impacted by the ePD.

The interviews were conducted based on a standard questionnaire covering questions on the following matters but not limited to these:

- Appropriateness of the current scope of the ePD;
- Coexistence between the ePD and the GDPR;
- Strengths and weaknesses of the ePD;
- Type and volume of costs incurred by businesses due to the ePD; and
- Future outlook of the ePD.

2.4.2 Interviews with associations

Several business associations were interviewed. The associations represented the interests of various industries affected by the ePD, such as:

- The hardware manufacturers and sharing content companies;
- The communications sector (e.g. TV services, mobile and telephony, OTTs);
- E-commerce; and
- Online advertising eco-systems.

The ePD had variable relevance for the different business sectors represented by the interviewed organisations. The ePD was highly relevant for the association representing the interests of telecoms. For other associations, the ePD was relevant to their daily practice in terms of unsolicited market communication (Article 13). For many others the experience in, and impact of the ePD was limited to Article 5(3) of the ePD, namely the “cookies” provision. Others seem to be unsure to what extent the ePD is relevant to them as they are unclear on the definition of electronic communication service and information society service.

The interviews were conducted based on a standard questionnaire covering questions on the following matters but not limited to these:

- Coexistence between the ePD and the GDPR;
- Strengths and weaknesses of the ePD;
- Cookies;
- Unsolicited communications;
- Type and volume of costs incurred by businesses due to the ePD; and
- Future outlook of the ePD.

2.4.3 Interviews with competent authorities

We have interviewed different authorities that have a competence related to the ePD. In most cases, several authorities (two or three) are competent for different parts of the implementation of the ePD content. The authorities were interviewed based on a standard questionnaire covering the following topics but not limited to these:

- Overall assessment of the content of the ePD;
- ePD impact on the protection of personal data and privacy in the telecom sector;
- ePD impact on the free flow of personal data;
- Relevance of the ePD;
- Awareness of citizens with regard to the topics covered in, and the requirements of ePD;
- Appropriateness of the scope of the ePD;
- Local implementation of the ePD;
- Strengths and weaknesses of the ePD and its individual provisions;
- Institutional set-up and tasks of the national competent authorities;
- Guidance and training; and
- Future outlook of the ePD.

3 Background to the initiative

In this section we outline the context and content of the ePD and present its intervention logic. We also provide an overview of the market relevant for the ePD.

3.1 Introduction

The study at hand concerns Directive 2002/58/EC on privacy and electronic communications[38], otherwise known as the ePD. The ePD aims to regulate the processing of personal data and the protection of privacy in the electronic communications sector.

In the following sub-sections the ePD and the context it operates in are presented. First, the relevance of the ePD is discussed in light of the market and technical environment it operates in, as well as citizens' needs in this respect in order to demonstrate the ePD's practical implications. Second, an overview of the content of the Directive is given, including by means of an intervention logic. Third, the relationship of the Directive with other EU legislation is discussed.

3.2 The relevance of the ePD

3.2.1 Relevant technological developments

The usage of **information and Communications Technology (ICT)** has been a key driver of economic and societal development across the world. ICT has matured and expanded to become the foundation of all modern innovative economic systems. As a consequence of the rapid digitalisation of the global economy, ICT can no longer be considered as a specific sector, but rather an **integral part of our society**.

Over the years, newer and more advanced ICT has been introduced in public communications networks and been made widely available to the general public, both in terms of accessibility as well as of cost. The rising Internet access rates of households in the EU28 is a good indication of the growing footprint of the EU information society. Whereas in 2007 a slight majority (55%) of EU households had Internet access, this proportion has continued to increase and reached 81% in 2014.[39]

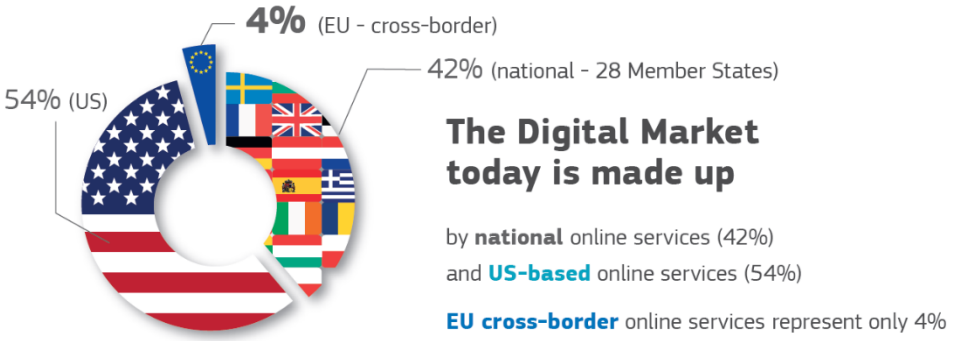
The digitalisation of the economy is considered to bring huge **opportunities for growth and innovation**. Indeed, the qualitative improvement and proliferation of ICT goes hand in hand with new business opportunities, as the free flow of data in general has been referred to as the "new gold" and

[38] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002.
[39] Eurostat (2015). *Information society statistics - households and individuals.* Retrieved from http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals (last accessed on April 7, 2016).

the fourth production factor after human resources, capital and commodities in the public and academic debate.[40]

While Europe has the capabilities to take a leading role in the global digital economy[41], it has so far been hampered by fragmentation and barriers that do not exist in the physical Single Market. For instance, at present the EU cross-border online services represent only 4%, while the national and US-based online services amount to nearly 50% respectively[42], as shown by the image below. If these barriers were to be removed within Europe, a contribution of an additional annual EUR 415 billion to European GDP is estimated to be possible[43].

Figure 5: Digital Market (shares per region)[44]



In addition to the economic opportunities, the increased usage of ICT brings along **new challenges for the free flow and protection of personal data**. Regulators have a hard time keeping pace with rapid technological developments allowing both private companies and public authorities to share and collect personal data on a large scale. At the same time, emerging regulatory voids bear the risk of insufficient protection of fundamental rights. Indeed, ICT has accrued the risk of over less control of individuals over their personal data which also deprives consumers of their trust in the security and privacy of individual communications. On the other hand, the misuse or leakage of personal data results all too often in unsolicited communications, mostly for marketing purposes. Closely related, a 2015 Special Eurobarometer study on Data Protection revealed that nearly 70% of the respondents are concerned that economic operators processing their personal data may use it for other purposes than the one it was originally collected for.[45] In addition, the same survey uncovered that consumers rather trust non-commercial businesses / institutions in relation to the processing of their personal data. Hence, the **confidentiality of communications is a central aspect of the smooth functioning of e-commerce and e-government services** and will determine sustainable economic growth, as well as effective and efficient public administration.

[40] Davenport, T. H., Barth, P. & Bean, R. (2012). How 'Big Data' Is Different. *MIT Sloan Management Review*, 54(1), p. 43-46.
[41] COMMUNICATION (COM(2015) 192 final) FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe /* COM/2015/0192 final
[42] https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/digital_single_market_factsheet_final_20150504.pdf
[43] COMMUNICATION (COM(2015) 192 final) FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe /* COM/2015/0192 final
[44] EC, Digital Single Market Factsheet, https://ec.europa.eu/priorities/sites/beta-political/files/dsm-factsheet_en.pdf
[45] European Commission (2015). *Special Eurobarometer (EB) 431 on Data Protection.* Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_fact_de_en.pdf (last accessed 8 September 2016).

The **ePD was adopted with a view to addressing these challenges**. Indeed, the rationale for the introduction of the ePD (and its predecessor[46]) stems from the fact that the general framework on data protection in the EU was not sufficiently specific and adapted to appropriately address the particular privacy and personal data protection issues in the electronic communications sector. The background and content of Directive 97/66 concerning the processing of personal data and the protection of privacy in the telecommunications sector and the relationship to the ePD is discussed in the following subsection.

3.2.2 The ePD's predecessor Directive 97/66/EC: background and content

The adoption of Directive 97/66/EC was prompted, on the one hand, by the implementation of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data[47] and, on the other hand, by the development of new information technologies in the communications sector.

The dual-pronged approach of the Directive 95/46/EC signified a shift towards the harmonisation of the provisions related to the protection of individuals with regard to the processing of personal data and on the free movement of such data.[48] At the same time**,** new telecommunications services were being developed, such as video-on-demand and digital mobile networks. These new services also raised implications for the confidentiality and privacy of the corresponding users.

In particular, the widespread adoption of the ISDN standards (Integrated Services for Digital Network) meant that traditional telephone networks were beginning to be used not just for the transmission of voice, but also of video, data, and other services. Therefore, Directive 97/66/EC was adopted in order to ensure the general protection of privacy in the telecommunications sector.

The scope of Directive 97/66/EC followed closely that of Directive 95/46/EC. More precisely, Directive 97/66/EC sought the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.[49] As *lex specialis* to Directive 95/46/EC, Directive 97/66/EC relied and was functionally bound by the former, particularly with regard to the definition of personal data.[50]

Regarding the services concerned, Directive 97/66/EC applied to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks in the Community. Specific reference was made to the Integrated Services Digital Network (ISDN) and public digital mobile networks.[51] Since Directive 97/66/EC focused on the telecommunications sector, only four terms were specifically defined: these were "subscriber", "user", "public telecommunications network", and "telecommunications service".[52]

[46] Directive 97/66 concerning the processing of personal data and the protection of privacy in the telecommunications sector:
[47] For an explanation of Directive 95/46/EC see section 3.4.1.
[48] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, *O.J.*, n° L 24, 30 January 1998, recital (1).
[49] Directive 97/66/EC, Article 1(1).
[50] Directive 97/66/EC, Article 1(2).
[51] Directive 97/66/EC, Article 3(1).
[52] For the definitions of these terms, see Directive 97/66/EC, Article 2.

The topic of security had but a limited mention in Directive 97/66/EC.[53] However the Directive already contained a data breach notification mechanism for the providers of telecommunications services[54].

3.2.3 Relationship between Directive 97/66/EC and the ePD

Directive 2002/58/EC replaced Directive 97/66/EC because the scope of the latter did not reliably take into account the recent development of new technologies such as the breakthrough adoption of the Internet. This reasoning is reflected in Recital 6 of Directive 2002/58/EC, which highlights the disruptive role of the Internet in traditional market structures. The widespread adoption of this technology gave rise to a new global infrastructure enabling the delivery of a wide range of electronic communications services. Therefore, publicly available electronic communications services over the Internet had to account for the new risks posed to the personal data and privacy of its users.

The need to ensure legal certainty weighed heavily in the adoption of the ePD. Despite the opinion of the Article 29 Working Party which supported the applicability of Directive 97/66/EC to Internet services in the same way as it applied to other forms of communication,[55] there was still uncertainty over the applicability of this instrument.[56]

To curb this legal ambiguity, but also to ensure that the ePD would not be easily overtaken by further technological developments, the European legislator opted for more technologically-neutral formulations in Directive 2002/58/EC, preferring instead to highlight the crucial role played by the onset of digital mobile networks whilst clarifying which electronic communication services were in scope.[57]

The main changes between Directive 97/66/EC and the original version of the ePD are thus the following:

- Extension of the scope of Directive 97/66/EC (specifically related to telecommunications services) to include electronic communications services in general, including with regard to such obligations as the duty to notify data breaches.
- Introduction of new definitions such as “location data” and “traffic data”. In time, the ePD would also address other concepts such as “cookies”. The latter term was given prominence in 2009 with the amendment provided by Directive 2009/136/EC, where it was incorporated, though not defined, in Article 5(3) of the ePD. The lack of an overt definition for “cookies” may stem from the wish to keep the ePD as technologically neutral as possible. Instead, the provision refers to the storing or accessing of information contained in the terminal equipment of a subscriber.
- Concerning Article 8 and the restriction of calling line identification, Directive 97/66/EC gave users the right to eliminate the presentation of the calling-line identification. Directive

[53] Directive 97/66/EC, Article 4(1): “*The provider of a publicly available telecommunications service must take appropriate technical and organizational measures to safeguard security of its services*”. (…)
[54] Directive 97/66/EC, Article 4(2). This requirement would be extended in Directive 2002/58/EC to encompass all providers of electronic communications services.
[55] Article 29 Working Party, Opinion 2/2000 concerning the general review of the telecommunications legal framework, adopted on 3rd February 2000, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp29_en.pdf, p. 3.
[56] K. ROSIER, « La directive 2002/58/CE vie privée et communications électroniques et la directive 95/46/CE relative au traitement des données à caractère personnel : comment les (ré)concilier ? », *Cahiers du CRID*, n° 31, p. 328-329.
[57] K. ROSIER, *ibidem*, p. 329.

2002/58/EC, however, is more prescriptive, stating that the service provider "must offer" this functionality.

3.3 The content of the ePD

3.3.1 Overview of the content and scope

The ePD (Directive 2002/58/EC) aims at regulating data protection and privacy in the digital age by introducing **specific requirements concerning privacy in the electronic communications sector**.

Indeed, as concerns the **scope** of the ePD, compared to the general data protection legal framework, it applies to the electronic communication sector only. The term electronic communications services deserves some further clarification and needs to be distinguished from information society services, as both types of services are regulated by a complex net of different legal regimes. The scope of the rules set out in the ePD is limited to services that qualify as an 'electronic communications service'.

These are defined in the Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive) as *"service normally provided for remuneration which consist wholly or mainly in the conveyance of signals on electronic communications networks* (…)".[58] Typically, this concerns voice telephony and Internet services such as electronic mail conveyance services. In contrast, information society services, defined as services "*normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*",[59] may not always be covered by the Framework Directive.[60] This is because such services do not always consist wholly or mainly in the conveyance of signals on electronic communications networks. For this reason, the same undertaking can offer both an electronic communications service, such as access to the Internet, and services not covered by the Framework Directive, such as the provision of web-based content.[61]

Certain information society services may also be subject to specific regulation. This is the case for electronic commerce, which is regulated by the E-Commerce Directive.[62] This instrument contains an important exemption in Article 15(1), according to which providers of such services are under no general obligation to monitor the information which they transmit or store, or seek facts or circumstances indicating illegal activity.[63] According to *L'Oréal v eBay International AG,* the key to define whether an information society service provider can rely upon this exemption is that the service must be provided neutrally by technical or automatic means and in a way that the intermediary does not assume responsibility for the content that it hosts.[64] Search engines such as Google may fall

[58] Article 2.c of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).
[59] Directive 98/48/EC of the European Parliament and of the Council of 28 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations [1998] OJ L217/18, art 1.
[60] See also Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification), which consolidated the amendments to Directive 98/48/EC.
[61] See Framework Directive, Recital 10.
[62] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L178/1.
[63] E-Commerce Directive, art 15(1).
[64] See L'Oréal SA v eBay International AG (2012) All ER (EC) 501 and the Google joined cases C-236/08, C-237/08, and C-238/08.

within these categories,[65] though it should be noted that the latter has been considered as a controller of personal data within the meaning of Directive 95/46/EC.[66]

Furthermore, the ePD only applies to *public or publicly available* electronic communications networks. This means that closed user groups and corporate networks are left outside the scope of the ePD and in these cases, the Personal Data Protection Directive is likely to apply.

As concerns the **content**, the ePD lays down a number of specific rules on, among others, security obligations for electronic communications service providers, obligations on the confidentiality of electronic communications, specific rules on the processing of traffic data and location data, as well as rules on unsolicited communications. In some situations, personal data may only be processed with the consent of the users. An overview of the main objectives and content of the ePD is provided in our intervention logic (cf. the following sub-section).

The ePD was **partly amended by Directive 2009/136/EC[67],** which is part of the Electronic Communications Package (cf. sub-section 3.4.2). The 2009 amendment resulted in fundamental changes, including:

- A reinforcement of the rules on security of the processing, notably by requiring electronic communications service providers to notify personal breaches;
- A requirement of prior consent for storing or accessing information stored in the user's terminal equipment;
- A reinforcement of the legal protection against unsolicited communications by ensuring that any individual or legal person with a legitimate interest may take legal action against infringements before the courts.

Due to the developments in the area of telecommunications, this reform was necessary in order to improve the consistency of regulation across Europe and to adapt to these developments. The EU Cookie Directive is designed to increase consumer protection, as it introduces important changes protecting and empowering users of electronic communications services. One of the provisions state that it is required for websites to obtain informed consent from visitors before they store information on a computer or any web-connected device. The Directive also deals with access to services, contractual rights, privacy, and policy participation.

3.3.2 Intervention logic of the ePD

In order to create a clear point of reference for the evaluation and impact assessment, it is necessary to carry out an analysis of the policy objectives and to establish the baseline against which to evaluate the achievement of these objectives.[68] The intervention logic is a helpful tool in this regard.

Below, the intervention logic for the ePD is provided.

The figure 5 below is to be read from left to right and consists of the following elements:

- Needs;

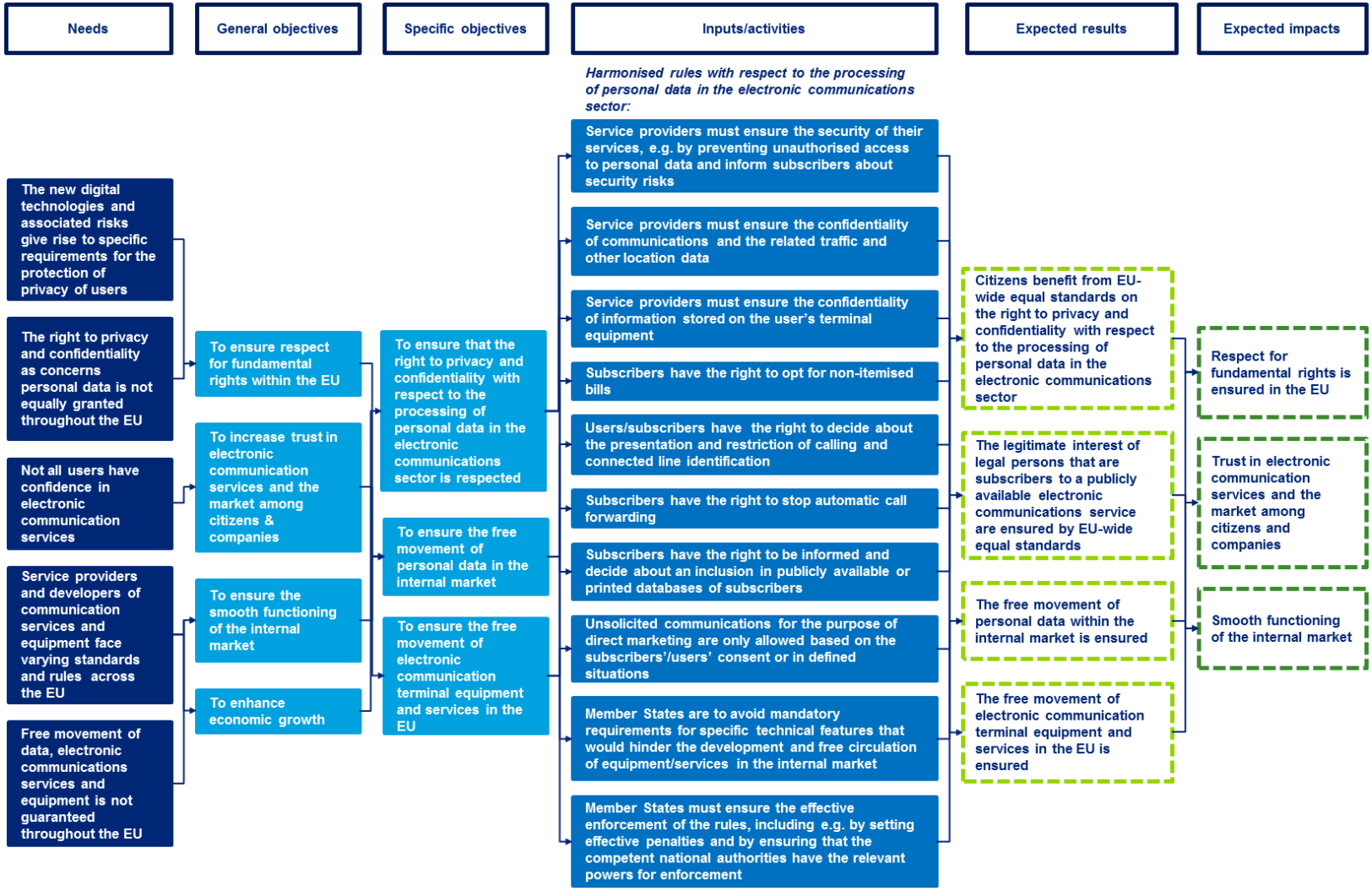
[65] Scaife, L. (2014). *Handbook of Social Media and the Law*, London: Informa Law from Routledge, p. 17.
[66] Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (EPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 41.
[67] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF
[68] European Commission, Better Regulation Guidelines, 19 May 2015, SWD(2015) 111 final, pp. 54-55, (http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm).

- Objectives (including general and specific objectives);
- Inputs/activities implemented to achieve the objectives;
- Expected results of the current rules; and
- Expected impacts relating to the current rules.

As concerns the objectives, we acknowledge that they are interconnected. On the one hand, the free movement of personal data could in certain situations be contradictory to the aim of ensuring the respect for the right to privacy and confidentiality and the minimisation of processing of personal data. On the other hand, it can also be argued that the free flow of personal data in fact depends on the existence of common standards in relation to privacy. After all, service providers and users may be less inclined to engage in cross-border activities if the rules on the protection of personal data are not clear and harmonised.

In the intervention logic, reference is made to *expected* results and impacts. Accordingly, the figure reflects the ePD as it was envisaged at the time of the adoption.

Figure 6 – Intervention logic



Source: Deloitte

3.4 Relationship with other pieces of legislation

The ePD is part of the EU's policy framework on the protection of personal data and privacy and the regulatory framework for electronic communications networks and services (Electronic Communications Package). Both areas are discussed below.

3.4.1 EU data protection legislation

The EU Data Protection Directive 95/46/EC

The cornerstone of the current European legal framework on personal data protection is **Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data** (Data Protection Directive or Directive)[69]. This Directive sets the *lex generalis* in terms of data protection in Europe and as such applies to all matters related to the processing of data protection, notwithstanding the sector, but provided that there is no sector-specific law likely to apply – *lex specialis.* Although this Directive was created in a period when the Internet was fairly young, it is still the reference text at European level on privacy and data protection.

The Data Protection Directive attempts to achieve a balance between the free movement of personal data within the single market and ensuring the fundamental rights and freedom of individuals, notably their right to privacy. In other words, the Directive pursues simultaneously the insurance of the functioning of the single market and the protection of fundamental rights. In order to achieve this dual objective, the Directive mandates the Member States to adopt legislation at local level, which implements the principles set in the Directive such as the proportionality, lawfulness, purpose limitation, transparency and accuracy principles.

The Directive covers two types of personal data. On the one hand, it deals with ordinary personal data that may be legitimately processed provided that this processing respects the data protection principles and falls under one of the legitimate basis for data processing. On the other hand, the Directive comprises the processing of special categories of personal data, known as *sensitive data*, which is in principle prohibited under the Directive, unless one of the exceptions foreseen by the Directive applies. The Directive also provides rules applicable to the transfer of personal data to third countries.

This Directive applies to all sectors, including the electronic communications sector, provided that the subject matter in question is not regulated by the *lex specialis* laid down by the ePD. Matters that are not regulated by the ePD and to which, in consequence, the Personal Data Protection Directive applies, include, for example, the obligations of the controller and the rights of individuals. The Directive applies as well to non-public electronic communications networks and non-publicly available electronic communications services, which do not fall under the scope of the ePD.

Thus, the Personal Data Protection Directive and the ePD are complementary, in that they both apply to the electronic communications sector, but regulate different matters. The general rule is that where provisions overlap, *lex specialis* overrides *lex generalis.* This means that, where the ePD provisions apply to a particular matter, the Personal Data Protection Directive does not apply. However, if no

[69] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN

specific rules exist in the ePD, the Personal Data Protection Directive will apply by default. Nonetheless, it is important to mention that once the General Data Protection Regulation (GDPR) enters into force, the Personal Data Protection Directive will be repealed and replaced by the GDPR. Therefore, it is crucial to ensure consistency and coherency between the ePD rules and the GDPR (see sub-section below).

The General Data Protection Regulation

On 25 January 2012, the European Commission adopted a proposal for a reform of the EU legal framework on the protection of personal data[70]. This reform includes the General Data Protection Regulation (GDPR). Once enforced, the GDPR will replace the former EU Personal Data Protection Directive. The objectives of the GDPR are to strengthen the rights of the individuals, to simplify the existing data protection framework and to apply a single set of rules on data protection that will apply directly within the whole EU territory. The reason for this reform is the aim of EU policy makers to allow the digital economy to develop across the internal market by increasing trust. To achieve trust, it is essential to create the necessary regulatory conditions and ensure a strong and more coherent data protection framework in the Union, backed by strong enforcement, which is the ambition of the GDPR.

On 15 December 2015, the European institutions agreed on a final text for the "Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data", which will apply as of May 2018.[71] Although the main data protection principles remain unchanged, the data protection reform will bring about some important changes. For instance, currently, the Personal Data Protection Directive seeks to harmonise national legislation by establishing minimum standards and objectives that the Member States need to meet. However, all the 28 EU Member States enact their own laws based on the EU Data Protection Directive, which results in legal fragmentation related to the implementation of the Directive and therefore varying standards of data protection among Member States (see also sub-section 4.3.5 on the transposition check). The GDPR aims at establishing high data protection standards, which are better harmonised and fit for the Internet age. As it takes the form of a regulation, as opposed to a directive, the GDPR will impose a uniform data protection regime in all EU Member States. Once the GDPR is in force it will apply in every Member State, without a need for the Member States to enact national legislation.

In the new Regulation, the EU introduces a number of new concepts, rights and obligations that will apply to all players offering services to individuals based in the European Union, notwithstanding the sector within they are active. The GDPR intends to strengthen citizens' control over the use of their personal data, while simplifying the regulatory landscape for business.

For instance, compared to its predecessor (Personal Data Protection Directive), the GDPR has an extended territorial scope and applies to controllers and processors located outside the EU provided that the processing activities relate to EU citizens. The GDPR reinforces as well the consent mechanism as it requires a clear affirmative act establishing a freely given, specific, informed and unambiguous consent. This means that silence, pre-ticked boxes or inactivity cannot be considered as consent. In addition, when the processing has multiple purposes, consent should be given for all of them. The burden to prove that consent has been given lies within the controller and not the data

[70] http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[71] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

subject. The GDPR introduces conditions applicable to the consent for children. For children below 16, the processing of personal data based on consent will be considered lawful only to the extent that the consent is given or authorised by the holder of parental responsibility. Another novelty introduced by the GDPR is the breach notification obligation which requires controllers to notify data breaches to the DPA and in some cases to the affected data subjects within 72 hours. Contrary to the Personal Data Protection Directive, the GDPR makes reference to concrete penalties and sets the maximum ceiling to 4% of the annual worldwide turnover or 20 million EUR. The GDPR puts a lot of focus on the necessity for controllers to undertake a risk-based approach and to implement Privacy by Design. Finally, the GDPR imposes explicit accountability to controllers urging them to take the necessary security measures and keep records and documentation allowing them to demonstrate compliance at any time. These are some but not all of the novelties introduced by the GDPR and relevant to this study.

3.4.2 The Electronic Communications Package

The ePD is part of the regulatory framework with regard to electronic communications (henceforth "Electronic Communications Package"). Overall, the Electronic Communications Package aims to encourage competition, to improve the functioning of the market and to guarantee basic user rights.

The Electronic Communications Package consists of five Directives and two Regulations. These instruments are presented in the table below and need to be taken into account while assessing the coherence of the ePD.

Table 9 – The main legal instruments of the Electronic Communications Package

Name of the instrument	Main content
The Framework Directive[72]	This directive establishes a harmonised framework for the regulation of electronic communications services, electronic communications networks, associated facilities and associated services. It establishes a set of procedures to ensure the harmonised application of the regulatory framework throughout the EU.
The Access Directive[73]	This directive encompasses the way in which EU countries regulate access to, and interconnection of, electronic communications networks and associated facilities. It establishes a regulatory framework for the relationships between suppliers of networks and services that will result in sustainable competition and interoperability of electronic communications services.
The Authorisation Directive[74]	This directive creates a legal framework to ensure the freedom to provide electronic communications networks and services throughout the European Union.
The Universal Service Directive[75]	This directive is intended to establish a minimum set of good-quality electronic communications services accessible to all users at an affordable price, while minimising market distortion.
The Directive on Privacy and	Information is exchanged through public electronic communication services such as the Internet and mobile and landline telephony and via their accompanying networks. These services and networks

[72] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services as amended by Directive 2009/140/EC and Regulation 544/2009, OJ L 108 of 24.4.2002, pp.33-50.
[73] Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities as amended by Directive 2009/140/EC, OJ L 108 of 24.4.2002, pp. 7-20.
[74] Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services as amended by Directive 2009/140/EC, OJ L 108, 24.4.2002 of pp. 21-32.
[75] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services as amended by Directive 2009/136/EC, OJ L 108 of 24.4.2002, pp. 51-77.

Name of the instrument	Main content
Electronic Communications[76]	require specific rules and safeguards to ensure the users' right to privacy and confidentiality. This is anchored in the ePD.
The Regulation on Body of European Regulators for Electronic Communications (BEREC)[77]	This regulation defines the rules on the establishment and operation of the Body of European Regulators for Electronic Communications (BEREC). BEREC advises the EU institutions on developing a better internal market for electronic communication networks and services and forms links between national regulatory authorities (NRAs) and the European Commission.
The Regulation on roaming on public mobile communications networks[78]	The aim of this regulation is to ensure that mobile phone users do not pay excessive prices for EU-wide roaming services (calls, text messages and Internet use) when travelling within the EU. In this sense it is intended to boost competition in the market for mobile phone users.

Source: Deloitte

On 14 September 2016, the European Commission published a proposal for a new European Electronic Communications Code which consists of a horizontal recasting of the four existing Directives (Framework, Authorisation, Access and Universal Service), and bringing them all under a single Directive. This review would assemble all measures that are applicable to electronic communications networks and electronic communications service providers, and would simplify the current structure. The code proposes increased competition and predictability for investments, better use of radio-frequencies, stronger consumer protection, a safer online environment for users and fairer rules for all players.

3.4.3 The R&TTE and Radio Equipment Directive

In addition to the GDPR and the instruments in the Electronic Communications Package, attention should also be given to the Radio and Telecommunication Terminal Equipment Directive ("R&TTE")[79], which was revised to become the Radio Equipment Directive (RED).[80] These directives have established a framework for placing and marketing radio and telecommunications terminal equipment within the single market. Since these instruments are not part of the Regulatory Framework for Electronic Communications, there are no provisions strictly overlapping with the ePD or creating specific challenges for the latter. Nevertheless, the former R&TTE and the Radio Equipment Directive contain certain provisions that refer to requirements set out in the ePD, to the extent that they provide that radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected.[81]

[76] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector as amended by Directive 2006/24/EC and Directive 2009/136/EC, OJ L 201 of 31.7.2002, pp 37-47.
[77] Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office, OJ L 337, 18.12.2009, p. 1-10.
[78] Regulation (EU) No 531/2012 of the European Parliament and of the Council of 13 June 2012 on roaming on public mobile communications networks within the Union Text, OJ L 172 of 30.6.2012, pp. 10-35.
[79] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (now repealed and replaced by the Radio Equipment Directive, see footnote *infra*);
[80] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.
[81] See Article 3(2)(c) *ex vi* Article 6(1) of the R&TTE and Article 3(1)(e) *ex vi* Article 10(1) of the RED.

The R&TTE covered all equipment that used the radio frequency spectrum, including GSM-compliant devices, ISDN terminals, and cable and PC modems. The R&TTE was later revised and replaced by the Radio Equipment Directive, applicable from 13 June 2016. For this reason, and notwithstanding the fact that products compliant under the repealed R&TTE can still be introduced to the market until 13 June 2017, the new RED will serve as the reference point for our subsequent analysis of the ePD.

The R&TTE (until June 2017) and the RED apply to all radio equipment and all equipment intended to be connected to public telecommunication networks. The major difference between the R&TTE and the Radio Equipment Directive is that the latter willnot cover wired telecommunications terminal equipment. On the other hand, radio determination (i.e., the determination of the position, velocity and/or other characteristics of an object, or the obtaining of information relating to these parameters, by means of the propagation properties of radio waves)[82] is now expressly covered (including RFID and motion detection).

The relation between the Radio Equipment Directive and the ePD should be considered for the following reasons:

- The Radio Equipment Directive only applies to radio equipment, excluding fixed line equipment and, as noted above, telecommunications terminal equipment. This scope, which would have been narrow at the time of the original R&TTE directive, is now significantly enlarged due to the prevalence of new forms of communication and recent consumer trends that veer away from the use of traditional forms of communication over fixed lines;
- The Radio Equipment Directive, like the ePD, is also concerned with the free movement of communications equipment on the single market, as evidenced by its Article 9;
- The Radio Equipment Directive contains provisions that dovetail with certain requirements from the ePD and data protection principles recently implemented by the GDPR.

With regard to the latter point, it is worth pointing out that the RED , the ePD and Directive 95/46/EC (and, in the future, the GDPR), are expressly linked by certain provisions. Amongst the requirements provided by the Radio Equipment Directive, Article 3(3)(e) sets out that radio equipment should incorporate "*safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected*". This requirement is reinforced by Article 10(1) of the Radio Equipment Directive, which imposes upon manufacturers of radio equipment the obligation to "*ensure that it has been designed and manufactured in accordance with the essential requirements set out in Article 3*". This reference is justified by the observation that the protection of privacy and data protection can be enhanced by particular features of radio equipment.[83]

When overlaid with the provisions of the ePD, Article 3(3)(e) of the Radio Equipment Directive effectively requires that certain categories or classes of radio equipment shall meet a number of essential requirements that are spelled out in an exhaustive way in the Radio Equipment Directive in Art. 3, §3. Noteworthy is that, amongst these essential requirements, figure notably the capability of the radio equipment to *incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected*[84]. Yet, the Radio Equipment Directive does not define such safeguards, rather, these are laid down in other instruments like the ePD or Directive 95/46/EC. Rather, the interplay between these instruments means that radio equipment should be designed in

[82] See Article 2(3) of the Radio Equipment Directive. See also International Telecommunication Union, Radio Regulations (2012), Article 1.9.
[83] See Recital 13 of the Radio Equipment Directive.
[84] Article 3 §3, letter (e) of the Radio Equipment Directive.

such a way as to allow the incorporation of safeguards to protect the right to privacy and the right to data protection, an approach similar to the concept of privacy by design more recently espoused by the GDPR. Manufacturers should therefore construct radio equipment that is capable of supporting the incorporation of safeguards, in compliance with privacy and personal data protection requirements stemming from other legal instruments such the ePD.

Looking into the Radio Equipment Directive from the angle of Article 4.1. and 4.2 of the ePD (security of processing)the construction of radio equipment must be carried out, *when relevant,* in such a way as to allow the protection of personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, an unauthorised or unlawful storage processing, access, or disclosure. Likewise, Article 14(3) of the ePD (*Technical features and standardisation*), states that, *where required*, terminal equipment should be constructed in a way that is compatible with the right of users to protect and control the use of their personal data. In both cases (i.e., the ePD and the Radio Equipment Directive), the letter of the two acts seems to suggest that a reasoned and selective approach should be followed when deciding which types and classes of radio equipment should indeed embed privacy-enhancing features.

In this sense, the Radio Equipment Directive and the ePD exhibit a potentially strong synergy due to the fact that they both apply to aspects related to electronic communications or to the equipment involved in such communications. Moreover, it is expected that at least certain categories or classes of equipment may be explicitly required to align with data protection and privacy safeguards as are now stipulated in the ePD and other horizontal data protection regulation (e.g., GDPR).

3.4.4 The Directive on security of network and information systems

The Directive on security of network and information systems (the "NIS Directive") is the first act of EU law dedicated to the topic of cybersecurity.[85] Its goal is to achieve a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market. To this end, the NIS Directive seeks to ensure the equivalence of cybersecurity capabilities across Member States and facilitate exchanges of information and cross-border cooperation.

The NIS Directive establishes security and notification requirements for operators of essential services and for digital services providers. It also creates a security incident response team network and obliges Member States to designate national competent authorities, single points of contact, and response teams with tasks related to the security of network and information systems.

It should be noted that the NIS Directive does not apply to undertakings already covered by the requirements laid out in the Framework Directive.[86] Therefore, those providers already covered by the Framework Directive and the ePD will not be subject to additional requirements stemming from the NIS Directive. Essentially, the NIS Directive is poised to serve as *lex generalis*, its requirements only applying in the absence of more specific regulation.[87] Since, as noted above, the Framework Directive does not encompass information society services that do not consist mainly or wholly in the conveyance of signals over electronic communications networks, these may be covered by the NIS if they are considered to be "operators of essential services" or "digital service providers",[88] and no other

[85] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016], OJ L194/1.
[86] See Article 1(3) of the NIS Directive.
[87] See Recital (9) for an overview of this relationship between present and future legal acts of the Union.
[88] See Article 4(6) and Article 5 of the NIS Directive for the definition of such categories.

specific regulation exists. Another consequences of this setup is that if the scope of the ePD were to be extended in the future so as to include certain information society services, the latter would cease to be subject to the requirements in the NIS Directive as long as equivalent provisions remained in the ePD.

3.5 The market covered by the ePD

3.5.1 The size of the telecommunications sector in the EU

Within the European Union, the telecommunication sector[89] is one of the crucial industries for the completion of the Digital Single Market. The table below provides an overview of the:

- Number of enterprises (2014);
- Number of persons employed (2014); and
- Annual turnover in 2014 of the EU telecommunications sector.[90]

The statistics provided in the table serve as a first high-level entrance point for the further analysis of the market covered by the ePD.

Table 10 – Annual enterprise statistics for the EU telecommunications sector

Member State	Number of enterprises (in thousands, 2014)	Number of persons employed (in thousands, 2014)	Annual turnover in 2014 (in million)
Austria	0.3	15.1	5,444.8 €
Belgium	1.5	24.3	12,296.1 €
Bulgaria	0.7	20.1	1,502.9 €
Croatia	0.3	9.0	1,644.5 €
Cyprus	0.1	3.9	671.2 €
Czech Republic	1.0	17.3	3,843.0 €
Denmark	0.4	18.7	5,697.7 €
Estonia	0.2	4.3	699.3 €
Finland	0.4	12.2	4,368.3 €
France	5.4	167.3	61,428.5 €
Germany	2.8	111.6	60,471.2 €
Greece[91]	0.2	22.6	6,411.8 €
Hungary	1.2	18.9	3,579.9 €
Ireland[91]	0.4	12.4	5,650.7 €
Italy[91]	4.3	94.0	44,077.6 €
Latvia	0.5	5.0	729.0 €
Lithuania	0.3	6.0	769.2 €
Luxembourg	0.1	4.8	4,377.4 €
Malta[92]	0.0	1.6	- €

[89] Eurostat defines this sector as being composed of business activities of providing telecommunications and related service activities, such as transmitting voice, data, text, sound and video. Over-The-Top Services are not explicitly mentioned in the Eurostat definition, yet included under the referenced definition of "*Telecommunications*" (J 61) in the *International Standard Industrial Classification of All Economic Activities, Rev.4*. Here, VOIP services are classified as "*Other telecommunication activities*" (J 6190).
[90] See Eurostat: "*Annual enterprise statistics for special aggregates of activities (NACE Rev. 2)* [sbs_na_sca_r2]", data for "*Telecommunications* (J61)"
[91] Eurostat data for 2012, final numbers for 2014 not available.
[92] No data on annual turnover available.

Member State	Number of enterprises (in thousands, 2014)	Number of persons employed (in thousands, 2014)	Annual turnover in 2014 (in million)
Netherlands	1.4	31.2	16,881.4 €
Poland	5.7	48.8	10,048.7 €
Portugal	0.7	15.0	5,533.7 €
Romania	2.4	43.4	4,271.4 €
Slovakia	0.3	10.5	2,208.3 €
Slovenia	0.3	5.0	1,361.6 €
Spain	4.9	59.7	31,020.8 €
Sweden[91]	1.0	27.2	12,666.5 €
United Kingdom	7.7	209.8	78,184.9 €
EU28	44.7	1,019.8	385,840.4 €

Source: Eurostat.

According to Eurostat, around 44.7 thousand enterprises are active in this market, accounting for a share of 0.2% of all businesses active in the EU. Around 90% of these enterprises are micro-enterprises, 99% are SMEs. Around 52% of all EU telecommunication enterprises were established in the United Kingdom, Poland, the Netherlands, Germany and France in 2014.

Overall, approx. one million citizens are employed in the telecommunications sector of which roughly 20% are active in SMEs.[93] In total, 56% of all employees in the EU telecommunications sector worked for enterprises in United Kingdom, France, Germany, Poland, and the Netherlands in 2014. When putting the number of persons employed in the telecommunications sector in relation to the overall number of citizens per Member State, it can be seen that Luxembourg, Cyprus, Denmark, Estonia, and the United Kingdom have comparatively high shares of citizens working in the telecommunications sector. None of these Member States, however, exceeds a share of 0.9%.[94]

The sector generates an annual turnover of 385 EURb. The United Kingdom, France, Germany, Poland, and the Netherlands accounted for 59% of the entire EU28 turnover in the telecommunications sector in 2012 (overall roughly 227 EURb). In terms of contribution of the telecommunication sector to the annual GDP pf each Member State, Eurostat data shows that the sector is largest in Luxembourg (9.5% of overall annual GDP in 2012), Estonia (4.5%), Bulgaria (4.3%), Croatia (4.1%), and the United Kingdom (3.8%).[95]

3.5.2 Over-The-Top services (OTTs)

A 2016 global forecast of the market for *Over-The-Top* (OTT) providers[96] shows that market is estimated to grow from USD 28.04 Billion in 2015 to USD 62.03 Billion by 2020 with a CAGR of

[93] Figure from 2011. Actual figure today likely to be higher. See: http://ec.europa.eu/eurostat/statistics-explained/images/4/4f/Sectoral_analysis_of_key_indicators%2C_telecommunications_%28NACE_Division_61%29%2C_EU-28%2C_2012_A.png

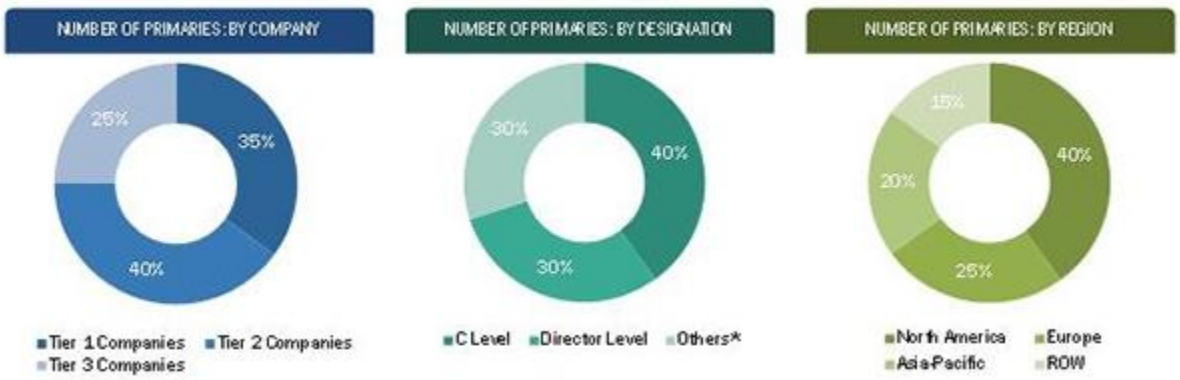
[94] This is based on internal calculations and cannot be directly concluded from the information sources we used for our analysis.

[95] Figures relate to 2012. The actual figures today are likely to be higher. See Eurostat: http://ec.europa.eu/eurostat/statistics-explained/images/9/9c/Key_indicators%2C_telecommunications_%28NACE_Division_61%29%2C_EU-28%2C_2012.png.

[96] (Over The Top) is a generic term commonly used to refer to the delivery of audio, video, and other media over the Internet without the involvement of a multiple-system operator in the control or distribution of the content. Thus, the term over-the-top (OTT) services is practically used to refer to online services which could substitute to some degree for traditional media and telecom services. Definition provided in the study of the European Parliament, Directorate-General for internal policies, policy department A: Economic and Scientific Policy, Over-the-Top (OTTs) players: Market dynamics and policy challenges, dd.December 2015, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf.

17.2%.[97] The report argues that market is in the growing stage in Europe and therefore OTT platforms in these regions have immense scope for enhancement. Overall, the North American region is expected to contribute the maximum market share to the overall OTT market.[98] As can be seen below, around 40% of primaries in the OTT market are expected to be established in North America by 2020 while 25% are expected to be European.

Figure 7 – Expected breakdown of profiles of primaries (in 2020)



Source: MarketsandMarkets

The report also acknowledges that diversified government regulations and policies present across domestic and international borders are restraining the growth of the OTT market.

According to the report, the European market is expected to grow at a similar pace (i.e. with a similar CAGR) as the North American market – albeit with a smaller overall market size. The Asian-Pacific, Middle East and African, and Latin American markets are smaller than the European and North American markets in terms of absolute size but are expected to grow faster than these two until 2020. This is depicted in the following figure.

Figure 8 – OTT market size and growth by region (in 2020)

Source: MarketsandMarkets

[97] http://www.marketsandmarkets.com/Market-Reports/over-the-top-ott-market-41276741.html
[98] http://www.prnewswire.com/news-releases/over-the-top-market-worth-6203-billion-usd-by-2020-572232561.html

Most provisions of the ePD do not apply to online communication services. This includes communication services that are not covered by the definition of electronic communication services employed by the ePD. Examples include *Skype* or *WhatsAppWhatsApp*.

Recent Eurobarometer data shows that mobile phones to make calls or send text messages are used by 74% of consumers every day while more traditional fixed phone line services are used by 38% each day. However, a large part of consumers also uses services every day that are not covered by the ePD: E-mail is used by 46% of consumers every day, OTTs for the purpose of instant messaging (e.g. WhatsApp) are used by 41% every day[99], and online social networks are used by 38% every day.[100]

The results of the public consultation on the evaluation and review of the regulatory framework for electronic communications demonstrate that consumers increasingly recognise a functional equivalence between traditional SMS/MMS services and OTT services like *WhatsApp* or traditional voice calls and OTT *Voice-over-IP* (VoIP) services like *Skype* and a potential for their substitution.[101]

The majority of popular OTT social network services was launched around 2010, notable exceptions being *Skype* (2003) and *LinkedIn* (2003), *Facebook* (2004) or *Twitter* (2006). Among these OTT services, there seems to be no imperative that older services necessarily have larger user bases than more recent market entrants: A recent survey from 2015 reports the most popular OTT call and messaging services among respondents from EU MS to be *Skype* (49%), *Facebook Messenger* (49%), *WhatsApp* (48%) and *Twitter* (23%).[102]

From a macro perspective, the number of OTT subscribers has grown in two waves since 2000. First on desktop devices from 2000 to 2010, and again with the increasing adoption of smartphones after 2009/2010.[103] Regarding adoption patterns from a micro perspective, OTT messaging and voice call services often experience growth in form of an s-shaped curve: After up to two years needed to gain a critical mass of users, the service frequently experiences exponential growth rates until the market is saturated.[104] Nevertheless, adoption and usage patterns may vary significantly in cross-country comparison for individual apps. In addition, there seem to be country-specific preferences for certain OTT messaging and *VoIP* services and the number of parallel services used (depending on the MS, more than one third to half of respondents use multiple OTT social networks).

Considering actual traffic volumes, the use of OTT services has increased considerably: The OTT's share of overall messaging traffic has already increased from 8.31% (2010) to 66.96% (2013) and is projected to rise to 90% until 2020.[105]

[99] Interestingly, the Eurobarometer data shows that for instant messaging OTTs, two large groups of consumers seem to exist: Those that use instant messaging every day and those that never use it. The proportion of consumers that uses it a few times per week / month is comparatively small. It can be assumed that age is an important factor with regard to the take-up of such services. While younger generations use instant messaging every day, the majority of older consumers do not use it at all. Therefore, it can be expected that the share of consumers who use instant messaging on a daily basis will increase over the next years.
[100] Flash Eurobarometer 443 (2016): e-Privacy. Data on 26,526 consumers collected between 6 and 8 July 2016. At the stage of drafting this report, the Eurobarometer results are only of provisional character.
[101] DLA Piper 2016: ETNO. Study on the revision of the ePrivacy Directive, p. 11; see also https://ec.europa.eu/digital-single-market/en/news/full-synopsis-report-public-consultation-evaluation-and-review-regulatory-framework-electronic
[102] Ecorys, 2016: Study on future trends and business models in communication services. Final report. A study prepared for the European Commission DG Communications Networks, Content & Technology, p. 37, 39
[103] Ibid. p. 41
[104] Ecorys, 2016: Study on future trends and business models in communication services. Final report. A study prepared for the European Commission DG Communications Networks, Content & Technology, p. 40
[105] Ibid. p. 15

Conversely, the use of SMS continues to decrease in almost all EU MS since 2010, albeit at a different pace: In Finland and Germany, SMS volumes have dropped to levels of 2006, while the decline has been slower in countries like Spain and France. Few countries observed stagnant volumes (Poland) or even a growth from previously low levels (Estonia).[106]

On the individual level, the average *WhatsApp* user is reported to send approximately 40 (while receiving around 80) messages per day as opposed to an estimated number of 4.5 SMS. This ratio of approximately 1:10 for daily SMS versus OTTs messages is likely to be much higher in practice, due to the reported parallel use of multiple messaging apps. [107]

Turning from messaging to voice call services, the developments appear to be similar but less pronounced in their magnitude. In general, European Electronic Communications Services (ECS) providers have been observing a steady decline in fixed line calls and steady increase of mobile calls (that have overtaken fixed line traffic shares ever since 2010). Despite this general trend, considerable variance across EU MS remains concerning the popularity or volume of fixed line phone calls.[108] The relationship of ECS and OTT providers offering voice calls is hard to ascertain. With regard to international calls, ETNO reports a rapidly growing popularity of *VoIP* services – despite still lagging behind traditional voice calls and their advantage of any-to-any connectivity with other providers, higher end-to-end quality and more reliable emergency services. The traffic volume of *Skype* increased by 36% in 2013, while traditional voice calls grew by 7%. During that same period, *Skype* calls amounted to a total of 214 billion minutes whereas traditional voice calls reached a total of 547 billion minutes.[109]

Based on these numbers, ETNO conclude that the OTT market presence and substitution of traditional telecommunication services can no longer be ignored.[110] While, this is certainly true, it is still questionable as to whether the presence for OTT service providers offering alternative services is the only cause for EU users changing their communication means as per figures above.

A recent study on behalf of the EC examines not only the rise of OTT services but also possible effects of changes in technology, the regulatory environment and economic growth.[111] Using the development of *WhatsApp* messages as an indicator, the rise of OTT displays no significant effect on the development of revenue, costs and profits for fixed line calls (rather changes in technology and regulation seem to have fostered competition and driven down prices).

In the mobile communications market, on the other hand, the rise of OTTs seems to have had a significant influence in reducing revenues and profits of ECS. Thus, while it is tempting to conclude that decreasing revenues and profits from mobile calls and SMSs are solely driven by the rise of OTTs, some of the developments had already been foreshadowed by increases in competition through the rise of broadband internet and smartphones, triggering changes in consumer behaviour and ensuing updates in business models (e.g. flat rate pricing).[112]

[106] Ibid. p. 45
[107] Ibid. p. 41
[108] Ecorys, 2016: Study on future trends and business models in communication services. Final report. A study prepared for the European Commission DG Communications Networks, Content & Technology, p. 42-44
[109] DLA Piper 2016: ETNO. Study on the revision of the ePrivacy Directive, p. 13
[110] DLA Piper 2016: ETNO. Study on the revision of the ePrivacy Directive, p. 13
[111] Ecorys, 2016: Study on future trends and business models in communication services. Final report. A study prepared for the European Commission DG Communications Networks, Content & Technology
[112] Ecorys, 2016: Study on future trends and business models in communication services. Final report. A study prepared for the European Commission DG Communications Networks, Content & Technology, p. 66f

Yet ECS so far compete in one ecosystem that is owned and operated by a large number of providers bound by standards of interoperability, serving an interconnected subgroup of end-users (i.e. services based on the E.164 numbering plan). OTT providers, on the other hand, compete between ecosystems and for subscribers using multiple similar services of competitors and without the need to follow standards of interoperability.[113]

3.5.3 The EU and US advertising markets

In this section, we present some information on the EU and US advertising markets. The two markets differ with regard to the presence of regulation: In the U.S. case, there are no strict laws explicitly aimed at Online Behavioural Advertisement (OBA) and transparency towards users. In the European Union, several laws and regulations apply to the OBA industry. The ePD has an indirect link to both markets through its provisions concerning the tracking of consumers and their online behaviour by means of cookies on websites (e.g. for the purpose of targeted online advertising), as well as – subsequently – sending consumers commercial communications containing marketing material. The purpose of the section is to give the reader a high-level overview of the relevance of online tracking and targeted advertisement for the sector and the size of both markets. Article 5(3) of the ePD affects the advertisement market via its rules on cookies.

3.5.3.1 The importance of (third-party) cookies

With regard to the online advertisement market, **cookies remain an important instrument in the online advertisement market** to identify and track users.[114] In order to know their audience and improve the match between website visitor interests and placed ads, website publishers and online advertisement industry alike crucially depend on web analytics information.

Cookies are (temporary) information logs: First-party cookies are placed on users' computers by the website that is actually visited (i.e. the second party), e.g. to recognize repeated visitors or remember the content of their shopping carts. **Third-party cookies**, on the other hand, are placed on the user's terminal by a website other than the one visited (generally in mutual agreement). In most cases, they contain a unique user ID and instruct the user's browser to contact the third-party whenever the user accesses any website also using the same third-party cookie solution. This enables the third-party to (1) identify users across websites and (2) record their movements, e.g. clicks or purchases. These logs are the backbone of online advertisement, nowadays mostly managed by third-party intermediaries linking advertisers and publishers offering ad spaces. Advertisement networks like *Google*'s *AdWords, AdSense* or *Doubleclick*, basically sell these blank spaces for publishers. Third-party web analytics operators like *Google Analytics, Facebook* or *comScore* help to optimise display ad delivery to the desired user segments through the tracking of their online behaviour. Linking databases of these third-party tracking networks increases advertisement revenues and the share of publishers selling ad spaces. While this practice enables nominally free online services for users, it

[113] Ecorys, 2016: Study on future trends and business models in communication services. Final report. A study prepared for the European Commission DG Communications Networks, Content & Technology, p. 100

[114] United States Senate (2015): Online advertising and hidden hazards to consumer security and data privacy majority and minority staff report. Permanent subcommittee on investigations. https://otalliance.org/system/files/files/resource/documents/report_-_online_advertising_hidden_hazards_to_consumer_security_date_privacy_may_15_20141.pdf.

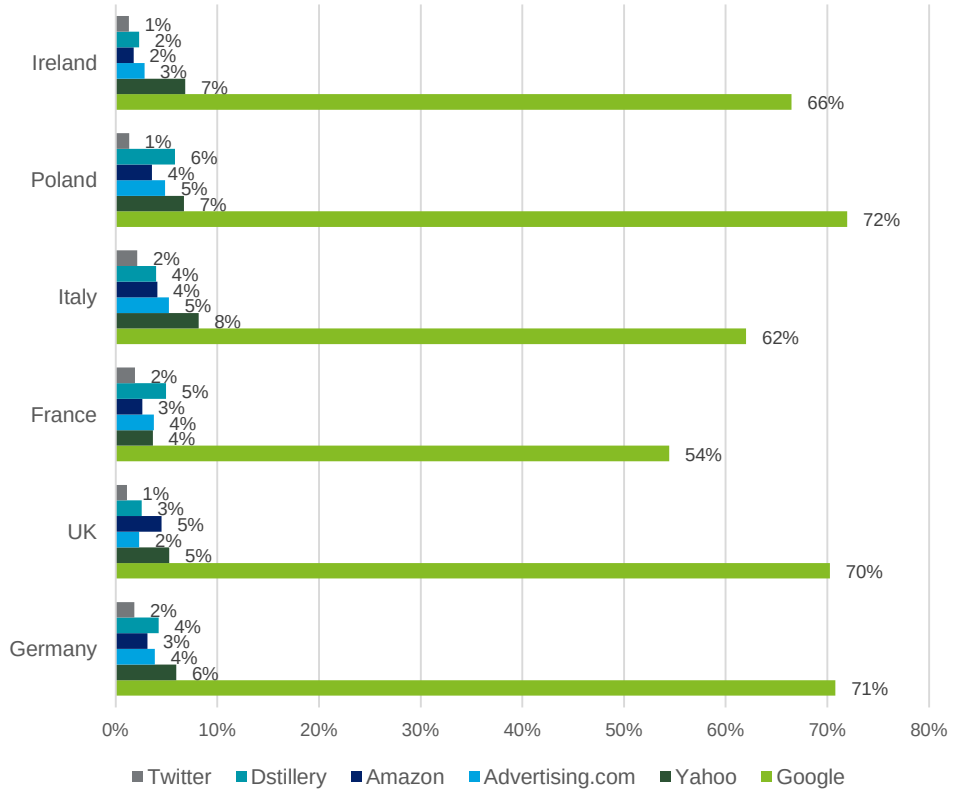
however raises serious doubt as to whether users would actually consent to tracking via cookies or other means if asked.[115]

The **market volume** for third-party tracking is **difficult to ascertain**, as most firms offer several, sometimes unrelated, products and most of the major websites rely on several different advertisement networks and web analytics solutions.

The "Cookie Sweep", carried out by the *Article 29 Working Party* in September 2014, provides insights on the general use of cookies on websites in eight EU Member States.[116] In a sample of 478 media, e-commerce and public sector websites, 28.9 cookies were on average placed by each site. Roughly 70% of these were third-party cookies, whereas only 30% constituted first-party cookies. Notable deviations from this ratio were only found in Greece and Slovenia, where more than half of the cookies on websites had a first-party origin. Most of the cookies observed were designed to remain on the users' systems after websites are closed: Approximately 86% of cookies constituted so-called persistent cookies, while only about 14% were session cookies (expiring right after the interaction with the website ended).

The 2014 Cookie Sweep also points to a considerable degree of **market concentration**: 25 third-party domains together reached a total share of more than 53.1% of all third-party cookies set on the websites under scrutiny. Additional desk research provided evidence in line with these observations. Figure 9 shows the prevalence of the six major third-party advertising network companies *Google*, *Yahoo* (Right Media), *AOL* (Advertising.com), *Amazon* (A9), *Dstillery* and *Twitter* for websites accessed in selected member states. *Google AdSense*, *AdWords* and subsidiary company *Doubleclick* are present on more than half of all websites in the EU member states presented, often linked with the *Google Analytics* Suite that enables further insights on visitor characteristics for website improvements.

Figure 9 – Share of third-party tracking tools by the major 6 advertisement networks on websites in selected



gulation, p. 16,
otection-tmt.pdf.
ted Kingdom took part
15): Cookie sweep

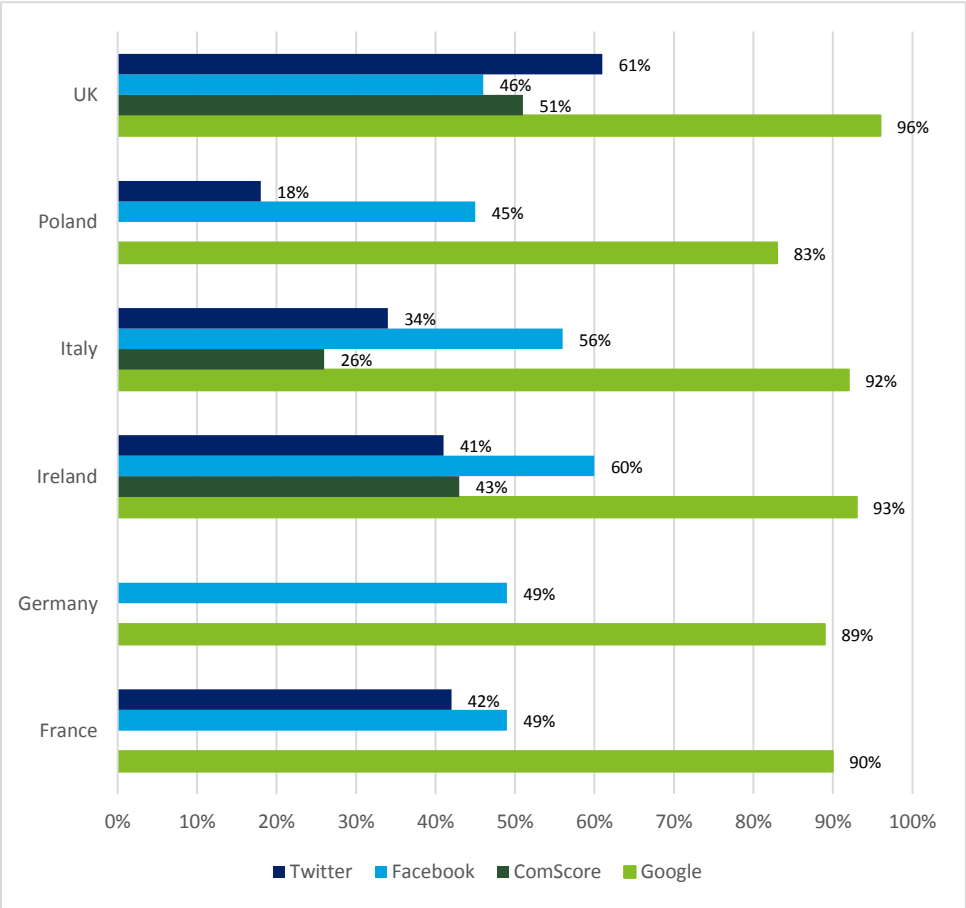
European markets

Source: Datanyze.com[117], public data for August 2016, graphical presentation by Deloitte

In a more general approach, the projects "Trackography" and "Me and my shadow" by *Tactical Tech* attempt to assess the market shares of "globally prevailing tracking companies" (employing browser cookies and other tracking technologies). The analysis was carried out in 2015 and covers more than 2500 prominent websites worldwide.[118] Again, by far the dominant company in this market is *Google* (*Google Analytics)*, found in 85% of all websites under scrutiny. Other, slightly less omnipresent operators of commercial tracking networks are *comScore*, *Facebook* and *Twitter* - although there seems to be considerable cross-country variance in market shares. A closer look at the EU Member States covered in the database reveals that additional operators like *Amazon.com* supply large shares of third party cookies in several markets.

The figure below portrays the share of third-party tracking tools originating from the four major companies *Google*, *comScore*, *Facebook*, and *Twitter* for selected EU Member States for which data is available.[119]

Figure 10 – Share of third-party tracking tools originating from the four major companies found on major news websites



[117] https://www.datanyze.com/market-share/advertising-networks; Datanyze provides public numbers of advertisement network market shares on Alexa top 1M websites, filtered by country.
[118] Due to its nature as an open-source project, Trackography only provides an insight for specific selection of countries where volunteers took part The project identifies third-party tracking operators in a sample of more than 2,500 news and media websites across 38 countries
[119] https://myshadow.org/trackography-meet-the-trackers.

Source: Tactical Tech (2015)

Insights: Implications of third-party tracking in practice

As mentioned above, **advertisers** of course profit from third party tracking and ad networks as they are able to reduce costs (e.g. of finding relevant users and ad spaces), as well as waste that decreases customer satisfaction (e.g. placing ads in the wrong places) and thereby increase profits.

Publishers relying on third-party tracking and ad networks benefit from the knowledge gathered about users and possible higher revenue generated from renting out ad spaces. Several web analytics tools offer a free version with reduced functionality (often aimed at smaller websites) and a premium version. The most employed tracking solution is *Google Analytics* with a self-reported customer base of 10 million websites. The pricing of its premium version, recently rebranded as *Google Analytics 360*, is based on "hits" (defined as user clicks or individually pre-determined events for actions on a website, e.g. an actual sale). The annual subscription fee for a website amounts to approximately EUR 135,000 until up to 500,000 hits per month, from there on increasing for growing numbers of hits. Above 20 billion hits per month, negation of individual pricing is advised according to the digital analytics consultancy (and *Google's* European partner) *Trakken*.[120]

Turning to the perspective of the **internet users,** the implications are twofold. On the one hand, **internet users** benefit from more customised and relevant content on websites that employ third party tracking. Far more beneficial in the view of most users might be that they can access the publisher's services for free – as they are financed through ad revenues optimised via tracking. On the other hand, a recent study showed that these third-party tracking instruments can slow down the load time for webpages and increase the data volume used while surfing. Disabling tracking via the *Firefox* in-browser protection decreased median load time for webpages by 44% and data usage by 39% (for a sample of top 200 *Alexa* news sites).[121] These numbers allude possible costs for users on traffic volume based internet access plans (popular in the mobile internet segment).

3.5.3.2 The EU advertising market

The European branch of the *Interactive Advertising Bureau* (www.*iab.europe.eu*) reports a total value of the EU online advertisement market of EUR 36.2bn in 2015 - an increase of almost EUR 30bn or close to 450% compared to a total market value of EUR 6.6bn in 2006.[122] Comparing the amounts spent on traditional and digital forms of advertisement, the latter has experienced a significant increase at the expense of the former (while the total market value of both forms fluctuated rather consistently around EUR 100bn). Indeed, online advertisement appears to be the main if not sole driver of growth in the sector: Without the growth of online advertisement by roughly 13%, the European market would have shrunk by almost 4% from 2014 to 2015.[123] In terms of total market value, online advertisement overtook TV (EUR 33.3bn) as the traditionally largest advertisement medium for the first time.

[120] Trakken.de (02.05.2016): Google Analytics 360 – Kosten und Preismodell, https://www.trakken.de/insights/google-analytics-360-was-kostet-das-eigentlich/

[121] Kontaxis, Georgios and Chew, Monica (2015): Tracking Protection in Firefox For Privacy and Performance, http://ieee-security.org/TC/SPW2015/W2SP/papers/W2SP_2015_submission_32.pdf.

[122] This corresponds to a CAGR of 20.5% for the period from 2006 to 2015; see also: http://www.iabeurope.eu/wp-content/uploads/2016/05/AdEx-Benchmark-Interact-Presentation-2015.pdf.

[123] In fact, the growth rates for online advertisement itself have fluctuated for the last decade: While the market experienced growth rates between 40% and 60% in 2007 and 2008, these numbers have dropped to values below 10% in 2009 and have remained relatively stable at a level of 12% to 13% ever since.

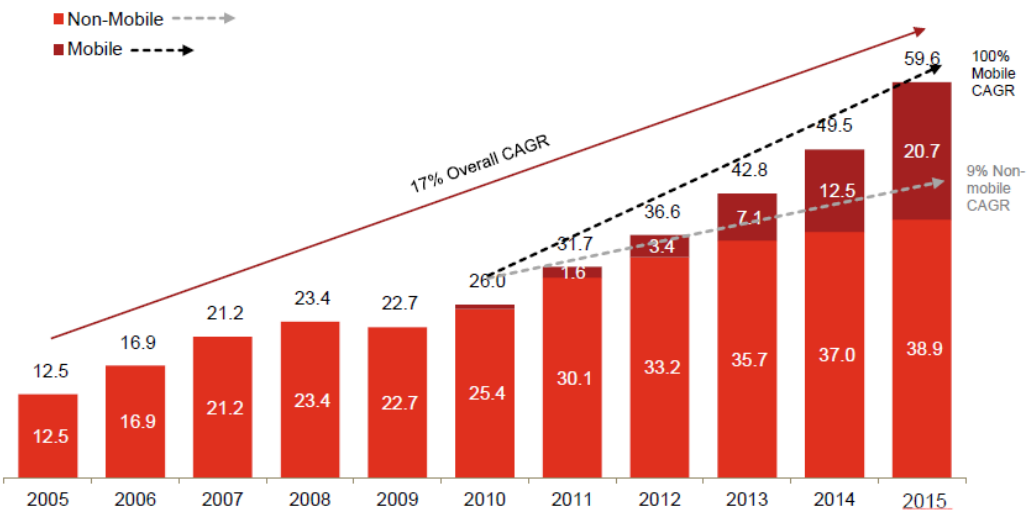
Two formats dominate the online advertisement in 2015: Paid-for-search[124] (roughly 46% in Western and 54% in Central and Eastern Europe) and display ads, also known as banner ads (with roughly 38% in Western and 41% in Eastern Europe). While display ads growth is steadily increasing since 2013 for Europe as a whole (from 14.9% to 17.4%), paid-for-search also displays a constant yet slightly lower growth rate (hovering around 12%). Still higher growth rates can be observed when looking at the sub-segment of mobile online advertisement, with mobile display ads growing by more than 60% and paid-for-search by roughly 57% from 2014 to 2015. During that same period, the format of videos ads also grew considerably faster (at a pace of 36%) than general online display ads and paid-for-search. Concerning the overall outlook, the developments for the mobile segment and video formats is expected to drive future growth. However, stagnation in paid-for-search and the complexity of devices, platforms and behaviours appear to cloud the industry's outlook.

3.5.3.3 The US internet advertising market

According to a 2016 PwC study on the US internet advertising market, the 2015 revenue totalled $ 59.6 billion for the full year 2015.[125] Hence, the Internet advertising market is the largest advertising market in the US, thus larger than the market for broadcast television ($ 40.6 billion), cable television ($ 25.7 billion), radio ($ 17.4 billion), newspaper ($ 15.1 billion), and magazines ($ 12.2 billion).

Since 2005, the US market has grown at a Compound Annual Growth Rate of 17% until today.

Figure 11 – OBA revenue in the US market (2005-2015, in billion USD)



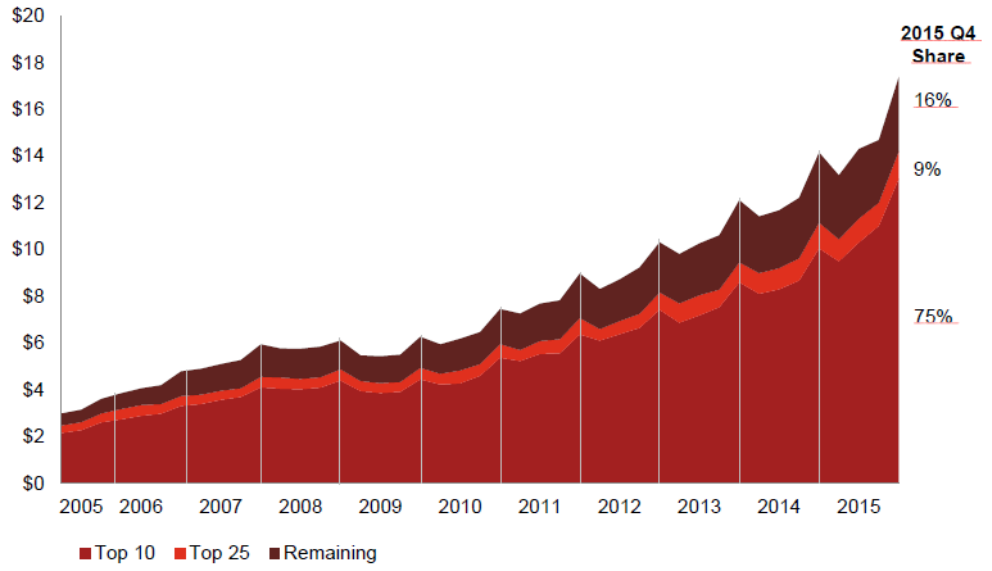
Source: IAB/PwC Internet Ad Revenue Report, FY 2015

In 2015, online advertising has continued to remain concentrated with the ten leading ad-selling companies, which accounted for 75% of total revenues in the fourth quarter of 2015.

[124] Paid-for-search is also known as *Search marketing* and describes "practice of placing an advert on a search engine result page based on the context of the search query" as iab.UK explains. Advertiser bid on search keywords in order to display relevant ads for users conducting the search. (https://www.iabuk.net/disciplines/search-marketing/guide#TDRQ2ck8m4F1QpkG.99)". Read more at https://www.iabuk.net/disciplines/search-marketing/guide#TDRQ2ck8m4F1QpkG.99"

[125] PwC (2016): IAB internet advertising revenue report 2015 full year results April 2016, https://www.iab.com/wp-content/uploads/2016/04/IAB-Internet-Advertising-Revenue-Report-FY-2015.pdf.

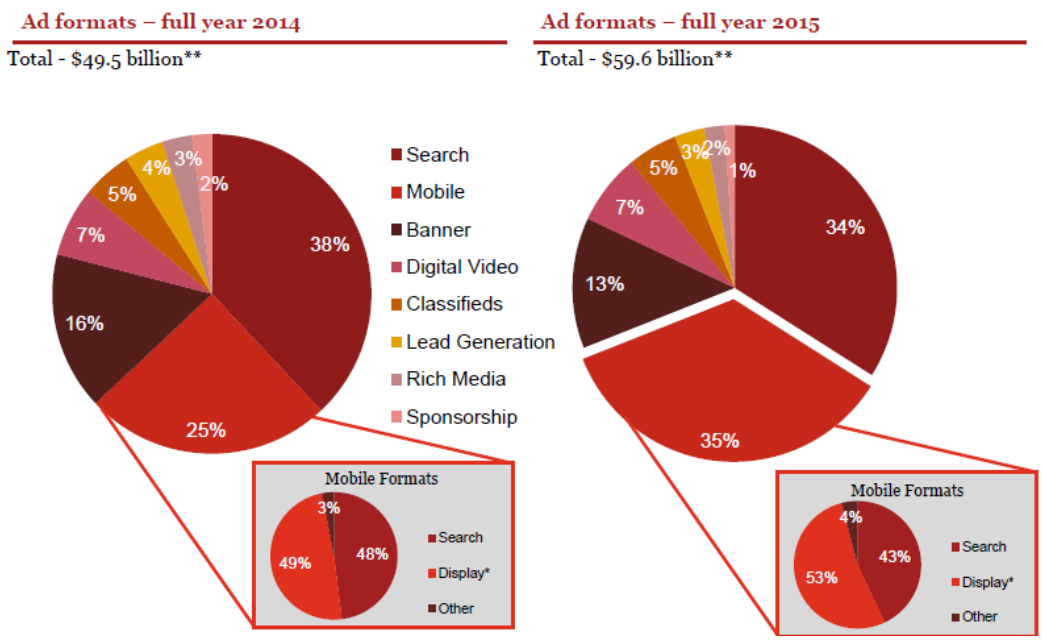
Figure 12 – OBA revenue concentration in the US market (2005-2015, in billion USD)



Source: IAB/PwC Internet Ad Revenue Report, FY 2015

Around 35% of online advertising revenue was generated through mobile formats such as display advertisement. In 2014, one year before, it was only 25%. This means that the importance of the mobile online advertisement market is growing.

Figure 13 – Share of OBA revenue per type of advertisement in the US market (2014 & 2015)



Source: IAB/PwC Internet Ad Revenue Report, FY 2015

As regards different industries and their share of the US online advertisement market, the *PwC* report[126] indicates that:

[126] PwC (2016): IAB internet advertising revenue report 2015 full year results April 2016, https://www.iab.com/wp-content/uploads/2016/04/IAB-Internet-Advertising-Revenue-Report-FY-2015.pdf, p.18

- Retail advertisers continue to represent the largest category of internet ad spending, accounting for 22% of total revenues in FY 2015;
- Financial Services advertisers accounted for 13% of revenues in FY 2015;
- Automotive advertisers accounted for 13% of revenues in FY 2015;
- Telecom companies accounted for 9% of revenues in FY 2015;
- Leisure Travel (airfare, hotels, and resorts) accounted for 9% of revenues in FY 2015;
- Consumer Packaged Goods represented 6% in FY 2015;
- Consumer Electronics and Computers advertisers represented 7% of revenues in FY 2015;
- Pharmaceutical/Healthcare accounted for 5% in FY 2015;
- Media accounted for 5% in FY 2015; and
- Entertainment accounted for 4% of FY 2015 revenues.

Task 1: REFIT exercise (transposition check and evaluation)

4 Transposition Check

In this section we outline the findings resulting from the transposition check of the ePD (the first part of Task 1 – REFIT). We also identify and discuss possible problems, gaps, overlaps and diverging transpositions of the ePD at local Member State level, taking into account the need to ensure a single market and free movement by avoiding fragmentation along national boundaries

4.1 Introduction

This Chapter presents the findings from the transposition check of the following nine (9) articles:

- Article 1;
- Article 2;
- Article 3;
- Article 4;
- Article 7;
- Article 8;
- Article 10;
- Article 11; and
- Article 12.

The REFIT exercise includes a transposition check that monitors national laws by conducting an in-depth analysis of national implementation of the provisions mentioned above. This transposition check involved a desktop research on the local provisions transposing the respective articles of the ePD. In addition to this research, the Deloitte network of local experts in each of the 28 Member States was contacted in order to confirm our findings and identify any outstanding gaps. The consultation with the local Deloitte Member Firms was made via a standard reporting template, which contained a number of questions on the transposition of the articles, the interpretation made by the competent authorities, relevant case law and implementing procedures adopted by the regulator, as well as the existing market practices for complying with the provisions.

The analysis sought to assess the information gathered through the transposition check, identifying and discussing common trends among Member States, deviations from the letter and the spirit of the ePD, national specificities or overlaps, and, in general, diverging transpositions. To this end, the following modes of transposition were considered:

- **Literal transposition**: meaning that the specific article was incorporated in the national legislation word-by-word or with a semantic equivalence to the formulation of the ePD;
- **Full transposition without material differences**: meaning that the provision was not literally incorporated in national legislation but that the requirements and objectives of the ePD have been fully transposed in local law;

- **Partial transposition**: meaning that the scope of the article was narrowed in national legislation, with the provisions of the ePD not being fully covered;
- **Full transposition but with a broader scope**: meaning that the provision was fully transposed but that national legislation provides additional details or requirements;
- **No transposition**: meaning that the requirements and objectives of the provision were not transposed in national legislation by any means.

Based on this categorisation and the analysis of the gathered information, we have drafted conclusions on the transposition of the nine articles in scope. The objective of these conclusions is to provide an overview of the extent to which the objectives of the ePD were implemented and whether the transposition of the scoped provisions posed specific challenges as to their interpretation. Throughout this analysis, the need to ensure a single market and free movement by avoiding fragmentation along national boundaries was consistently taken into account.

4.2 Main findings of the 2015 Study on the ePrivacy Directive

In February 2015, the European Commission concluded a Study on the ePrivacy Directive (SMART 2013/0071) with the objective to assess the transposition, effectiveness and compatibility of the ePD with the proposed General Data Protection Regulation. The study focused on the following provisions of the ePrivacy Directive: Article 3 on scope, Article 5.1 on confidentiality of communications, Article 5(3) on confidentiality of terminal equipment, Article 6 on traffic data, Article 9 on location data and Article 13 on unsolicited communications.

Scope of application (Article 3) - The survey of the transposition of Article 3 in the national legislation of the Member States has demonstrated that several provisions of the ePD have been transposed in another legal framework such as consumer protection or information society services, and thus might have a different scope than the one defined by Article 3. It was therefore recommended to broaden the scope of the ePD, and make its provisions applicable to information society services and other added-value services provided via public electronic communications networks.

Confidentiality (Article 5) – According to the findings, all the Member states had in their national legislation provision dealing with the protection of confidentiality of private communications long time before the adoption of this provision in the ePD in 2002. In this light, the transposition of Article 5.1 did not have a harmonizing effect. With regard to the second paragraph of Article 5 which relates to a "business exception" authorizing the recording of communications and traffic data when carried out for lawful business practice, the transposition by Member States varies significantly. For instance, some Member States have restricted this exception to the electronic communication sector while others applied it to all sectors. The study recommends a clarification of the scope of both paragraphs in order to obtain a uniform transposition and implementation of this provision throughout the Union. With regard to Article 5.1., the provision could be made applicable to "confidentiality of communications and the related use of traffic data by means of a public or publicly accessible privacy communications network". Concerning the second paragraph of Article 5, the current restriction could be widened to other situations in which recording of communications in an employment context seems to be justified, such as quality control or legitimate supervision of work performance.

Article 5.3 has already been amended in 2009, however, this amendment has not yet been transposed by all Member States. There is a need for EU-wide guidance on how to implement this amendment in practice. In addition, the Article mentions two exemptions from the need for the user's

or subscriber's consent for storing or having access to information stored on his terminal equipment, namely, the case of *'technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network'*, or *'as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service'*. The 2015 study has proposed a slightly broader formulation, and to add a specific exemption for cookies used to obtain web-site usage statistics.

Traffic and location data (Articles 6 and 9) – According to the study, Article 6 on Traffic Data was more or less correctly transposed by the Member States. However, looking at the enforcement, it appears that important differences subsist among Member States. While article 6(3), stipulates that traffic data may be processed to the extent and for the duration necessary for the services or marketing only based on user's prior consent, in practice some mobile operators mention in their terms and conditions the possibility of processing user and traffic data for a duration of two years after the end of the contract.

Regarding the provisions on location data in article 9, the study raises concern with regard to the fact that this provision regulates only a fraction of location based services and does not cover location based services that are offered to the members of a private network for instance, even though privacy risks may be the same or even greater.

In this regard, the study recommends to modify the wording of Article 6 and 9 in order to make them applicable to all services that collect and further process traffic and location data, and ensure a correct transposition into the national legislation.

Unsolicited Direct Marketing Communications (Article 13) – According to the study, Member States have adequately transposed Article 13(1) into their national legislation. However, this provision has been interpreted in such a way that it is not applicable to messages exchanged via information society services. In this regard, the study recommends to extend the opt-in rule of Article 13(1) to e-mail messages transmitted via information society services. In addition, the Directive stops short of specifying the rules that should be put in place for subscribers being are legal persons.

4.3 Transposition Check in the 28 Member States

4.3.1 Scope of Application (Articles 1, 2, and 3)

Article 1 – Scope and Aim

Article 1 outlines the scope and the dual aim of the ePD, which is to: (1) ensure an equivalent level of protection of the right to privacy and confidentiality with respect to the processing of personal data in the electronic communications sector and (2) to ensure the free movement of such data, electronic communication equipment, and services in the Community. The ePD applies to both natural and legal persons. However, public security and defence activities do not fall under its scope.

The majority of Member States did not transpose this article literally. However, in most cases, the objective of ensuring personal data protection in the electronic communications sector has been reflected in the local implementing acts. In contrast, the transposition check revealed that the large majority of Member States did not expressly refer in their laws to the objective of ensuring the free movement of data in the telecommunications sector.

A few countries, such as Italy, France and Malta did not transpose this article at all.

It is worth pointing out that the legal instruments transposing the ePD often have a broader scope than the ePD itself. In certain cases, the national laws transpose other Directives; in others, they regulate the entire telecommunications sector, incorporating the ePD in one of their "chapters". Moreover, these laws often fail to expressly refer to the protection of personal data in the telecommunication sector as a main goal, a finding that may be partially ascribed to the wider framework into which the ePD is embedded.

Examples of Member States whose local laws provide for a broader scope are Poland, Portugal, Romania, Slovakia and Slovenia. Latvia's national law, for example, sets out to promote and develop competition in the provision of electronic communications networks and services. Similarly, the law of Denmark states that the objective of the transposing legal act is to promote efficient and innovative market for electronic communications. More examples of implementing legal acts not specifically referring to the objective of protecting personal data are the laws of Spain, Sweden, Denmark and Lithuania. In other cases, such as the Czech Republic, the ePD is transposed in different legal acts and therefore the objective of personal data protection is not expressly reflected.

Given the programmatic nature of this provision of the ePD and the fact that is primarily addressed to Member States, the omission of explicit references to the dual aim of the Directive in the corresponding national laws does not seem to constitute an obstacle to the protection of fundamental rights and freedoms or the free movement of personal data, electronic communication, equipment, and services. However, it can be argued that the lack of a direct reference to the protection of these rights in the electronic communication sector creates some obscurity as to the exact scope of these rules.

Article 2 - Definitions

Article 2 of the ePD provides the definitions of "user", "traffic data", "location data", "communication", "value added service", "electronic mail", and "personal data breach". For the definition of "consent" the ePD refers to the definition set out in Directive 95/46/EC.

The majority of the Member States, including Greece, Lithuania, Malta, Slovenia, and Portugal, have adopted a literal transposition of the definitions provided by the ePD. Many of the Member States, such as Austria, Denmark, Greece, Slovakia, Romania, and Spain, have included additional definitions. For example Austria's law sets out the meaning of *"content data",* "*access data*", *"cell ID", "subscriber identifier", "internet telephone service*", and "*internet access service*". Danish law provides an interesting example of a broad list of definitions. Among others, Danish law provides a definition for the terms *"provider", "commercial provider", "end-user", "network termination point", "voice telephony service", "network access"* and *"interconnection".* In addition, it is interesting to note that the Danish law distinguishes between "*electronic communication services*" and "*public electronic communication services"*. In the same vein, the same distinction is applied for *"electronic communications networks"* and "*public electronic communications networks".*

The major diverging point with the ePD in many of the implementing acts relates to the definition of "user". Some countries have included legal persons in the definition of "user". This is the case of Belgium, Luxembourg, Bulgaria, and Croatia. Notwithstanding the fact that the ePD also protects the legitimate interests of subscribers who are legal persons, the definition of user in the ePD refers only to natural persons. In Cyprus, for example, the law refers to "consumer" and not to "user" although the

meaning appears to be the same. Other countries such as Greece and Bulgaria provide both the definition of “user” and “subscriber”.

Some countries such as Estonia, France, and Latvia, did not transpose or transposed only partially Article 2 of the ePD in their laws. For instance, France does not provide a definition for “user” and “location data”. However, French law provides other definitions for terms such as “telecommunications operator”.

From an enforcement perspective, for example in Austria, there is case law over the definition of “electronic email”. In its decision 2003/03/0284 the Austrian Supreme Administrative Court concluded that the terms “electronic mail” and “e-mail” cannot be equated, since the scope of electronic mail goes beyond mere e-mails and the qualification of IP address as traffic data. The Austrian Supreme Administrative Court (“Verwaltungsgerichtshof”) ruled in his decision 2007/05/0280 that dynamic IP-addresses are not considered ”master data”, but “traffic data” which is processed to transfer information to a communications network.

In general, it can be concluded that this article was transposed literally by most of the Member States. Apart from the fact that many of the latter have additional definitions in their implementing acts, no major disparities were found on the transposition of this article. While the expansion of the notion of “user” so as to include legal persons is a noteworthy deviation, this does not seem to impact or contradict the dual aims of the ePD. Moreover, the ePD is functionally bound to the definition of “personal data” in Directive 95/46/EC, an instrument that does not contemplate the protection of legal persons with regard to the processing of their data. However, the definition of *“communication”* has been most of the time literally transposed or not transposed. This is important as the transposition and interpretation of the definition of *“communication”* is particularly sensitive as it is affects largely the scope of the ePD.

Article 3 – Services Concerned

Article 3 limits the scope of the ePD to publically available telecommunications services in public communications networks only. This means that the ePD is mostly limited to traditional telecommunications services and excludes providers of alternative communication services such as Internet Telephony, e-mail and instant messaging (e.g. Skype, Gmail and WhatsApp).

The transposition check of this article revealed considerable disparities related to the transposition and interpretation of this article among Member States. Except for some Member States[127], most of the Member States did not transpose literally this article in their local laws. Many countries, such as Belgium, Denmark, France, Finland, Latvia, Sweden Germany and the UK, appear not to have transposed this article at all in their local laws.

Even among those Member States that transposed this article literally, there are different interpretations as to the extent of its scope. In particular, the implementing acts of some Member States have interpreted this term broadly as to include over-the-top providers (“OTTs”). Nevertheless, it has to be noted that the large majority of Member States do not seem to interpret the law in such a way as to generally include these services.

Based on case law, enforcement decisions in some countries have extended the scope to include OTTs. For instance, Austria interprets its implementing provisions broadly, and considers services

[127] Cyprus, Estonia, Greece, Ireland, Italy, Luxembourg, Malta, Portugal, Romania

such as Skype to fall under the scope of electronic communication services. This interpretation has been confirmed by decision R 8/08-03 of the Telekom-Control Commission. The case law in other countries such as Italy, France, Slovenia, and Spain also appears to lean towards extending the scope of the rules to OTTs. For example, the debate in Italy on whether OTTs are covered or not is currently ongoing. However, it is interesting to note that Italy interprets Voice-over-IP (VoIP) services as falling under the scope of this provision. Similarly, in Germany, there are conflicting decisions and opinions on whether these rules should apply to OTTs and, in such a case, to which categories of providers. By contrast, in the Czech Republic, OTTs are covered by Act No. 480/2004 Coll. on Certain Information Society Services (ISSA) which is a specific act implementing the EU legislation related to the services of the information society (i.e. the services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services). The ISSA regulates the liability of the providers of such services and the rules on dissemination of unsolicited commercial communications. The ISSA implements Article 13 of the Directive on unsolicited communications.

A recent example of a legislative act which is drafted in such a way as to conceivably include OTTs is the so-called "Macron Law" in France.[128] It subjects any provider of an electronic communication service to the public to the obligation of declaring such activity to the competent authority (and, according to an accompanying recital, to any "other obligations that might ensue"). While the new provision does not expressly refer to OTTs, it is likely that the case law will be able to rely upon this provision to extend the scope of covered services.

A few countries, such as Austria, Bulgaria and Latvia, have also included private networks under the scope. By contrast, the large majority of Member States exclude private networks and information society services in general, from the scope of their implementing acts.[129] Once again, case law often denotes a different approach. In France, a 2005 judgement from the Paris Court of appeal ruled that employers who gave Internet access to their staff should not be able to enjoy any distinction as regards the public providers of such services.[130]

In conclusion, the transposition check of this article reveals that Member States have diverging views on whether the ePD should apply to OTTs and private networks. No law in any Member State specifically includes OTTs under its scope, but in some cases there is now a well-established judicial or administrative practice in interpreting the scope broadly so as to include these services. While this disparity in treatment does not hinder the protection of personal data in connection with those processing operations expressly covered by the ePD, it does possibly cause disturbances in the free flow of such data between Member States. In addition, the different interpretations of the scope of the ePD lead to inconsistent enforcement among EU Member States and therefore to legal uncertainty and probably *forum shopping*. The fact that some Member States interpret the scope of the ePD broadly in order to include private networks and OTTs can be seen as an indicator that this article is not any more in line with the technological developments.

[128] LOI n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques (Loi Macron).
[129] Specifically, Belgium, Bulgaria, the Czech Republic, and Germany.
[130] Paris Court of Appeal, *BNP Paribas v World Press Online*.

4.3.2 Article 4 – Security of Processing

Similarly to the obligations on security measures stemming from Directive 95/46/EC, Article 4 of the ePD requires service providers to implement appropriate technical and organisational security measures taking into account the risk presented. Article 4 is more detailed on the security requirements and imposes new security obligations compared to Directive 95/46/EC. Article 4 imposes a minimum level of security measures to be implemented by service providers, which consists in:

- Access management on a need-to-know basis (personal data must be access only by authorised personnel for legally authorised purposes);
- Measures for protecting the integrity and availability of data (protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure);
- Security policy.

In addition, in case of risk of a security breach, the service providers are required to inform the subscribers of the risk and take the necessary measures. If a security breach occurs, the service provider shall in addition notify the DPA by describing the nature of the personal data breach, the contact points where more information can be obtained, and by recommending measures to mitigate the possible adverse effects of the personal data breach. Regarding security breaches, the service providers must maintain an inventory of data breaches. The last two paragraphs of this article relate to the ability of national DPAs to audit the security measures implemented by service providers and refer to the guidance that might be issues on the topic by ENISA and Article 29 Working Party.

Due to the length of his article, the transposition check was performed per paragraph in order to be as accurate as possible and to be consistent with the approach undertaken for other articles containing of similar length or density. Observations on the transposition of this Article as a whole shall follow this approach.

Paragraph 1 of Article 4 requires the provider of a publicly available electronic communications service to take technical and organisational measures to safeguard security of its services appropriate to the risk presented. Many of the Member States have transposed this paragraph literally (Belgium, Croatia, Czech Republic, Denmark, Greece, Hungary, Ireland, Latvia, Netherlands, Spain and the UK).

Finland has transposed this article only partially as its implementing law does not make specific reference to technical and organisational measures. Nevertheless, Section 243 of the implementing law imposes a high level of information security for communications network and services. Only Malta seems not to have transposed this paragraph.

The large majority of Member States (Austria, Bulgaria, Cyprus, Germany, Italy, Lithuania, Luxembourg, Portugal, Romania, Slovakia, and Sweden) have transposed this paragraph fully, even if the transposition was not always performed literally. The remaining countries (Estonia, France, Poland and Slovenia) have also transposed this paragraph in a satisfactory manner. For most of them (Estonia, France, Poland and Slovenia) the implementing acts have broadened the scope of this paragraph in relation to the original provision in the ePD.

Paragraph 1a of Article 4 imposes a minimum level of security measures that services shall implement in order to:

- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,
- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,
- ensure the implementation of a security policy with respect to the processing of personal data.

In addition, this paragraph states that relevant national authorities shall have the power to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should attain.

Many of the countries (Belgium, Croatia, Denmark, Greece, Ireland, Latvia, Luxembourg, Romania, and Spain) have transposed this paragraph literally. Some countries (Bulgaria, Denmark, Lithuania, Malta and Portugal) have also fully transposed this paragraph, albeit without changes to the original wording of the Directive. Others have transposed the paragraph only partially such as Austria, Czech Republic, Finland, Hungary and the Netherlands. For instance, Austria and the Netherlands do not refer to the ability of DPAs to audit the measures implemented. In stark contrast, it would appear that a number of Member States have not transposed this paragraph at all (Cyprus, Germany, Italy, Malta, Poland, Sweden, UK). As for the remaining Member States (Estonia, France, Slovakia, Slovenia) transposition of this paragraph has been achieved but with a broader scope that the original provision.

Paragraph 2 of Article 4 sets out an obligation for the provider to notify the subscriber in case that there is a risk of data breach. If this risk lies outside the scope of the measures to be taken by the service provider, the latter is bound to communicate to the subscriber the existence of any possible remedies, including an indication of the likely costs involved.

A few of countries have literally transposed this article (Belgium, Greece, Ireland, Latvia, Romania, and Spain). Although the majority (Austria, Croatia, Cyprus, Czech Republic, Hungary, Italy, Lithuania, Luxembourg, Malta, Netherlands, Portugal, and Sweden) have not transposed this paragraph literally, no material differences have been observed between the various transposition acts. On the other hand, Member States such as Bulgaria and the UK have transposed the paragraph only partially, and a number of countries have not transposed this paragraph at all (Denmark, Finland, and Germany). The remaining countries have transposed the article fully but have extended its scope compared to the ePD (Estonia, France, Poland, Slovakia, and Slovenia). For instance, the law in France is more detailed on the content of the breach notification. In addition, the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés "**CNIL**") has provided guidance on the self-evaluation of data breaches risks and the forms to be used for notification purposes.

Paragraph 3 of Article 4 also concerns data breach notifications. However, this provision addresses actual data breaches that have occurred, rather than the mere risk of such an eventuality (as was the case in the previous paragraph). In the event of a data breach, the provider has an obligation to notify the competent authority and the subscriber or individual concerned if the breach is likely to have adverse effects, unless the competent authority decided that the measures implemented are appropriate to the data breach. In addition this paragraph clarifies that the notification shall contain at least the nature of the data breach, the contact points where more information can be obtained, mitigation measures for the adverse effects, the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

A few countries such as Belgium, Greece, Ireland, Malta, Romania and Spain have transposed this paragraph literally. Others have not transposed the text literally but have fully transposed the paragraph without any material differences (such is the case with Austria, Bulgaria, Croatia, Hungary, Luxembourg, and Portugal. Germany and Cyprus have not transposed at all this paragraph while other countries have transposed it only partially (Czech Republic, Denmark, Finland, Netherlands, Sweden and UK). For instance, the Netherlands transposed this paragraph only in relation to the part which provides the obligation to keep an inventory or record of data breaches (an obligation under Paragraph 4 of Article 4 of the ePD). The rest of the Member States (Estonia, France, Italy, Latvia, Lithuania, Poland, Slovakia, and Slovenia) have fully transposed the paragraph but with a wider scope than in the Directive. For instance, in Latvia, the law alludes to documentation on internal procedures for the investigation and prevention of breaches.

Paragraph 4 of Article 4 refers to the guidelines and instructions adopted by competent authorities in relation to the technical implementing measures and the ability of competent authorities to audit the compliance with the notification obligation. This paragraph requires that providers keep an inventory of data breaches.

Only a few countries seem to have literally transposed this paragraph.[131] Some countries have transposed the article fully although they did not follow the exact wording of the ePD.[132] Quite a few countries such as Austria, Croatia, Cyprus, Germany, Poland, Romania and the UK did not transpose this paragraph at all while the Czech Republic, Denmark, Finland, Hungary and Sweden have transposed the article partially. The remaining Member States seem to have transposed this paragraph with a broader scope.[133]

Finally, Paragraph 5 of Article 4 provides that the Commission may adopt technical implementing measures following consultations with the European Network and Information Security Agency (ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, in order to ensure consistency.

The large majority of Member States did not transpose this paragraph at all, which can be attributed to the fact that this provision is addressed to the Commission rather than to Member States directly.[134] Nevertheless, Some Member States (Belgium, Denmark, Greece, Ireland, Lithuania, Spain, and UK) have transposed this paragraph more or less literally. The remaining Member States (France, Latvia, Luxembourg, and Slovenia) have transposed this paragraph with additional clarifications. For instance, the law in Luxembourg refers to criminal sanctions.

If we consider the transposition of Article 4 as a whole, it should be noted that the transposition has been largely achieved across Member States. There were no cases were found of a clear lack of transposition.

Some countries such as Portugal, Slovenia and the United Kingdom provide further details and requirements to those found in Article 4 of the ePD. For example in its local implementing act, Portugal required service providers of electronic communication services to establish internal procedures for responding to requests for accessing users' personal data. At the request of the DPAs,

[131] Belgium, Denmark, Greece, Ireland, Spain, and Luxembourg.
[132] Bulgaria, Lithuania, Malta, Netherlands, and Portugal.
[133] Estonia, France, Italy, Latvia, Slovakia, and Slovenia.
[134] Austria, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Germany, Hungary, Italy, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, and Sweden.

providers of electronic communication services are due to provide information related to the procedures, number of requests, legal grounds of the request and the answers provided.

In general, the majority of Member States did not transpose this article in a literal manner.[135] Some minor local differences and specificities were identified during the transposition check. For instance, Austria refers to "risk of breach of confidentiality" (Sec. 95 Para 2 of the Austrian Federal Telecommunication Act 2003, or "TKG") instead of "risk of breach of the security of the network" as Article 4 of the ePD. According to Article 4(3) of the ePD, the data subjects affected by the data breach may not be informed about the occurrence of certain technological protection measures have been implemented that "render the data unintelligible". The Austrian act requires instead that "the technological protection measures (...) ensure that the data is not accessible to any person who is not authorized to use it" (Sec 95a Para 2 TKG).

The Luxembourgish law also differs from the Directive on several points. It does not refer to the "state of the art and the cost of the implementation of the measures" nor does it refer to a "level of security appropriate to the risk presented" as the ePD does. Nevertheless, it requires that in the event of breach or risk of a breach, service providers and operators to take appropriate remedial measures at their sole expense. In the event of imminent risk of a breach, the Luxembourgish law limits the obligation of notification to "breach of the security of the network or services which may compromise the confidentiality of communications" and it does not condition the information on possible remedies to the risk lying outside the scope of the measures to be taken by the service provider. Regarding the powers of the CNPD, Luxembourgish law refers to a specific fines that could be imposed in case of non-compliance with the breach notification obligation. Concretely, it refers to fines that could go up to 50 000 euros. In the same vein, it foresees criminal sanctions for any persons contravening to the provisions of the Article including imprisonment and fine between 251 000 and 125 000 euros.

In Estonia for example, the law is more specific than the ePD as it specifies a definition for data breach, the information to be included in the notice, and the information to be included in the records of data breach.

Similarly, France's local act is more specific and detailed on the security requirements, and the audits carried out by the *Agence nationale de la sécurité des systèmes d'information* ("ANSSI"). However it appears that in France, market operators do not take measures to comply with Paragraph 2 of Article 4 on the obligation to inform the subscriber on security breaches risks.

In Lithuania, the Regulation on Security and Integrity of Public Communications Networks, Public Electronic Communications Services and Electronic Communication Hosting Services sets the requirement to adopt internal rules on security management. Additional requirements are established by the Communications Regulatory Authority.

In the Netherlands, the local legislation transposing the ePD contains specifications of the 'rules' National Authorities may adopt. Further specifications are available in the Dutch Personal Data Protection Act and Data Breach Notification Act. Moreover, the local legislation contains additional topics to be reported with regard to data breach inventory. In the Netherlands organizations need to report a breach within 72 hours after discovery, which means that they may not be able to implement recovery measures before the notification, reporting the intended measures instead.

[135][135] Such is the case of Austria, Bulgaria, Cyprus, Czech Republic, Estonia, France, Hungary, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Slovakia, and Sweden.

Latvian law additionally mentions in the Regulation No. 627 of Cabinet of Ministers Article that at least once a year a company must provide a training for the responsible persons in the field of data protection and IT security and provide personal data breach risk analysis. The electronic communications provider shall establish an internal procedure ensuring personal data breach investigation and prevention. In addition the internal procedures shall include the (i) processing of personal data risk analysis; (ii) measures to be taken after the personal data breach detection; (iii) the personal data breach investigation and management procedures. Moreover, Latvian act specifies that the domain holder shall ensure that it conducts IT-security audit and submits a report from certified IT-auditor once a year to the Regulator which is based on special Regulations of Cabinet of Ministers No 366 from 1 July 2014.

With regard to guidelines and recommendations in this area, it appears that the competent national authorities of some Member States are more active than others. For example, Poland does appear to not have specific guidelines on the implementation of security measures. By contrast, Denmark's DPA has issued guidelines on the reporting of data breaches while Portugal and Italy have issued recommendations on the security measures to be adapted. The *Commission nationale pour la protection des données* ("CNPD") of Luxembourg has issued an opinion in favour of specific measures regarding storage.

In Lithuania, the State Data Protection Inspectorate has provided recommendations on security of public electronic communications services and networks. The State Data Protection Inspectorate is entitled to audit security of personal data privacy and validity of personal data processing. Audits are carried out in case of received complaint or as a preventive measure. Further, the State Data Protection Inspectorate is entitled to examine confidentiality of communications according to the Regulation on Communications Confidentiality Audit. However, despite the fact that the implementing regulation on audit is established, according to the findings of the State Control Institution, the State Data protection Inspectorate does not adequately apply risk assessment and management systems while organising and arranging supervision. Preventative investigations and prior checks mostly are conducted in written, bureaucratic form with no clear view how the data should be registered and processed further, also a few transitional stages are needed, the lack of technical opportunities for data controllers to declare compliance with relevant requirements. One of the problems that arise in practice related to the audits, is that the Inspectorate doesn't receive data (as a package) due to the lack of automatic management and protection of private data in public sector. The relevant data is collected for different purposes by various institutions, and is not on consolidated basis. Also the monitoring processes and measures are not harmonized.

In Latvia, there are guidelines on the security of personal data developed by the Data State Inspectorate which is Latvian data privacy authority. However, the main security function of the electronic communication is provided by a special institution "Information Technology Security Incident Response Institution of the Republic of Latvia" ("CERT.LV"). CERT.LV has issued various guidelines, recommendations and action-models for state authorities, but also individuals and electronic services merchants which are made in accordance with Regulations of Cabinet of Ministers No 327 from 26 April 2011 "Regarding the Information to be Included in the Action Plan of a Merchant of Electronic Communications, the Control of the Implementation of Such Plan and the Procedures, by which End Users shall be Temporarily Disconnected from the Electronic Communications Network".

With respect to the rights of the competent authority for enforcement, Czech law (Section 88(7) of the ICA) authorizes the Czech Office for Personal Data Protection to issue an act of secondary legislation for the purposes set forth by Article 4(4) of the Directive. Even though the Czech Office for Personal Data Protection has not yet issued such act of secondary legislation (and such act is not even being prepared yet to our knowledge), this empowerment goes beyond Article 4(4) of the Directive, which presupposes an issuance of guidelines by the competent authority. Unlike such guidelines, the act of secondary legislation would be legally binding.

Regarding the enforcement of these provisions, we have received information from Greece over a couple of causes related to data breaches related to the lack of consent or spam[136]. In Slovenia, we have been informed of a decision of the Higher Court of Ljubljana on operators' due diligence to inform subscribers of possible security risks[137]. In conclusion, Article 4 was transposed by all Member States with no appreciable deviations except for Paragraph 5 which, in most cases, was not transposed due to the fact that that it relates to the European Commission. Even if a number of Member States elected to enact additional security requirements, the dual aim of the ePD does not seem to be hindered by these national specificities.

4.3.3 Users Rights and Exceptions (Articles 7-8, 10-12)

Article 7 – Itemised billing

Article 7 of the ePD imposes the obligation for Member States to incorporate in their national legislation the right for subscribers to receive non-itemised bills. Moreover, this provision allows Member States to apply national measures to reconcile this right with the right to privacy of calling users and called subscribers.

The majority of Member States have fully transposed this article, laying down the right to receive non-itemised bills and the right to receive itemised bills. A few countries such as Spain, Portugal, Ireland and Cyprus have transposed this article more or less literally. It appears that four countries did not transpose this article (Belgium, Croatia, Denmark and Slovakia).

In most cases, Member States ventured beyond a literal transposition to provide additional details regarding the implementation of this right. In some countries, the default rule is to receive itemised bills, with non-itemised bills being provided only at request. In other Member States, the default rule is to provide bills which implement a method for protecting the identification of the phone numbers on the bill.

Examples of countries where, by default, the service provider shall provide bills that are non-itemised or where the some of the phone digits are hidden are Germany, Italy, Romania, and Finland. In these countries itemised bills can be provided at request.

In Germany, itemised bills are to be issued only if the subscriber demands such billing prior to the respective accounting period in textual form, whereby partial anonymization of dialled telephone numbers may be requested as well. A brief survey on the major telecommunications providers in Germany confirmed that itemised billing is subject to a prior and explicit request of the customer.

[136] 86/2013 Committee (Hellenic Data Protection Authority) (618799) - Personal data breach without subscriber's consent.
91/2013 Committee (Hellenic Data Protection Authority) (618798) - Personal data breach used for spam purposes.
3513/2010 Administrative Court of First Instance (614552) - Personal data usage without subscriber's consent.
[137] Judgements no. II Cp 584/2011 of 24 Aug. 2011 and no. II Cp 2995/2009 of 24 June 2010

Such requests may be in most cases transmitted via the concerned provider's online platform. Germany has also implemented special requirements for the issuing of itemised bills for telephone lines assigned for whole households, companies and public authorities. However, these provisions do not account for service providers that serve closed groups of communications participants, if and as far as such services are solely provided to these groups. Moreover, itemised bills must not disclose communications connections to persons and legal entities that are listed by the German Federal Network Agency in their capacity to provide callers with pastoral care, assistance in cases of social emergencies and similar cases, and where it can normally be expected that the respective caller wants to remain anonymous.

In Italy, the default legal requirement is that the final three digits of the phone number must be omitted from the bill. Similarly, in Finland, the telecommunications operator, upon request by the subscriber, shall provide the bill in a form where the last three digits of the phone number are obscured or the itemisation is otherwise presented in such a way that the other party of the communication cannot be identified.

Some national laws such as the one of Czech Republic do not refer expressly to non-itemised billing but require the implementation of methods allowing to achieve increased data protection, such as excluding a certain number of digits. Other legislations such as the one of Latvia, Poland and Slovenia set a taxonomy between two levels of itemisation: "basic" and "detailed". In these countries, the default rule is to provide bills itemised at a "basic level". "Detailed" itemisation can be provided at request.

Slovenia and Lithuania specify in their laws that only the minimum necessary information should be provided on the bill allowing to subscribers to control their costs.

Slovenia, Hungary and Luxembourg provide in their laws that free-of-charge calls should not be presented in the bill.

Lastly, many of the Member States such as Austria, Italy, Finland, Slovenia, include in their legislation that these services shall be provided free-of-charge. We have been informed of a decision in Slovenia related to the destruction of itemised billing[138].

In sum, notwithstanding the lack of transposition by the Member States identified above, it appears that the first paragraph of Article 7 was carried over to national legislation in such a way as to ensure equivalent rights across Member States. However, there are major differences in the way that Member States reconcile this right with the right to privacy of calling users and called subscribers. In some cases, Member States have used the discretionary margin provided by the second part of this provision to establish opposing default requirements.

Article 8 – Calling and connected line identification

Article 8 of the ePD sets out the following requirements:

- The possibility for users to prevent the presentation of the calling line on per-call basis;
- The possibility for users to prevent the presentation of incoming calls;
- The possibility to reject incoming calls where the calling line identification is prevented;

[138] IC Decision no. 0612-19/2008 of 27 Feb. 2008

- The possibility for users to prevent the presentation of the connected line identification to the calling user;
- The application of all of the above to third countries.

It appears that this article has been transposed in all the Member States except in Malta. For a large majority of Member States, the transposition of these provisions was literal to a certain extent.[139] Ireland added that service providers shall provide this option free of charge.

Some Member States such as Bulgaria, Finland, Poland, and Lithuania accurately reflect the rationale of this article in their laws, but remain silent on whether this requirement applies to third countries.

In Germany for instance, the taxonomy of Article 8 was slightly altered. Namely, Section 102 TKG does not differentiate between the rights of users and subscribers rights. Instead, both calling and receiving parties must be allowed to prevent the presentation of the calling line identification by simple and free of charge means, both on a per-call and per-line basis. A peculiarity contained in the German transposition of Article 8 lies in the prohibition of preventing calling line identification if the calling party engages in telephone calls for the purpose of advertising. Again, these provisions do not account for service providers that serve closed groups of communications participants, if and as far as such services are solely provided to these groups.

Some countries, such as Estonia and Finland have added in their national legislation that some of these options will be implemented where “technically feasible”. In Hungary for instance, Article 8 is transposed by lower level national legislation setting out rules on the presentation of calling line identification.[140]

It is important to note that the scope of this article in almost all of the Member States appears to be limited to telephone operators. Only France and Austria appear to have a broader scope regarding this provision. In France, this requirement applies to all networks accessible to the public. In Austria, it applies to communications service operators which are defined as "*undertaking which exercises legal control over the functions in their entirety that are needed to provide the respective communications service and which offers the service to others*”.

Without prejudice to these specificities, it can be concluded that the transposition of this article was carried out in a satisfactory manner across all Member States, ensuring the harmonisation of rules in this area.

Article 10 – Exceptions

Article 10 of the ePD provides for admissible exceptions to the rights set out in Article 8 on the presentation and restriction of calling and connected line identification. Namely, Article 10 allows to Member States to override these rights in the case of emergency calls or while tracing malicious or nuisance calls. These limitations must be implemented via transparent procedures and on a temporary basis.

[139] Such is the case of Austria, Belgium, Croatia, Cyprus, Czech Republic, Denmark, Greece, Ireland, Italy, Latvia, Luxembourg, Netherlands, Portugal, Romania, Slovenia, Spain, and Sweden.
[140] Regulation No. 3/2011. (IX. 26.) of the National Media and Electronic Communications Authority on the Planned Division of Electronic Communication System Identifiers.

The large majority of Member States fully transposed this article, adopting the literal phrasing of the ePD.[141] Some countries such as Latvia, Luxembourg, Poland and Slovenia transpose this article throughout several provisions. However, most Member States provide further details on the situations and conditions under which such limitations may take place. For example Bulgaria added that the rights stated in Article 8 of the ePD may be overridden in the case of calls to services responsible for security, defence and internal order.

Similarly, Finland specifies that limitations apply when complying with the right of the police to access information under separate provisions and that the information shall be only disclosed to authorities that by law have a right to dispose of such information.

In the same vein, Romanian law adds a third paragraph, which states that "*the exceptions referred to in paragraphs (1) and (2) shall be permitted under the conditions set out by the Ombudsman, with consultation of ANRC*". However, pursuant to a brief informal consultation with the National Authority for Management and Regulation in Communications (ANCOM) on this topic, it appears that no specific conditions have hitherto been adopted by the Romanian Ombudsman with respect to these exceptions.

The Netherlands, on the other hand, specifies that in case of malicious calls) the subscriber can request the number of the network determination point that is calling, name, address, postcode and town/city of the malicious caller. In addition to this, the provider has an obligation to conduct a research after such a request and determine whether the details should be provided. Regarding emergency calls, the law further defines the data that can be stored/recorded and made available in case of emergency calls or in order to combating the abuse of a public emergency number. The maximum period during which numbers and data can be retained is two months of incoming calls, including the date and time for emergency calls public services.

Slovakian legislation also provides further specifications such as detailed specification of the data with regard to emergency calls (telephone number, name, surname, permanent residence etc.). Slovakian legislation also stipulates that in case of a call from a mobile network with an unavailable number, the international mobile equipment number (IMEI) should be provided.

In Portugal, in case of "*calls that upset the peace of the family or the intimacy of private life*", the displaying of the identification of the calling line is conditional upon an opinion by the Portuguese DPA. In addition, this cancellation can only last for 30 days. The Portuguese law also adds an information duty regarding data holders (article 10, § 4) and in which manner (§ 5) this information duty should be performed.

Two Member States (Austria and Hungary) appear to have transposed this article only where emergency calls are concerned, leaving out the exception related to the handling of nuisance calls.

Only Malta and Germany appear not to have transposed this article. Section 102 TKG deals with the issue of calling line identification, but it does not provide for an explicit obligation of providers to inform about the exceptions under Article 10 of the ePD. According to Section 45n Paras. 1, 2 No. 3, 3 No. 7 lit. f) the competent authorities are entitled to issue a legislative decree dealing with the informational duties of telecommunications providers concerning *inter alia* calling line identification. The Federal Network Agency issued a first draft for a respective legislative decree in 2013. However, this draft has

[141] This includes Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Portugal, Poland, Romania, Spain, Sweden, Slovakia, and Slovenia.

not entered into force yet. It should be noted in any case that the draft does not lay down an obligation to inform the subscriber of the exemptions enabled by Article 10 of the Directive. Having said that, according to a brief survey, the major telecommunications providers in Germany seem to voluntarily comply with the requirements set out in Article 10.

From an enforcement perspective, in Greece for example, it was reported that regarding the malicious or nuisance calls, exist specific detailed procedures to be followed in order to secure the transparency. These procedures may be found in the guidance issued by the Hellenic Authority for the Information and Communication Security and Privacy (A.D.A.E.)[142].Regarding emergency calls to the competent public organisations dealing with such calls or to private emergency assistance organisations, recognised by the State, the A.D.A.E. has equally issued specific procedures[143], to be followed outlining all other technical details pertaining to the implementation of the present provision as described in an act.

In sum, the transposition of this provision was carried out across all Member States in such a way as to provide a harmonised background. Due to the sensitive nature of the subject-matter and the need to adopt specific procedures for dealing with emergency situations and nuisance calls, it is not surprising to see a variety of national approaches, with different degrees of detail and granularity. However, these differences are do not constitute material obstacles to the objectives of the ePD.

Article 11 – Automatic call forwarding

Article 11 of the ePD requires Member States to introduce in their local laws the right for subscribers to be able to stop automatic calls forwarded by a third party. This right should be provided by using simple means and free of charge.

The big majority of the Member States[144] have transposed more or less literally this article. Others such as Poland and Spain did not transpose literally the article. However, they have fully transposed the requirements stemming from article 11 into their national law and no material differences have been observed. As an example of how this right is implemented into practice, in Austria, in order to stop the automatic call forwarding, subscribers need to send a specific code to the operator, which will restrict the automatic call forwarding. In Czech Republic, service providers implement this right differently. The telecom operators offer an ex post cancellation of an automatic call forward based on the request of the respective subscriber. However, there are reasons to believe that the issue arises at the moment when a third party establishes an automatic call forward to a subscriber's terminal as the respective subscriber is not notified or in any other way informed about the establishment of the automatic call forward to the subscriber's terminal and no consent of such subscriber is required. While answering the forwarded call, the subscriber is not notified about the fact that the call is being forwarded to the subscriber's terminal from a third party's line. Therefore, it may be difficult in some cases for the subscriber to identify the information needed for requesting the cancellation of the automatic call forwarding. In such cases, the compliance of the providers with Article 11 of the Directive is disputable.

[142] ADAE, issue no. 1853, 21/12/2006
http://www.adae.gr/fileadmin/docs/nomoi/fek%20kakovoules.pdf, which amended by act with issue no. 2359, 20/11/2009, http://www.adae.gr/fileadmin/docs/nomoi/prakseis/FEK_2359-B-20.11.2009.pdf
[143] ADAE; issue no. 1898, 17/09/2008
http://www.adae.gr/fileadmin/docs/nomoi/FEK1898.2008.pdf
[144] These include Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Ireland, Italy, Latvia, Portugal, Romania, Slovakia, Slovenia, and Sweden.

Some countries provide additional provisions. For instance, Austria and Belgium provide that operators involved in automatic call forwarding need to cooperate. Ireland adds as well an obligation for undertakings to inform its subscribers on the scope of this right.

Estonia narrows the scope of this right and provides in its implementing act that this right shall be implemented where "*technically feasible*".

In Germany, this obligation does not apply to service providers that serve closed groups of communications participants, if and as far as such services are solely provided to these groups.

Netherlands, submits the exercise of this right on the request of the user.

Only Hungary appears not to have transposed this provision.

Overall, it can be concluded that Article 11 of the ePD was satisfactorily transposed across Member States, ensuring an equivalent level of protection to users.

Article 12 – Directories of subscribers

Due to the length of this article, the transposition check has been performed paragraph per paragraph.

Paragraph 1 has been transposed literally by the large majority of Member States.[145] Even in those cases where Member States did not adopt a literal transposition, no material differences have been observed.[146]

For example, Cyprus has transposed the first part of this paragraph literally, adding however that personal data may only be stored in directories limited to what is necessary to identify a particular subscriber, unless the subscriber has unambiguously consented to the publication of additional personal data.

With regard to paragraph 2 of this article, the same countries that transposed literally the first paragraph have also transposed the second paragraph in a similar manner. For those who deviated from the phrasing of the ePD, no material differences could be found. Only Germany appears not to have transposed this paragraph entirely.

Paragraph 3 has also been transposed literally by most of the Member States. However, Austria did not opt for the possibility to ask for additional consent. A strict purpose restriction clause applies in this respect. Contrary to the first two paragraphs of this article, some countries did not transpose this paragraph at all (Belgium, Estonia, Finland, Luxembourg, Sweden and UK).

Regarding paragraph 4, the large majority of the Member States[147] did not transpose it at all as the national law applies to legal and natural persons.

In sum, it would seem that this article has been adequately transposed across almost all Member States as far as the rights of subscribers are concerned.

[145] These include Bulgaria, Croatia, Czech Republic, Estonia, Finland, Greece, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Portugal, Romania, Slovakia, Slovenia,Sweden, UK.
[146] Such is the case of Austria, Belgium, Cyprus, France, Hungary, Ireland, Italy, Poland, and Spain.
[147] Austria, Bulgaria, Cyprus, Czech Republic, Estonia, France, Greece, Ireland, Italy, Lithuania, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, UK

4.3.4 Conclusions on the transposition check per article

Based on the information obtained in the course of the transposition check and the individual conclusions expounded above, we can present the following findings:

- Article 1 – Scope and Aim

Although, this article was transposed in the majority of the Member States, its transposition varies largely from one Member State to another. This is due to the fact that, on the one hand, some Member States have transposed the ePD provisions as part of their wider national framework regulating the electronic communications sector which goes beyond the sole aim of protecting personal data in the electronic communications sector. On the other hand, part of the Member States have transposed the ePD provisions in a single legislative act dedicated to the ePD and in these cases, the transposition of this article is more or less literal. Finally, other Member States transposed various ePD provisions across different national legislations. Nonetheless, the varying transposition across Member States of this particular article should not be perceived as an obstacle for achieving the objectives pursued by the ePD as the nature of this article is rather programmatic while the actual achievement of the ePD objectives depends on the transposition of the provisions laying down rights and obligations.

- Article 2 – Definitions

This article was completely transposed in the big majority of the Member States and no specific deviations have been observed from the rationale and text of the ePD. In some cases, Member States have included additional definitions in their national law. The importance of this article is crucial as it determines to a large extent the scope of the law. The fact that Member States have faithfully reflected the provisions of this article in their national laws indicates that the scope of the ePD has been respected.

- Article 3 – Services Concerned

The transposition check showed that more than half of the Member States transposed this article in its entirety, while others transposed it partially. Based solely on the transposition of this article, it appears that the letter and rationale of the ePD has been respected and coherently reflected. However, looking at the enforcement practices, it appears that there are some important differences in the way this provision is interpreted and applied. In fact, some Member States apply a broad interpretation of this provision and include under its scope OTTs and private networks. Therefore, despite the overall accurate and complete transposition of this provision, the disparity in the enforcement practices creates asymmetric conditions and legal uncertainty in the EU single market. This can be seen as an indicator that this article is not any more in line with the technological developments.

- Article 4 – Security of Processing

The majority of the Member States have completely transposed the first four paragraphs of this article and no specific deviations have been observed other than in some cases the national law is more detailed than the ePD. On the contrary, paragraph 5 of this article was not transposed in its majority which can be attributed to the fact that this provision is addressed to the Commission rather than to Member States directly. It should be concluded that the transposition by the Member State was successful in implementing the minimum standard for the secure processing of personal data in the electronic communications sector as prescribed by the ePD. Based solely on the transposition check, it could be assumed that this article is still relevant. However, during the interviews with stakeholders,

many raised concern over the coherence between this article and the GDPR. For instance, both the ePD and the GDPR impose a breach notification obligation and many believe that such dual regime is likely to create legal uncertainty. For more information on the results of the interviews, please refer to section 2.4.

- Article 7 – Itemised billing

In the majority of cases, this article has been fully transposed. The purpose of this article is to ensure the right of users to receive non-itemised bills in view of protecting their privacy. In this light, it should be concluded that this objective has been successfully achieved through the transposition notwithstanding the fact that some Member States subject this right to the request of the user, whereas in other Member States, receiving non-itemised bills is the default rule.

- Article 8 Calling and connected line identification

This article has been completely transposed and no specific deviations have been observed which means that allegedly no specific issues can be reported in relation to this article. However, during the interviews with stakeholders, many described the provisions of this article as obsolete and unnecessary.

- Article 10 – Exceptions
- In sum, the transposition of this provision was carried out across all Member States in such a way as to provide a harmonised background. Due to the sensitive nature of the subject-matter and the need to adopt specific procedures for dealing with emergency situations and nuisance calls, it is not surprising to see a variety of national approaches, with different degrees of detail and granularity. However, these differences are do not constitute material obstacles to the objectives of the ePD.Article 11 – Automatic call forwarding

Overall, it can be concluded that Article 11 of the ePD was satisfactorily transposed across Member States, ensuring an equivalent level of protection to users. There are no specific issues to be reported in relation to this provision.

- Article 12 – Directories of subscribers

This article has been completely transposed across almost all Member States as far as the rights of subscribers are concerned. However, the interviews with stakeholders revealed some reluctance as to the relevance of these provisions nowadays.

4.3.5 Conclusions on the overall transposition check

- Overall, Member States have relied on the formulation provided by the ePD, notwithstanding the many deviations that occur in terms of form, specific local requirements, and applicable procedures. Cases of semantic equivalence are very common across the various forms of transposition.
- With the exception of a number of areas such as itemised billing or the mechanisms for handling nuisance calls, the provisions of the ePD have been almost entirely transposed across Member States. Although national approaches vary considerably in terms of procedure and requirements, it is possible to discern a common level of protection of users and subscribers across all Member States, evidence that the ePD has been instrumental in providing a minimum, harmonised background.

- The question of whether OTT service providers and private networks are subject to the requirements of the ePD and the corresponding national implementing acts has not been uniformly addressed in the transposition of the ePD. Member States vary considerably in their approach to this topic. Therefore, the role and importance of case law and administrative decisions in each Member State therefore cannot be overstated.
- While no national implementing law explicitly refers to the inclusion of OTT services and private networks, a number of cases have arisen where administrative decisions, taking into account the functional equivalence between services traditionally covered by the ePD and these new forms of communication, ruled that the national law also applied to at least a part of these services. VoIP services seem to be particularly in scope in those Member States where this extensive interpretation was adopted. This represents a deviation in the transposition of the ePD, which was not originally intended to cover these types of services. In other Member States, we have found that there is a lively but ultimately inconclusive debate on whether such services should be covered by the ePD or the corresponding national acts.
- It is reasonable to conclude, based on this uneven transposition of the ePD, that the current situation obscures the level of legal certainty by obliging operators and users to consult secondary sources of law, some of which might not always be readily accessible or drafted with the principal concern of clarity. More importantly, the current *status quo* provides for appreciable differences in legal treatment across Member States, creating an uneven playing field for operators and a potential obstacle to the goals set out by the ePD.
- The ePD was transposed by means of a great variety of legal instruments. While some Member States adopted specific legal acts designed solely for the transposition, others incorporated the provisions of ePD in existing laws, and occasionally into their omnibus telecommunications regulations. While this still represents transposition, there were cases in which the specific references to the protection of privacy and confidentiality in the ePD did not immediately result from the implementing act.

5 Answers to the evaluation questions

In this chapter, we present our findings related to the second part of Task 1 – REFIT, the answers to the evaluation questions. The analysis is structured according to the Articles of the ePD and the evaluation criteria (effectiveness, efficiency, relevance, coherence and EU added value) to be examined.

5.1 Introduction

This section presents our findings for the purpose of the REFIT exercise.

The analyses provided in the following sub-sections are based on the following information sources:

- Desk research, including:
  - Literature;
  - Statistics;
  - Transposition check;
  - An analysis of the European Commission's public consultation[148];
  - The results of the Flash Eurobarometer 443 on e-Privacy;[149]
  - Other types of documents provided by the Commission, including the minutes of two workshops that were held by the Commission in spring 2016;[150]
- Legal analyses in relation to the coherence of the ePD with other instruments;
- An analysis of Deloitte's online surveys with businesses and competent authorities; and
- Inputs received based on interviews carried out.

As concerns the content of this chapter, it first provides an overview of the evaluation criteria and questions that form the basis for the analysis, followed by a high-level overview of our findings per topic and evaluation criterion. In the subsequent sections, we provide a more detailed article by article analysis of the **effectiveness, efficiency, relevance, coherence and EU added value of each of the provisions**. The sub-sections on the individual articles also contain a short description of the main aspects of the relevant article. The analysis related to some articles has been clustered due to their close interlinkages.

[148] See: https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive. Our analyses focuses on key closed questions dealing with the evaluation of the current legal framework. The aspects relating to potential future changes (policy options) have only been taken into account to a limited extent.
[149] Survey requested by the European Commission, Directorate-General for Directorate General Digital Single Market and coordinated by the Directorate-General for Communication, carried out by TNS Political & Social. For this report we used the preliminary raw data.
[150] One of the workshops involved national competent authorities for the ePD, while the other workshop gathered various stakeholders from the industry, civil society and consumer associations.

With regard to the assessment of the **effectiveness** of the ePD, most of the articles can be related directly to the *operational objectives* identified, as indicated in the following table.

Table 11 – Links between operational objectives and the different articles

Operational objectives of the ePD	Relevant articles
To ensure the security of services	Article 4
To ensure the confidentiality of communications as well as the related traffic data and other location data	Articles 5(1) and (2), 6 and 9
To ensure the confidentiality of information stored on the user's terminal equipment	Article 5(3)
To ensure that subscribers and users have a possibility to opt for non-itemised billing	Article 7
To ensure that called and calling subscribers/users have possibilities for control over call line identification	Articles 8 and 10
To ensure that subscribers have the right to stop automatic call forwarding	Article 11
To ensure that have the right to be informed and decide about an inclusion in publicly available or printed databases of subscribers	Article 12
To protect citizens/consumers and legal persons against unsolicited communications	Article 13
To avoid mandatory requirements for specific technical features that would hinder the development and free circulation of equipment/services in the internal market	Article 14
Horizontal aspect: To ensure the effective enforcement of the ePD	Article 15a

Source: Deloitte

In the following article-by-article analysis of the effectiveness of the ePD, reference is made to the relevant *operational* objectives. The overall analysis related to the *specific* and *general objectives* has been carried out horizontally, across the articles (based on the detailed analysis for the different articles / operational objectives; see chapter 5.15). However, Articles 1-3 relating to the scope have a more horizontal reach. Therefore, we rather considered the specific objectives in the section dealing with the scope.

5.2 Evaluation questions

As indicated above, and in line with the ToR and the *Better Regulation Guidelines*, our analysis covers the following five evaluation criteria:

- Effectiveness;
- Efficiency;
- Relevance;
- Coherence; and
- EU added value.

Table 12 outlines our understanding of the evaluation criteria in the context of this study.

Table 12 – Our understanding of the evaluation criteria

Evaluation criterion	Discussion

Evaluation criterion	Discussion
Effectiveness	Under effectiveness, we assess the extent to which the ePD has reached or progressed towards its general, specific and operational objectives, in particular its confidentiality and internal market objectives. This includes determining the progress made and the extent to which the Directive may have fallen short of achieving its objectives. In this context, we take into account all the different provisions established in the Directive, including rules on confidentiality and security or the rights of subscribers in relation to unsolicited communications. Our understanding of the objectives to be achieved is presented in the draft intervention logic (see section 3.3.2). In addition, factors that contribute to success or failure and why/whether/how these are linked to the ePD, as well as any unexpected or unintended effects are identified.[151] In order to assess the effectiveness of the ePD, we take into account indicators at the level of the outputs (transposition in the Member States), results and impacts. We note here that it is usually challenging to establish a **cause-effect relationship** between an intervention and potential broader impacts. In line with the *Better Regulation Guidelines* (p. 55), we aim to investigate cause-effect relationships with the help of qualitative reasoned arguments. Our methodological approach, which is based on cross-referencing various sources of data and involving various stakeholders, facilitates this process.
Efficiency	In general terms, efficiency considers the relationship between the resources used by an intervention and the changes generated by it in terms of the achievement of the objectives.[152] Under the efficiency criterion, we will e.g. analyse the costs and benefits associated with the provisions of the ePD for the different stakeholders involved and in how far the costs are proportionate. It is in this context important to distinguish between different stakeholders, including the users of services, SMEs and public administrations, as they could face different costs and benefits.
Relevance	Under relevance, we will assess in how far the provisions of the ePD and the entire Directive have been and remain relevant for the needs in the EU. In line with the *Better Regulation Guidelines* (p. 58), this is done in separate steps: - *Identification of the needs* related to e-privacy; and - Assessment in how far the *objectives* correspond with the needs. Under the relevance criterion, we consider in particular changes in the market and technology as well as the connection to the GDPR, the RED, and the NIS Directive.
Coherence	In general terms, the assessment of coherence looks at the consistency of the ePD with other instruments ("externally") and between different provisions of the ePD ("internally")[153]. As concerns the internal coherence, we will analyse how well the different provisions of the ePD operate together to achieve the objectives of the Directive. In addition, we will analyse how well the ePD as a whole operates or is expected to operate with other legal instruments such as the regulatory framework for electronic communications networks and services (Electronic Communications Package).[154] The ePD is part of this package, which is subject to a larger evaluation and reform initiative.[155] Another relevant instrument to consider in this respect is the upcoming GDPR. This includes e.g. an analysis of overlaps, contradictions and synergies. Lastly, the ePD's coherence is assessed against the Directive on radio equipment and telecommunications terminal equipment, the RED and the NIS Directive.

[151] European Commission, Better Regulation Guidelines, 19 May 2015, SWD (2015) 111 final, p. 57, -(http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm).
[152] European Commission, Better Regulation Guidelines, 19 May 2015, SWD(2015) 111 final, p. 57, -(http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm).
[153] European Commission, Better Regulation Guidelines, 19 May 2015, SWD(2015) 111 final, p. 59, (http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm).
[154] Including (in addition to the ePD): Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services; Directive 2002/20/EC on the authorisation of electronic communications networks and services; Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities; Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services.
[155] See the REFIT Roadmap: Evaluation and Reform of the Regulatory Framework for electronic communications networks and services (REFIT), http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_007_evaluation__elec_communication_networks_en.pdf.

Evaluation criterion	Discussion
EU added value	The analysis of EU added value serves to establish whether the ePD brings an added value compared to what could have been achieved at national, regional or local level.[156] This is closely linked to the principle of subsidiarity that determines that the EU should only act if the intended results cannot be achieved at lower political level.[157] In order to analyse the EU added value, we will examine if the positive effects of the ePD could not have been achieved otherwise. In line with the *Better Regulation Toolbox*[158], we develop qualitative arguments, based on the input of experts, to provide analyses in relation to this evaluation criterion.

Source: Deloitte based on the European Commission's Better Regulation Guidelines

Table 13 specifies the evaluation questions that are answered as part of our analysis. Although – strictly speaking – the status quo is not an evaluation criterion, we have still indicated in the table the specific questions addressed as part of our study in this regard in line with the *Better Regulation Guidelines*.

The evaluation questions reflect the initial list of questions identified by the Commission (ToR, p. 9). In this regard, it can be noted that in the table below, we diverge from the formulation of questions in the ToR to some extent. More specifically, we have in some places formulated the questions more broadly. In these cases, the specific aspects raised in the questions in the ToR are still be covered as part of our analysis. In some cases, we consider them as judgement criteria and/or indicators. The questions contained in the ToR have been complemented by a limited number of additional questions from the *Better Regulation Guidelines*.

Further information regarding judgment criteria, the operationalisation (incl. qualitative and quantitative indicators) of the criteria, as well as relevant information sources is provided in our Analytical Framework (see Annex).

Table 13 – Evaluation questions (incl. status quo)

Evaluation criterion	Specific questions
Status quo	• What is the origin of the ePD, i.e. what problems did it set out to address? How did the problem evolve over time?[159]
	• What is the status with regard to the transposition?[160]
	• What is the current situation for different stakeholders? How are they affected by the intervention, including its different elements?[161]
Effectiveness	• To what extent have the operational objectives of the ePD been achieved?
	• To what extent have the specific objectives of the ePD been achieved?
	• To what extent have the general objectives of the ePD been achieved?
	• To what extent can the progressing towards the objectives be credited to the ePD? To what extent did external factors influence the achievements?

[156] Ibid. p. 60.
[157] Article 5(3) TEU.
[158] European Commission, Better Regulation "Toolbox", complementing the Better Regulation Guidelines presented in SWD (2015) 111, p. 275 (http://ec.europa.eu/smart-regulation/guidelines/docs/br_toolbox_en.pdf).
[159] Initial analysis concerning the origin of the ePD is provided in the context section.
[160] See chapter 4.
[161] An initial analysis is provided as part of the assessment of effectiveness of the different articles.

Evaluation criterion	Specific questions
	• Where expectations have not been met, what obstacles hindered their achievement?
Efficiency	• To what extent has the intervention been cost-effective?
	• To what extent have the costs of each provision of the ePD and of the ePD as a whole been justified and proportionate, given the benefits that were achieved?
	• Could the objectives be achieved at a lower cost?
	• What factors influenced the efficiency of the current rules?
Relevance	• Is there still a need for the specific rules contained in the ePD?[162]
	• Are the Articles of the ePD still relevant today?[163]
	• To what extent are the original objectives of the ePD still in line with the needs at the EU level?
Coherence	• To what extent is the intervention coherent internally?
	• To what extent is this intervention coherent with other interventions which have similar objectives?
	• To what extent is the intervention coherent with wider EU policy?
EU added value	• Is there still added value for EU intervention, compared to what is done at national or regional level in the fields covered by the ePD?

Source: Deloitte

The following section provides an overview of the trends and findings regarding the achievement of each evaluation criterion per Article. More detailed findings are presented as of section 5.4.

5.3 Overview of findings

In this section, we provide an overview table regarding the achievement of the evaluation criteria in relation to each Article. The assessment is based on the information available and accessible based on the tasks implemented.

We have used a colour coding for this table that indicates identified trends regarding the extent to which an evaluation criterion seems to be achieved based on the information available:

- Achieved / tends to be achieved;
- Partially achieved or not achieved; and
- Insufficient information to assess or criterion not relevant.

Table 14 – Findings / trends regarding the achievement of the evaluation criteria

Topic	Effectiveness	Efficiency	Relevance	Coherence	EU added value
Scope of application and definitions (Article 1, 2 and 3)					
Security of processing (Article 4)					
Security of communications (Article 5.1 and 5.2)					
Confidentiality of information					

[162] Given that the new GDPR already updates and modernises the EU data protection framework to guarantee privacy rights in the digital age.
[163] In light of the changed market, technological and regulatory landscape.

Topic	Effectiveness	Efficiency	Relevance	Coherence	EU added value
stored on users' terminal equipment (Article 5.3)					
Traffic data and other location data (Article 6 and 9)					
Itemised billing (Article 7)					
Presentation and restriction of calling and connected line identification (Articles 8 and 10)					
Automatic call forwarding (Article 11)					
Directories of subscribers (Article 12)					
Unsolicited communications (Article 13)					
Development and free circulation of electronic communication equipment and services (Article 14)					
Implementation and enforcement (Article 15a)					

Source: Deloitte.

More detailed findings (i.e. the basis for this overview table) can be found as of section 5.4.

5.4 Scope of application and definitions (Articles 1, 2 and 3)

The ePD establishes specific rules concerning **privacy in the electronic communication sector**.

Overview of the scope and definitions

Based on Article 1, the ePD applies to **electronic communications services**.

This term deserves some further clarification and needs to be distinguished from information society services, as both types of services are regulated by a complex net of different legal regimes.

The scope of the rules set out in the ePD is limited to services that qualify as an 'electronic communications service', which are defined in the 2002 Framework Directive on a common regulatory framework for electronic communications networks and services (the "Framework Directive") as a *"service normally provided for remuneration which consist wholly or mainly in the conveyance of signals on electronic communications networks (…)"*[164]. Typically, this concerns telephone and internet contracts. In contrast, information society services, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks, are not included in the scope of the ePD.[165]

Furthermore, the ePD only applies to *publicly available* electronic communications services in public communications networks (Article 3). This means that closed user groups and corporate networks are not covered by the ePD. In these cases, the Personal Data Protection Directive (or GDPR in the future) is likely to apply, though only where personal data is concerned.

[164] Article 2.c of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).
[165] As defined in Article 1 of Directive 98/34/EC.

In Article 2, the ePD provides definitions for the following terms:

- User[166];
- Traffic data;
- Location data;
- Communication;
- Consent;
- Value added service;
- Electronic mail; and
- Personal data breach.

5.4.1 Effectiveness

Key finding of the analysis: Not fully effective

Under this criterion, the extent to which the provisions have allowed the ePD to reach its policy objectives is examined. In this context, we consider the specific objectives of the ePD, namely:[167]

- To ensure that the right to privacy and confidentiality with respect to the processing of personal data in the electronic communications sector is respected;
- To ensure the free movement of personal data in the internal market; and
- To ensure the free movement of electronic communication terminal equipment and services in the EU.

The main finding of this analysis is that the **scope** of the ePD is **not fully effective,** as a number of challenges hindering the achievement of the objectives have been identified. In particular, it was found that the scope is no longer appropriate in light of the technological and market developments, notably because online communication services are not covered. This is, for example, reflected in the responses of competent authorities to Deloitte's online survey, which show that authorities are more supportive of the appropriateness of the scope in the past than in the future.[168] In addition, there are ambiguities in relation to the scope, e.g. in relation to the types of networks covered. Closely related, the **definitions** are not fully appropriate either.

In this section we discuss the following aspects separately:

- The scope based on Articles 1 and 3; and
- Definitions.

[166] The term **subscriber** is, in contrast to "user", not defined in the ePD. Instead, the definition of subscriber contained in the Framework Directive is applicable, according to which a subscriber is "**any natural person or legal entity who or which is party to a contract** with the provider of publicly available electronic communications services for the supply of such services", Article 2(k) Framework Directive.
[167] These are reflected in our intervention logic presented in section 3.3.2.
[168] Indeed, more than half of the respondents (21 out of 30) agreed or strongly agreed that the current scope has ensured that the ePD has made a significant positive impact with regard to the protection of privacy in the electronic communications sector in the past.. The level of agreement is slightly lower when it comes to the capability of the scope to deal with current and prospective challenges. Further details can be found in Annex C.

Scope based on Articles 1 and 3

The analysis of the effectiveness of the scope of the ePD has been structured around the following themes:

- The types of services covered;
- The types of data covered; and
- The types of users/subscribers covered.

As indicated in the text box at the start of this section, the **types of services** covered by the ePD based on Articles 1 and 3 include public or publicly available electronic communication services. However, there are certain provisions that have an atypical scope. The following table presents the scope of the different provisions, giving examples of specific types of services based on the definitions of the ePD.[169]

Table 15 – Initial overview of the scope in relation to the types of services covered per provision

Provisions of the ePD	Explanation
Articles with a typical scope	
Security of processing (Article 4)	- These provisions follow the scope as defined in Articles 1 and 3 of the ePD and thus apply to **public or publicly available electronic communications services**. - Examples of **included services**: o Internet providers o Telephone providers - Examples of **excluded services**: o Private networks and services (such as purely corporate networks) o OTT services, including communications (WhatsApp, Skype, Facetime), providers of online television and video services (Netflix, YouTube, Google play), other applications (social networks, online baking, e-Health). One notable exception are VoIP services offering fixed inbound and outbound phone numbers for users, which are therefore regarded as ECS in the Universal Service Directive.[170] o Webmail providers o Advertising networks (e.g. online marketing company, providers of smart phone apps)
Traffic data and other location data (Article 6 and 9)	
Itemised billing (Article 7)	
Presentation and restriction of calling and connected line identification (Articles 8 and 10)	
Automatic call forwarding (Article 11)	
Directories of subscribers (Article 12)	
Articles with an atypical scope	
Security of communications (Article 5.1 and 5.2)	- There are different opinions on the scope of these provisions. According to the EDPS, the scope of this provision is broader than what is set out in Articles 1 and 3, covering not only public or publicly electronic communications services.[171] It may also be argued based on the wording of the article that it aims at protecting communications in general.[172]

[169] Some of these services may still be covered in some Member States, depending on the transposition (see chapter 4).
[170] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p. 80
[171] European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Proposal for a Directive on privacy and electronic communications', Brussels, (2008/C 181/01), 10 April 2008, par 33.
[172] Cf. Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 25.

Provisions of the ePD	Explanation
Confidentiality of information stored on users' terminal equipment (Article 5.3)	- This provision is broader in scope compared to what is set out in Article 1 and 3. It applies to anyone storing or accessing information (e.g. cookies) on a user's device.[173]
Unsolicited communications (Article 13)	- This provision is broader in scope compared to what is set out in Article 1 and 3. It applies to anyone potentially sending out spam using electronic communication services, including e.g. online shops.

Source: Deloitte

It has been pointed out that the scope of the ePD predominantly follows a "**service-centric approach**" as the scope is defined by the types of services covered, namely public or publicly available electronic communications services. This has one main **advantage**: it is rather straightforward for service providers to decide whether or not the ePD applies to them, as they only need to decide whether or not they offer a public or publicly available electronic communications services.[174]

Yet, several challenges relating to this definition of the scope have been identified, including that the scope may be too narrow and not entirely clear. These aspects are elaborated below.

Various stakeholders have criticised that the scope of the ePD in relation to the types of services covered in their view is **too narrow based on the definition of electronic communication services**, potentially hindering the achievement of the right to privacy and confidentiality with respect to the processing of personal data in the electronic communications sector.

The ePD only applies, for the most part, to **traditional telecommunication service providers**, i.e. those providers that are responsible for carrying signals over an electronic communications network.[175] As indicated in Table 15, most provisions do not apply to the delivery of audio, video, and other media over the Internet without the involvement of a multiple-system operator in the control or distribution of the content.

The term "over-the-top" is used to refer to these new services. While this term has no legal meaning, BEREC has defined an OTT service as a content, service, or application that is provided to the end user over the public Internet.[176] It has further divided OTTs into three categories:[177]

- OTT-0: an electronic communication service;
- OTT-1: a service that does not fall under the current definition of an electronic communication service but potentially competes with the latter;
- OTT-2: other information society services.

Examples of OTT services are provided in Table 15.

A lack of protection of substitutable services via the ePD might result in a **void of protection**.[178] From a user's perspective, this is difficult to understand since the service-centric approach of the ePD "can

[173] Cf. Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 27.
[174] Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 73.
[175] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15039), p. 5; European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, p. 4.
[176] BEREC Report on OTT services [2016], http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5751-berec-report-on-ott-services_0.pdf, p 14
[177] ibid, p. 4.

lead to – from a user perspective – arbitrary differences between protections for different but functionally equivalent services."[179] This is reflected in the replies to the Commission's public consultation: almost two thirds (58.3%) of all respondents indicated that the scope is currently too narrow, as OTTs are not covered.[180] Even more respondents from the group of citizens and civil society shared this opinion (76%). Similarly, in Deloitte's online survey and interviews, **competent authorities considered this to be the most serious problem in relation to the scope**: In the online survey, the fact that OTTs are currently not covered was considered a serious problem by 17 out of 30 authorities (56.7%) and a moderate problem by 8 authorities (26.7%).[181] Also the interviewed authorities agreed unanimously that the scope is too narrow in this respect.

As concerns the business perspective, the difference in treatment leads to an **uneven playing field,** as businesses providing similar services are covered by different legal regimes.[182] On this basis, the fact that OTTs are not covered by the ePD were in particular considered to be problematic by Telecom providers interviewed by Deloitte. It was argued that the legal treatment is currently not symmetrical vis-à-vis similar services. Most other types of businesses took a slightly different perspective. For example, an OTT provider argued that there are important differences between traditional Telecoms and OTT provider that justify a different treatment: they highlighted in this context that users are dependent on the services of traditional Telecom providers, whereas they can freely choose which OTT providers they want to use or not. Details on the competitive relationship between providers of OTTs and ECS are presented in the following text box.

Competitive Relationship between ECS and OTT service providers

Since OTT service providers are not themselves responsible for the conveyance of signals over an electronic communications network, they do not fall under the ePD and its obligations. On this basis, OTTs are subject to more general regulatory frameworks, including the European data and consumer protection framework, which do not include specific obligations relating to communication services.

In general, OTT services have broader opportunities to use user data, e.g. on traffic and location, apart from simply enabling communications.[183] Due to the obligations under Art. 6, 9 and 13 of the ePD, ECS are prevented from using certain assets to develop new business models in order to

[178] European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, p. 4; Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 2; Communication COM(2015) 192 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, p. 9 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

[179] Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 33. It was also pointed out that users may in some cases not even aware whether they use electronic communications services or other, e.g. VoIP, services.

[180] Respondents were asked: "Should the scope be broadened so that over-the-top service providers (so called "OTTs") offer the same level of protection when they provide communications services such as Voice over IP, instant messaging, emailing over social networks)." 58% of respondents agree with broadening the scope to OTTs. In addition 10% of respondents agree in part.

[181] The detailed survey analysis can be found in Annex C.

[182] European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, p. 4; Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 2; Communication COM(2015) 192 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, p. 9 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

[183] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p.129

compete with OTTs and generate new revenue streams: This is most obvious in the case of the (personalised) **advertisement revenue model**[184]**,** which can be seen as a central OTT business model. ECS cannot engage in storing, analysing and selling or sharing user data on traffic and location with third party advertisers to deliver ads.[185] With regard to unsolicited communications for the purpose of direct marketing, ECS need to obtain prior consent from users and are only allowed to use this consent for offering similar services.[186] Unsolicited communications sent via OTT platforms like social networks are so far not assumed to be affected or restricted by Art. 13 of the ePD.[187]

This is reflected in the business models employed by ECS and OTTs, which vary considerably. ECS providers mostly follow direct payment revenue models for their services, demanding subscription fees and pre- or post-payment of services. OTTs are able to pursue a more diverse array of revenue models, for example offer their services through selling/placing (personalised) advertisement, demand one-time or recurring software licenses, or selling devices through which users can access the full service or a dedicated store with apps.[188] These models tend to rely more on use of customer data than direct reimbursement.

Several ECS providers have attempted to launch OTT services, for example social network apps like Libon (Orange) or Tuenti (Telefonica).[189] While they offer services similar to OTT competitors (WhatsApp, Skype, etc.) they apparently fail to attract users, possibly due to their late start, but also potentially because they initially only offered package deals (direct payment) rather than freemium models (e.g. ad financed services).[190] Thus, although ECS and OTTs offer increasingly functionally equivalent services, the sector-specific restrictions create boundary problems in the development of new products by ECS and prevent competition between ECS and OTT providers on equal terms.[191]

The interpretation and implementation of the scope varies across Member States. Indeed, some Member States have extended the ePD provisions to OTT services.[192] An overview is presented in the table below.

Table 16 – The coverage of OTTs within the scope of national implementing legislation

Country	OTTs covered	OTTs not covered	Case-by-case	No information/ unclear
Austria	X			
Belgium				X
Bulgaria	X			

[184] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. ch. 5.4.2
[185] Mentioned in stakeholder interviews with EU ECS providers, also: Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p.128,
[186] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p.129
[187] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p.128, 130
[188] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p. 102
[189] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p. 99
[190] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. ch. 5.4.1
[191] DLA Piper 2016: ETNO. Study on the revision of the ePrivacy Directive, p. 16
[192] European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, p. 4.

Country	OTTs covered	OTTs not covered	Case-by-case	No information/ unclear
Croatia				X
Cyprus				X
Czech Republic		X		
Denmark				X
Estonia		X		
Finland				X
France	X			
Germany			X	
Greece	X			
Hungary				X
Ireland		X		
Italy			X	
Latvia	X			
Lithuania				X
Luxembourg		X		
Malta				X
Netherlands		X		
Poland		X		
Portugal		X		
Romania		X		
Slovakia		X		
Slovenia	X			
Spain	X			
Sweden				X
UK				X
Overall	7	9	2	10

Source: Deloitte – Transposition check

Spain, UK, Austria, France, Estonia, Croatia, Finland, Denmark, Latvia, Norway, The Netherlands, Germany and Spain consider VoIP with access to telephone number an electronic communications service[193] Contrary peer-peer VoIP does not constitute the said service by the countries previously mentioned.[194] In the Czech Republic VoIP communication is considered an electronic communications services solely in cases where the communication is secured by a third party (external) provider within the scope of such provider's business. The German competent authority explained that they consider the scope of the ePD to be unclear in this respect. In practice, they spend a lot of time on this aspect, including to determine whether individual services should be covered under the scope of the rules of the ePD. An example is *Gmail*, which was dealt with in a court case.

[193] Swedish Post and Telecom Agency (PTS), "Which services and networks are subject to the Electronic Communications Act", guidance, 11 March 2009, Stockholm, p. 16.
[194] Swedish Post and Telecom Agency (PTS), "Which services and networks are subject to the Electronic Communications Act", guidance, 11 March 2009, Stockholm, p. 16.

Case example: Proceedings between the German Federal Network Agency and Google on whether Gmail is to be considered a telecommunications service

The Federal Network Agency in Germany required Google to register Gmail as a telecommunications service under German law. Google countered with a lawsuit as it argued that Gmail do not meet the requirements. More specifically, Google argued that they do not have control of the technical signalling as they do not have an own telecommunication network and use the open internet instead.

However, the court decided that Gmail should indeed be covered by these rules, arguing that a decision should be based on a functional assessment.[195]

Closed (private) user groups and corporate networks are also excluded from the scope of the ePD.[196] In this context, there is a lack of clarity which services qualify as a publicly available electronic communications services in public communications networks. For example, not all Member States agree that cases such as **Wi-Fi access offered by an airport or internet access provided in internet cafes and shopping malls** qualify as publicly available electronic communications services in public communications networks.[197] This was also considered as one of the more relevant problems by respondents to Deloitte's survey with competent authorities.[198] Indeed, it was noted by the Article 29 Working Party that the distinction between public and private networks is not always clear, as private and public elements are increasingly intertwined.[199] Examples of such ambiguous services according to the Article 29 Working Party include:

- Internet access provided to ten thousands of students at a university;
- Internet access provided by multinational companies to their employees; and
- Internet access provided to any visitor of a cybercafé.

Furthermore, some stakeholders (including e.g. some competent authorities interviewed by Deloitte) argue that it is a weakness of the ePD that private networks are excluded, as this hampers the achievement of the ePD's privacy related objectives.[200]

Feedback received from 29 businesses on the **online survey** implemented as part of this study shows that businesses are mixed with regard to their assessment of the scope of the ePD. On a scale from 1 to 5 (with 1 being 'strongly disagree' and 5 being 'strongly agree'), businesses have provided the following feedback on statements regarding the scope of the ePD:

[195] VG Köln, Urteil vom 11. November 2015, Az. 21 K 450/15.
[196] European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, p. 4.
[197] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15039), p. 5.
[198] The detailed survey analysis can be found in Annex C.
[199] Article 29 Working Party, 'Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)' (WP150), p. 4. See also: Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 16; European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, pp. 24 ff.
[200] European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, p. 4. In Deloitte's survey with competent authorities, most authorities considered this to be a moderate problem (10 out of 30). In addition some considered this to be a serious (3) or moderate (4) problem. The detailed survey analysis can be found in Annex C.

Table 17 – Businesses' assessment of the scope of the ePD (total n° of responses = 29)

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree	Cannot answer
The scope of the ePD is ambiguous. For example, it is not easy to understand the type of services covered in its scope	1	5	7	7	3	3
The scope of the ePD is too narrow from a technical perspective. For example, it does not cover all communication services, such as OTTs	3	4	8	5	3	2
The scope of the ePD is too broad. For example, it covers types of services or areas that will no longer be relevant in the future	0	4	12	4	5	2
The scope of ePD is conflicting in view of other regulations we have to respect in our business	1	3	8	6	7	2
The scope of ePD is now "out of date" compared to technological developments (e.g. provision of electronic communications services via online platforms – so called Over-the-top Services)	2	1	7	9	6	3
The scope of ePD is now "out of date" compared to new Regulations and the new General Data Protection Regulation, the draft NIS Directive	0	1	7	8	9	2

Source: Responses to the online survey by businesses, tabulation by Deloitte. The cells with the highest number of responses are marked in light blue.

As can be seen above, businesses seem to be undecided whether or not the scope of the ePD is ambiguous. One explanation for this may be that the scope might be clear for some provisions while it is ambiguous for others. However, businesses rather seem to agree with the statement that the scope of ePD is now "out of date" compared to technological developments (e.g. provision of electronic communications services via online platforms).

By contrast, businesses seem to slightly disagree to the statement that the scope of the ePD is too narrow from a technical perspective (e.g. regarding the coverage of OTTs). However, businesses seem to agree with statements in relation to the scope being too broad in relation to types of services or areas that will no longer be relevant in the future.

In general terms, it **may also lead to ambiguity that some of the provisions have a different scope than others** (cf. Table 15), although this is not very clearly stated in the ePD.

Turning to the scope in terms of the **type of data** protected, some difficulties could be identified. In general terms, the focus of the ePD is the protection of personal data, as e.g. stated in Article 3. However, some provisions also apply to non-personal data, e.g. the provision of traffic data or some provisions applying to legal persons.

Furthermore, it was raised in a workshop relating to the future of the e-privacy legal framework that it is questionable if both **personal data *in situ*** (i.e. in the possession of regulated entities) and ***in transit*** should be regulated.[201] In addition, it was argued during a workshop with national competent authorities that the **notion of personal data may be too narrow**, e.g. in a telephone there might be

[201] European Commission (April 12, 2016). *Towards a future proof ePrivacy Legal Framework*. Minutes, p. 17.

data other than personal data which yet needs protection.[202] Such lack of clarities potentially hinder the effectiveness, as they can lead to divergent application.

Finally, as concerns the **types of users/subscribers covered**, it can be considered as a strength that the ePD does not only apply to natural persons, but (in relation to some provisions) also to legal persons.[203]

Definitions

The table below includes the (shortened) definitions provided in Article 2 of the ePD.

Table 18 – Definitions provided in Article 2 of the ePD

Term	Definition
User[204]	Any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service.
Traffic data	Any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.
Location data	Any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user.
Communi-cation	Any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information. *This includes web browsing and using online video services.*[205]
Consent	Corresponds to the data subject's consent in Directive 95/46/EC (Data Protection Directive).
Value added service	Any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof.
Electronic mail	Any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.

Source: Deloitte

Below we discuss the functioning of these definitions, including in relation to:

- The concept of consent;
- The definitions of traffic and location data;
- The definition of "electronic mail";
- Transposition in the Member States; and

[202] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 1.
[203] Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), Adopted on 19 July 2016 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf, p. 5-6.
[204] The term **subscriber** is, in contrast to "user", not defined in the ePD. Instead, the definition of subscriber contained in the Framework Directive is applicable, according to which a subscriber is "**any natural person or legal entity who or which is party to a contract** with the provider of publicly available electronic communications services for the supply of such services", Article 2(k) Framework Directive.
[205] Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 25.

- The completeness of the definitions.

Specifically in relation to the **concept of consent**, it can be noted that the definition would change once the GDPR is in force. According to Articles 2(h) and 7 of the Data Protection Directive, consent means the freely given, specific, and informed agreement to the processing and the consent must be unambiguous. In the future, such reference would need to refer to the GDPR, which uses a more specific definition. Based on Article 4 (11) of the GDPR, consent also needs to be freely given, specific, informed and unambiguous indication, but in addition must be indicated "by a statement or by a clear affirmative action". Recitals 42 and 43 of the GDPR provide further details on the conditions for a valid consent.

Furthermore, based on a review of the available literature, it appears that there are currently some **difficulties in relation to the practical application of the concept of consent**. For example, there are doubts as to whether the consent mechanism in relation to information (e.g. in the form of cookies) stored on the user's terminal equipment (Article 5.3 of the ePD) is adequate to protect the users' privacy. This is discussed further in section 5.7. Such difficulties may potentially hinder the achievement of the right to privacy.

It was pointed out by the WP29 that the definitions on **traffic and location data** may be difficult to apply. It argues that the distinction between content and traffic data is no longer clear-cut. Nowadays, in digital communications a distinction between the contents of communication and related traffic data is not always made. For example, URL's must contain both elements of content (visited webpages which content can be read from the URL's anchor and parameters) and traffic data (host names). Difficulties may arise on this basis, for example "when a network provider engages in packet inspection and the analysis reveals the contents of communication between users and third parties (the visited URL's)."[206]

In relation to the **definition of "electronic mail"** it can be noted that this is kept rather open and therefore covers various types of services. Hence, safeguards provided for subscribers against intrusion into their privacy by unsolicited communications for direct marketing purposes by means of electronic mail should also be applicable to SMS, MMS and other kinds of similar applications.[207] This may contribute positively to the privacy and internal market related objectives of the ePD. Indeed, it may be considered a **strength** that the ePD sets out to be **"technology neutral"**, i.e. that it applies to different technologies and is thus less prone to result in future regulatory gaps due to technological developments in terms of new, innovative communication tools. The principle of technology neutrality aims to "not to impose, nor discriminate in favour of, the use of a particular type of technology, but to ensure that the same service is regulated in an equivalent manner, irrespective of the means by which it is delivered".[208]

Based on the **transposition** check carried out as part of this study, that this article was transposed literally by most of the Member States. Apart from the fact that many of the latter have additional

[206] Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), Adopted on 19 July 2016 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf, pp. 9-10.
[207] This formulation is made in Recital 67 of the Citizens' Rights Directive (2009/163/EC).
[208] Commission of the European Communities (1999). *Towards a new framework for Electronic Communications infrastructure and associated services - The 1999 Communications Review*, COM(1999) 539 final, p. vi. For a detailed analysis on the principle of technology neutrality in the EC telecommunications regulations, see Van der Haar, I. (2008). *Principle of technological neutrality in EC telecommunications regulation* (DPhil thesis, Tilburg University).

definitions[209] in their implementing acts, no major disparities were found on the transposition of this article. While some differences have been uncovered, for example in relation to the definition of the term "user", these do not seem to hinder the effectiveness of the ePD.

Considering the **completeness of the definitions**, it can be noted that the fact that many Member States provided additional definitions could mean that the definitions in the ePD were not sufficient. This is reflected in Deloitte's online survey with competent authorities, in which 16 out of 30 respondents indicated that some additional definitions may be needed, including for instance a definition on unsolicited marketing communications.[210] In addition, some interviewees representing business associations and other stakeholders indicated that the definitions are one of the weaknesses of the ePD. They noted that some terms are currently unclear, including e.g. the terms "electronic communications", "similar products" in Art. 13 (2) on unsolicited communications and "calling" (does this include VoIP).

5.4.2 Efficiency

Key finding of the analysis: Criterion not relevant

As the provisions on the scope and definitions are not "active" provisions this criterion is not relevant in this context.

This said, indirect costs for businesses, authorities and citizens may occur based on ambiguities of the scope, as unclear aspects need to be interpreted. Furthermore, telecom providers incur opportunity costs vis-à-vis their OTT competitors.

As the provisions on the scope and definitions are not "active" provisions, i.e. they do not imply any activities for businesses or competent authorities, this criterion is not relevant in this context.

This said, indirect costs for businesses, authorities and citizens may occur based on ambiguities of the scope, as unclear aspects need to be interpreted. This was, for example, highlighted by two competent authorities interviewed by Deloitte in relation to the coverage of OTTs. One authority estimates that two FTE deal with questions related to the interpretation of the scope of the ePD. This includes individual cases (e.g. businesses contacting them to ask whether the rules of the ePD apply to them), but also workshops on such matters. The authority has been dealing with such questions regularly for years now. The time they spent on this has increased with the spread of OTTs.

Furthermore, the vast majority of the telecoms indicated that the biggest cost stemming from the ePD relates to the opportunity cost of not being able to benefit from the same conditions as OTTs. In comparison to OTTs, telecom providers are hindered in exploring new business opportunities and usages of data. The businesses consulted were, however, not able to quantify these costs.

5.4.3 Relevance

Key finding of the analysis: Relevance not fully confirmed

The **scope** of the ePD is not considered fully relevant any longer in light of recent technological

[209] Many of the Member States, such as Austria, Greece, Slovakia, Romania, and Spain, have included further definitions. For example Austria's law sets out the meaning of "content data", "access data", "cell ID", "subscriber identifier", "internet telephone service", and "internet access service".
[210] The detailed survey analysis can be found in Annex C.

developments. While in general the need to have specific rules for data protection in the electronic communications sector is confirmed, the scope is not considered to be fully appropriate in light of the needs of consumers, notably because it does not cover services that are increasingly used by citizens as substitutes for traditional electronic communication services. Closely related, the **definitions** are no longer relevant either, e.g. as some definitions are no longer appropriate while others are missing.

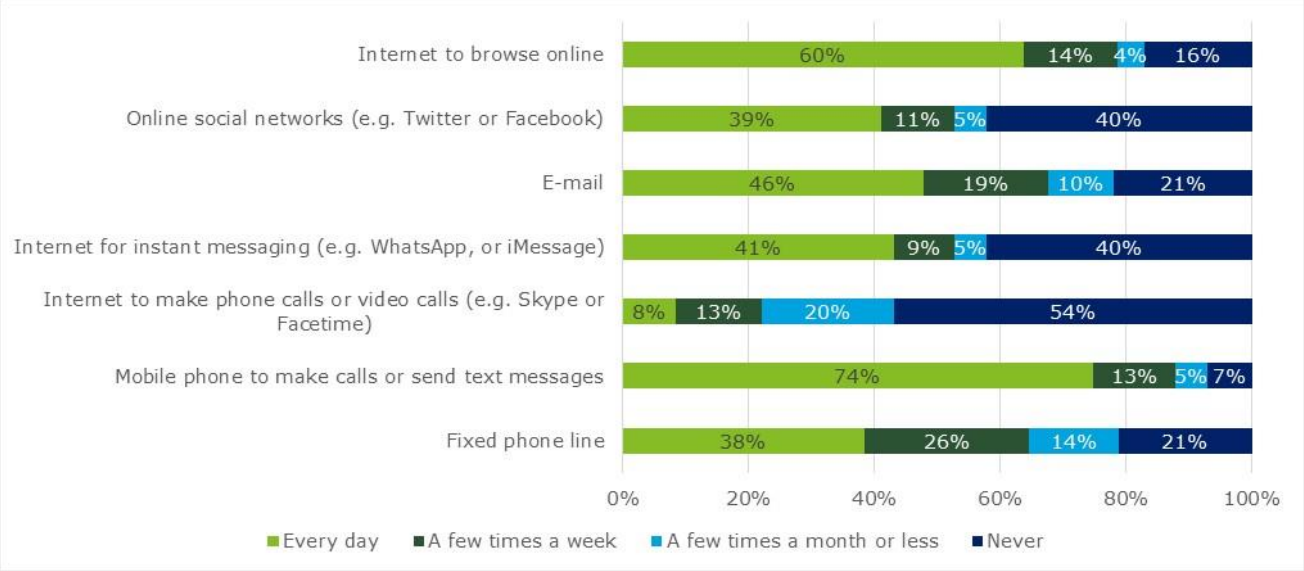
In general terms, the **scope** of the ePD is still relevant in the sense that it provides for specific rules on privacy in the electronic communications sector. From a legal perspective, the ePD is tributary to the fundamental rights of confidentiality of communications and personal data protection, enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the "Charter").[211] While Directive 95/46/EC and the GDPR are elaborations of the right to personal data protection, the ePD is the only instrument in the EU to contain specific privacy rules for electronic communications.[212]

In the same vein, BEREC highlights the relevance of having a specialised set of provisions on data protection, privacy and confidentiality in the electronic communications sector, even if the ePD goes beyond this scope in certain aspects.[213] The importance of having specific rules for the electronic communications sector is also supported by the Article 29 Working Party.

Another aspect to be considered when assessing the relevance of the ePD's scope is its strong interaction with the Radio Equipment Directive.

Considering the relevance of the scope of the ePD, it is important to take the **perspective of consumers** and the types of services they use. Available Eurobarometer data[214] shows that that the services covered by the ePD are generally used by consumers (see Figure 14).

Figure 14 – Usage patterns of citizens regarding different types of telecom services



Source: Eurobarometer, graphical representation by Deloitte.

[211] Charter of Fundamental Rights of the European Union [2012] C 326/02, arts 7 and 8.)
[212] Article 29 Working Party, Opinion 3/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC) [2016] WP240, p 4.
[213] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133. http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive p.2
[214] Flash Eurobarometer 443 (2016): e-Privacy. Data on 26,526 consumers collected between 6 and 8 July 2016. At this stage, the Eurobarometer results are only of provisional character.

The **ePD covers important parts of consumers' everyday communication means**. However, **very important parts are also excluded from its scope** – in particular communication means that are expected to become more important over the next couple of years (both societal, as well as financially in terms of businesses' turnover) and that are especially used by younger generations. See also section 5.4.1 for a description of the scope.

For instance, mobile phones to make calls or send text messages are used by 74% of consumers every day while the Internet is used by 60% of consumers on a daily basis. More traditional fixed phone line services are used by 38% each day. This shows that the scope of the ePD with regard to these types of services is still relevant today (and probably will remain relevant over the next couple of years).

However, a large part of consumers also uses services every day that are not covered by the ePD:

- Email is used by 46% of consumers every day;
- OTTs for the purpose of instant messaging (e.g. WhatsApp) are used by 41% every day[215]; and
- Online social networks are used by 38% every day.

The notable exception here is the usage of the Internet to make phone calls or video calls (e.g. via Skype or Facetime). More than half of consumers never use this type of service. However, it can reasonably expected that this figure is going to decrease over the upcoming years with take-up rates for Internet based audio and video communication increasing.

This shows that communication means that are used by, typically, younger consumers on a daily basis are excluded from the ePD. In practice, this means that an important segment of users (i.e. data subjects) are deprived, possibly unknowingly, of the confidentiality of communications offered to users of more traditional means of communications under the current ePD. This is a critical point, not only from the perspective of the market players, but also in light of the young consumers within the user group that may not be fully aware of the privacy risks involved in this type of electronic communication services. On this basis, the **definitions** are not fully relevant either. In particular, the definition of "communication" (Article 2.d) is not sufficiently broad in line with the considerations above.[216] Furthermore, some stakeholders consulted by Deloitte indicated that some additional definitions may be needed, including for instance unsolicited marketing communications.[217]

5.4.4 Coherence

Key finding of the analysis: Coherence tends to be confirmed

The ePD interacts with a number of other legal instruments, including relating to data protection as well as the online environment. The coherence of the ePD with other relevant instruments tends to be confirmed, although there may be a lack of clarity as to which services are covered by the ePD

[215] Interestingly, the Eurobarometer data shows that for instant messaging OTTs, two large groups of consumers seem to exist: Those that use instant messaging every day and those that never use it. The proportion of consumers that uses it a few times per week / month is comparatively small. It can be assumed that age is an important factor with regard to the take-up of such services. While younger generations use instant messaging every day, the majority of older consumers do not use it at all. Therefore, it can be expected that the share of consumers who use instant messaging on a daily basis will increase over the next years.

[216] This is supported by the WP29. See: Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), Adopted on 19 July 2016 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf, p. 9.

[217] This was raised in Deloitte's online survey with competent authorities (the detailed survey analysis can be found in Annex C) and in interviews. See also the section on effectiveness.

and which by the GDPR.

In the table below, we present the connection between the ePD and the GDPR as well as the Electronic Communications package. For each relevant provision[218] we provide a brief summary, using the following colour code[219]:

- Green: positive relationship (e.g. synergies);
- Grey: neutral relationship/no challenges nor positive aspects identified; and
- Yellow: potential challenges.

Further details are provided in Annex.

The table shows that for all but one provisions, neither specific challenges nor positive aspects could be identified. In some cases there may be a lack of clarity as to when the ePD and when the GDPR applies, as the distinction of "publicly available and non-publicly available electronic communications services" is not clear-cut, especially from the perspective of the user. Furthermore, the ePD provides rules that encompass both personal data and data generated by electronic communications systems that are not personal data, which may be processed by parties that do not necessarily conform to the category of data controller or data processor. Consequently, there is some of overlap with Directive 95/46/EC and the GDPR.[220] This reflects the general ambiguities identified in relation to the scope, which are explained in the section on effectiveness.

Table 19 – Coherence of Articles 1, 2 and 3 with the GDPR and the Electronic Communications package

Provision in the ePD	Provision in the other instrument	Main findings
GDPR		
Scope and aim (Article 1)	- Subject-matter and objectives (Article 1) - Material scope (Article 2)	Close connection, as the ePD acts as *lex specialis* in relation to the GDPR. However, the relationship is clear.
Definitions (Article 2)	Definitions (Article 4)	ePD to be adjusted to refer to the GDPR instead of the General Data Protection Directive. However, no challenges could be identified.
Services concerned (Article 3)	Material scope (Article 2)	There may be a lack of clarity as to when the ePD and when the GDPR applies, as the distinction of "public or publicly available electronic communications services" is not always clear, especially from a user perspective.
Electronic Communications Package		
Framework Directive		
Scope and aim (Article 1)	Scope and aim (Article 1)	Both instruments have the same scope.
Definitions (Article 2)	Definitions (Article 2)	The relevant definitions are in line
Services concerned (Article 3)	Scope and aim (Article 1)	Both instruments have the same scope

[218] We only list those instruments and provisions that a have connection to the ePD.
[219] The summaries and colour classification are to be seen as indicative.
[220] Article 29 Working Party, Opinion 3/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC) [2016] WP240, p 5. Most of the competent authorities responding to Deloitte's online survey considered this to be a minor problem (13 out of 30). Fewer considered as a moderate (7) or serious (6) problem. The detailed survey analysis can be found in Annex C.

Provision in the ePD	Provision in the other instrument	Main findings
Access Directive		
Scope and aim (Article 1)	Scope and aim (Article 1)	The two instruments have entirely different scopes and no overlapping areas.
Authorisation Directive		
Scope and aim (Article 1)	Objective and Scope (Article 1)	The ePD and the Authorisation Directives set out to regulate different aspects of the internal market. They are coherent with one another and do not incur in any discernible overlaps.
Services concerned (Article 3)	Objective and Scope (Article 1)	See the row on Article 1 of the ePD.
Universal Services Directive		
Scope and aim (Article 1)	Subject-matter and scope (Article 1)	The two Directives have markedly different aims and scopes, with very few overlapping areas between them.
Regulation on Body of European Regulators for Electronic Communications (BEREC)		
Scope and aim (Article 1)	Establishment (Article 1)	BEREC and the ePD neither overlap nor conflict.
Regulation on roaming on public mobile communications networks		
Scope and aim (Article 1)	Subject-matter and scope (Article 1)	The ePD and the Regulation on Roaming on Public Mobile Communications Networks have entirely different scopes and aims.
Definitions (Article 2)	Definitions (Article 2)	While there may be some connections as concerns some of the terms, there is no discernible overlap between the two instruments.
Radio Equipment Directive		
Scope and aim (Article 1)	- Subject matter and scope (Article 1)	The instruments have different scopes and do not overlap. However, equipment covered by the Radio Equipment Directive can be used for communications covered by the ePD.
NIS Directive		
Scope and aim (Article 1)	- Subject matter and scope (Article 1)	The instruments have different scopes and do not overlap. Information society services that do not fall under the scope of the ePD may be subject to the specific rules in the NIS Directive.

Source: Deloitte.

In its response to the ePrivacy Directive questionnaire, BEREC states that the general data protection EU legislative framework (specifically, the GDPR) and the e-Privacy Directive have historically pursued distinct objectives.[221] The ePrivacy legislation, which shall deal with the electronic communications sector-specific issues, will continue to play a key role. However, according to BEREC, the current provisions should be reviewed and, if needed, updated, in order to streamline the relevant discipline while guaranteeing that the current standard of protection is not undermined and avoiding overlaps between the ePD and the GDPR.

A difference between the two pieces of legislation lies in Article 95 of the GDPR, which stipulates that the Regulation may not "impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in

[221] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133. http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive p.4

public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC". The purpose of this provision is to avoid overlaps and to ensure that the GDPR does not apply in cases where the ePrivacy Directive contains specific obligations with the same objective. Apart from this, the GDPR should apply in all other cases where personal data is implicated.

However, since traffic, communication and location data are in most cases personal data, some overlap between the ePrivacy instrument and the GDPR is inevitable, the WP29 notes.[222] In these cases, the WP29 urges the EC to ensure that in addition to a high level of confidentiality, the level of personal data protection in the GDPR is not undermined. Therefore, it is the opinion of the WP29 that the revised ePD should "keep the substance of existing provisions but make them more effective and workable in practice, by extending the scope of the rules on geolocation and traffic data to all parties, while simultaneously introducing more precisely defined conditions that take the intrusiveness of the processing of communication data to the private life of users thoroughly into account".[223]

5.4.5 EU added value

Key finding of the analysis: EU added value is confirmed

The EU added value of specific rules on privacy in the electronic communications sector can be confirmed, notably based on the cross-border nature of the topic. Based on an increased cross-border flow of personal data, it can be argued that the EU is best placed to ensure common standards in this area.

It was already recognised at the time of the adoption of Directive 95/46/EC and the ePD itself that there is a **need to address data protection, including in the electronic communications sector, at the EU level**. It was argued that the establishment of the internal market as well as the introduction of new telecommunications networks would necessarily lead to a substantial increase in cross-border flows of personal data. A potential difference in levels of protection was expected to constitute a barrier to the functioning of the internal market, as data exchanges may be hindered.[224]

This assessment is still valid today, as also pointed out in the recent Impact Assessment on the GDPR. The EU is best placed to ensure an effective and consistent protection for individuals, in particular when personal data is transferred across borders, as common standards are required for this purpose.[225]

It can further be noted that none of the stakeholders consulted as part of this assignment declined an EU added value of specific rules on privacy in the electronic communications sector.

[222] Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), Adopted on 19 July 2016 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf, p. 5.
[223] Ibid. p.5.
[224] Recitals (5), (6), (7), and (8) of Directive 95/46/EC; Recital (8) of the ePD.
[225] Impact Assessment Accompanying the document "Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 10 final, p. 37.

5.5 Obligations for service providers on the security of processing and notification of personal data breaches (Article 4)

Article 4 aims at ensuring the **security** of electronic communication services.

Overview of the content

Article 4(1) of the ePD lays down a general obligation for service providers to **safeguard security** of its services, following a risk assessment approach. More specifically, in case of risks of breaches of security, the service providers must inform their subscribers of the risk (Article 4.2). On this basis, service providers **must inform the subscribers about particular risks that could be caused by the use of a service** (e.g. sniffing of communication if an unsecure Wi-Fi connection is used).[226]

According to Article 4(3) service providers must, in the case of personal data breaches, without undue delay:

- Notify the competent national authority in all cases; and
- Notify the subscriber or individual concerned if the breach is likely to adversely affect that person.

To ensure the successful application of these provisions, Articles 4(1) and 4(4) specify the powers the national competent authorities shall have. In particular, they shall be able to carry out audits and they may adopt guidelines or instructions. Furthermore, the Commission may adopt technical implementing measures after consulting with ENISA, the Article 29 Working Party and the EDPS.

5.5.1 Effectiveness

Key finding of the analysis: Effectiveness not fully ensured

The effectiveness of Article 4 does not seem to be fully ensured based on a number of challenges identified potentially hindering the achievement of the objective to ensure security of services. In particular, there are some ambiguities (e.g. to what extent the security obligations apply to non-personal data) and practical difficulties when it comes to the application of personal data breach notifications (confusion for businesses about which authority to contact, confusion based on the duplication with the GDPR, few breaches are notified hinting towards a low level of compliance, enforcement powers of authorities not always appropriate).

As a starting point, there is **no specification if the security obligations in Article 4(1) and 4(2) should apply to personal data or also to non-personal data.** Although some explicit references to "personal data" are made e.g. in Article 4(1a), the "security of services" refers rather to the overall functionality and provision of the service, including personal data but possibly also other aspects. Security in this context, as well as laid down in Article 13a of the Framework Directive **2002/21**, is usually "information security", i.e. the protection of the confidentiality, integrity and availability of information.[227] Based on this lack of clarity, the standards service providers implement may vary, possibly hindering the full achievement of secure services.

[226] Ibid, p. 12.
[227] ENISA (June 2016). *Working paper on the review of the ePrivacy Directive. Article 4 – Security of processing*, p. 13-15, p. 9.

The **obligation to inform subscribers of security risks (Article 4.2)** and the rules on the **notification of personal data breaches (Article 4.3)** may positively contribute to the security of processing as they ensure that any breaches must be notified to the competent authorities and in some cases to individuals. The provisions also ensure that competent authorities are closely involved in the case breaches and give them powers, e.g. to require service providers to notify the individuals concerned. However, several challenges have been identified in relation to these provisions.

As concerns the **obligation to inform subscribers of security risks (Article 4.2)**, ENISA pointed out that there are difficulties relating to its practical application. In particular, there is **little guidance** about the type of risks and proposed mitigating measures that the providers should be informing for.[228] On this basis, the quality of information provided to subscribers may vary.

In the EC's public consultation, slightly more than one third of the respondents indicated that they had encountered difficulties with the **notification of personal data breaches**.[229] It is striking that problems were in particular encountered by the group of citizens and civil society (73%) and public bodies (59%). In contrast, only 13% of respondents from the industry indicated that they faced problems.

Table 20 – Extent to which respondents encountered problems in relation to the rules on security of processing, per stakeholder group.

Stakeholder group	Yes	No	No opinion	Total nr.
Industry	12,8%	78,0%	9,1%	164
Citizens & civil society	72,8%	17,9%	9,2%	184
Public bodies	59,3%	33,3%	7,4%	27
All replies	45,6%	45,3%	9,1%	375

Source: Deloitte based on EC public consultation.

As concerns the business perspective, the results of Deloitte's online survey with businesses are – in spite of a very low participation rate – similar to the results of the public consultation. Based on the online survey with businesses the ePD's provisions regarding the security of processing were a problem for only 14% of the businesses that indicated this particular provision is of practical relevance for them (i.e. one business in the sample). Although this is only based on a very limited set of responses, it can be seen that there seem to be provisions that have caused problems for more businesses. However, in the interviews, some businesses reported ambiguities in relation to the provisions on breach notifications, including;

- It is unclear which national authority needs to be contacted for the personal data and security breach notifications, which creates further legal uncertainty and costs;
- The relationship between the procedures on personal data breach notifications in the ePD and the GDPR is not clear in this respect; and
- It is not clear what constitutes a significant breach of security that needs to be notified (possibly leading to differences in which types of breaches are actually reported).

Furthermore, ENISA argued that the rules may actually be too strict. The ePD and GDPR introduce two similar notification schemes for breaches, where the core objectives are the same. However, the

[228] ENISA (June 2016). *Working paper on the review of the ePrivacy Directive. Article 4 – Security of processing*, p. 13-15, p. 12-13.
[229] Question: "Have you encountered problems in applying/understanding the rules (in your role of provider or as individual)?". 120 respondent answered "Yes", 106 answered "No" and 104 did not have an opinion.

GDPR provisions are generally less strict, e.g. the deadline for notifying the supervisory authority of breaches is more flexible in the GDPR than in the ePD (72 versus 24 hours). While stricter rules may strengthen the provisions, it has been argued by ENISA that the **GDPR scheme seems to be preferable** to the one of the ePD. This argument is based on that the GDPR scheme has the potential to achieve the same objective, allowing for more efficiency and better quality of results.[230] This tends to be confirmed by the interviews with businesses, as some businesses mentioned that the procedure contained in the ePD is too complex and costly. Of course, it is still unclear how the GDPR will actually play out in practice. This is a general problem and also why some argue to rather carry out the REFIT of the ePD after there is evidence on the enforcement of the GDPR.[231]

Many of the **competent authorities interviewed by Deloitte criticised that there are different notification regimes**, with most commenting on the two regimes of personal data breaches contained in the ePD and the GDPR. One authority also referred to security breaches, indicating that there is another regime in Article 13 of the Framework Directive. It appears that currently companies need to notify two different authorities in several Member States, which creates additional and unjustified burden for businesses and confusion over the competency related to breaches according to the interviewees.

Furthermore, according to some authorities, **the breach notification provision is good on theoretical level but ineffective in practice**. This is confirmed by the inexistent or very low numbers of breach notifications in many Member States. Some authorities explained that the lack of criteria makes it difficult to determine which breaches need to be notified and not. Correspondingly, some authorities responding to Deloitte's online survey indicated that businesses in some cases fail to report personal data breaches.

Table 21 – Reported incidents of personal data breaches in selected EU Member States

Member State	2010	2011	2012	2013	2014	2015
Belgium	/	/	0	0	4	1
Croatia				0	0	0
Cyprus	0	0	0	0	0	0
Estonia				1	2	5
Germany	-	-	17	66	112	261
Greece (HDPA)[232]	n/a	n/a	0	0	0	4
Greece (ADAE)	4	7	5	16	30	11
Ireland	410	1167	1592	1507	2188	2317
Romania					1	3
Sweden			5	4	16	24
United Kingdom			491	381	308	550
Total	**414**	**1174**	**2110**	**1975**	**2661**	**3176**

Source: Responses of competent authorities to the online survey implemented by Deloitte as part of this assignment.

[230] ENISA (June 2016). *Working paper on the review of the ePrivacy Directive. Article 4 – Security of processing*, p. 13-15, p. 13-15.
[231] European Commission (April 12, 2016). *Towards a future proof ePrivacy Legal Framework*. Minutes, p. 14.
[232] HDPA: minor incidents only; Obligation for providers to submit a Data Breach Notification to the supervising authorities (both the HDPA and ADAE) has only been imposed in 2012

Based on the online survey with competent authorities the most frequent type of breach entailed that personal data stored or transmitted was subject to accidental, unauthorised or unlawful destruction, loss, alteration or disclosure (incl. data leakage, unlawful sharing with third parties).[233]

Finally, the level of security actually ensured by Article 4 may be hindered by the **practical implementation and enforcement**. In particular, it was pointed out during a workshop the Commission held with competent authorities that not all competent authorities have the power to enact penalties in case of violations of Article 4.[234] On a positive note, the transposition check carried out for the purpose of this study shows that most Member States transposed all relevant parts of this article. On this basis, the effectiveness of this article in achieving secure processing is not hindered in most Member States. Indeed, almost half of the Member States[235] appear to have transposed this article more or less literally. Most of the remaining countries did not transpose this article in a literal manner in their local laws.[236] However, no material differences from the content of Article 4 are observed, although there are some local differences and specificities.[237] Only one country, Finland, did not transpose this article at all. Germany transposed it only partially. Cyprus, on the other hand, transposed this article but made no reference to audit, and paragraphs 1a, 3, 4 and 5 are not or not completely covered. Further details on the transposition in the Member States can be found in chapter 4.

5.5.2 Efficiency

Key finding of the analysis: Partially efficient

Overall, this provision is one of the most costly provisions, both for businesses and competent authorities. Nevertheless, some of these costs (e.g. the data breach notification) are only incurred in case of an actual breach, which is an incentive for implementing adequate security requirements. As not all of these costs seem to be justified (e.g. because duplications with other instruments exist), this provision is only considered **partially efficient**.

Below we discuss:

- The types and (as far as possible) magnitude of costs related to Article 4 for businesses and competent authorities; and
- The appropriateness of these costs.

With respect to the **types and magnitude of costs** related to Article 4, we note that this provision is one of the more costly provisions for businesses and competent authorities, as it entails several concrete obligations.

For **businesses**, the following main **types of costs** are potentially involved:

- **Implementation of the security standards based on Article 4(1)**: This concerns all businesses within the scope of the ePD. It was explained during the interviews with

[233] Further details can be found in the annex.
[234] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 4.
[235] Belgium, Croatia, Denmark, Greece, Ireland, Poland, Portugal, Romania, Slovenia, Spain, and United Kingdom.
[236236] Such is the case of Austria, Bulgaria, Cyprus, Czech Republic, Estonia, France, Hungary, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Slovakia, and Sweden.
[237] In Estonia for example, the law is more specific than the ePD as it specifies a definition for data breach, the information to be included in the notice, and the information to be included in the records of data breach.

businesses that the bulk of these costs was incurred after the adoption of the ePD. Some efforts in relation to maintenance and updates e.g. of relevant IT systems may be necessary on a regular basis. However, these ongoing costs are not considered to be substantial by the businesses we interviewed. Furthermore, businesses argued that they would take similar measures also without the ePD.

- **Interaction with competent authorities in the context of audits:** This only concerns businesses that are audited by a competent authority. Based on statistics Deloitte received by competent authorities, relatively few businesses are audited regularly, e.g. because some authorities only take action based on a suspicion. The costs depend on the procedures in the Member States. For example, if an audit is announced, some preparation may be involved. Furthermore, time may be needed to interact with the authorities and provide ad hoc information.
- **Notification of subscribers in case of security breaches based on Article 4(2)**. This concerns only businesses where relevant breaches occur. In such cases, costs may be related to checking, which subscribers are involved and interacting with them. In addition, businesses may need to pay fines for breaches.
- **Dealing with personal data breaches based on Article 4(3) and (4)**: This concerns only businesses where relevant breaches occur. Businesses need to notify the competent authorities of relevant breaches and in some cases also subscribers. This may e.g. entail filling in forms and answering questions by the authorities. In addition, businesses need to prepare an inventory of personal data breaches. In addition, businesses may need to pay fines for breaches.

Businesses have indicated that they incurred a significant amount of compliance cost with Article 4 after the adoption of these rules (some in 1997, others in 2002 and also as regards the data breach notification in 2009).

However, this statement should be moderated by the fact that businesses may often have to comply with similar technical and security obligations under various pieces of legislation (e.g. the Framework Directive or the Data Protection Directive). Therefore, they may refer to costs that they incur under all these legislations. One can also argue that the cost of Article 4 of the ePD would have been incurred anyway under the obligations to comply with the Data Protection Directive and now the GDPR.

Some details in relation to the magnitude of these costs are provided below.

In a 2014 survey commissioned by the *UK Department for Business Innovation & Skills*, businesses provided insights on compliance costs related to **maintaining security standards,** at least partly related to Article 4(1).[238] In general, 572 responding firms reported that complying with laws and regulation accounted for 13% of their overall information security expenditure.[239] The following case example based on stakeholder interviews conducted by Deloitte provides insights on the possible structure of these expenditures to maintain security standards.

Case example Art. 4: Costs incurred by a telecom provider in relation to security

A South-Eastern European telecommunication service provider indicated as part of an interview that the magnitude of the initial investments is unknown. However, the business representative was

[238] Security breaches were understood to include are all forms of attacks on company systems, viruses and malicious software or human error that led to a loss or theft of intellectual property and staff or customer data.
[239] UK Department for Business, Innovation and Skills (2016): Information security breaches survey 2014, p.1, 4.

able to indicate that, on an annual basis, 10,000 EUR are incurred with regard to checking and maintaining the security of the existing system.

The overall annual revenue of the interviewed business was indicated to be 210 million Euro. Therefore, the costs related to Art. 4 in this case are approx. 0.005% of the business' total annual turnover.

Such tasks are, however, not carried out by the company itself but rather by an external consultancy as part of a (public) procurement procedure. The consultants that check the security of the system work around 14 days per year.

The costs in relation to **personal data breaches** appear to be the most significant for those businesses having faced relevant breaches. A previous GDPR Impact Assessment report estimated the total number of data protection breach notifications within the EU at 3,000 in 2012, based on numbers by the UK DPA from 2008/2009 extrapolated for the EU28.[240] Responses provided to a Deloitte online survey by competent authorities indicate that this number is likely to be higher. Regarding the size of breaches, a recent study by the *Ponemon Institute* and *IBM* indicates that in between January 2015 and March 2016, the average number of breached records in European countries ranged from 19,900 (Italy) to 23,900 (Germany).[241]

Estimates for the magnitude of costs in relation to personal data breaches vary considerably. The **total cost of the data protection breaches** mentioned above has been estimated at EUR 1.2 Mio. per year in the GDPR impact assessment. This number is based on the assumption that the average cost for businesses to deal with these notifications was EUR 400.[242] The study conducted by *IBM* and the *Ponemon Institute* alludes to higher numbers. Their country report for France already indicates total costs of data breaches for businesses of EUR 3.5 Mio in 2016 alone. This is based on an estimated average per capita cost of a data breach in the communications sector of approximately EUR 155.[243]

The variance in estimates points to difficulties to ascertain the share of compliance costs associated with reporting personal data breaches to competent authorities. This is due to a possible variety of different tasks involved in the notification and investigation of personal data breaches. The *Ponemon Institute* and *IBM* differentiate two general **cost elements** incurred by businesses related to these necessary tasks, namely:

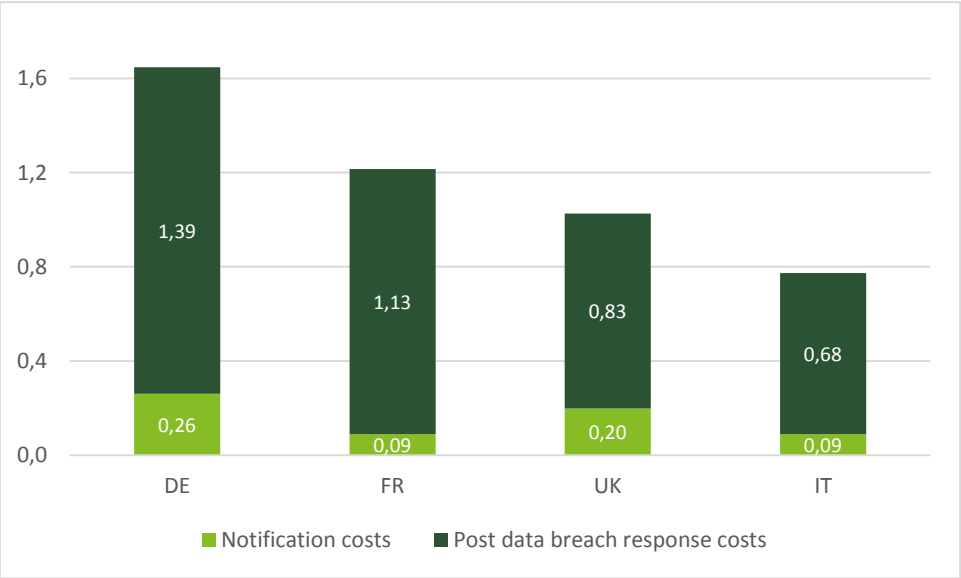
- **Notification costs**, including the:
  - Creation of contact databases;
  - Determination of all regulatory requirements;
  - Engagement of outside experts;
  - Postal expenditures, email bounce-backs and inbound communication set-up; and
- **Post data breach response costs**, including
  - Help desk activities;
  - Inbound communications;

[240] Commission Staff Working Paper on Impact Assessment on the General Data Protection Regulation proposal, 25.01.2012, SEC 2012(72), Annex 9 and p101
[241] Ponemon Institute (June 2016): Cost of Data Breach Study. Global Analysis, p. 8.
[242] Commission Staff Working Paper on Impact Assessment on the General Data Protection Regulation proposal, 25.01.2012, SEC 2012(72), Annex 9 and p101
[243] The global average per capita cost of a data breach in the communications sector is estimated at EUR 164 in the same time period, see Ponemon Institute (June 2016): Cost of Data Breach Study. Global Analysis, p. 8.

- Special investigative activities;
- Remediation;
- Legal expenditures;
- Product discounts;
- Identity protection services; and
- Regulatory interventions. [244]

Figure 15 presents an estimate for these two cost elements incurred by businesses in selected EU Member States, illustrating their relationship.

Figure 15 – Aggregated notification and response costs for businesses in selected EU MS between 01/2015 and 03/2016 (in EUR Mio.)



Source: Ponemon Institute (June 2016): Cost of Data Breach Study. Global Analysis. Graphical representation by Deloitte.

A different approach is adopted in the previous impact assessment in the context of network and information security (NIS) legislation in the European Union, in which the focus was on general staff costs to carry out all of the tasks mentioned above.[245] The causes and incidence of notifications vary between the context of the ePD and the NIS context due to different requirements in the relevant Framework Directive 2002/21/EC (Art. 13a and 13b). Nevertheless, cost equivalence of reporting itself is assumed due to similar processes.

Excluding any estimates on the costs of setting up necessary internal business organisation (assumed to be already included in any adequate risk management approach), the **notification costs** are estimated using staff costs and time requirements. The costs for a staff person entrusted with reporting and follow-up activities are assumed to be EUR 60,000.[246] Presupposing that reporting activities are similar to those under Art 13a (Framework Directive 2002/21/EC) and that no further analysis within the organisations are necessary, time required for notification is assumed to be one 0.5 working days. Combining these two factors, the average cost for reporting one incident is EUR

[244] Ponemon Institute (June 2016): Cost of Data Breach Study. Global Analysis, p. 18, 19.
[245] European Commission (2013): Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union, Annex 4.
[246] This number is based on information gathered in the "Action Programme Reducing Administrative Burdens in Europe", using the salary information category "Professional" in the EU27 (increased by 25% to include overhead costs).

125.[247] While this number is not considered to be very significant for businesses, it may underestimate the expenses due to a very narrow definition of work steps and staff involved in the notification process.

With regard to **post data breach response costs**, investigations are considered as a significant driver of costs.[248] The cost of investigations and audits may vary considerably from case to case due to differences in:

- The **level of complexity** of a given enterprise, the IT systems and the root cause of a given breach incident, and
- The **methodology** adopted by the Member State authority in charge of the investigation.

Based on experiences from the United Kingdom, the study proposes an average duration of 5 months per investigation, requiring one FTE on the side of an affected ECS providers. Based on the presumed standard salary cost of EUR 60,000, this leads to an expected cost of EUR 25,000 per investigation. During interviews conducted by Deloitte, stakeholders in the sector highlighted the complexity of cost estimates regarding notifications and post-breach response. Their responses are briefly summarised in the following case example.

Case example Art. 4: Cost estimates by telecommunication operators

In general, telecommunication service providers have acknowledged the importance of security measures. Although it does not (yet) serve as a valid sales argument vis-à-vis the customers according to industry representatives, investments into the security and confidentiality are of utmost importance to safeguard customers trust and loyalty to service providers.

However, albeit the importance of security and confidentiality from a business continuity perspective, the feedback received as part of the interviews shows that it is – according to the businesses – extremely difficult to estimate the cost of the ePD's security provisions separately.

Several reasons have been cited for this: (1) The ePD is not the only source of costs for businesses as the have to implement technical measures under several legislative instruments, incl. consumer protection measures. (2) Estimates of costs require extensive internal work on the side of the businesses between across organisational departments (e.g. litigation, compliance department, and marketing department). Hence, it is seen by businesses also as a cost in itself to estimate the costs of the ePD.

From the perspective of **competent authorities**, Article 4 tends to be one of the most time-consuming provisions – with variations across Member States.

In the online survey carried out by Deloitte, authorities indicated that the **most time-consuming** tasks[249] were the following:

[247] Calculating the number includes the following steps: EUR 60.000 /12 months / 20 days / 2 = EUR 125.
[248] It is important to note that the frequency and cause of audits differs between the NIS context and the situation under the ePD. The impact assessment only considers investigations following notifications (thus not covering regular audits by authorities) and assumes that they only take place in 10 to 20 per cent of all cases.
[249] Authorities were asked to indicate how long it takes to deal the following tasks: Preventive audits of individual service providers to check whether service providers comply with the security obligations; Preventive audits of individual service providers to check whether service providers comply with their notification obligations; Audits of individual service providers based on complaints; Dealing with a personal data breach of one service provider (Article 4), including reviewing notifications and reacting; Sanctioning of individual service providers; Drafting or one new guidance document; Updating one existing

- Preventive audits of individual service providers to check whether service providers comply with the security obligations; and
- Preventive audits of individual service providers to check whether service providers comply with their notification obligations.

Individual data breach notifications also tend to be quite time-consuming, depending on the authority asked. The actual number of data breaches dealt with varies significantly per Member State.[250] The actual time spent depends very much on the Member State. Three authorities indicated that this takes less than one working day, four indicated that it takes between 1 day and less than a week and three authorities indicated that it takes 1 week or more.

As concerns the **appropriateness of these costs**, several stakeholders in the online survey and interviews pointed out that the efficiency may be hindered based on the interaction of the ePD with other instruments. More specifically, it was argued that there might be **too many reporting obligations under the various legislative acts** (GDPR, ePD, Network and Information Security Directive, Framework Directive), creating administrative burden, and in some cases the same incidents are reported to different authorities causing duplications.

5.5.3 Relevance

Key finding of the analysis: Partially relevant

There are doubts as to the relevance of all parts of this provision, notably because there are some overlaps with other legal instruments, in particular most of the provision overlaps with the GDPR. Stakeholders were most critical of Article 4(3), whereas there is some support to retain Article 4(1) and 4(2).

Below we examine the relevance of the security obligations by paragraph, showing that there are doubts as to the relevance of these provisions, in particular Article 4(3).

The usefulness of **Article 4(1) relation to the general security obligations** has been questioned by ENISA based on that Article 13a of the Framework Directive captures a broader obligation for the security and integrity of networks and services. Therefore, Article 4(1) does not add any new obligation for providers of publicly available electronic communications services.[251] In Deloitte's online survey with competent authorities, participants were more supportive of this provision: one third of the participants (10 out of 30) indicated that this provision is important or useful to retain "as is". Eleven indicated that it is important or useful to retain, but with changes. Only one authority indicated that this provision does not need to be retained. Similarly, BEREC states that these provisions may be retained in the ePD in spite of overlaps with the GDPR, but that there would need to be adjustments.[252]

guidance document; Developing recommendations on good practices; Delivering one training course on the application of the Directive; Organising an information campaign; Other, please specify.

[250] For example, in 2015, the highest number of complaints was reported for Ireland (2317), followed by the UK (550). Sweden (24), Greece (15), Estonia (5), Romania (3) and Belgium (1) followed with significantly less. Cyprus and Croatia reported that no breaches occurred. No information is available for the other Member States.[source?]

[251] ENISA (June 2016). *Working paper on the review of the ePrivacy Directive. Article 4 – Security of processing*, p. 13-15, p. 9.

[252] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133. http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive, p.3

There tends to be support among stakeholders to retain **Article 4(2) relating to the obligation of service providers to inform subscribers of security risks**. According to ENISA, this provision is relevant to keep also in light of the GDPR. Article 4(2) stresses the risk of loss of confidentiality (rather than risks related to unavailability of the service or the network). Such obligation is not part of the GDPR and specific to the electronic communications sector. BEREC states that these provisions may be retained in the ePD in spite of overlaps with the GDPR, but that there would need to be adjustments.[253] In Deloitte's online survey with competent authorities, participants were also supportive of this provision: almost one third of the participants (8 out of 30) indicated that this provision is important or useful to retain "as is". Eleven indicated that it is important or useful to retain, but with changes. Only three authorities indicated that this provision does not need to be retained.

Stakeholders tend to be most critical of **Article 4(3) relating to notifications of personal data breaches**. According to ENISA, this article is not really needed anymore with the coming into force of the GDPR. If it is kept, providers of publicly available electronic communications services would be subject to two different notification schemes, causing confusion without adding any higher levels of protection. This was also argued by van Hoboken and Borgesius and by some competent authorities interviewed by Deloitte. BEREC states that these provisions may be retained in the ePD in spite of overlaps with the GDPR, but that there would need to be adjustments.[254] In Deloitte's survey with competent authorities, participants were less supportive of Article 4(3) compared to Article 4(1) and (2). Only 17% (5 out of 30) indicated that this provision is important or useful to retain "as is". Eleven indicated that it is important or useful to retain, but with changes. Seven authorities (23%) indicated that this provision does not need to be retained. In the EC's public consultation, of the 341 respondents that replied to the relevant question, half (171) indicated that it is relevant, while the other half (170) indicated that it is not.

Article 4(4) and (5) relating to the possibility for competent authorities and the Commission to adopt guidelines/implementing measures may no longer be needed in light of Articles 31 and 32 on personal data breaches in the GDPR. Yet, it was also argued by ENISA that this depends also on the legal instrument that is chosen for the new ePrivacy regime.[255] We note that the question whether these provisions are still relevant is closely linked to the relevance of the other three paragraphs.

5.5.4 Coherence

Key finding of the analysis: limited coherence in the light of recent legal developments

While Article 4 works rather well with the Electronic Communications Package and the RED, there are several overlaps with the GDPR. Notably, the GDPR also contains rules on security and personal data breaches as laid down in Article 4(1)-(3) of the ePD. However, the GDPR is even more detailed in some aspects. On this basis, the coherence is proved to be limited.

[253] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133. http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive, p.3

[254] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133. http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive, p.3

255 ENISA (June 2016). Working paper on the review of the ePrivacy Directive. Article 4 – Security of processing, p. 13-15.

In the table below, we present the connection between the ePD and the GDPR, the Electronic Communications package and the RED. For each relevant provision[256] we provide a brief summary, using the following colour code[257]:

- Green: positive relationship (e.g. synergies);
- Grey: neutral relationship/no challenges nor positive aspects identified; and
- Yellow: potential challenges.

Further details are provided in Annex.

The table shows that the relationship with the GDPR is challenging, whereas the ePD and the Framework Directive work well together. There are interesting synergies with the Radio Equipment Directive, since radio equipment must be constructed with certain privacy and data protection requirements in mind.

Table 22 – Coherence of Article 4 with the GDPR, the Electronic Communications package and the RED

Provision in the ePD	Provision in the other instrument	Main findings
GDPR		
Security of Processing (Article 4.1 and 4.2)	- Principles relating to processing of personal data (Article 5) - Security of processing (Article 32)	Article 4 of the ePD does not "*complement and particularise*" the GDPR in relation to this provision. Indeed, it can be argued that the GDPR is more detailed than to the ePD.
Notification of personal data breaches (Article 4.3 and 4.4)	- Notification of a personal data breach to the supervisory authority (Article 33) - Communication of a personal data breach to the data subject (Article 34)	The procedures for personal data breaches vary considerably; thus, the same business may need to follow different procedures in case it offers electronic communications and other services
Electronic Communications Package		
Framework Directive		
Security of processing (Article 4.1 and 4.2)	Security and integrity (Article 13a.1 and 13a.2)	There is an overlap, but it is justified. The ePD particularises the provisions contained in the Framework Directive.
Security of processing (Article 4.3 and 4.4)	Security and integrity (Article 13a.3 and 13a.4)	There is an overlap, but it is justified. The ePD particularises the provisions contained in the Framework Directive.
Radio Equipment Directive		
Security of processing (Article 4.1 and 4.2)	Essential Requirements (Article 3.3)	A synergy exists wherein radio equipment must be constructed in such a way as to incorporate safeguards to protect the privacy and personal data of the user and subscriber, as set out in the ePD.

Source: Deloitte.

BEREC also comments on the specific rules on breach notifications (Article 4(1a), (3), (4) and (5) of the ePD)) in relation to the GDPR, highlighting that there are significant differences which may lead to confusion and an increased administrative burden.[258]

[256] We only list those instruments and provisions that a have connection to the ePD.
[257] The summaries and colour classification are to be seen as indicative.

Some further tendencies may be deduced from the EC's public consultation. The respondents were asked whether the security obligations of the ePD are coherent with the security requirements set forth in the following legal instruments:

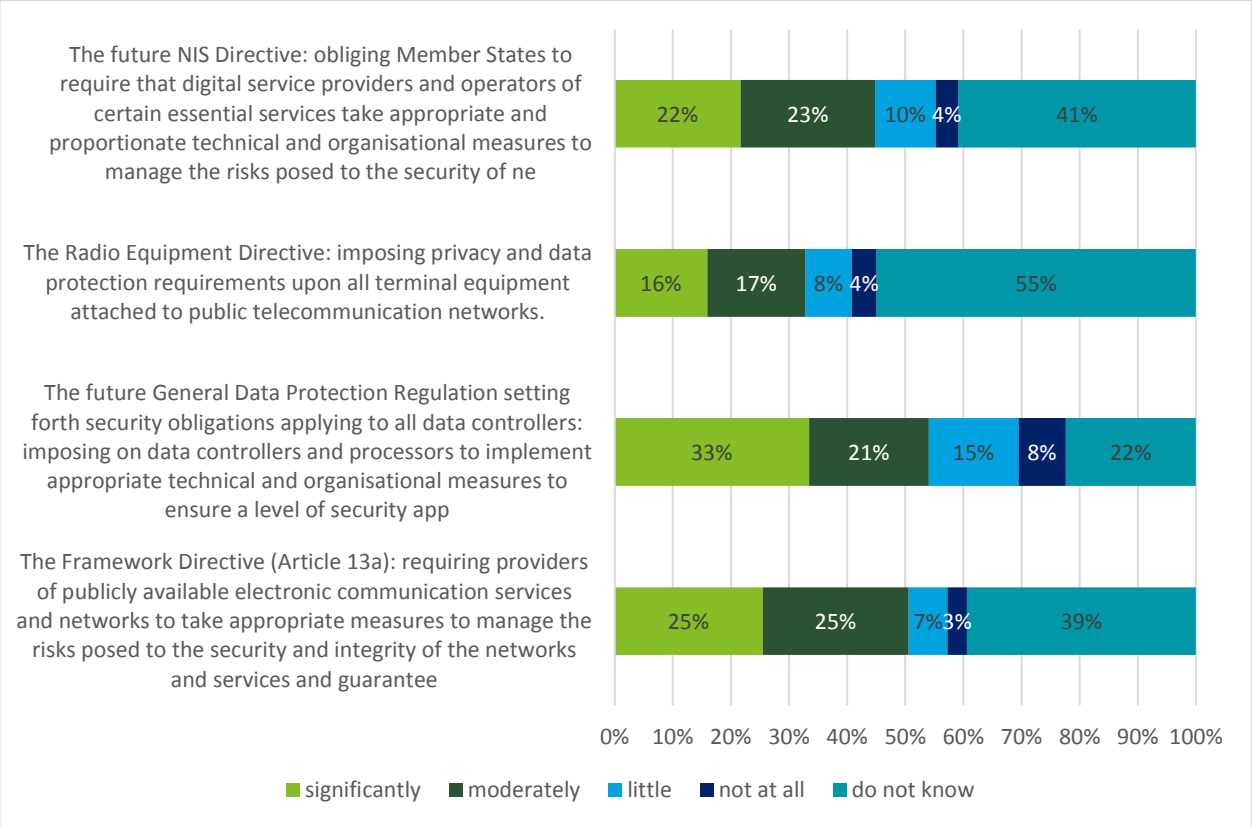
- The Framework Directive;
- The GDPR;
- The Radio Equipment Directive[259]; and
- The NIS Directive.

As shown in the figure below, the responses vary greatly and high shares of the respondents answered "Do not know" for each option. This makes it difficult to draw general conclusions in relation to the coherence. Yet, according to the results of the public consultation, a higher share of respondents consider the ePD to be "moderately" or "significantly" coherent with all of the relevant instruments, compared to those who stated that the ePD is only "little" or "not at all" coherent with the instruments mentioned. The highest share of respondents had an opinion in relation to the GDPR, with 33% of respondents stating that it is "significantly" coherent and 21% stating that it is "moderately" coherent. Roughly the same share of respondents had an opinion on the NIS Directive and the Framework Directive (around 60% provided an opinion on each of these two). Of these, the ePD was considered slightly more coherent with the Framework Directive (50% choosing "significantly" or "moderately" coherent) than the NIS Directive (45% choosing "significantly" or "moderately" coherent).

[258] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133. http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive, p.3

[259] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

Figure 16 – Coherence of security requirements of ePD with other legal instruments



Source: Deloitte based on EC public consultation.

5.5.5 EU added value

Key finding of the analysis: EU added value tends to be confirmed

Personal data and security breaches are not an issue that is bound by Member States' borders. Therefore, there is an added value of having a specific provision concerning the security of processing and notification of personal data breaches at the EU level. This was not denied by any of the stakeholders consulted.

As highlighted in section 5.4.5, in light of the establishment of the internal market there is a **need to address data protection, including in the electronic communications sector, at the EU level**.[260] Similarly, personal data and security breaches are not an issue that is bound by Member States' borders. Therefore, there is an added value of having a specific provision concerning the security of processing and notification of personal data breaches at the EU level.

However, no further specific information was identified with regard to the EU added value of this provision. At the same time, this means that none of the stakeholders consulted as part of this assignment declined an EU added value of this provision.

[260] Recitals (5), (6), (7), and (8) of Directive 95/46/EC; Recital (8) of the ePD.

5.6 Confidentiality of electronic communications (Article 5.1 and 5.2)

Article 5(1) and (2) aim at ensuring the right to **confidentiality of communications**.

Overview of the content

Article 5(1) obliges the Member States to put into place legislation prohibiting listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned.[261]

This also applies to web browsing and using online video services. Van Hoboken and Borgesius point out that "monitoring people's web browsing is thus only allowed after their consent."[262]

Article 5(2) clarifies that the need to safeguard the confidentiality of communications does not preclude any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice. This includes practices carried out for the purpose of providing evidence of a commercial transaction or of any other business communication. This provision is often designated as the "business exception"[263]

5.6.1 Effectiveness

Key finding of the analysis: Partially effective

While Article 5(1) and (2) supported the achievement of the objective to ensure confidentiality of communications, **some issues** that potentially act as barriers in this respect have been identified. In particular, our research shows that some stakeholders faced obstacles in the practical application of this provision. Such difficulties may arise because the wording of the provisions is not sufficiently clear and potentially not in line with recent technological developments, also leading to varying implementation across Member States. Another issue raised by many stakeholders relates to the general scope of the ePD: it was criticised that in many Member States the provisions only apply to traditional telecom providers, not to OTTs. On the basis of these issues, citizens cannot rely on equal standards on the confidentiality of communications.

Overall, the ePD has had a positive impact on the protection of the confidentiality of communications. This was, for example, highlighted by the competent authorities interviewed by Deloitte and is also reflected in Deloitte's online survey with competent authorities. Yet, a number of challenges hinder the effectiveness of this provision. In the public consultation, around half of the respondents indicated that they faced **problems in the practical application of the rules on the confidentiality of communications**.[264] A comparably high share of respondents from the group of industry (59%)

[261] Exceptions to these rules may be based on Article 15(1), e.g. relating to public security. Furthermore, "this paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality."

[262] Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 25.

[263] European Commission (2015). *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation.* Final Report, (https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data), p. 11.

[264] We note in this context that the public consultation asked about the functioning of the rules on the "confidentiality of communications". Thus, there was no differentiation between the rules on the confidentiality of communications (Article 5.1 and 5.2) and the rules on the confidentiality of information stored on the users' terminal equipment (Article 5.3). As both aspects are entitled "confidentiality of communications in the ePD, it is not clear which aspects respondents referred to.

indicated that they encountered problems. Fewer respondents from the group of public bodies (21%) indicated that they encountered problem.

Table 23 – Extent to which respondents encountered problems in relation to the rules on confidentiality of communications, per stakeholder group

Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	59,0%	26,3%	14,7%	156
Citizens & civil society	44,5%	33,5%	22,0%	173
Public bodies	21,1%	52,6%	26,3%	19
All replies	49,7%	31,3%	19,0%	348

Source: Deloitte based on EC public consultation.

Based on the online survey with businesses implemented as part of this project, the ePD's provisions regarding the confidentiality of information stored on the users' terminal equipment were a problem for ten of 16 businesses that indicated this particular provision is of practical relevance for them.

Some specific issues have been identified.

First, according to national enforcement authorities the **wording of the provisions is not sufficiently clear and potentially not in line with recent technological developments.** For example, 13 out of 29 (45%) of the competent authorities responding to Deloitte's online survey considered it a serious problem that it is not sufficiently clear what type of communications data is in scope. Another five authorities considered this as a moderate problem. In addition, eight out of 29 (26%) considered it a serious problem that the wording of this provision is not in line with modern technologies, while another eight considered this a moderate problem.

Ambiguity in relation to this provision was also raised by van Hoboken and Borgesius, who pointed out that "the broad formulation of article 5(1) could imply that Member States' positive obligations extend to services involved in electronic communications that are not publicly available electronic communications services in the strict sense of the ePD. Thus, Member States would have to ensure that nobody interferes with the confidentiality of communications and related traffic data flowing over public communications networks."[265] Indeed, according to the EDPS, the scope of this provision is broader than what is set out in Articles 1 and 3, covering not only public or publicly electronic communications services. This was considered a strength by the EDPS.[266]

It may be based on this ambiguity that Article 5 (and in particular its paragraph 2) has been transposed very differently by Member States with **some applying it only to the telecommunications sectors and others to all sectors**, e.g. registration of telephone conversations by call centres.[267]

On this basis, it should be noted that, although Article 5(1) obliges the Member States to put into place legislation to ensure the right to confidentiality of communications, **very important parts of consumers everyday communication means are excluded from the scope of the ePD** (see section 5.4.3). This was criticised by several stakeholders consulted as part of this study. Thus, if the

[265] Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 24.
[266] European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Proposal for a Directive on privacy and electronic communications', Brussels, (2008/C 181/01), 10 April 2008, par 33.
[267] European Commission (April 12, 2016). *Towards a future proof ePrivacy Legal Framework*. Minutes, p. 4.

right to confidentiality of communications regarding specific telecom services such as email (used by 46% of consumers every day according to Eurobarometer data [268]); OTTs for the purpose of instant messaging (e.g. WhatsApp; used by 41% every day), and online social networks (used by 38% every day) is not ensured, it can be argued that the effectiveness of Article 5(1) and 5(2) is hindered – at least in some Member States.[269]

Another point relating to the clarity of Article 5(1) was raised by the WP29. According to its position on the review of the ePD, the current phrasing of that provision has caused confusion because it refers to "communications and the related traffic data". [270] The connection between this provision and the specific provisions on traffic data (Article 6) may not be clear according to WP29. It further argues that the distinction between content and traffic data is no longer clear-cut.[271] This was also raised in Deloitte's online survey with competent authorities.

A final issue potentially hindering the effectiveness of Article 5(1) and (2) relates to the **awareness of citizens**. Interestingly, Eurobarometer data[272] also reveals that the majority of consumers assumes that, according to law:

- Instant messaging and online voice conversations are confidential and nobody can access them without consumers' permission (58% of consumers think this is case);
- Nobody can store information (e.g. cookies used to track you) on computers, smartphones or tablets without consumers' permission (58%); and
- Personal information (e.g. photos, calendar, history of calls) on computers, smartphones or tablets can only be accessed if consumers' have given permission (67%).

Consumers' assumption if related items are true or false are presented in Figure 17.

[268] Flash Eurobarometer 443 (2016): e-Privacy. Data on 26,526 consumers collected between 6 and 8 July 2016. At this stage, the Eurobarometer results are only of provisional character.
[269] The notable exception here is the usage of the Internet to make phone calls or video calls (e.g. via Skype or Facetime) which is only used by 8% of consumers every day according to Eurobarometer data.
[270] This is supported by the WP29. See: Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), Adopted on 19 July 2016 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf, p. 9.
[271] The WP29 explains that "Digital communication is governed by technical protocols that do not necessarily distinguish between the contents of communication and related traffic data. For example the http protocol prescribes the use of URL's that contain both elements of content (visited webpages which content can be read from the URL's anchor and parameters) and traffic data (host names)." This is supported by the WP29. See: Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), Adopted on 19 July 2016 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf, pp. 9-10.
[272] Flash Eurobarometer 443 (2016): e-Privacy. Data on 26,526 consumers collected between 6 and 8 July 2016. At this stage, the Eurobarometer results are only of provisional character.

Figure 17 – Consumers' assumptions concerning the scope of legislation regarding electronic communication

Source: Eurobarometer, graphical representation by Deloitte.

5.6.2 Efficiency

Key finding of the analysis: Tends to be efficient

This provision has led to significant costs for businesses, including the setting up of IT infrastructure. However, these costs can be considered proportionate in light of the aim of ensuring confidentiality of communications. We also note that some of these costs may overlap with the security provisions, in case the IT solutions to ensure security and confidentiality overlap.

Additional undue costs may ensue for businesses based on the ambiguous wording of the provision and the fact that its implementation varies significantly across Member States (cf. the previous sub-section). Such costs may in particular relate to legal advice.

Finally, there are opportunity costs as the provisions render certain business models invalid. These costs can be considered proportionate in light of the aim of ensuring confidentiality of communications.

As part of the online survey with businesses implemented for this project, some feedback in relation to the types of costs has been received, which is presented below.

Three businesses out of seven that answered the respective question indicated that the most significant problem concerning the confidentiality of communication is that they incurred costs to comply with the provisions due to which they encountered decreased turnover / profit of the business.

One business indicated that the one-off costs (CAPEX) per 100,000 subscribers are between more than 500,000 and 1 million Euro per year, while the recurring costs (OPEX) per 100,000 subscribers are between more than 100,000 and 500,000 Euro per year.

One business also indicated that costs linked to the ePD for them are higher than 1% of their business's total annual turnover.

For two businesses that answered the question, the most important cost elements concerning the confidentiality of communications relate to:

- Development / adaptation of technical infrastructure and / or software; and

- Costs for advisory services, e.g. concerning legal interpretation of provisions.

In addition, the only two businesses that answered the respective question regarding the confidentiality of communications indicated they would not have implemented these measures if it were not due to the ePD, e.g. to cope with general market or technological developments. These businesses also indicated that the costs have increased regarding the confidentiality of communications since the adoption of the ePD.

The **proportionality of these costs** in relation to the benefits achieved by this rule was addressed in the EC public consultation. In general, two thirds of the respondents from industry considered that the ePD had created additional costs for businesses. Nevertheless, the views of the different respondents groups are divided as to whether or not the costs of compliance with the ePD are proportionate to the objectives pursued, in particular the confidentiality of communications: A third of all respondents consider that these costs are proportionate and a third disagree. In the industry, the majority of respondents (65.3%) do not think that the costs are proportionate. However, the majority of citizens and the civil society (57.1%) as well as public bodies (72.7%) think they are proportionate. We note in this context that costs to set up IT infrastructure and supervisory mechanisms to ensure compliance with these provisions may be justified in light of the objective to ensure the confidentiality of communications and can, therefore, be considered proportionate. However, undue costs for businesses may arise based on the ambiguities of the wording of this provision and the fact that its implementation varies significantly across Member States, as outlined in the previous sub-section. Such undue costs may, for example, relate to legal advice (cf. also the results of Deloitte's online survey with businesses).

In interviews and the online survey with businesses conducted by Deloitte, some stakeholders indicated that there are **opportunity costs** as the provisions render certain business models invalid. For example, telecom providers indicated in interviews that ECS lose out on potential business activities and opportunities in possible Big Data services, in particular compared to providers of OTTs. It can be argued, however, that such restrictions may be justified based on the aim to ensure privacy for consumers.

5.6.3 Relevance

Key finding of the analysis: Relevance tends to be confirmed

Overall, the **relevance of specific rules on the confidentiality of communications tends to be confirmed**. This is in particular based on the fact that citizens regard this as an important issue, while no similar rules are contained in the in Directive 95/46/EC or the GDPR. However, the relevance of these provisions is weakened by its restriction to traditional telecom providers in most Member States.

Articles 5(1) and 5(2) have **no direct equivalent in Directive 95/46/EC or the GDPR**. The general data protection instruments do not refer to the prohibition of listening, tapping, storing, or otherwise intercepting communications and their related data. This is supported by several stakeholders interviewed by Deloitte as well as BEREC.[273] Similarly, the WP29 argues that ensuring confidentiality

[273] BEREC, in its response to the ePrivacy Directive questionnaire, argues that confidentiality of communication is one of the fundamental provisions of the ePD, and that Article 5 therefore remains relevant.

of communications is a key objective of the ePD and that it is still relevant to have a "general prohibition of the interception/surveillance/monitoring of the content of electronic communications". [274]

Also the respondents to the EC's public consultation were mostly supportive of the relevance of these provisions. More specifically, close to two thirds (61%) of all respondents indicated that there is an added value of having specific rules on the confidentiality of electronic communications for the electronic communications sector.[275] This view is in particular supported by citizens and civil society as well as public bodies (83% and 89% respectively). On the contrary, two thirds (63%) of the respondents from the industry did not consider that there is an added value of having specific rules on the confidentiality of electronic communications for the electronic communications sector.

Table 24 – Extent to which respondents see an added value in the rules on confidentiality of communications, per stakeholder group

Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	31,1%	63,4%	5,6%	161
Citizens & civil society	83,4%	9,9%	6,6%	181
Public bodies	88,9%	7,4%	3,7%	27
All replies	61,0%	33,1%	6,0%	369

Source: Deloitte based on EC public consultation.

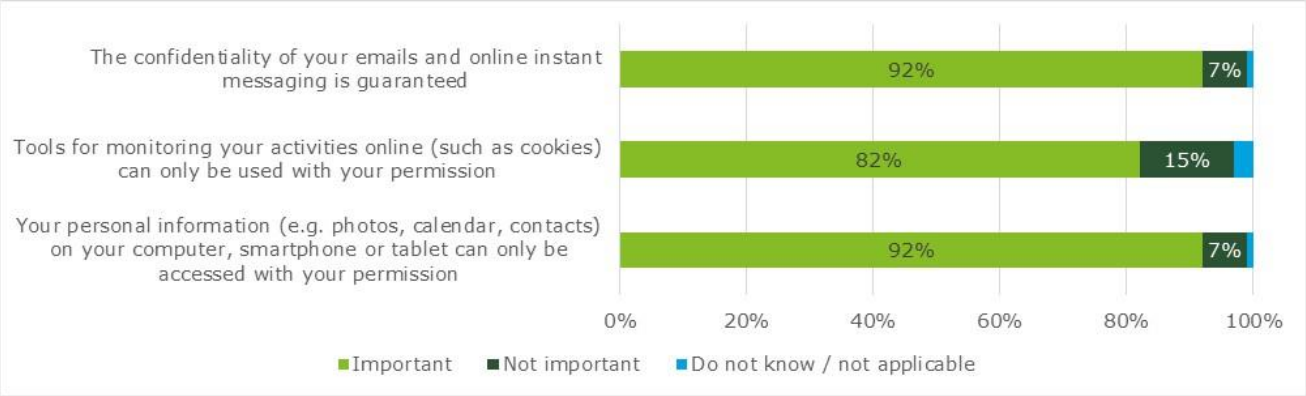
However, both BEREC and WP29 point out that the scope of Article 5(1) and (2) may be too narrow, possibly hindering its relevance. According to the WP29, users reasonably expect that confidentiality obligations apply to any communication provider. [276] BEREC highlights that the scope is not in line with recent technological developments, including new means of communications that bring new challenges in relation to privacy.[277] This point is related to the overall scope of the ePD, which is discussed in section 5.4.

This is supported by several stakeholders interviewed by Deloitte as well as the results of the Eurobarometer on ePrivacy.

The importance of guaranteeing the confidentiality of emails and online instant messaging for consumers supports this argument. Eurobarometer data shows that 92% of consumers find this important (72% 'very important', 20% 'fairly important'). Only 7% of consumers indicate that confidentiality of emails and online instant messaging is not important to them (see Figure 18).

[274] Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), Adopted on 19 July 2016 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf, p. 9.
[275] We note in this context that the public consultation asked about the added value of the rules on the "confidentiality of communications". Thus, there was no differentiation between the rules on the confidentiality of communications (Article 5.1 and 5.2) and the rules on the confidentiality of information stored on the users' terminal equipment (Article 5.3). As both aspects are entitled "confidentiality of communications in the ePD, it is not clear which aspects respondents referred to.
[276] Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), Adopted on 19 July 2016 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf, p. 9.
[277] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133 http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive p.5

Figure 18 – Importance of confidentiality and security of electronic communication services for consumers



Source: Eurobarometer, graphical representation by Deloitte.

Finally, according to Eurobarometer data, 90% of consumers think they should be able to encrypt their messages and calls, so they are only read by the recipient.

5.6.4 Coherence

Key finding of the analysis: Coherence tends to be confirmed

The external coherence of Article 5(1) and (2) can be confirmed, as no challenges have been identified. In contrast, while no similar rules are contained in the GDPR, there is a noteworthy synergy between the ePD and the Radio Equipment Directive, to the extent that the equipment covered by the latter must be able to support the safeguards for the protection of privacy and personal data set out by the ePD.

As concerns the internal coherence, some lack of clarity was identified in relation to other articles of the ePD, including Article 3 as well as Articles 6 and 9.

In the table below, we present the connection between the ePD and the GDPR, the Electronic Communications package and the Radio Equipment Directive. For each relevant provision[278] we provide a brief summary, using the following colour code[279]:

- Green: positive relationship (e.g. synergies);
- Grey: neutral relationship/no challenges nor positive aspects identified; and
- Yellow: potential challenges.

Further details are provided in Annex.

The table shows that there are connections to the GDPR and the Access Directive. In both cases, the instruments seem to work together without difficulties. There is also a noteworthy synergy between the ePD and the Radio Equipment Directive, to the extent that the equipment covered by the latter must be able to support the safeguards for the protection of privacy and personal data set out by the ePD.

[278] We only list those instruments and provisions that a have connection to the ePD.
[279] The summaries and colour classification are to be seen as indicative.

Table 25 – Coherence of Article 5(1) and (2) with the GDPR, the Electronic Communications package and the Radio Equipment Directive

Provision in the ePD	Provision in the other instrument	Main findings
GDPR		
Confidentiality of the Communications (Article 5.1 and 5.2)	- Principles relating to processing of personal data (Article 5.f)	No challenges have been identified.
Electronic Communications Package		
Access Directive		
Confidentiality of communications (Article 5)	Rights and obligations for undertakings (Article 4.3)	There is a connection between these provisions, but no challenges have been identified.
Radio Equipment Directive		
Confidentiality of communications (Article 5)	Essential Requirements (Article 3.3)	A synergy exists wherein radio equipment must be constructed in such a way as to incorporate safeguards to protect the privacy and personal data of the user and subscriber, as set out in the ePD.

Source: Deloitte.

In its analysis of the external coherence of the ePD, BEREC[280] points out that while the GDPR applies to all processing of personal data by automated means, it is not specifically designed to protect fundamental rights (e.g. privacy) in relation to unstructured data in transit, i.e. information being transmitted on an electronic communications network. Therefore, the application of the GDPR is limited to information that can be directly or indirectly related to a natural person. This excludes other types of information, such as information relating to legal persons or unidentifiable persons.

The ePD, on the other hand, particularises and complements the GDPR as it is designed to protect other fundamental rights (e.g. confidentiality) in relation to unstructured data in transit, i.e. information being transmitted on an electronic communications network. This goes beyond the remit of the GDPR, which applies to all processing of personal data by automated means, excluding legal persons.

This follows from Recitals 2 and 3 of the ePD and according to Article 1(1), the ePD aims to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to both privacy and confidentiality. This is further emphasised by Article 1(2), according to which the ePD also aims for protection of the legitimate interests of subscribers who are legal persons.

The principle of confidentiality of communications is closely linked to Article 7 of the Charter, according to which everyone has the right to respect for his or her private and family life, home and communications, as well as Article 8(1) of the European Convention on Human Rights (ECHR). Confidentiality of communications can be crucial to ensure other fundamental rights and freedoms, such as privacy, the right to freedom of expression and the right to private property.

BEREC emphasises that while the GDPR adequately protects the right to protection of personal data, it cannot fully achieve the objective of ensuring confidentiality of communications as it has a wider scope.

[280] BEREC (2016) 'BEREC Response to the ePrivacy Directive questionnaire', BoR (16) 133 http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive p.5

In relation to the **internal coherence** (i.e. between the different provisions of the ePD), BEREC also points to a lack of clarity among its members over the application of article 5 vis-à-vis article 3. The former could be interpreted as covering all services provided over an ECN (including all OTT services), and the latter could be seen as applying to only ECN/S[281].The public body suggest that the confidentiality rule should apply to all communication services provided over ECS / ECN (in other words, services/apps that provide communications between a finite number of persons or parties by electronic means), regardless of the underlying technology[282]. This was also raised by the stakeholders consulted as part of this study. Furthermore, some businesses and competent authorities indicated that the separation between Article 5(1) and (2) via-a-vis Articles 6 and 9 causes confusion, as the separation between communication data and traffic/location data is not always clear cut.

5.6.5 EU added value

Key finding of the analysis: EU added value confirmed

As communications are not bound by borders, a clear EU added value of harmonised rules on the confidentiality of communications can be seen. This is supported by the stakeholder consultations carried out as part of this project and the EC's public consultation.

Article 5(1) and (2) aim at ensuring the right to confidentiality of communications across the EU, by introducing harmonised standards. It can be argued that this cannot be achieved by Member States alone, as communications are not bound by borders (in particular within the internal market) and Member States' standards on this varied before the introduction of the ePD. The EU added value of these provisions is supported by the stakeholder consultations carried out as part of this project and the EC's public consultation. The results of the latter are presented in detail below.

As part of the Commission's public consultation, stakeholders were queried concerning the necessity of EU rules to ensure an equivalent level of protection (full protection) across the EU regarding the right to privacy and confidentiality with respect to the processing of personal data in the electronic communications sector. A statistical overview of the responses is provide below.

Table 26 – Necessity of EU rules to ensure an equivalent level of protection (full protection) across the EU regarding the right to privacy and confidentiality

	Yes	No	No opinion	Yes	No	No opinion	Nr. of responses
Industry	56	102	3	35%	63%	2%	161
Citizens & civil society	167	12	6	90%	6%	3%	185
Public bodies	27	3	0	90%	10%	0%	30
Total	250	117	9	66%	31%	2%	376

[281] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133 http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive p.10

[282] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133 http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive p.2

Source: EC public consultation, tabulation by Deloitte

Overall, 376 responses were received regarding this question. Two thirds of respondents indicated that EU rules are necessary to ensure this objective while close to the other third indicated the opposite (31%). Interestingly, almost all respondents did have an opinion on this question (only 2% did not have opinion).

Analysing the responses received in more detail, the data shows that citizens and civil society organisations, as well as public bodies are heavily supporting EU rules on the right to privacy and confidentiality (90% each confirmed the necessity of the rules). Of all positive responses, 67% were provided by citizens and civil society organisations, 22% came from the industry, and 11% from public bodies.

A more detailed look at responses received from the industry shows, however, that 63% are not in favour of EU rules to ensure an equivalent level of protection across the EU regarding the right to privacy and confidentiality while 22% replied positively. 2% of businesses did not have an opinion on this

In addition, the Commission's public consultation asked stakeholders if the Directive has proven to have a clear EU added value to achieve the following objectives:

- Increasing confidentiality of electronic communications in Europe; and
- Harmonising confidentiality of electronic communications in Europe.

Overall, the following feedback was received from industry, citizens and civil society organisations, as well as from public bodies.

Table 27 – Respondents' agreement with the EU added value of rules regarding increasing and harmonising confidentiality

	Strongly agree	Agree	Disagree	Strongly disagree	Do not know	Total
Increasing confidentiality	39	138	78	44	42	341
Harmonising confidentiality	40	125	90	39	50	344
Total	79	263	168	83	92	685
Increasing confidentiality	11%	40%	23%	13%	12%	100%
Harmonising	12%	36%	26%	11%	15%	100%
Total	12%	38%	25%	12%	13%	100%

Source: EC public consultation, tabulation by Deloitte.

The table above shows that the majority of respondents (strongly agree) that the Directive has proven to have a clear EU added value in relation to both increasing and harmonising confidentiality in the EU. However, the proportion of respondents that do not agree is comparatively large (37% overall).

Therefore, it is important to look at the distribution of responses counting out those that did not have an opinion on this subject. Albeit the overall result – responses agreeing that the rules have an added value in relation to both increasing and harmonising confidentiality – the difference between both in terms of respondent shares decrease when respondents that do not have an opinion are not counted. This is presented in the table below.

Table 28 – Respondents' agreement with the EU added value of rules regarding confidentiality

	Agree	Disagree	Total
Increasing confidentiality	59%	41%	100%
Harmonising confidentiality	57%	43%	100%
Total	57%	43%	100%

Source: EC public consultation, tabulation by Deloitte.

5.7 Confidentiality of information stored on the users' terminal equipment (Article 5.3)

Article 5(3) of the ePD aims to ensure the **confidentiality of information stored on the users' terminal equipm**ent, in particular by increasing awareness and empowering users.

Overview of the content

This provision applies to applications that access information on users' devices (e.g. laptops, smartphones), such as traffic and location data or contact lists. For instance, Article 5(3) regulates the use of third-party tracking cookies. The provision requires that such technologies may only access the users' devices upon prior and informed consent. This requirement stems from the revision of the ePD in 2009.[283]

5.7.1 Effectiveness

Key finding of the analysis: Partially effective

Based on our findings, there is **room for improvement as concerns the effectiveness of this provision**. Although some strengths have been identified, several challenges were raised by various stakeholders and in the literature. These include in particular ambiguities in relation to the scope of this provision, the fact that the scope may be too broad, limited transparency and effectiveness of the consent mechanism as well as difficulties relating to enforcement. Based on these challenges, this provision is burdensome for businesses, while the effective added value for citizens may be improved.

The overall assessment of this provision by businesses and competent authorities shows that the provision is not fully effective. Based on the online survey with businesses implemented as part of this study, the Directive's provision regarding the confidentiality of information stored on the users' terminal equipment was a problem for ten of 16 businesses that indicated this particular provision is of practical relevance for them. Competent authorities responding to Deloitte's online survey were also critical of this provision. No respondent assessed the overall functioning of Article 5(3) as "excellent" or "very good" and only three out of 30 (10%) indicated that it functions "good". Most respondents indicated that Article 5(3) functions "fair" (13 or 43%) and another three assessed its functioning as "poor".

Some specific issues are discussed below around the following themes:

[283] Recital 24 of ePrivacy Directive.

- Scope of this provision;
- The consent mechanism; and
- Enforcement.

> **Cookies** are a "short alphanumeric text which is stored (and later retrieved) on the data subject's terminal equipment by a network provider". For instance, they are used for memorising preferences, storing session information or identifying a data subject through a unique identifier.[284]

Considering the **scope** of Article 5(3), it may be considered a strength that the article is phrased in a technologically neutral way. Although this provision is often referred to as the **"cookie law"**, it is applicable not only to cookies but also to **any other technology used to store or gain access to information** stored in individuals' technical equipment (spyware, malware, etc.).[285] Indeed, "Article 5(3) applies to anyone that stores or accesses information, such as a cookie, on a user's device, including if no personal data are involved."[286] This includes, for example apps accessing information on a user's smartphone, such as location data or a user's contact list or parties that want to secretly store spyware on a user's device.[287]

However, it has been raised by different stakeholders that despite this neutral formulation, **not all relevant techniques may be covered** by Article 5(3). According to some stakeholders, there is at least a lack of clarity relating to the coverage of some techniques, hindering its effectiveness. Examples of aspects that are not explicitly covered include **Wi-Fi tracking, near field communication (NFC), and Bluetooth**.[288]

Furthermore, there is ambiguity with regard to the coverage of certain other practices. For example, some techniques for tracking browsing activities, e.g. **device fingerprinting**, may not be caught by this Article.[289] However, in relation to fingerprinting, the Article 29 Working Party has clarified in its opinion that Article 5(3) of the ePD shall apply. Closely related to this, in a workshop the Commission held with competent authorities it was criticised that the provision does not prevent unlimited tracking.[290].

In addition, a lack of clarity in relation to the coverage of **ad blocker detectors**, installed by e.g. online newspapers, to give access to their site including the advertising, was pointed out in the workshop with competent authorities. In this context, the Commission has confirmed that such technologies do in fact breach the ePD, as they work by storing a script on the user's device.[291]

Furthermore, some national competent authorities and other stakeholders consider **the scope too broad**.[292] For example, some stakeholders have argued that the provision should not cover technologies that are not privacy invasive. Currently Article 5(3) contains two exceptions where prior

[284] Ibid, p. 6.
[285] Article 29 Data Protection Working Party (2010). *Opinion 2/2010 on online behavioural advertising*, 00909/10/EN, WP 171, p. 8.
[286] Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 27.
[287] Ibid, para. 27.
[288] Ibid, p. 1.
[289] European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, p. 5.
[290] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 2.
[291] DLA Piper (2016). *EUROPE: Does the use of ad-blocker detectors breach the e-Privacy Directive?*, (http://blogs.dlapiper.com/privacymatters/does-the-use-of-ad-blocker-detectors-breach-the-e-privacy-directive/).
[292] Cf. e.g. European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 1.

consent of the user is not needed. According to the 2015 study on the ePD[293], these exceptions are not sufficient. For example, cookies that are exclusively used for website usage statistics **("first party analytics cookies")** should not require consent, as recommended by the Article 29 Working Party. Dutch legislation, for instance, already includes such an exemption.[294] In another stakeholder workshop organised by the Commission in 2016, there was high support for a **categorisation of different types of cookies.**[295] On the other hand, some stakeholders argue that consent should also be given on the **integration of third party components** into services (e.g. social media buttons, analytics) or equipment (e.g. sensors in smart devices), which may access to information of the user.[296] It was also raised in interviews with businesses that the advertisement industry is heavily affected by this provision, in particular as it does not distinguish between different types of cookies.

Statistics on the type of cookies actually used

The 2014 "Cookie Sweep" analysis initiated by the WP29 and carried out in eight Member States[297] found that **the majority of the cookies are persistent third-party cookies**. In the Cookie Sweep, 16555 cookies were recorded on 478 sites, 70% of which were third-party cookies. 86% were persistent cookies and 14% were session cookies. In addition, it was found that 74 out of 474 websites only used first party cookies. In addition, 15 out of 474 only used session cookies (first and third party).[298] More detailed information is portrayed in section 3.5.3.

Turning to the **consent mechanism** established by Article 5(3), it may in general be considered a strength that users are given a choice about information stored on their terminal equipment. However, several issues hindering the effectiveness of this mechanism have been identified.

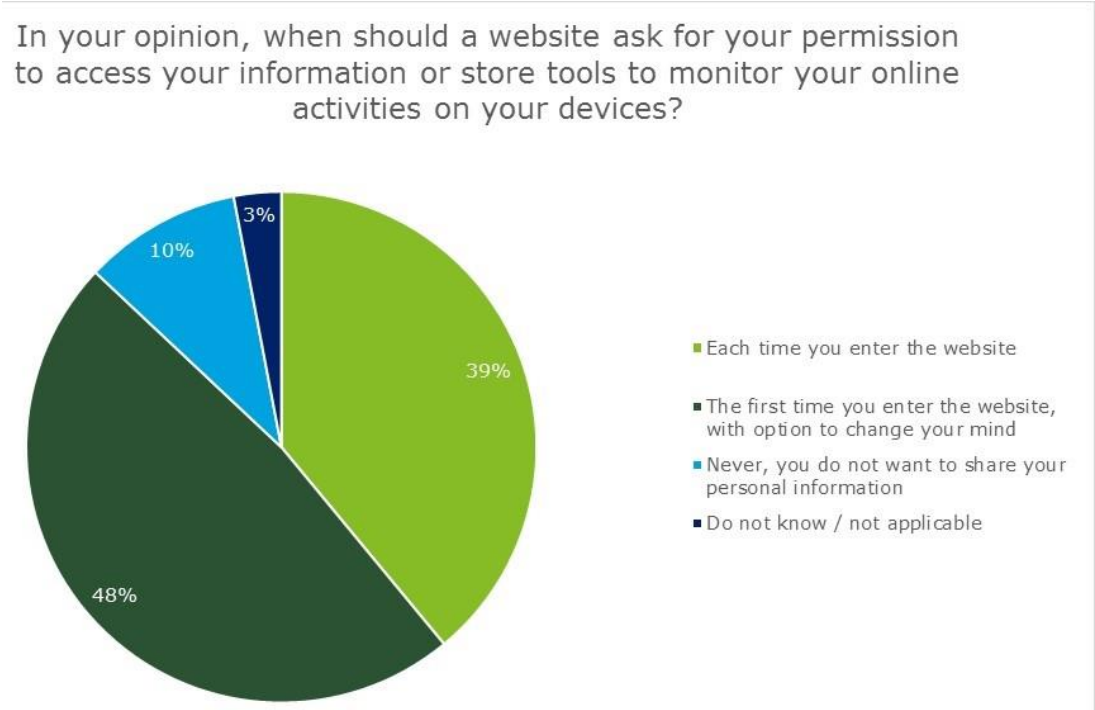
One point of criticism relates to the **transparency of the consent mechanism.** More specifically, there are often no transparent tools to withdraw or manage consent. User may currently not be well informed, e.g. by showing a well-known icon when giving consent, as was suggested by one competent authority in a meeting with the Commission in 2016. The authority argued that this would make it easier for users to block third party cookies in the browser.

In addition, there seems to be a lack of clarity in relation to the **modalities of giving consent and the information that should be given to the users**.[299] Indeed, for some users and subscribers it may not be clear that giving mere consent can provide a justification to comprehensively track their behaviour in the online environment ("profiling").[300] On this basis, giving consent might trigger that users get a false sense of protection.[301] Similarly, it was pointed out at the workshop the Commission held with competent authorities that there is a danger of an information overload and too much complexity.[302]

[293] ePrivacy Study SMART 2013/0071.
[294] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15039), p. 8.
[295] European Commission (April 12, 2016). *Towards a future proof ePrivacy Legal Framework*. Minutes, p. 10.
[296] Ibid, p. 9.
[297] CZ, DK, FR, GR, NL, SI, ES, UK.
[298] Article 29 Data Protection Working Party (2015), Cookie Sweep Combined Analysis – Report, WP 229.
[299] European Commission (2015). *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*. Final Report, (https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data), p. 13.
[300] Ibid, p. 13.
[301] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15039), p. 8.
[302] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 1.

Additional issues have been identified in relation to the possibility to express prior informed consent to processing of information via **the configuration of browser settings**. Initially, this possibility led to uncertainty.[303] Furthermore, the effectiveness of fending off cookies via browser settings may be hindered. In particular, default browser settings do not provide the consumer with a granularity of choice and it may only work in 10% of app cases.[304] As concerns the **citizens' perspective** on the consent mechanism, the Eurobarometer 443 on eprivacy showed that more than half of EU consumers (58%) assume that according to the law, nobody can store information (e.g. cookies used to track you) on their computer, smartphone or tablet without their permission (see Figure 17). However, consumers seem to be in undecided with regard to the question *when* a website should ask for their permission to access their information or store tools to monitor consumers' online activities on their devices. While 48% have indicated that a website should ask for their permission the first time consumers enter the website (with an option to change their minds later), 39% indicated that a website should ask for their permission each time they enter the website (please see also the pie-chart below).

Figure 19 – Consumers' preferences with regard to the timing of websites asking for permission to access information or store tools



Source: Eurobarometer443 on ePrivacy, graphical representation by Deloitte.

Finally, critics argue that the provision does not ensure that users have a real choice when it comes to cookies. Although users seemingly have a choice, they are in fact sometimes **not able to access the content of a website** if consent to the use of cookies is not given.[305] This is particularly critical if they are **really in need of the requested service (e.g. a website with health or traffic jam information)**

[303] European Commission (2015). *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*. Final Report, (https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data), p. 12.
[304] European Commission (April 12, 2016). *Towards a future proof ePrivacy Legal Framework*. Minutes, p. 11.
[305] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 2.

resulting in *de facto* "market power" of website providers.[306] On this basis, the confidentiality of information stored on users' terminal equipment may be safeguarded. However, users arguably do not have a real choice if the use of certain websites depends on their consent to cookies.

Another hindering factor relates to the **enforcement** of the rules. For example, during the meeting the Commission held with competent authorities in 2016, participants pointed out that the varying enforcement in the Member States has resulted in an **unequal level playing field and market distortions**. Some Member States enforce the article focusing only on privacy-intrusive cookies (tracking cookies) instead of covering all relevant aspects according to the ePD. There is room for manoeuvre whether the use of cookies with low risk to threat privacy should depend on consent or whether they should rather be set by default.[307]

Based on these issues relating to the scope, the consent mechanism and enforcement, competent authorities interviewed by Deloitte pointed out that this provision causes an **unnecessarily high burden for businesses, while the usefulness for citizens is not optimal**.

5.7.2 Efficiency

Key finding of the analysis: Partially efficient

The efficiency of Article 5(3) is not fully ensured. This is due to the fact that this provision tends to be the main cost factor associated by businesses with the ePD, while not all the costs appear to be justified and the benefits for citizens have been questioned. In particular, based on the ambiguities relating to the scope and consent mechanism, businesses may spend more time than needed on implementing the consent mechanism and possibly need to invest in legal advice. Furthermore, based on the fact that Article 5(3) does not make a distinction between different types of cookies, businesses that only use non-privacy invasive cookies also need to obtain consent. At the same time, users feel annoyed by the consent mechanism, which often does not provide a real choice.

Considering the **business perspective**, in the public consultation as well as interviews and an online survey with businesses conducted by Deloitte, several stakeholders highlighted that Article 5(3) is in fact the main cost factor relating to the ePD. As concerns the exact costs for businesses, the estimates vary widely. According to a 2014 study conducted by ITIF the **average compliance costs would be around €900** per website/company, although the calculation of such costs is not demonstrated.[308] The ITIF study indicated that these costs included costs for legal advice, updates to privacy policies, and technical updates to websites and would be incurred once per website, i.e. at the time of the introduction of the new policy.[309] This study was indeed cited by different stakeholders consulted as part of this initiative, implying that this estimate is considered realistic by these

[306] Ibid, p. 8.
[307] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 2.
[308] The Information Technology & Innovation Foundation, Daniel Castro and Alan McQuinn, "*The Economic Costs of the European Union's Cookie Notification Policy*", November 2014 (US).
[309] The study also indicated that there could be additional recurring costs for maintenance. For instance, some companies customise their website's cookie policies to each user's preference. It is explained that these costs could lie between a few hundred or tens of thousands dollars annually per website. However, such costs are not directly based on the ePD and are, therefore, not considered further at this point.

stakeholders.[310] However, there were also a few stakeholders that indicated that compliance costs would be significantly higher or lower.

Important clarification regarding the estimate for the average compliance costs

The figure of 900 Euro of compliance costs needs to be understood as an average value across all size classes of businesses, across all industries, and across all Member States. It is only an average, i.e. not a median value or a fixed value that all businesses incur in any case.

Quite naturally, differences exist between smaller and larger businesses, as well as between businesses in different industries and Member States – a small nationally operating start-up for instance has different costs than a global IT enterprise. This is due to the differences in their websites' complexity, as well as the operations behind administrating the respective website.

Therefore, it is by no means a contradiction if stakeholders indicated that compliance costs would be significantly higher or lower than the 900 Euro.

For instance, an internet content provider replying to the public consultation indicated that the costs to implement the cookie banner would be relatively small and could be similar to the annual costs of hosting a website. A large IT hardware and network systems company reported significantly higher annual costs: they estimate annual costs for a cookie opt-out tool of ca EUR 280,000, and additional costs of ca EUR 70,000 for a trained resource. An online retailer estimated that the costs relating to the implementation of the cookie banner lie around 1150 Euro per website. However, additional costs occur to deal with customers who complain about seeing the banner even after consenting (e.g. because they clear their browser history or move to a new browser). Some more detailed case examples relating to costs for the cookie provision are provided in the text boxes below.

Case example Art. 5(3): Costs of cookie consent for a browser provider

The representative of one of the major browser providers indicated as part of an interview that the ePD is relevant to the company due to its provisions concerning the cookie consent (Art. 5.3) and unsolicited communication (Art.13).

While it was not possible to estimate costs quantitatively in absolute terms (i.e. in terms of Euro), it was still possible for the interviewee to indicate that costs related to ePD are **<0.1%** of the company's annual turnover while costs related in general to data protection account for more than 1% of the annual turnover.

This means, in other words, that the costs related to the ePD can be expected to be less than one tenth of the overall costs of data protection for the browser provider. Thus, it was argued in qualitative terms, the costs related the ePD are negligible for this particular business.

Case example Art. 5(3): Costs of cookie consent for an IT hardware and network equipment manufacturer

A large-scale hardware and network equipment manufacturer that is active at the global level has

[310] For example, eleven participants to the public consultation mentioned this study in relation to the costs for businesses stemming from the ePD. However, we note in this context that six of these were associated with the Interactive Advertisement Bureau IAB. Others included businesses or citizens.

reported that they are affected by the provisions of Art 5(3) to a sizeable extent. The company's websites use cookies, which is why they need to comply with Article 5(3). Costs stem from the need to integrate and maintain cookie notification tools on their websites.

More specifically, as part of the interview, the company representative indicated that *annual* license costs of around EUR 280,000 are incurred for a software that governs their global cookie banner solution. It was also reported that this number is dependent on the number of actual visitors of the website. This means that the more visitors a website has, the higher the price for the software license.[311] In addition, the representative indicated that one trained full-time resource is required to administer the tool, adding annual costs of approximately EUR 70,000.

In addition, the business also indicated that an additional 77,600 EUR can be expected to be incurred in relation to general work and management of the company's privacy core team (48,000 EUR[312]), as well as the maintenance of the system (28,800 EUR[313]).

Thus, the overall annual value of compliance costs for the global IT hardware and network equipment manufacturer is around 430,000 EUR.

This means that the annual costs of cookie consent for an IT hardware and network equipment manufacturer exceed the estimate used for the quantitative model by far. Although this may be an extreme example, it can reasonably expected that other companies operating at a global scale incur similar annual costs. Such an estimate serves to balance the general applicability of the 900 EUR estimated by ITIF for website compliance towards specific types of businesses.[314]

Case example Art. 5(3): Breakdown of the costs of the compliance with online privacy regulations for an IT hardware and network equipment manufacturer

In addition to the overall estimate of 430,000 EUR incurred annually by a large-scale IT hardware and network equipment manufacturer that operates at the global level, the business has also tried to break down these costs and compare them with those incurred by an "average small business".

The feedback received shows that the compliance costs with regard to Art.5(3) are less than 0.01% of the annual revenue generated through online applications and advertisement of partner companies, while for an "average small business" the costs are expected to be at 0.02% of the annual revenue. This means that, in relative terms, average small businesses are expected to incur twice as much costs in respect of their revenue than global enterprises (economies of scale).

The following example has been provided:

	Annual online revenue	Costs for ePrivacy	% of revenue
"Average SME"	EUR 5,000,000[315]	EUR 1,000	0.02%

[311] A practical example of such a cookie consent software is: https://www.ensighten.com/
[312] 10 employees meeting bi-weekly (i.e. 24 times per year) for two hours at an hourly rate of 100 EUR.
[313] 2 employees working on system maintenance at an average hourly rate of 50 EUR solving, on average 3 "system bugs" per month (i.e. 36 per year) that take on average 8 hours to fix each.
[314] In fact, the 900 EUR may be appropriate for the majority of businesses that make use of smaller, lean websites as their operations and budget do not allow for a large-scale web presence. It seems, however, there are different types of businesses and particular size classes for which the 900 EUR does not seem to be a fitting assumption.
[315] The average annual revenue of a small business with a website is $5.03 million. See: https://www.entrepreneur.com/page/216022

Global enterprise	EUR 1,000,000,000	500,000	0.05%

Case example Art. 5(3): Companies with cross-border operations in general

As part of the interviews carried out, a business association representing the digital economy indicated that large member companies with cross-border operations incur aggregated compliance costs ranging from 10,000 EUR to 700,000 EUR. This estimate was provided not as a *per annum* value but as an overall value per business.

The business association itself has incurred 4,000 EUR to 6,000 EUR to implement its cookie banner solution. In view of the 900 EUR estimate by ITIF, the estimate by the business association could also be a benchmark for the costs incurred by SMEs.

Such an estimate serves to balance the general applicability of the 900 EUR estimated by ITIF for website compliance towards specific types of businesses.

Case example Art. 5(3): Costs incurred by online publishers

As part of the interviews carried out, business associations in the area of newspaper and online publishing (digital news and media content) have indicated that their members can be reasonably expected to incur up to 120,000 EUR of initial compliance costs to set up a cookie banner on their website and related technical changes.

In addition, the total maintenance costs add 80,000 EUR to 130,000 EUR to this initial investment.

Thus, according to this information, businesses in the publishing industry incur a total amount of between 200,000 EUR and 250,000 EUR (i.e. not per annum but over time) for the compliance of their websites with Art. 5(3).

Such an estimate serves to balance the general applicability of the 900 EUR estimated by ITIF for website compliance towards specific types of businesses.

Costs incurred by businesses relating to Art. 5(3) have been estimated by Deloitte together with costs due to Art.13. Thus, only an overall amount is available. The most important quantitative findings in this respect (i.e. concerning the compliance costs for businesses stemming from both Art. 5(3) and Art. 13) are presented in section 6.2.2 (Table 57). The table contains quantitative results of the economic analysis for the REFIT exercise:

- Number of businesses affected (in million)
- Compliance costs (in million Euro)
- Average compliance cost per business (in Euro)
- Administrative burden (in million Euro)
- Average costs from admin. burden per business (in Euro)

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises. A detailed explanation of the underlying assumptions and the model used to estimate these compliance costs are provided in Annex A.

As shown in the examples above and Deloitte's analysis, some businesses do incur significant **compliance costs** in relation to this provision. It was, furthermore, pointed out by the businesses and business associations consulted as part of this study that **opportunity costs** occur. For the businesses complying with this provision and the advertisement industry, opportunity costs may, according to the interviewees, be based on the dissuasive effect on users, who may stop using the services of a websites. The fears of users may not always be legitimate, as also websites using non-privacy invasive cookies need to install a consent mechanism. Especially, small or medium sized businesses referred to the opportunity costs that they experienced due to the cookies provisions which threatens their business potentials. They experienced loss of revenue as they lose users and it is too costly for them to obtain consent.

Based on the shortcomings identified in relation to the effectiveness of this provision (see section 5.7.1), **not all these costs appear to be justified**. Notably, based on the ambiguities relating to the scope and consent mechanism, businesses may spend more time than needed on implementing the consent mechanism and possibly need to invest in legal advice. Furthermore, based on the fact that Article 5(3) does not make a distinction between different types of cookies, businesses that only use non-privacy invasive cookies also need to obtain consent. Based on the 2014 Cookie Sweep, 74 out of 474 websites only used first party cookies. In addition, 15 out of 474 only used session cookies (first and third party).[316]

Turning to the **perspective of the user**, there may be a risk that users are overburdened with giving consent in situations where it is not absolutely necessary.[317] This is closely related to the critique that the article does not contain sufficient exceptions. In addition, frequent consent mechanisms, such as banners on websites, might disrupt the users' Internet experience according to the advertising industry.[318] Furthermore, it was pointed out in the previous sub-section that the effectiveness of the cookie banner is hindered, in particular because the consent mechanism may not be sufficiently transparent and users do not have a real choice as access to services is typically denied if they do not consent to cookies. As the benefits for users are limited, it can be argued that the high costs for businesses are not justified.

5.7.3 Relevance

Key finding of the analysis: Relevance tends to be confirmed

From the perspective of citizens, it may be argued that the provisions are **relevant to safeguard the privacy of users.** We also note that this provision does not have any legal equivalent in other instruments. The relevance is also supported by the competent authorities responding to Deloitte's online survey. However, while Article 5(3) is considered important to retain, the content is not considered to be fully in line with businesses' and consumers' needs. In particular, as shown in the previous sub-sections, based on the ambiguities relating to the scope and consent mechanism, the implementation is burdensome for businesses with limited added value for citizens.

[316] Article 29 Data Protection Working Party (2015), Cookie Sweep Combined Analysis – Report, WP 229.
[317] European Commission (April 12, 2016). *Towards a future proof ePrivacy Legal Framework*. Minutes, p. 6.
[318] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 2.

From the perspective of citizens, it may be argued that the provisions are **relevant to safeguard the privacy of users**: As indicated in the Background paper to the EC's public consultation[319], citizens may have very **sensitive information in their smart phones and computers**, and thus they can be considered as a part of their privacy sphere, which must be protected.

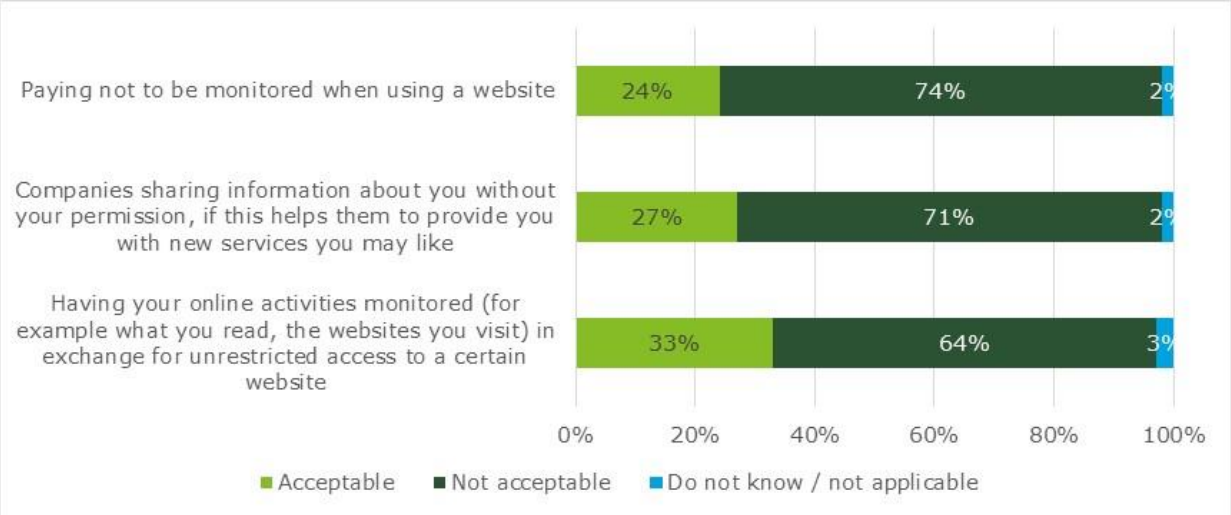
This is confirmed by Eurobarometer data.[320] It can be seen that 60% of consumers use the Internet to browse online every day with an additional 14% using it a few times a week (see Figure 14 in section 5.4.3).

However, for the majority of EU consumers according to Eurobarometer data, it is not acceptable for consumers:

- To have their online activities monitored (for example what they read, the websites they visit) in exchange for unrestricted access to a certain website; and
- That companies share information about them without their permission, if this helps them to provide consumers with new services they may like.

The detailed Eurobarometer on ePrivacy results in this respect are provided below.

Figure 20 – Users' action to ensure confidentiality of the information stored in their terminal equipment

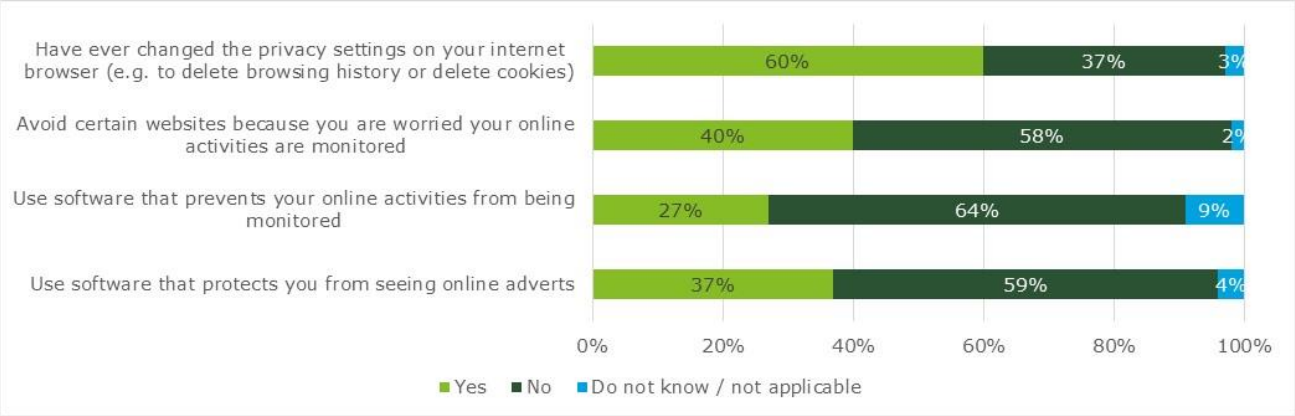


Source: Eurobarometer, graphical representation by Deloitte.

Consumers also actively take measures to ensure the confidentiality of information stored on their terminal equipment (see Figure 21).

[319] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15039), p. 8.
[320] Flash Eurobarometer 443 (2016): e-Privacy. Data on 26,526 consumers collected between 6 and 8 July 2016. At this stage, the Eurobarometer results are only of provisional character.

Figure 21 – Users' action to ensure confidentiality of the information stored in their terminal equipment

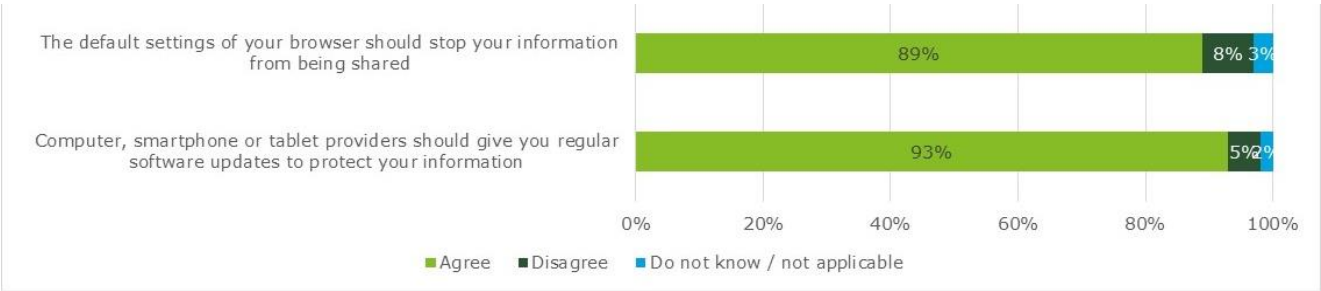


Source: Eurobarometer, graphical representation by Deloitte.

As can be seen above, six in ten consumers have ever changed the privacy settings on their internet browser (e.g. to delete browsing history or delete cookies). Moreover, 40% of consumers avoid certain websites because you are worried your online activities are monitored. However, only a minority of consumers uses software that prevents your online activities from being monitored and / or software that protects them from seeing online adverts.

Furthermore, it is important to 82% of consumers that tools for monitoring their activities online (such as cookies) can only be used with their permission (see Figure 18). In a similar vein, 89% of consumers think the default settings of their browser should stop the information stored on their terminal equipment from being shared, e.g. by means of regular software updates to protect such information by computer, smartphone or tablet providers (93% of consumers agree with such a statement, see Figure 22.

Figure 22 – Consumers' agreement with potential privacy enhancing measures by service providers



Source: Eurobarometer, graphical representation by Deloitte.

The relevance is further confirmed by the fact that **this provision has no direct equivalent in other legal acts**, including Directive 95/46/EC or the GDPR. The specificity of Article 5(3) of the ePD lies in providing a specific basis for the processing of personal data: user consent. As has been remarked, this requirement limits the possible legal grounds that can be used to justify the collection of personal data.[321] Absent the ePD, processing of personal data would be able occur under one of the six admissible legal grounds provided by Directive 95/46/EC or the GDPR, including in relation to legitimate interests of the data controller. The Article 29 Working Party has argued that, while specific

[321] Article 29 Working Party, Opinion 3/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC) [2016] WP240, p 4.

legal obligations can justify the processing of the data, there is no doubt that the consent requirement should prevail over other legal grounds.[322] The WP29 also highlighted that this provision will remain relevant in the future, e.g. based on the further development of the Internet of Things, will which lead to an increase in the processing of personal data.

However, the WP29 and other stakeholders consulted indicated that, while it is relevant to retain Article 5(3), the content is not fully appropriate in light of the market situation and technological development. This was based in particular on the fact that the article does not make a distinction between different types of cookies and that the usefulness for users is questioned (see section 5.7.1). This is, e.g. reflected in Deloitte's online survey with competent authorities. The majority of respondents (19 out 30, 63%) indicated that the provision is "important to retain, but with changes". In addition, two authorities indicated that is "important to retain as is" and two that it is "useful to retain, but with changes". No authority indicated that this provision does not need to be retained.

5.7.4 Coherence

Key finding of the analysis: Coherence tends to be confirmed

No significant challenges hindering the **internal coherence** have been identified.

As concerns the **external coherence**, there may be potential ambiguities based on the interaction of Article 5(3) and the GDPR, notably that it is not clear what level of information has to be provided to a subscriber who is not a natural person. On the other hand, the relationship with the RED allows for synergies, as the RED provides for radio equipment which is constructed in such a way as to support the prevention of the unlawful access to information stored in communication terminals.

With respect to the interaction with general policy goals of the EU, the provision is in line with EU's goal to safeguard fundamental rights. While it may be argued that it does not support the establishment of the internal market by restricting the tracking of users, this restriction can be justified based on the rationale to protect citizens' privacy.

Below, we discuss our observations in relation to the interaction of Article 5(3) with:

- Other provisions of the ePD;
- The GDPR, the Electronic Communications Package and the RED; and
- The goals of the EU to establish a **Digital Single Market** and to protect fundamental rights**.**

As concerns the **interaction with other provisions of the ePD**, it can be noted that Article 5(3) of the ePD has an atypical scope in that "it applies to anyone that wishes to store or access information on a user's device, including if not personal data are involved. The provision applies to "information", and not to the narrower concept of personal data".[323] This fact has, however, not been raised as a challenge by any of the stakeholders consulted.

In the table below, we present the **connection between the ePD and the GDPR, the Electronic Communications package and the RED**. For each relevant provision[324] we provide a brief summary, using the following colour code[325]:

[322] ibid.
[323] Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 27.
[324] We only list those instruments and provisions that a have connection to the ePD.

- Green: positive relationship (e.g. synergies);
- Grey: neutral relationship/no challenges nor positive aspects identified; and
- Yellow: potential challenges.

Further details are provided in the Annex.

The table shows that there are potential challenges in relation to the coherence with the GDPR. The relationship of the ePD and the **GDPR** was discussed at a stakeholder workshop organised by the Commission. On this occasion, it was e.g. raised the definition of consent in the GDPR is different from that in the ePD.

On the other hand, the Radio Equipment Directive is synergetic with the ePD. While this synergy does not clarify the situation outlined in the previous paragraph, it does provide for radio equipment which is constructed in such a way as to support the prevention of the unlawful access to information stored in communication terminals.

Table 29 – Coherence of Article 5(3) with the GDPR, the Electronic Communications package and the RED

Provision in the ePD	Provision in the other instrument	Main findings
GDPR		
Confidentiality of the Communications (Article 5.3)	- Conditions for consent (Article 7)	From the interplay between the provisions in the ePD and the GDPR, it is not clear what level of information has to be provided to a subscriber who is not a natural person.
Electronic Communications Package		
Access Directive		
Confidentiality of communications (Article 5)	Rights and obligations for undertakings (Article 4.3)	There is a connection between these provisions, but no challenges identified.
Radio Equipment Directive		
Confidentiality of communications (Article 5.3)	Essential Requirements (Article 3.3)	A synergy exists wherein radio equipment must be constructed in such a way as to incorporate safeguards to protect the privacy and personal data of the user and subscriber, as set out in the ePD.

Source: Deloitte.

In addition, some stakeholders have argued that aspects of this provision are not in line with the goal of the EU to establish a **Digital Single Market**. More specifically, it was argued at a stakeholder workshop organised by the Commission that forbidding the tracking of users (and related techniques) could hamper data-driven innovation.[326] This is confirmed by the fact that several interviewees from the business perspective indicated that the provision is quite burdensome for businesses that need to comply with it as well as the advertisement industry. However, this may be justified at least partially by the rationale to **protect the privacy of citizens**, which is fully in line with the general goal of the EU to protect the fundamental rights of its citizens.

[325] The summaries and colour classification are to be seen as indicative.
[326] European Commission (April 12, 2016). *Towards a future proof ePrivacy Legal Framework*. Minutes, p. 1.

5.7.5 EU added value

Key finding of the analysis: EU added value tends to be confirmed

The confidentiality of communications and the use of websites is a transnational issue that is not restricted by Member States' borders, as also recognised by stakeholders. If this matter were solved at the national level, businesses would need to adjust their approach for every EU Member State and consumers would face a lack of transparency. On this basis, there is an added value to have common standards in place.

Article 5(3) of the ePD aims to ensure the **confidentiality of information stored on the users' terminal equipm**ent, in particular by increasing awareness and empowering users.

It can be argued that this cannot be achieved by Member States alone, as communications and the use of websites are not bound by borders (in particular within the internal market) and Member States' standards on this varied before the introduction of the ePD. Furthermore, in many cases the companies placing the cookies will not be located in the same Member State as the user or even outside the EU: As shown by the 2014 Cookie Sweep, 70% of all cookies are placed by third parties. We showed in section 3.5.3 that there are only very few companies placing these cookies.

We note in this context that it was pointed out at a stakeholder workshop organised by the Commission that, while it is recognised that the matter is of transnational nature, the EU level may not be the right level for the rules put into place by Article 5(3). It was argued that standardisation should take place preferably at the global level, as companies, could be less eager to operate in Europe if the EU has its own set of rules.[327] Nevertheless, it is still considered to be an added value to have a specific provision at least at the EU level than having purely national legislation, which would mean that businesses would need to adapt their approach for every EU Member State. For consumers, this would mean that they would face different standards, depending on the origin of a website, which would not be transparent.

5.8 Specific rules on traffic and location data (Articles 6 and 9)

Articles 6 and 9 aim at protecting the confidentiality of communications and the related traffic and location data.

Traffic data is data processed for the purpose of conveying communications via an electronic communications network or for the purpose of billing such communications. Examples include the time of a communication or the address of those involved. Location data indicate the geographic location of a user's terminal equipment. Location data can be sensitive, as it can e.g. disclose visits to hospitals or religious places.[328]

Traffic and location data is used by services providers, for example, to:

- Offer value-added services (e.g. location services);
- Filter of malicious content or spam; or
- Analyse customer behaviour.

[327] European Commission (April 12, 2016). *Towards a future proof ePrivacy Legal Framework*. Minutes, p. 7.
[328] Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, paras. 18-19.

Overview of the content

Article 6(1) lays down the general principle concerning **traffic data** relating to subscribers/users that is processed and stored by the provider: It must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. However, there are certain exceptions:

- Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed until the end of the period during which the bill may lawfully be challenged or payment pursued (Article 6.2). The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing (Article 6.4).
- Processing of traffic data for the purpose of marketing electronic communications services or for the provision of value added services is only allowed to the extent and for the duration necessary and if the subscriber/user has given his or her prior consent. Users/subscribers may withdraw their consent for the processing of traffic data at any time (Article 6.3).

In general, processing of traffic data may only be carried out by persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service. Processing must be restricted to what is necessary for the purposes of such activities.

Based on Article 6(6), competent bodies may be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Article 9 lays down the rules on **location data other than traffic data**, relating to users/subscribers. Similarly to traffic data, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers (Article 9.1).

The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers may withdraw their consent for the processing of location data other than traffic data at any time (Article 9.1). Also after giving consent, the user/subscriber may temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication, using a simple means and free of charge (Article 9.2).

Processing of such data is allowed only to the extent and for the duration necessary for the provision of a value added service and must be carried out by persons acting under the authority of the provider or of the third party providing the value added service (Article 9.3).

5.8.1 Effectiveness

Key finding of the analysis: Not fully effective

Based on the limited evidence available, the effectiveness of the specific provisions on traffic and

location data does not seem to be fully achieved, as a number of problems seem to occur in relation to their application. First, the scope of Articles 6 and 9 only covers a small part of location based services, which is related to the general scope of the ePD which focuses on traditional telecom providers. In addition, there are ambiguities based on the interaction between Article 6 and 9 as well between the two Articles and Article 5(1) and (2), as it is difficult to distinguish between the different categories of data. Considering the exceptions under which traffic data and location data may be processed, it is questionable whether the possibility of processing traffic data for the purposes of subscriber billing and interconnection payments provided in Article 6.2 is still necessary considering that providers usually offer flat rate contracts. Turning to the consent mechanism, it was pointed out in the Commission's background paper to the public consultation that there are cases where traffic and location data might be used without consent. Finally, the provisions do not always seem to be enforced properly.

Based on the EC's public consultation a majority of respondents (45% or 173 of 332) faced problems in applying/understanding the rules on traffic and location data. The share of respondents who indicated that they faced problems is slightly higher in the industry (48%) compared to citizens and civil society (42%).

Table 30 – Extent to which respondents encountered problems in relation to the rules on traffic and other location data, per stakeholder group

Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	48,2%	18,4%	33,3%	*141*
Citizens & civil society	41,6%	31,2%	27,2%	*173*
Public bodies	44,4%	38,9%	16,7%	*18*
All replies	44,6%	26,2%	29,2%	*332*

Source: Deloitte based on EC public consultation.

Similarly, the assessment of the functioning of these provisions by competent authorities responding to Deloitte's online survey is rather mixed, with some authorities indicating the provisions only function poorly (3 out of 30 for Article 6, 4 out of 30 for Article 9) or fairly (6 out of 30 for Article 6, 8 out of 30 for Article 9). A slightly lower share of respondents indicated that the provisions function well, very well or excellent.

Table 31 – Competent authorities' assessment of the functioning of Articles 6 and 9

Please indicate for the following provisions how well they function. For example, you could consider the number of breaches and complaints you have received.							
Answer Options	**Poor**	**Fair**	**Good**	**Very good**	**Excellent**	**Cannot answer**	**Response Count**
Specific rules on traffic data (Article 6)	3	6	6	3	1	11	30
Specific rules on location data other than traffic data (Article 9)	4	8	4	3	0	11	30
answered question							**30**
skipped question							**4**

Source: Deloitte.

Below we discuss the assessment in more detail, referring to:

- The scope of the provisions, including its interaction with other provisions/legal instruments;
- The exceptions under which processing is allowed;
- The consent mechanism; and
- Enforcement.

It has been criticised by different stakeholders that the **scope** of these provisions may be too narrow in relation to different aspects. These issues are largely based on the definition of electronic communication services and the following exclusion of OTTs[329], which is discussed in section 5.1. For example, it was argued in the Commission's 2015 study on the ePD that only **a fraction of location based services is regulated:** The ePD only covers those services which rely on the processing of location data other than traffic data offered via a public communications network or in a publicly available electronic communications service.[330] Indeed, the Article 29 Working Party clarified in an opinion that the ePD applies only to the processing of location data by telecom providers and that location services provided by information society services, such as apps providing geo-localisation services, are currently excluded from the scope.[331]

In addition, the scope of these provision does not seem to be entirely clear. For example, it is **not clear whether traffic data is automatically personal data,** meaning that it is linked to a natural person, and as such in need of protection under the ePD. Representatives of national competent authorities have e.g. discussed this topic and concluded that traffic data is, in most cases, directly or indirectly linked to a natural person. However, phenomena such as the transfer of data from one machine to another might increase the grey area concerning the treatment of traffic data as personal data.[332]

Further ambiguities have been identified in relation to the **interaction of Articles 6 and 9 with other provisions and legal instruments**. In particular, it was pointed out by several competent authorities that it is not clear what type of data falls under Article 9, as most type of location data actually falls under Article 6. The authorities explained that the difference between "traffic data" and "location data, other than traffic data" is difficult to ascertain and apply in practice. A few authorities indicated that they do not consider this an issue. Similarly, some businesses and competent authorities indicated that the separation between Article 5(1) and (2) via-a-vis Articles 6 and 9 causes confusion, as the separation between communication data and traffic/location data is not always clear cut.

Considering the **exceptions** under which traffic data and location data may be processed, it is **questionable whether the possibility of processing traffic data for the purposes of subscriber billing and interconnection payments provided in Article 6.2 is still necessary** in light of the types of contracts typically offered in the electronic communications sector. Flat rate subscriptions dominate today's electronic communications market. Furthermore, the dissemination of zero rating of Internet services – a practice which exempts particular data from counting against the user's data cap or accruing any excess usage charges when the specific Internet services are used – also casts doubt on the necessity of processing traffic data for the purpose of billing users. This is of particular

[329] Cf. e.g. European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 3.
[330] European Commission (2015). *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation.* Final Report, (https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data), p. 12.
[331] Article 29 Data protection Working Party (2011). *Opinion 13/2011 on Geolocation services on smart mobile devices*, 881/11/EN, WP 185, (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf), p. 8.
[332] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 3.

relevance as it has been argued that some service providers tend to stretch the concept of processing traffic data for the purpose of billing. This way, the user "pays" the (unlimited) use of the Internet service free of charge by blindly giving away his/her traffic data.[333] This potentially hinders the achievement of the objective to ensure the confidentiality of communications and the related traffic and location data.

Turning to the **consent mechanism**, it was pointed out in the Commission's background paper to the public consultation that there are cases where traffic and location data might be used without consent:[334]

- In virtue of Article 4 of the ePD email providers might be allowed to set up filtering systems to detect a virus and to safeguard the security of their services[335]; and
- Location information must be available to authorities handling emergency calls regardless of consent (see Article 26.5 of the Universal Service Directive).

Finally, some challenges have been raised in relation to the **enforcement** of these provisions. For example, in relation to Article 6(3) it has been pointed out on different occasions that in practice some mobile operators mention the possibility of processing user and traffic data in their general terms and conditions, without further information. Some of these terms and conditions grant the operator a right to process the data for a duration of two years after the end of the contract.[336]

5.8.2 Efficiency

Key finding of the analysis: Insufficient information to assess

Although businesses reported that they incurred some costs in relation to these provisions, **no information is available on the magnitude of such costs**. Businesses mainly incur compliance costs and opportunity costs.

Compliance costs notably relate to the development / adaptation of technical infrastructure and / or software. These costs may be justified based on the added level of protection for users. Based on the ambiguities explained above (see section 5.8.1), it is also possible that businesses incur additional undue costs on legal advice, e.g. in case it is not clear under which regime a specific service falls. In addition, this may entail costs for competent authorities, as these may need to deal with unclear cases.

Opportunity costs are incurred by providers of traditional telecom providers that face restrictions which do not apply to their OTT competitors.

[333] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 3.
[334] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15039), p. 9.
[335] Working Party 29 Opinion 2/2006 on privacy issues related to the provision of email screening services, adopted on 21 February 2006.
[336] This has for example been reported by the Belgian consumers' organisation "Test-Achats" in a report of October 2014, summarised in their magazine "Budget & Droit", January-February 2014, p. 10-11. See also European Commission (2015). *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*. Final Report, (https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data), p. 81.

Although businesses reported that they incurred some costs in relation to these provisions, **no information is available on the magnitude of such costs**. In the following we discuss the types of costs that may be involved.

In the online survey carried out by Deloitte, seven out eleven businesses indicated that they incurred costs in relation to these provisions. The most relevant aspects causing these costs were indicated to be:

- Submitting information to competent national authorities (e.g. on security breaches);
- Development / adaptation of technical infrastructure and / or software; and
- Lost business opportunities (i.e. opportunity costs).

The first point relates to **administrative burden**. We note that Article 6 and 9 do not include a direct obligation to inform authorities of security provisions. This would rather be based on Article 4 and should thus not impact on the efficiency of Articles 6 and 9.

The second point relates to **compliance costs**. It is expected that the development / adaptation of technical infrastructure and / or software would mostly entail investment costs incurred when first implementing these provisions. Additional costs in this respect may be incurred in relation to the maintenance of such systems and possible adaptions in case of a need to update the systems or fix errors. Another factor likely to cause compliance costs are the obligations to inform subscribers included in these provisions. Indeed, information of / communication with subscribers and users was also mentioned by one business replying to the online survey. Such costs may be justified based on the added protection of privacy for users.

Based on the ambiguities explained above (see section 5.8.1), it is also possible that businesses incur additional undue costs on legal advice, e.g. in case it is not clear under which regime a specific service falls. In addition, this may entail costs for competent authorities, as these may need to deal with unclear cases.

The third point relates **opportunity costs** ensuing based on these provisions. This point has also been confirmed as part of the interviews. More details can be found in the following text box.

Case example Arts. 6 and 9: Opportunity costs for telecommunication service providers

Representatives of the incumbent telecommunication service providers of both a Western European and Scandinavian Member State indicated in the respective interviews with them that their business faces significant opportunity costs due to the ePD's rules on traffic and location data.

Such opportunity costs relate to the potential revenue such companies could generate if they were allowed to develop and market similar services as OTTs and exploit the respective data.

It was explained that, while OTTs for instance, are able to exploit the data they receive from users in order to develop and market new services, traditional telecommunication service providers face economic pressure and disadvantages to keep up with modern communication technologies as users tend to switch to "more pragmatic and modern" communication means that are considered as "more flexible" than those currently offered by telecommunication service providers under the ePD.

This means that, while telecommunication service providers currently lose customers to other services such as VoIP and/or instant messaging, revenues generated by traditional telecom services also decline in an effort to maintain the customer base through lower consumer prices.

Nevertheless, none of the business spokespersons was able to quantify the opportunity costs as

they are not relevant for current business operations. Such figures would only be estimated in case a business would like to expand their operations to new markets and types of services – which is not the case under current ePD rules and is unlikely to be in the future according to the interviewees.

5.8.3 Relevance

Key finding of the analysis: Relevance tends to be confirmed

While it is confirmed that it is relevant to keep rules on the processing of traffic and location data, the format of the current rules is questioned. In particular, a number of ambiguities relating to the application of these provisions has been identified.

In general terms it was argued in the EC's background paper to the public consultation that the provisions and the consent mechanisms they introduce are relevant for citizens in light of the following:[337]

- Such data, particularly if stored over time, allow to draw precise conclusions on individuals' private life (daily movement, residence, social relationships, activities etc.); and
- In modern societies people need to have access to electronic communication services for most part of their daily lives.

At the same time, there are no express rules relating to the processing of traffic and location data in other legal instruments, such as the GDPR. Indeed, competent authorities interviewed by Deloitte considered it a strength of the ePD that it includes clear rules on traffic data and that the grounds for using processing traffic data are restricted.

The relevance of these provisions is also supported by the respondents to the EC's public consultation. The majority (54.8%) of all respondents confirms that there is an added value of having specific rules on traffic and location data for the electronic communications sector. This opinion is particularly supported by large majorities from the group of citizens and civil society (73.1%) as well as the public bodies (92.3%). In contrast, the majority (66.2%) of the respondents from the industry does not see an added value of having specific rules on traffic and location data for the electronic communications sector.

The BEREC view[338] is that the Articles 6 and 9 are still relevant. However, it pointed out some shortcomings in relation to the format, indicating that there are certain ambiguities (e.g. whether location and traffic data, including IP addresses, should always be considered as personal data) and that Article 6 may not be fully in line with recent technological developments.[339] This reflects our findings under the criterion effectiveness (see section 5.8.1).

[337] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15039), p. 9.
[338] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133 http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive p.2
[339] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133 http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive p.5

5.8.4 Coherence

Key finding of the analysis: Partially coherent

While Articles 6 and 9 work rather well with other instruments, notably the GDPR, challenges have been identified in relation to the **internal coherence**. In particular, the distinction between the different types of data covered by Article 6, 9 and 5 may not always be clear in practice.

In the table below, we present the connection between the ePD and the GDPR[340]. For each relevant provision[341] we provide a brief summary, using the following colour code[342]:

- Green: positive relationship (e.g. synergies);
- Grey: neutral relationship/no challenges nor positive aspects identified; and
- Yellow: potential challenges.

Further details are provided in Annex.

The table shows that the processing of traffic and location data is not expressly regulated in the GDPR. No challenges in relation to the interaction of the ePD and the GDPR have been identified. We note in this context that some stakeholders raised concerns with regard to the coexistence between these two articles and the rules in the GDPR. For instance, it was pointed out that Article 6 and 9 require consent for the processing of traffic and location data whereas the GDPR provides alternative legal basis for processing such data.

Table 32 – Coherence of Articles 6 and 9 with the GDPR

Provision in the ePD	Provision in the other instrument	Main findings
Traffic Data (Article 6)	- Traffic Data is not expressly regulated in the GDPR.	No challenges have been identified. The ePD complements the rules of the GDPR in providing specific rules on the processing of traffic data.
Location Data Other than Traffic Data (Article 9)	The GDPR does not expressly regulate the processing of location data other than traffic data.	No challenges have been identified. The ePD complements the rules of the GDPR in providing specific rules on the processing of location data.

Source: Deloitte.

As concerns the **internal coherence**, it was pointed out by several competent authorities that it is not clear what type of data falls under Article 9, as most type of location data actually falls under Article 6. The authorities explained that the difference between "traffic data" and "location data, other than traffic data" is difficult to ascertain and apply in practice. A few authorities indicated that they do not consider this an issue. Furthermore, some businesses and competent authorities indicated that the separation between Article 5(1) and (2) via-a-vis Articles 6 and 9 causes confusion, as the separation between communication data and traffic/location data is not always clear cut.

[340] No related provisions in the Electronic Communications Package have been identified.
[341] We only list those instruments and provisions that a have connection to the ePD.
[342] The summaries and colour classification are to be seen as indicative.

5.8.5 EU added value

Key finding of the analysis: EU added value confirmed

As communications and location-based services are not bound by borders, a clear EU added value of harmonised rules on the protection of traffic data and location data can be seen.

Articles 6 and 9 aim at protecting the confidentiality of communications and the related traffic and location data, by introducing harmonised standards. It can be argued that this cannot be achieved by Member States alone, as communications and location-based services are not bound by borders (in particular within the internal market) and Member States' standards on this varied before the introduction of the ePD. At the same time, none of the stakeholders consulted as part of this assignment declined an EU added value of this provision.

5.9 Itemised billing of invoices (Article 7)

Article 7 aims to ensure the right to privacy of calling and called users by providing a possibility of opting for non-itemised billing.

Overview of the content

Itemised bills allow verifying if the fees charged for a service are correct. However, if the **service is used by various persons (i.e. a service used by all members of a family)**, this may jeopardise users' privacy.

Therefore, Article 7(1) ensures that subscribers shall have a right to receive non-itemised bills. It is specifically acknowledged that national laws need to reconcile the right of subscribers to receive itemised bills with the right to privacy of called and calling users (Article 7.2).

5.9.1 Effectiveness

Key finding of the analysis: Effectiveness tends to be confirmed

Based on the available evidence, this provision seems to function rather effectively. However, some moderate challenges have been identified, e.g. there may be problems in relation to service contracts concluded by employers for their employees (the right to the employee's privacy may be endangered if the employer needs itemised billing). However, these issues do not appear to significantly hinder the effectiveness. There are no serious issues in relation to the transposition of this provision either.

In the EC's public consultation, only few respondents (17% or 54 of 325) indicated that they have faced problems in applying/understanding the rules on itemised billing, whereas 43% (140 respondents) did not face problems. It has to be noted in this regard that quite a high number of respondents (40% or 131 of 325) did not have an opinion in this regard. We note in this context that this provision does not apply to all types of services providers. It is mostly relevant for telephony and internet contracts.

Table 33 – Extent to which respondents encountered problems in relation to the rules on itemised billing, per stakeholder group

Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	16,3%	29,6%	54,1%	135
Citizens & civil society	18,5%	51,4%	30,1%	173
Public bodies	0,0%	64,7%	35,3%	17
All replies	16,6%	43,1%	40,3%	325

Source: Deloitte based on EC public consultation.

One difficulty relating to a specific situation was, identified at the workshop the Commission held with competent authorities. It was indicated that the **application of this provision in the employment context** may pose difficulties. More specifically, it was pointed out that when it comes to service contracts concluded by employers for their employees, the right to the employee's privacy may be endangered if the employer needs itemised billing. There has been case law on this aspect in at least one Member State.[343] This issue was confirmed by Deloitte's survey with competent authorities. A quarter of the respondents considered this to be a moderate problem, while another quarter indicated that this was a minor problem. In addition, 10% indicated that this is a serious problem. Several of the authorities also indicated that it is a problem (mostly moderate or minor) that it is unclear what type of privacy enhancing methodologies the ePD implies and to what extent these are implemented by the service providers.

The transposition check carried out for the purpose of this study showed that there are no issues in relation to the transposition of this provision in most Member States. It appears that the first paragraph of Article 7 was transposed in national legislation in such a way as to ensure equivalent rights across Member States. However, there are major differences in the way that Member States reconcile this right with the right to privacy of calling users and called subscribers. In some cases, Member States have used the discretionary margin provided by the second part of this provision to establish opposing default requirements. The majority of Member States have fully transposed this article, laying down the right to receive non-itemised bills and the right to receive itemised bills. A few countries such as Spain, Portugal, Ireland and Cyprus have transposed this article more or less literally. In most cases, Member States ventured beyond a literal transposition to provide additional details regarding the implementation of this right. In some countries, the default rule is to receive itemised bills, with non-itemised bills being provided only at request. In other Member States, the default rule is to provide bills which implement a method for protecting the identification of the phone numbers on the bill. It appears that four countries did not transpose this article (Belgium, Croatia, Denmark and Slovakia). Further details on the transposition can be found in chapter 4.

5.9.2 Efficiency

Key finding of the analysis: Insufficient information to assess

Stakeholders have emphasised the significant costs for the initial implementation of the provisions on non-itemised bills. However, no quantitative evidence is available. There are different opinions as to the benefits of this provision for consumers.

[343] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 5.

The information on **compliance costs for businesses** related to these provisions is limited.

In general terms, respondents to the European Commission's public consultation and interviewees indicated that significant costs were involved for the initial implementation of the provisions on non-itemised bills. Such costs related in particular to IT infrastructure. Some small recurrent costs may relate to the maintenance of such systems. As concerns the proportionality of such costs, Telecom operators explained that the services were not requested by customers. Yet, we note that respondents to the public consultation largely confirmed the relevance of this section, as explained in the previous section.

As concerns the **perspective of subscribers**, our transposition check found that many of the Member States such as Austria, Italy, Finland, Slovenia, include in their legislation that these services shall be provided free-of-charge. While this is positive, it is possible that subscribers face costs for changing the type of billing (e.g. changing from itemised billing to non-itemised billing) in the other Member States.

5.9.3 Relevance

Key finding of the analysis: Relevance tends to be confirmed

There are no similar rules in any other EU legal instrument, e.g. the GDPR, supporting the relevance of this provision. The relevance of this provision is also largely supported by the stakeholders consulted. However, we note that the support of this provision was overall stronger among citizens and civil society, while the industry seems to be more critical, arguing e.g. that customers do not demand these services.

There are no similar rules in any other EU legal instrument, e.g. the GDPR, supporting the relevance of this provision. The relevance of this provision is also largely supported by the stakeholders consulted.

On the basis of the EC's public consultation, the relevance of the provision on itemised invoicing is confirmed to some degree, although there are differences depending on the way the question is phrased and the types of stakeholders asked.

When asked whether they see an added value of having specific rules on the itemised billing of invoices for the electronic communications sector, 34% (121) respondents chose "Yes" and 31% (109) chose "No". Thus, although slightly more respondents see an added value of this provision, the difference is very small. It is also noteworthy that a high share of respondents (35% or 124 of 354) actually do not have an opinion on this question. As stated in section 5.9.1, this may be based on the fact that this provision is not relevant for all participating businesses.

Table 34 – Extent to which respondents see an added value in the rules on itemised billing, per stakeholder group

Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	8,9%	45,2%	45,9%	146
Citizens & civil society	47,3%	21,4%	31,3%	182
Public bodies	84,6%	15,4%	0,0%	26
All replies	34,2%	30,8%	35,0%	354

Source: Deloitte based on EC public consultation.

Respondents were also asked whether certain provisions continue to be relevant, should be amended or deleted. The majority of respondents (161) indicated that the provision on itemised billing continues to be relevant and should be kept. Only 19 respondents indicated that it should be amended. 63 respondents indicated that the provision should be deleted. As concerns the views of different stakeholder groups, the support of this provision was overall stronger among citizens and civil society, while the industry seems to be more critical. This was confirmed in interviews with Telecom providers, who explained that the services were usually not requested by customers. On this basis, they did not see the need to uphold this provision.

By contrast, BEREC[344] stated that Article 7 is relevant, but could be strengthened by extending it to all services using numbering resources (i.e. E.164), and potentially to other types of identifiers, such as SIP URIs. This is confirmed by Deloitte's online survey with competent authorities. Only 6.7% or two authorities indicated that this provision does not need to be retained, whereas two thirds indicated that it would be important or useful to retain this provision, although some changes may be needed.

5.9.4 Coherence

Key finding of the analysis: Coherence confirmed

The coherence of this provision is confirmed as there are no similar or contradictory rules contained in any of the instruments studied.

Based on an analysis of the coherence of this provision towards the GDPR and the Electronic Communications Package, no challenges have been identified. Indeed, there are no similar rules contained in any of the instruments studied.

5.9.5 EU added value

Key finding of the analysis: Limited EU added value

Itemised billing of invoices is considered to be an issue that does have limited EU added value. The provision is expected to contribute to ensure that citizens have the same rights across the EU.

At the same time, however, the share of citizens that makes use of itemised billing today – in particular in a cross-border context – is expected to be fairly small compared to the overall number of users.

Although difference exist in how the Member States have transposed this provision, citizens still benefit from having equal rights across the EU in this matter.

In addition, the ePD's nature as a Directive does not guarantee by default that citizens have the same rights towards itemised billing across the EU as Member States are free to transpose the Directive differently into national law.

No more specific information was identified with regard to the EU added value of this provision. At the same time, this means that none of the stakeholders consulted as part of this assignment declined an EU added value of this provision.

[344] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133. http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive p. 3

5.10 Presentation and restriction of calling and connected line (Articles 8 and 10)

This article aims to ensure a possibility for users and subscribers to decide about the presentation and restriction of calling and connected line identification, thus contributing to the right to privacy.

Overview of the content

Article 8 lays down requirements for service providers concerning situations where presentation of calling line identification is offered. Service providers must inform the public of the possibilities relating to call line identification (Article 8.6).

According to Article 8(1), *calling users* must have the possibility to prevent the presentation of the calling line identification on a per-call basis, using a simple means and free of charge. The *calling subscriber* must have this possibility on a per-line basis.

Based on Article 8(2)-(4), the *called subscriber* must have the possibility to prevent the presentation of the calling line identification of incoming calls, using a simple means and free of charge for reasonable use of this function. In addition, the called subscriber must have the possibility of rejecting anonymous incoming calls, using a simple means. Finally, the called subscriber must have the possibility of preventing the presentation of the connected line identification to the calling user, using a simple means and free of charge.

These requirements also apply in relation to calls from or to third countries (Article 8.5).

According to Article 10, there are two cases when the caller decision to hide the presentation of the calling line identification may be overridden:

- When a subscriber requests the tracing of malicious nuisance calls; and
- In the case of organisations engaged in emergency calls, law enforcement authorities, ambulance, fire brigades, for the purpose of responding to such calls.

5.10.1 Effectiveness

Key finding of the analysis: Effectiveness tends to be confirmed

These provisions function rather well. No serious issues relating to this provision could be identified, which may imply that it is rather effective in reaching its objective. There are some minor or moderate challenges (e.g. it is unclear how providers or authorities should respond to users/subscribers who want to know who gave a call or through which line the call came in if there is a restriction to identify the calling and connected line). However, the effectiveness of these provisions does not appear to be significantly hindered based on these challenges. This is supported by the different stakeholder consultations carried out by Deloitte as well as the EC's public consultation and desk research. There are no serious issues in relation to the transposition of these provisions either.

Based on the EC's public consultation, only few respondents (25%) reported to have faced problems in applying/understanding the rules on control over calling line identification, whereas 36% of the

respondents stated that they did not face problems. It has to be noted in this regard that quite a high number of respondents (39%) did not have an opinion in this regard.

Table 35 – Extent to which respondents encountered problems in relation to the rules on control over calling line identification, per stakeholder group

Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	20,9%	26,9%	52,2%	134
Citizens & civil society	27,6%	43,1%	29,3%	174
Public bodies	23,5%	41,2%	35,3%	17
All replies	24,6%	36,3%	39,1%	325

Source: Deloitte based on EC public consultation.

Based on the online survey with businesses implemented as part of this project the Directive's provisions regarding the presentation and restriction of calling and connected line identification were a problem for two of six businesses that indicated this particular provision is of practical relevance for them.

According to the competent authorities responding to Deloitte's online survey, this article functions rather well. When asked about the functioning of the different provision, the majority of respondents indicated that Article 8 functions well (23.3%) or very well (13.3%). Similarly, when asked about problems in relation to this provision, few serious challenges are reported by the responding national competent authorities, as portrayed in the following table

Table 36 – Challenges reported in the context of Article 8 (total n° of responses = 28)

	Not at all a problem	Minor problem	Moderate problem	Serious problem	Cannot answer
The restrictions of this article are not sufficient now as they apply only to telephony services	2	6	7	4	9
It is unclear how providers or authorities should respond to users/subscribers who want to know who gave a call or through which line the call came in if there is a restriction to identify the calling and connected line	1	6	10	2	9
It is unclear how the providers should inform the public about the presentation of calling and/or connected line identification, where offered (e.g. make explicit reference of these possibilities on providers' privacy statement)	3	9	5	1	10
These obligations for service providers are no longer relevant, as some of the aspects covered by this provision are available to users as functions on modern cell phones	6	5	4	2	11
There is a lack of clarity relating to how these rules can be applied in relation to service contracts concluded by employers for their employees	6	4	5	0	13

Source: Information provided by competent authorities of the EU Member States, tabulation by Deloitte. Green marked cells denote highest values per row.

During the interviews carried out by Deloitte, some competent authorities have pointed towards potential additional concerns regarding the effectiveness of the provision as part of the interviews carried out. These concerns related to:

- The increased risk of fraud, e.g. the possibility of 'spoofing' the number displayed so that individuals cannot directly contact the caller;
- Users' inability to identify marketing calls by withholding the calling line identification; and
- Technical issues with offering anonymous call rejection at network level on mobile networks

Furthermore, one competent authority shared that there are practical difficulties in relation to this provision. Based on national law, service providers must ensure that users are able to use these services free of charge, including e.g. to block calls from anonymous numbers. However, the telecom providers did not implement these rules properly. They argue that they are too expensive and are not needed by users. So far, the national telecom agency has thus not forced implementation. Sometimes they receive complaints by citizens on this. However, there are only few requests (around 50 per year) and no citizen has insisted on their rights in this respect. This also touches upon the efficiency of the provision (see below).

Based on the **transposition check** carried out for the purpose of this study, it appears that the transposition of Article 8 was carried out in a satisfactory manner across the Member States, ensuring the harmonisation of rules in this area. Indeed, it was found that this article has been transposed in all the Member States except Malta. For a large majority of Member States, the transposition of these provisions was literal to a certain extent.[345] Some Member States such as Bulgaria, Finland, Poland, and Lithuania accurately reflect the rationale of this article in their laws, but remain silent on whether this requirement applies to third countries. Some Member States have added some specificities. For example, a peculiarity contained in the German transposition of Article 8 lies in the prohibition of preventing calling line identification if the calling party engages in telephone calls for the purpose of advertising.

As concerns Article 10, the transposition in Member States does not seem to hinder the effectiveness of this provision either. The large majority of Member States fully transposed this article, adopting the literal phrasing of the ePD.[346] Some countries such as Latvia, Luxembourg, Poland and Slovenia transpose this article throughout several provisions. However, most Member States provide further details on the situations and conditions under which such limitations may take place. For example Bulgaria added that the rights stated in Article 8 of the ePD may be overridden in the case of calls to services responsible for security, defence and internal order. Two Member States (Austria and Hungary) appear to have transposed this article only where emergency calls are concerned, leaving out the exception related to the handling of nuisance calls. Only Germany appears not to have transposed this article. Section 102 TKG deals with the issue of calling line identification, but it does not provide for an explicit obligation of providers to inform about the exceptions under Article 10 of the ePD.[347] This said, according our expert, the major telecommunications providers in Germany seem to voluntarily comply with the requirements set out in Article 10.

[345] Such is the case of Austria, Belgium, Croatia, Cyprus, Czech Republic, Denmark, Greece, Ireland, Italy, Latvia, Luxembourg, Netherlands, Portugal, Romania, Slovenia, Spain, and Sweden.
[346] This includes Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Portugal, Poland, Romania, Spain, Sweden, Slovakia, and Slovenia.
[347] According to Section 45n Paras. 1, 2 No. 3, 3 No. 7 lit. f) the competent authorities are entitled to issue a legislative decree dealing with the informational duties of telecommunications providers concerning inter alia calling line identification. The Federal Network Agency issued a first draft for a respective legislative decree in 2013. However, this draft has not entered into

5.10.2 Efficiency

Key finding of the analysis: Efficiency is limited

In general terms, respondents to the European Commission's public consultation and interviewees indicated that significant costs were involved for the initial implementation of the provision on calling and connected line identification.

Such costs related in particular to IT infrastructure. Some small recurrent costs may relate to the maintenance of such systems. As concerns the proportionality of such costs, Telecom operators explained that the services were not requested by customers.

Further information on **compliance costs for businesses** related to these provisions is limited.

It is important to acknowledge, however, that locating callers linked to emergency calls is a very important feature that contributes to the effectiveness of the service. Although such a service may not be efficient in terms of costs-benefit-ratio, it has not been raised by any stakeholder as an issue.

Case example Arts. 8 and 10: Compliance costs a large-scale telecommunication service provider

The representative of a large-scale telecommunications service provider that is active in several Member States and third-countries indicated that his company incurred a significant amount of costs concerning the development and implementation of technical solutions regarding the presentation and restriction of calling line identification.

In addition, it was also explained that similar costs were incurred with regard to other provisions of the ePD which, today, seem outdated from both a technical, as well as from the customers' perspective.

It was asserted that the development and implementation of these technical solutions which are today mostly built-in by default in devices were, at the time at which telecom operators incurred respective costs not demanded by customers and, thus, little used by them.

Overall, the interviewee indicated, however, that relevant compliance costs are impossible to measure as they were incurred somewhere in the past – even before most of the current staff was employed at the company.

5.10.3 Relevance

Key finding of the analysis: Relevance tends to be limited

The relevance of this provision can be confirmed as no similar rules are contained in the GDPR. However, concerns were voiced that calling line identification would have most probably been replaced by alternative solutions in line with the technological developments if not for the existing legal obligation to have it in place. Indeed, the presentation and restriction of calling and connected line identification is a feature that is today built in by design by device manufacturers. However, this is so far mostly valid for modern mobile phones, but not necessarily for fixed phones.

force yet. It should be noted in any case that the draft does not lay down an obligation to inform the subscriber of the exemptions enabled by Article 10 of the Directive.

As highlighted in the EC's background paper to the public consultation, the rules in Article 10 are **specific to the electronic communication sector**. No similar rules are contained in the GDPR.[348] This supports the relevance of this provision, although potential overlaps with other instruments still need to be examined (see the section on coherence).

Nevertheless, interviews with business associations have pointed towards the perception that measures covered in the ePD would have been offered based on customer demand (i.e. and not due to legislation). Concerns were voiced that measures that appear to be outdated such as calling line identification would have been most probably replaced by alternative solutions in line with the technological developments. Indeed, the presentation and restriction of calling and connected line identification is a feature that is today built in by design by device manufacturers. However, this is so far mostly valid for modern mobile phones, but not necessarily for fixed phones.

A relative majority (40%) of all respondents to the EC's public consultation confirmed an added value of having specific rules on the presentation and restriction of calling and connected line for the electronic communications sector. Almost one in three (32%) of all respondents did, however, not have an opinion on this issue. Absolute majorities of the respondents from the groups of the citizens and civil society (56%) and of the public bodies (89%) endorse an added value of having specific rules. Responses from the industry point in the opposite direction, with around 43% of respondents each not seeing an added value of having specific rules (44%) and not having an opinion on this topic (43%).

Table 37 – Extent to which respondents see an added value in the rules on control over calling line identification, per stakeholder group

Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	13,0%	43,8%	43,2%	146
Citizens & civil society	55,5%	18,1%	26,4%	182
Public bodies	88,5%	3,8%	7,7%	26
All replies	40,4%	27,7%	31,9%	354

Source: Deloitte based on EC public consultation.

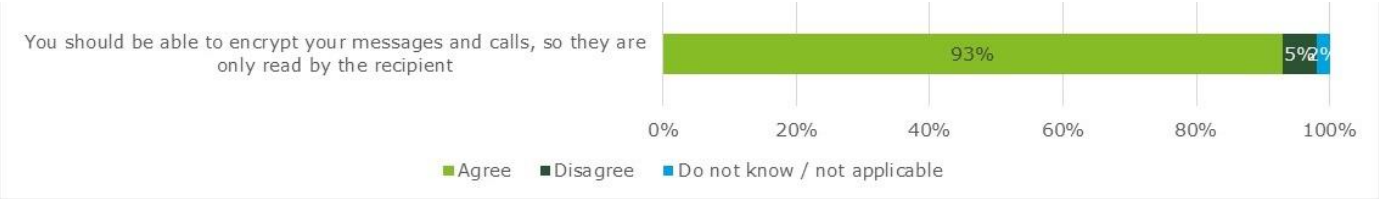
The respondents were also asked whether certain provisions continue to be relevant, should be amended or deleted. The majority of respondents (158) indicated that the provision on control over call line identification continues to be relevant and should be kept. Only 27 respondents indicated that it should be amended. Sixty-one respondents indicated that the provision should be deleted. As concerns the views of different stakeholder groups, the support of this provision was strong among citizens and civil society, while the industry seems to be more critical. This was confirmed by the telecom providers that explained that the services were usually not requested by customers. On this basis, they did not see the need to uphold this provision.

According to Eurobarometer[349] 74% of EU **consumers** use their mobile phones to make calls or send text messages every day while an additional 13 % uses it for this purpose 'a few times a week' (see Figure 14 in section 5.4.3). Hence, the use of mobile phones is make calls or send text messages forms an essential part of consumers' communication behaviour.

[348] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive), p. 10.
[349] Flash Eurobarometer 443 (2016): e-Privacy. Data on 26,526 consumers collected between 6 and 8 July 2016. At this stage, the Eurobarometer results are only of provisional character.

In addition, 90% of consumers think they should be able to encrypt your messages and calls, so they are only read by the recipient (see section 5.10.1).

Figure 23 – Consumers' assessment regarding the encryption of messages



Source: Eurobarometer, graphical representation by Deloitte.

Therefore, as the use of mobile phones is relevant to the consumers – especially from the perspective of confidentiality of communications, ensuring a possibility for users and subscribers to decide about the presentation and restriction of calling and connected line identification is an important measure to contribute to consumers' right to privacy.

BEREC[350] stated that the Article 8 rule on presentation/restriction of calling is relevant, but its scope is not wide enough.

5.10.4 Coherence

Key finding of the analysis: Coherence confirmed

The analysis has shown that, as a *lex specialis* that particularises a specific situation, the provision is coherent with the GDPR and the Electronic Communications Package.

Based on an analysis of the coherence of this provision towards the GDPR and the Electronic Communications Package, no challenges have been identified. Indeed, there are no similar rules contained in any of the instruments studied.

The ePD particularises a specific situation that is not otherwise regulated in the Directive or GDPR. The rights afforded to the subscribers may be derived from the application of general principles in the latter two instruments (for natural persons). However, it is to be considered that the ePD brings forth greater clarity as to the exercise of such rights (for example, by obliging providers to offer this functionality free of charge).

As mentioned with regard to other provisions of the ePD, a reference may be made to Article 3(3) of the Radio Equipment Directive in so far as the latter mandates the construction of radio equipment capable of supporting the incorporation of safeguards designed to protect the privacy and the personal data of the users and subscribers. In this particular case, such provision means that radio equipment, where applicable, must not be constructed in such a way as to impede the presentation restriction of the calling line identification, amongst the other possibilities conferred upon users and subscribers.

[350] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133. http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive p. 3

5.10.5 EU added value

Key finding of the analysis: Limited EU added value

Although differences exist in how the Member States have transposed this provision, citizens still benefit from having equal rights across the EU in this matter.

The presentation and restriction of calling and connected line identification is a feature that is today often built in by design by device manufacturers (in particular for mobile phones) that are not necessarily (only) bound by EU law when designing their products.

Thus, it is not the provision that enables citizens to make use of their rights but much rather the manufacturers of devices that apply international (not EU) standards in their product design

A similar argumentation as for itemised billing (see section 5.9) is applicable to this provision regarding citizens having the same rights across the EU.

5.11 Automatic call forwarding (Article 11)

This article aims to protect users' and subscribers' right to privacy.

Overview of the content

According to Article 11, subscribers must have the possibility of stopping automatic call forwarding by a third party, using a simple means and free of charge.

5.11.1 Effectiveness

Key finding of the analysis: Effectiveness tends to be confirmed

The effectiveness of this provision tends to be confirmed as no serious issues have been identified. The provision appears to function rather well. The moderate challenges identified (e.g. it is unclear which safeguards should be provided for subscribers against the nuisance caused by automatic call forwarding by others) did not appear to seriously hinder the effectiveness of this provision. This is supported by the different stakeholder consultations carried out by Deloitte as well as the EC's public consultation and desk research. There are no serious issues in relation to the transposition of this provision either.

Only limited information is available regarding the effectiveness of the ePD's provision concerning the possibility to stop automatic call forwarding by a third party. On this basis, no serious challenges have been identified.

In general, the scope of the Article does not cover OTTs, which may be a barrier for ensuring the full effectiveness of Article 11 (cf. also section 5.1).

Although a large part of the respondents (44%) did not have an opinion on this, the results of the European Commission's public consultation show that close to 70% of the respondents that had an opinion (123 of 191) had not encountered any problems in applying / understanding the rules regarding automatic call forwarding.

- *Industry:* Of the overall 63 respondents that had an opinion, 36 (57%) had not encountered any problems, while 27 (43%) answered in the affirmative;

- *Citizens and civil society organisations:* Of the overall 108 respondents that had an opinion, 78 (72%) stated that they had not encountered any problems, while 30 (28%) answered opposite;
- Only one of ten public bodies that had an opinion indicated that they had encountered problems.

Table 38 – Extent to which respondents encountered problems in relation to the rules on automatic call forwarding, per stakeholder group

Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	20,1%	26,9%	53,0%	134
Citizens & civil society	17,5%	45,6%	36,8%	171
Public bodies	5,9%	52,9%	41,2%	17
All replies	18,0%	38,2%	43,8%	322

Source: Deloitte based on EC public consultation.

As the majority of stakeholders across the different groups indicated that they have not encountered problems with regard to Article 11, it can be argued that the provision is effective in reaching its objectives.

Based on the online survey with businesses implemented as part of this project, the Directive's provisions regarding automatic call forwarding were a problem for one of four businesses that indicated this particular provision is of practical relevance for them.

According to the competent authorities responding to Deloitte's online survey, this article functions rather well. When asked about the functioning of the different provision, the majority of respondents indicated that Article 11 functions well (26.7%) or fair (20%). Similarly, the competent authorities did not point to any serious challenges as part of the online survey or interviews. However, about a third of respondents of the online survey considered it a moderate problem that it is unclear which safeguards should be provided for subscribers against the nuisance caused by automatic call forwarding by others. In addition, one authority raised the issue that call forwarding should require the consent of the subscriber to whom the call is forwarded.

Based on the ways Member States have transposed this provision into their national laws, the effectiveness of Article 11 is not hindered in all but one Member States. Indeed, the big majority of Member States[351] have transposed more or less literally this article. Others such as Poland and Spain did not transpose literally the article. However, they have fully transposed the requirements stemming from article 11 into their national law and no material differences have been observed. As an example of how this right is implemented into practice, in Austria, in order to stop the automatic call forwarding, subscribers need to send a specific code to the operator, which will restrict the automatic call forwarding. Only Hungary appears not to have transposed this provision.

5.11.2 Efficiency

Key finding of the analysis: Efficiency is limited

[351] These include Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Ireland, Italy, Latvia, Portugal, Romania, Slovakia, Slovenia, and Sweden.

The efficiency of this provision tends to be limited as the costs incurred by businesses to implement the possibility of stopping automatic call forwarding are much rather caused by legislative obligations than actual customer demand.

The information on **compliance costs for businesses** related to these provisions is limited.

In general terms, respondents to the European Commission's public consultation and interviewees indicated that significant costs were involved for the initial implementation of the provisions on automatic call forwarding. Such costs related in particular to IT infrastructure. Some small recurrent costs may relate to the maintenance of such systems. As concerns the proportionality of such costs, Telecom operators explained that the services were not requested by customers. On this basis, the efficiency of these provisions may be questioned.

5.11.3 Relevance

Key finding of the analysis: Insufficient information to assess

It is difficult to draw a conclusion on the relevance of this provision due to the mixed data available. On the one hand, ensuring a possibility of stopping automatic call forwarding by a third party theoretically contributes to ensuring citizens' privacy while on the other hand, the responses to the public consultation do not give a clear picture in this matter. Moreover, telecom operators have emphasised that customers have not demanded such a feature.

As presented in section 5.10.3, the use of mobile phones is relevant to the consumers – especially from the perspective of confidentiality of communications. Thus, ensuring a possibility of stopping automatic call forwarding by a third party contributes to ensuring citizens' privacy.

However, the evidence for evaluating the relevance of having specific rules on automatic call forwarding for the electronic communications sector is scarce. The **overall results of the EC's public consultation are mixed** and consequently the relevance of Article 11 can neither be confirmed nor be rejected. While citizens and civil society as well as public bodies indicate that the article is relevant, responses from the industry suggest the opposite.

More concretely, the results of the EC's public consultation reveal that **most respondents (36%) do not have an opinion on the question** if there is an added value of having specific rules. This may suggest either indifference or lack of knowledge in relation to this article. Of those who have an opinion, the respondents indicating that there is an added value of having specific rules (35%) prevail over those indicating that there is no added value of having specific rules (29%). In particular, a relative majority (49%) of the respondents from the group of the citizens and civil society and an absolute majority (81%) of the respondents from the group of the public bodies endorse an added value of having specific rules. In contrast, **a high share (45%) of the respondents from the industry indicates that there is no added value of having specific rules.** This was confirmed in interviews with Telecom providers, who explained that the services were usually not requested by customers. On this basis, they did not see the need to uphold this provision. It can be noted that an even higher share of respondents to the public consultation indicated that they do not have an opinion on this issue (46%). Again, this may partially be explained by the fact that this provision is only relevant to specific types of businesses (telephony).

Table 39 – Extent to which respondents see an added value in the rules on automatic call forwarding, per stakeholder group

Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	9,6%	44,5%	45,9%	146
Citizens & civil society	48,4%	19,8%	31,9%	182
Public bodies	80,8%	3,8%	15,4%	26
All replies	34,7%	28,8%	36,4%	354

Source: Deloitte based on EC public consultation.

In its opinion on the ePrivacy Directive questionnaire, BEREC[352] stated that Article11 and the rule related to automatic call forwarding is relevant, but could be strengthened by extending it to all services using numbering resources (i.e. E.164), and potentially to other types of identifiers, such as SIP URIs.

5.11.4 Coherence

Key finding of the analysis: Coherence confirmed

The coherence of this provision is confirmed as no issues have been identified vis-à-vis the GDPR and the Electronic Communications Package.

Based on an analysis of the coherence of this provision towards the GDPR and the Electronic Communications Package, no challenges have been identified. Indeed, there are no similar rules contained in any of the instruments studied.

Automatic call forwarding is a specific subject addressed by the ePD. The closest parallel in the GDPR is the right to object to the processing of personal data under Article 21 of the GDPR, which however has a different scope. Unlike the right to stop automatic call forwarding, however, the right to object to the processing of personal data is broader and hinges on specific legal conditions.

Article 3(3) of the Radio Equipment Directive also sets out that radio equipment should allow for the incorporation of safeguards to protect the privacy and personal data of users and subscribers, which would include the possibility of acknowledging the choice made by the subscriber in in stopping the automatic forwarding of calls.

[352] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133. http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive p. 3

5.11.5 EU added value

Key finding of the analysis: Limited EU added value

Automatic call forwarding is a feature that is today built in by design by device manufacturers that are not necessarily (only) bound by EU law when designing their products. Thus, it is not the provision that enables citizens to make use of their rights but much rather the manufacturers of devices that apply international (not EU) standards in their product design.

Although difference exist in how the Member States have transposed this provision, citizens still benefit from having equal rights across the EU in this matter.

In addition, a similar argumentation as for itemised billing (see section 5.9) is applicable to this provision regarding citizens having the same rights across the EU. The ePD's nature as a Directive does not guarantee by default that citizens have the same rights towards itemised billing across the EU as Member States are free to transpose the Directive differently into national law.

5.12 Directories of subscribers (Article 12)

This provision aims at strengthening of the right of an online subscriber to **withdraw his/her name from an online public directory of subscribers**, e.g. an AOL customer could ask to have its email address removed from a publicly available list of AOL subscribers.[353]

Overview of the content

According to Article 12(1), subscribers who are natural persons must be informed about the purpose(s) of a printed or electronic directory of subscribers available/obtainable to the public, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory. Such information must be provided free of charge and before they are included in the directory.

In addition, Article 12(2), aims at ensuring that subscribers who are natural persons are given the opportunity to:

- Determine whether their personal data are included in a public directory;
- Determine which data is included (based on relevance); and
- Verify, correct or withdraw such data.

Subscribers must be able to do this free of charge.

In accordance with Article 12(3), Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.

Finally, the Member States shall also ensure in line with Article 12(4), in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.

[353] Edwards, L. (ed.) (2005). *The New Legal Framework for E-Commerce in Europe*. Oxford and Portland, Oregon: Hart Publishing, p. 48.

5.12.1 Effectiveness

Key finding of the analysis: Effectiveness tends to be confirmed

This provision appears to function rather effectively, as no serious challenges have been identified. However, there are doubts whether service providers actually inform subscribers of their inclusion in a public directory or if they do so, whether they are sufficiently transparent. This implies that this provision is not effectively enforced in all Member States.

In general, the scope of the Article does not cover OTTs, which may be a barrier for ensuring the full effectiveness of Article 12 (cf. also section 5.1).

Although a large part of the respondents (44%) did not have an opinion on this, according to the results of the ECs public consultation, close to 63% of respondents that had an opinion (115 of 183) had not encountered any problems in applying/understanding the rules regarding directories of subscribers.[354]

- *Industry:* Of the overall 63 responses that had an opinion, 33 (52%) had not encountered any problems, while 30 (48%) answered in the affirmative;
- *Citizens and civil society organisations:* Of the overall 106 responses that had an opinion, 71 (67%) had not encountered any problems, while 35 (33%) answered in the opposite;
- Only three of eleven public bodies that had an opinion indicated that they had encountered problems.

Table 40 – Extent to which respondents encountered problems in relation to the rules on directories of subscribers, per stakeholder group

Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	22,2%	26,7%	51,1%	135
Citizens & civil society	20,2%	41,0%	38,7%	173
Public bodies	17,6%	47,1%	35,3%	17
All replies	20,9%	35,4%	43,7%	325

Source: Deloitte based on EC public consultation.

As the majority of stakeholders across the different groups stated that they had not encountered any problems with regard to Article 12, it can be argued that the provision is effective in reaching its objectives.

Based on the online survey with businesses implemented as part of this project the Directive's provisions regarding directories of subscribers were a problem for one of six businesses that indicated this particular provision is of practical relevance for them.

According to the competent authorities responding to Deloitte's online survey, this article functions rather well. When asked about the functioning of the different provision, the majority of respondents indicated that Article 12 functions well (26.7%). In addition, 16.7% each indicated that the provision functions very well or fair. Similarly, the majority of competent authorities indicated that there are only moderate challenges in relation to this provision. In particular, there is doubt whether service

[354] It should be kept in mind, however, that a large part of respondents (141 of 322, 44%) did not have opinion about this.

providers actually inform subscribers of their inclusion in a public directory or if they do so, whether they are sufficiently transparent.

Table 41 – Challenges reported in the context of Article 12 (total n° of responses = 28)

	Not at all a problem	Minor problem	Moderate problem	Serious problem	Cannot answer
In practice, service providers fail to inform subscribers of their inclusion in a public directory or if they do so, they are not transparent enough (e.g. in privacy statements)	3	5	9	6	5
The conditions under which a consent is valid and how the consent should be delivered are not clear	6	3	9	4	6
The provision leaves it open to Member States to require additional consent in some situations (Article 12.3), leading to divergent practices and confusion	3	9	6	3	7

Source: Information provided by competent authorities of the EU Member States, tabulation by Deloitte. Blue marked cells denote highest values per row.

Based on the transposition check, the effectiveness of Article 12 is largely supported. Indeed, this article has been adequately transposed across almost all Member States as far as the rights of subscribers are concerned. Article 12(1)-(3) were transposed literally by the majority of Member States.[355] In most other Member States, no material differences have been observed. However, Article 12(2) was not completely transposed by Germany. Paragraph 3 was transposed with some differences in Austria[356] and not at all in Belgium, Estonia, Finland, and Sweden. As concerns paragraph 4, the large majority of the Member States did not transpose it at all as the national law applies to legal and natural persons.

Directories of subscribers are a pre-requisite for unsolicited marketing communications sent and received through the Internet, as well as through calls (see Article 13). 61% of EU consumers have indicated in the Eurobarometer survey[357] that they receive too many unsolicited calls offering them goods or services (see section 5.13). Similar to Article 13, this can be used as an argument that Article 12 does not reach its full effectiveness from the perspective of EU consumers.[358]

5.12.2 Efficiency

Key finding of the analysis: Insufficient information to assess

The information on compliance costs for businesses related to this article is limited.

[355] These include Bulgaria, Croatia, Czech Republic, Estonia, Finland, Greece, Latvia, Lithuania, Netherlands, Portugal, Romania, Slovakia, Slovenia, and Sweden.
[356] Austria did not opt for the possibility to ask for additional consent. A strict purpose restriction clause applies in this respect.
[357] Flash Eurobarometer 443 (2016): e-Privacy. Data on 26,526 consumers collected between 6 and 8 July 2016. At this stage, the Eurobarometer results are only of provisional character.
[358] At the level of individual cases, however, the question if the number of calls received is appropriate or not (i.e. 'too many' or not) depends of course of the number of instances in which an individual consumer has given his or her consent to being contacted.

It was pointed out in the public consultation that it involves significant information duties to subscribers. However, no information is available as concerns the magnitude of such costs.

Telecom operators have indicated, however, that there is a continuous cost to share information on subscribers with directories and to keep this information up to date. Such costs can be expected to increase with the number of subscribers. However, none of the stakeholders interviewed was able to provide a quantitative assessment of these costs.

5.12.3 Relevance

Key finding of the analysis: Relevance tends to be confirmed

The relevance of this provision tends to be confirmed, based on the fact that there are no similar rules in any other EU legal instrument and that directories of subscribers are a pre-requisite for unsolicited marketing communications sent and received through the Internet, as well as through calls. This is confirmed by competent authorities and citizens. However, doubts were voiced by businesses: Telecom operators do not necessarily see the relevance of a legal obligation due to customer demand and competition driven market.

There are no similar rules in any other EU legal instrument, e.g. the GDPR, supporting the relevance of this provisions. The relevance may further be confirmed by the fact that directories of subscribers are a pre-requisite for unsolicited marketing communications sent and received through the Internet, as well as through calls (see Article 13).

This is largely confirmed from the perspective of competent authorities and citizens.

Feedback from the competent authorities during the meeting with the European Commission in 2016[359] on benefits of specific privacy provisions of the ePD regarding subscriber directories suggest that Article 12 is relevant – albeit the implementation differing between Member States. The reason for this is that directories are the primary sources of unsolicited marketing calls, which are especially cumbersome for citizens. This is confirmed by Deloitte's online survey with competent authorities. Only 6.7% or two authorities indicated that this provision does not need to be retained, whereas 70% indicated that it would be important or useful to retain this provision, although some changes may be needed.

BEREC[360] states that Article 12 is relevant, but considered it a weakness that the Article does not cover legal entities.

The input from stakeholders to the public consultation is mixed as to the relevance of Article 12 and the results depend notably on the type of the responding stakeholders. Close to 40% of all respondents indicate that there is an added value of having specific rules. However, it is noteworthy that **a comparatively high share of all respondents did not have an opinion on this topic** (32%), being indicative of either indifference or lack of knowledge in relation to this article. The share of respondents not having an opinion on this **topic** (32%), being indicative of either indifference or lack of knowledge in relation to this article. Of those respondents from the industry who have an opinion, most indicated that there is no added value of having specific rules (also 42%). This was confirmed in

[359] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 5.
[360] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133. http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive p. 3

interviews with Telecom providers, who explained that the services were usually not requested by customers. On this basis, they did not see the need to uphold this provision. In contrast, absolute majorities of the respondents from the groups of the citizens and civil society (54%) and of the public bodies (69%) confirmed an added value of having specific rules.

Table 42 – Extent to which respondents see an added value in the rules on directories of subscribers, per stakeholder group

Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	15,2%	42,4%	42,4%	151
Citizens & civil society	54,4%	19,2%	26,4%	182
Public bodies	69,2%	23,1%	7,7%	26
All replies	39,0%	29,2%	31,8%	359

Source: Deloitte based on EC public consultation.

In line with these results, as part of the interviews carried out with telecom operators, it was emphasised that many of the measures regarding privacy (incl. directories of subscribers) would have been implemented by the telecoms due to the customer demand and competition driven market – i.e. also in the absence of a legal obligation to do so. Thus, telecom operators do not necessarily see the relevance of this provision.

In addition, telecom operators also believe that provisions concerning the directories for subscribers and calling line identification are now outdated.

5.12.4 Coherence

Key finding of the analysis: Coherence confirmed

The coherence of this provision is confirmed as no issues have been identified vis-à-vis the GDPR and the Electronic Communications Package.

Based on an analysis of the coherence of this provision towards the GDPR and the Electronic Communications Package, no challenges have been identified.

This provision is specific to the ePD and complements the general legal framework, bringing forth greater clarity as to the exercise of such rights. In comparison with Directive 95/56/EC and the GDPR, it also covers the protection of the rights of legal persons.

No significant connections with the Electronic Communications Framework have been identified.

Further details are provided in Annex F.

5.12.5 EU added value

Key finding of the analysis: EU added value tends to be confirmed

Although difference exist in how the Member States have transposed this provision, citizens still benefit from having equal rights across the EU in this matter.

The provision on directories of subscribers is considered to have EU added value as citizens benefit from having equal rights across the EU. In addition, businesses benefit from potentially similar

standards in the Member States. This being said, as a Directive, the ePD leaves leeway for Member States to differ in their national transposition from EU law which is considered to be a barrier for the EU added value of the provisions. While no specific further information was identified in this regard, none of the stakeholders consulted as part of this assignment declined its EU added value.

5.13 Unsolicited marketing communications sent and received through the Internet (Article 13)

Article 13 aims to protect citizens and legal persons against unsolicited marketing communications.

Overview of the content

According to **Article 13(1)**, the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who are natural persons that have given their prior consent.

This means that, in line with **Article 13(2)** – where a natural or legal person obtains from its customers their electronic contact details for electronic mail in the context of the sale of a product or a service – the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services.

However, customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.

Following **Article 13(3)** relating to natural persons, Member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed:

- Either without the consent of the subscribers or users concerned;
- In respect of subscribers or users who do not wish to receive these communications;
- The choice between these options is to be determined by national legislation; or
- Both options must be free of charge for the subscriber or user.

Nevertheless, **Article 13(4)** prohibits sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender, which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene Article 6 of Directive 2000/31/EC.

Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected according to **Article 13(5)**.

Finally, according to **Article 13(6)**, Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to Article 13 may bring legal proceedings. In addition, Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article.

5.13.1 Effectiveness

Key finding of the analysis: Limited effectiveness

Based on the information available, it seems that Article 13 could not fully achieve its objective of protecting citizens and legal persons against unsolicited marketing communications. Based on citizens' perceptions and information (incl. statistics) provided by competent authorities, citizens still receive a high number of unsolicited marketing communications. The main reason cited by different types of stakeholders were the fact that the provisions allows for leeway in its implementation and that it contains several ambiguities. On this basis, the provision and is implemented in a fragmented manner in the Member States.

In general terms, a significant number of stakeholders faced problems with Article 13. As part of the EC's public consultation, almost half of the respondents indicated that they faced problems in applying or understanding the rules on unsolicited marketing communications. The share of those stating they faced problems is highest for citizens and civil society (55%). In the group belonging to the industry, slightly more respondents stated that they did not face problems (39%) compared to those who did face problems (37%).

Table 43 – Extent to which respondents encountered problems in relation to the rules on unsolicited marketing communications, per stakeholder group

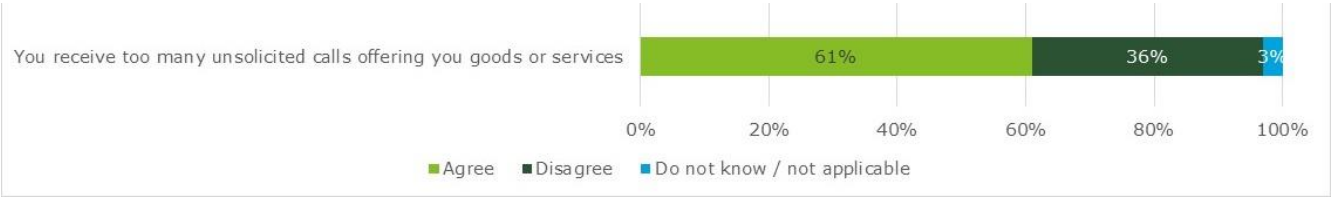
Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	37,4%	38,8%	23,7%	139
Citizens & civil society	54,5%	28,1%	17,4%	178
Public bodies	44,4%	33,3%	22,2%	18
All replies	46,9%	32,8%	20,3%	335

Source: Deloitte based on EC public consultation.

As part of the online survey with businesses implemented as part of this project, the Directive's provisions regarding unsolicited communications were a problem for ten of 18 businesses that indicated this particular provision is of practical relevance for them. Two of these businesses indicated that the most important problems refer to the clarity of the provisions (which has an effect on the implementation of the provisions in our services, e.g. in relation to storage), as well as to the incurred costs to comply with the provisions, e.g. concerning investments. In addition, it was raised as problematic that the implementation differs across Member States. For these two businesses, the existing problems resulted in a distortion of competition, e.g. between smaller and larger service providers, as well as decreased turnover / profit of them.

As concerns consumers' perception of the effectiveness of this provision, 61% of EU consumers have indicated that they receive too many unsolicited calls offering them goods or services.

Figure 24 – Consumers' assessment of the amount of unsolicited calls



Source: Eurobarometer, graphical representation by Deloitte.

Therefore, it can be argued that the Article does not fully reach its objectives as the majority of consumers, although they need to give their consent to receiving marketing communications, still find that they receive too many unsolicited calls offering them goods and services.[361]

This is confirmed by statistics gathered from the Member States as part of this initiative. The table below provides an overview of complaints by citizen received per Member State, including only Member States for which data was available at the time of the analysis.[362] For the Member States reflected, the number of complaints has increased between 2010 and 2015. UK and Germany received the highest number of complaints.

Table 44 – Complaints by citizens concerning Article 13 by Member State and year

Member State	2010	2011	2012	2013	2014	2015
Belgium	170	284	453	289	316	218
Bulgaria	0	0	0	87	100	45
Croatia	N/A	N/A	N/A	0	0	0
Cyprus	660	465	251	332	122	128
France				1071	932	2057
Germany	55,778	35,829	24,063	59,018	60,953	72,099
Greece	87	118	229	193	211	117
Ireland	231	253	606	204	176	104
Poland						91
Slovakia	128	91	132	288	155	95
Sweden				46	49	66
United Kingdom			79,018	199,376	175,248	166,663
Total	**57,054**	**37,040**	**104,752**	**260,904**	**238,262**	**241,683**

Source: Deloitte based on data made available by the competent authorities.

In comparison with the other provisions of the ePD, most competent authorities received the highest number of complaints for Article 13.[363] For example, the Greek DPA estimates that around 90% of all complaints received in relation to the ePD relate to Article 13.

Turning to the reasons for this lack of effectiveness, the most serious issue identified relates to the fact that Article 13 is implemented in a fragmented manner, notably due to a number of specific issues that have been identified as part of the research and stakeholder consultations carried out as part of this project:

- The possibility for Member States to choose between an opt-in and opt-out regime (Article 13.3);
- The possibility for Member States to choose how to deal with legal persons (Article 13.5); and
- Ambiguities relating to different provisions.

These are discussed in detail below.

[361] The extent to which the number of unsolicited marketing communications is inappropriate depends, of course, on the amount of instances in which each individual consumer has given his or her consent to receiving such communication.
[362] BE, BG, CY, DE, FR, GR, HR, IE, PL, SK, SE, UK.
[363] Based on statistics provided by the auhtorities and statements made in interviews Deloitte carried out with the authorities.

Based on the fact that **Article 13(3) leaves the possibility for Member States to choose between an opt-in and opt-out regime**, two different systems exist in the EU, leading to difficulties for various stakeholders.

The table below illustrates the wide diversity of regimes on unsolicited communications calls (with human intervention) and the fragmentation of the rules in the EU.

Table 45 – Opt-in and opt-out regimes per Member State

Member States	Number of businesses	Fixed-line phones		Mobile phones	
		Opt-in	Opt-out	Opt-in	Opt-out
Austria	321,661	X		X	
Belgium	593,421		X	X	
Bulgaria	319,856	X		X	
Croatia	147,337		X		X
Cyprus	46,938	X		X	
Czech Republic	995,754		X		X
Denmark	212,740	X[1]	X[2]	X[1]	X[2]
Estonia	64,040		X		X
Finland	229,248		X		X
France	3,188,138		X	X	
Germany	2,193,135	X[1]	X[3]	X[1]	X[3]
Greece	700,166		X		X
Hungary	514,537	X		X	
Ireland	146,741		X	X	
Italy	3,715,164		X		X
Latvia	100,491	X		X	
Lithuania	174,611	X		X	
Luxembourg	31,385	X		X	
Malta	26,193		X		X
Netherlands	1,054,562		X		X
Poland	1,549,326		X		X
Portugal	781,823	X		X	
Romania	455,852	X		X	
Slovakia	400,683	X[1]	X[3]	X[1]	X[3]
Slovenia	130,088		X		X
Spain	2,377,191		X	X	
Sweden	673,218		X		X
United Kingdom	1,841,715		X		X
		11	19	15	15
Number / share of businesses affected	22,986,014	4,771,889	20,238,860	11,077,380	13,933,369
		21%	88%	48%	61%

Source: European Commission, tabulation by Deloitte. [1]For 'consumers'; [2] For 'businesses'; [3] For 'other market players'. Statistical data from taken from Eurostat (most recent data from 2014).

The table shows that in relation to fixed-line phones, 24% of EU businesses currently are governed by an opt-in regime while the share is 52% in relation to mobile phones. By contrast, 88% of EU businesses are currently governed by an opt-out regime in relation fixed-line phones while 61% are governed by an opt-out regime for mobile phones.

All different stakeholder groups voiced concerns in relation to this provision. Business associations and businesses, for instance, have voiced concerns as part of the interviews over the fragmented

implementation of the provision in Article 13, especially with regard to the different interpretations of consent (opt-in vs. opt-out).

The different interpretations of Member States regarding the form of consent (opt-in vs opt-out) was also raised as an important issue by competent authorities interviewed by Deloitte and in Deloitte's online survey with competent authorities. The fact that Member States decide on the national level whether citizens are required to opt-out or opt-in with regard to unsolicited marketing communications is reported to pose a serious challenge by 8 out of 28 respondents while eight competent authorities also questioned the clarity of the conditions according to which it is possible to send direct marketing emails to users. Thus, overall, the effectiveness of this provision is limited for competent national authorities due to its ambiguity.

According to the responses received as part of the European Commission's public consultation, two thirds of respondents (63.6%) indicate that Member States should not retain the possibility to choose between an opt-in and opt-out regime for direct marketing telephone calls (with human interaction) directed toward individual citizens. This is valid across the stakeholders from industry, citizens and civil society organisations, as well as public bodies.

Hence, it can be argued that stakeholders see the possibility for Member States to choose between a prior consent (opt-in) and a right to object (opt-out) regime as a problem which, in turn, is an argument that the provision does not fully ensure reaching its objectives effectively.

Another aspect where the articles leaves leeway to Member States related to legal persons. Article 13(5) provides the **possibility for Member States to choose how to deal with legal persons**. More specifically, the provision specifies that the opt-in or opt-out consent regimes apply to natural persons. While Member States shall also ensure that the interests of legal persons are protected, it is not specified how this may be done. This may create fragmentation among Member States and thus have a negative effect on the Article's effectiveness in reaching its objectives. Indeed, 61% of respondents indicate that Member States should not retain the possibility to choose between and opt-in and opt-out regime for direct marketing communications to legal persons (automatic calling machines, fax, e-mail and telephone calls with human interactions).

Some additional **ambiguities have been identified in relation to the specific provisions** of the Article, as discussed below.

Article 13(1):

In relation to Article 13(1) confusion exists as to whether or not the Article is applicable to messages sent by means of **information society services**, in particular via so-called "webmail" or via social media platforms such as Facebook, Twitter, etc.[364] In addition, it is not fully clear if "direct marketing" encompasses as well **political marketing or fundraising** activities.[365]

Moreover, in light of the GDPR, stakeholders pointed out that there is need to clarify the definition of consent and the terms "unambiguous" vs "explicit".

[364] European Commission (2015), *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*. Final Report, (https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data), p. 89f.
[365] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 6.

Article 13(2):

Available evidence suggests that there are a number of ambiguities in relation to the application of this paragraph. These relate, for instance, to questions such as:

- Is browsing products and services on a website already part of a sale or its negotiations respectively and accordingly sufficient to allow for sending spam afterwards?[366]
- Is sending spam allowed in relation to similar products and services to those that were bought?[367]

Furthermore, it is not clear if spam is in practice only sent on the basis of identity details given away in a sale or also by simple browsing in an online shop, clicking on cookies, having access to exclusive sites or subscribing to a newsletter/voucher.[368]

In addition, it is not always clear if only the legal or natural persons that collected the identity details in a sale is allowed to send spam, or also subsidiaries or mother companies.[369]

It was also pointed out by a number of business associations that Article 13 is not well understood, especially regarding the objection rule for collecting email addresses. One interviewee specified that it is not clear for businesses under which circumstances they are allowed to use for marketing purposes the email addresses received from user's account registration while the users have not purchased goods or services yet.

Article 13(3):

It is not clear if Article 13(3) covers commercial communications received by users of social media (e.g. in their News Feed page) or whether such practices are covered by the opt-in regime applicable to e-mail.

5.13.2 Efficiency

Key finding of the analysis: Efficiency tends to be limited

Given that ambiguities exist for all types of stakeholders concerning the substance of this provision, as well as diverging approaches by Member States (transposed into national law) – which hamper the effectiveness of the provision – the costs related to this provision do not seem to be proportionate in all cases.

The evidence on the costs of compliance with Article 13 is limited.

Costs incurred by businesses relating to Art. 13 have been estimated together with costs due to Art. 5(3).[370] Thus, only an overall amount is available. The most important quantitative findings in this respect (i.e. concerning the compliance costs for businesses stemming from both Art. 5(3) and Art. 13) are presented in section 6.2.2, Table 57. The table contains quantitative results of the economic analysis for the REFIT exercise:

- Number of businesses affected (in million)

[366] Edwards, L. (ed.) (2005). The New Legal Framework for E-Commerce in Europe. Oxford and Portland, Oregon: Hart Publishing, p. 47.
[367] Ibid, p. 47.
[368] Ibid, p. 47.
[369] Art. 29 Working Party Opinion on Article 13 of Directive 2002/58/EC.
[370] The approach for estimating the costs is explained in the Economic Analysis Annex.

- Compliance costs (in million Euro)
- Average compliance cost per business (in Euro)
- Administrative burden (in million Euro)
- Average costs from admin. burden per business (in Euro)

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

A detailed explanation of the underlying assumptions and the model used to estimate these compliance costs are provided in Annex A.

Given that, as part of the interviews carried out, businesses have indicated that ambiguities exist – as well as difficulties through diverging interpretations of Member States – which hamper the effectiveness of the provision, the costs related to this provision do not seem to be proportionate in all cases. However, this has not explicitly been pointed out by any of the stakeholders consulted as part of this project as e.g. businesses generally see the costs related to legal obligations as costs they have to incur anyway – irrespective of whether they are proportionate or not.

As concerns the costs for businesses, according to Deloitte business survey, some trends regarding the costs of compliance with the unsolicited provisions have appeared, although the below figures cannot be considered as highly representative due to the limited number of respondents.

Overall, **five of eleven businesses** indicated in the online survey that they **incurred significant costs** in relation to the ePD's provisions concerning unsolicited communications. Article 13 was one of the three provisions that most businesses associated costs with.[371] The most expensive cost elements for these businesses concerned:

- Development / adaptation of technical infrastructure and / or software (3 businesses);
- Development and provision of training (1 business);
- Preparation of audits by competent national authorities (1 business); and
- Costs for advisory services, e.g. concerning legal interpretation of provisions.

Only few businesses were able to specify the amount of costs incurred by this provision:

- Between more than 1 million and 5 million Euro of one-off costs (CAPEX) per 100,000 subscribers, e.g. related to technical infrastructure for the storage of data (1 company).
- An average yearly cost (in Euro) of around 100,000 Euro (1 company);

This shows that the costs are difficult to measure for businesses and may vary significantly depending on the type and size of business.

It can be noted that three out of the five businesses that incurred significant costs in relation to Article 13 stated that they would have implemented some of the measures / the measures in a similar fashion also without the ePD in place.

Table 45 presents information on differences between Member States in respect of their opt-in and opt-out regimes, as well as the potential number of businesses affected by each of these regimes.

In the European Commission's public consultation, several respondents specifically raised Article 13 when asked about the costs incurred in relation to the ePD. While no specific numbers were provided,

[371] After the rules on confidentiality of communications (six businesses) and the rules on traffic and location data (five businesses).

it was indicated that costs are incurred in relation to adaptations in telemarketing procedures, e.g. initial costs to check opt-out registers (Robinson lists) the revision of lists, offering text-script on opt-out possibility and assistance in registering with related registers.

In addition to the compliance costs related to the direct implementation of the ePD, businesses also incurred **opportunity costs** for lost business opportunities. In Deloitte's business survey, all five businesses that indicated to have incurred costs in relation to Article 13 agreed that these costs included opportunity costs. This was also raised by several respondents to the public consultation as well as in interviews carried out by Deloitte. It was explained that unsolicited communication is in some ways the backbone of the entire industry in terms of marketing and sales. The necessity of prior consent by users in order to be contacted reduces potential business opportunities in marketing and sales.

Based on the high number of complaints received on these provisions, **competent authorities** have to dedicate substantial resources to this issue. Although it was not possible for competent authorities to provide inputs on the magnitude of such costs, some exemplary evidence was collected. For example, one DPA outlined their activities (excluding general dealing with requests) in relation to the ePD in a survey carried out by Deloitte. Between 2010 and 2015, Article 13 was clearly the provision the authority was most active on. It listed in total 11 activities for these years, including the publication of a brochure, guidance on how to technically obtain consent and enforcement in general. In comparison, one to three activities were carried out in relation to other provisions, namely Article 4(1) and 4(2), 5(2), 5(3), 8(3) and 12. Furthermore, the authority estimates that around 90% of all requests or complaints the authority receives on the ePD relate to Article 13. In this context, the UK authority Ofcom explained that the enforcement of Article 13 is challenging. Ofcom highlighted that it is particularly difficult to trace the source of such calls including based on the large number of different sources. For example, during May to October 2015 Ofcom identified nearly 8,000 different telephone numbers as the source of silent and abandoned calls.[372]

Case example Art. 13: The benefits of unsolicited communication

A representative of a UK-based online news and print outlet indicated as part of an interview that it is regarded as one of the key strengths of the ePD that it allows for unsolicited communication, especially in traditional markets (such as advertisement). He emphasised that the benefit of the ePD in this regard is that the rules would be clear and understandable to them and "work in practice" now. However, he also indicated that it took some time for his organisation to adapt to the current rules.

In addition, the interviewee pointed out that the current rules on unsolicited communication may be a barrier for businesses to develop alternative, modern revenue-generating models in the area of digital advertisement as the businesses could always fall back and rely on unsolicited communication as a baseline.

The interviewee was not able though to estimate any costs in relation to unsolicited communication for his organisation. He was only able to qualify that associated opportunity costs (i.e. forgone revenue if unsolicited communication would not be possible) could threaten businesses' revenue model, especially in the online news and print industry, as customers could always revert to

[372] See: ICO-OFCOM, Tackling Nuisance Calls and messages (December 2015): http://stakeholders.ofcom.org.uk/binaries/consultations/silentcalls/JAP_Update_Dec2015.pdf

alternative news sources in case a given news outlet would charge for its services. Essentially, the interviewee explained, online newspapers have turned into a commodity and the only way to actually make profitable business today (by simultaneously keeping up quality standards of journalism) in that industry is to rely on unsolicited communication and the use of online advertisement based on tracking users.

Case example Art. 13: Fines (i.e. costs) imposed by a data protection authority of a large Member State

The officer interviewed of a data protection authority in a large Western European Member State indicated that his organisation, in 2016 alone, issued fines totalling approx. 1.8 million Euro to companies behind nuisance marketing. Those firms were responsible for more than 70 million calls and more than 500,000 spam text messages.

More specifically, the fines included:

- A 410,000 EUR fine for a firm responsible for over 46 million automated nuisance calls.
- A 59,000 EUR fine for a company which sent more than 500,000 texts urging people to support its campaign to leave the EU.
- A 295,000 EUR fine for a claims management company that made 17.5 million calls asking people if they had suffered hearing loss at work.

It was also pointed out that the DPA received more than 93,000 complaints so far in 2016 from citizens who have received nuisance calls and texts.

Case example Art. 13: Fines (i.e. costs) imposed by a data protection authority of a small Member State

An officer of a South-East European data protection authority indicated that between 2012 and 2013, the DPA has received approx. 20 complaints in relation to Art. 13.

Out of these 20 complaints relating to Art. 13, two cases resulted in which fines were imposed on one business each due to data leakage.

While the first business had to pay a fine of 30,000 EUR, the second business was only charged with a fine of 10,000 EUR.

5.13.3 Relevance

Key finding of the analysis: Relevance confirmed

As part of the EC's public consultation, the majority citizens and civil society organisation, as well as public bodies have supported the relevance of this provision. By contrast, the majority of respondents from the industry does not confirm an added value of specific rules on unsolicited marketing communications.

The relevance of having specific rules on unsolicited marketing communications sent and received through electronic communications can be evaluated on the basis of evidence gathered by desk research and the EC's public consultation. Overall, the **relevance of Article 13 can be confirmed**, yet citizens and civil society as well as public bodies on the hand and the industry on the other hand do not share this opinion.

Desk research revealed some **potential grey areas** and need for clarification related to this article. For instance, with regard to Article 13.2 it is questionable if undesired spam can in practice only be sent and received on the basis of identity details given away in a sale or also by simple browsing in an online shop, having access to exclusive sites or subscribing to a newsletter/voucher which can be conceived of as a part of a sale or its negotiations and thus as a door-opener to send spam.[373] Furthermore, questions have been raised about what classifies as "similar products and services" to those that were bought.[374] Only this example shows that provisions of Article 13 might mismatch needs or problems and that it might thus not be completely relevant.

However, according to the stakeholder opinions gathered in the EC's public **consultation more than a half of the respondents (57%) confirm that there is an added value** of having specific rules on unsolicited marketing communications sent and received through the Internet. Large majorities of the respondents from the groups of the citizens and civil society (90%) and of the public bodies (86%) support this overall tendency. For instance, BEREC[375] states that Article 13 is relevant, and notes that the current ePD is stricter than the GDPR as it requires opt-in instead of opt-out, which is the preferred means of limiting spam to a minimum.

In contrast, the majority (63%) of the respondents from the industry does not confirm an added value of specific rules on unsolicited marketing communications sent and received through the Internet. The **clear opposition of the industry** might particularly stem from the advertising industry and its interest to conduct its business without restriction.

Table 46 – Extent to which respondents see an added value in the rules on unsolicited marketing communications, per stakeholder group

Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	26,8%	64,1%	9,2%	153
Citizens & civil society	77,2%	15,2%	7,6%	184
Public bodies	85,7%	7,1%	7,1%	28
All replies	56,7%	35,1%	8,2%	365

Source: Deloitte based on EC public consultation.

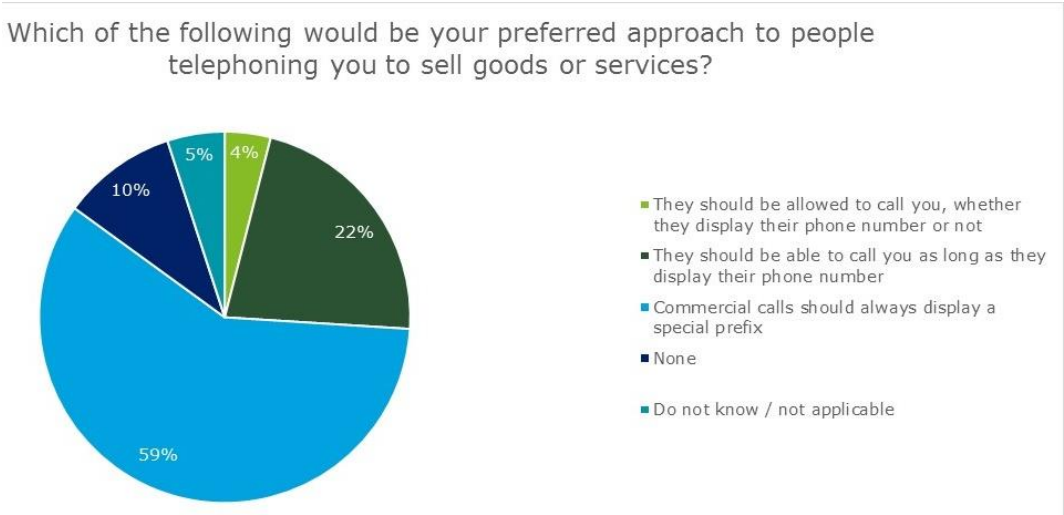
The relevance of this provision is further confirmed by the Eurobarometer on ePrivacy: The results show that EU consumers have a clear preference for an identification of people telephoning them to sell goods or services by means of:

- Display a special prefix to commercial calls (59%); and / or
- Displaying their phone number (22%).

[373] Edwards, L. (ed.) (2005). The New Legal Framework for E-Commerce in Europe. Oxford and Portland, Oregon: Hart Publishing, p. 47.
[374] Ibid, p. 47.
[375] BEREC (2016) 'BEREC Response to the eprivacy Directive questionnaire', BoR (16) 133. http://www.berec.europa.eu/eng/document_register/subject_matter/berec/opinions/6137-berec-response-to-the-ec-questionnaire-on-the-eprivacy-directive p. 3

The detailed Eurobarometer results regarding consumers' preferences concerning the identification of commercial calls are provided in the pie-chart below.

Figure 25 – Consumers' preferences regarding the identification of commercial calls



Source: Eurobarometer, graphical representation by Deloitte.

5.13.4 Coherence

Key finding of the analysis: Coherence partially confirmed

Based on the evidence available, there are no challenges in relation to the external coherence of this provision. However, there could be potential challenges in relation to the internal coherence. This is due to the leeway for Member States to decide about the specificities of their national regimes (opt-in vs. opt-out, see Table 45), as well as the incoherence of the regimes under Art. 13(1) and 13(3) perceived by different types of stakeholders.

Based on an analysis of the coherence of this provision towards the GDPR and the Electronic Communications Package, it was found that there are no similar rules contained in any of the instruments studied.

As part of the European Commission's public consultation, respondents where queried regarding – based on Article 13(3) – the choice left to Member States to make telemarketing calls subject either to prior consent or to a right to object, as well as the (internal) coherence of this provisions with Article 13(1). While 111 respondents (31%) indicated that Articles 13(3) and 13(1) would be coherent, a majority of 176 respondents (49%) disagreed.

Interestingly, differences exist between the responses received from specific stakeholder groups. As can be seen in the table below, each stakeholder group has a very different view from each other as regards the coherence of Articles 13(1) and 13(3). While industry stakeholders seem to be rather unsure about the coherence of the Article's provisions, citizens and civil society stakeholders, as well as public bodies seem to have comparatively strong opinion: in both groups a large majority indicated that the provisions are not coherent.

Table 47 – Responses of different stakeholder groups regarding the coherence of Art. 13(1) and 13(3)

	Yes	No	No opinion	Total nr. of

				responses
Industry	41,4%	31,8%	26,8%	157
Citizens and civil society	21,2%	61,5%	17,3%	179
Public bodies	30,8%	61,5%	7,7%	26
All replies	30,7%	48,6%	20,7%	362

Source: European Commission's public consultation, tabulation by Deloitte

5.13.5 EU added value

Key finding of the analysis: EU added value confirmed

There is a clear EU added value of this provision as both businesses and citizens potentially benefit from a set of similar rules and rights across the EU. However, the ePD leaves leeway for Member States to differ in their national transposition from EU law which is considered to be a barrier for achievement of the *full* EU added value of the provision.

5.14 Development and free circulation of electronic communication equipment and services (Article 14)

The objective of Article 14 is to avoid mandatory requirements for specific technical features that would hinder the development and free circulation of equipment/services in the internal market.

Overview of the content

Based on Article 14(1) Member States shall ensure that no mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

It is, however, possible that specific technical features in electronic communications equipment are needed to ensure the implementation of other provisions of the ePD. In this case, Member States must inform the Commission (Article 14.2).

According to Article 14(3), it is allowed to adopt measures ensuring that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data.

5.14.1 Effectiveness

Key finding of the analysis: Insufficient information to assess

Very limited information relating to the functioning of this article at the operational level is available.

Based on the online survey with businesses implemented as part of this project one of five businesses that indicated that this provision is of practical relevant for them indicated that they faced a problem with this provision.

5.14.2 Efficiency

Key finding of the analysis: Insufficient information to assess

The information on **compliance costs for businesses** related to these provisions is limited.

Case example Art. 14: Costs incurred by a global telecom equipment manufacturer

As part of an interview, the representative of a global, non-EU telecom equipment manufacturer ensured that that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data.

According to the interviewee, the development and implementation of such technical solutions in their devices is associated with significant costs.

Selling terminals with Android software, enriched by own customisations and applications, the company maintains a department of 200 full-time developers whose task is also partially to develop relevant technical solutions to protect and control the use of their personal data.

The interviewee asserted that the costs for the development of such solutions today range from 5 Mio. EUR to 10 Mio. EUR and have increased significantly in view of the requirements of the ePD.

5.14.3 Relevance

Key finding of the analysis: Insufficient information to assess

No specific information was identified with regard to the EU added value of this provision. At the same time, this means that none of the stakeholders consulted as part of this assignment declined an EU added value of this provision.

5.14.4 Coherence

Key finding of the analysis: Coherence confirmed

The coherence of this provision is confirmed as no issues have been identified vis-à-vis the GDPR and the Electronic Communications Package. A positive relationship has been established in relation to the RED, as the ePD and the RED complement each other.

Based on an analysis of the coherence of this provision towards the GDPR, the Electronic Communications Package and the RED, no challenges have been identified. A positive relationship has been established in relation to the RED, as the ePD and the RED complement each other. Furthermore, this provision reflects the aim to establish an internal market.

In the table below, we present the connection between the ePD and the GDPR as well as the Electronic Communications package. For each relevant provision[376] we provide a brief summary, using the following colour code[377]:

[376] We only list those instruments and provisions that a have connection to the ePD.
[377] The summaries and colour classification are to be seen as indicative.

- Green: positive relationship (e.g. synergies);
- Grey: neutral relationship/no challenges nor positive aspects identified; and
- Yellow: potential challenges.

Further details are provided in Annex.

Table 48 – Coherence of Article 14 with the GDPR, the Electronic Communications package and the RED

Provision in the ePD	Provision in the other instrument	Main findings
GDPR		
Technical Features and Standardisation (Article 14)	- Data protection by design and by default (Article 25)	Paragraph 1 of Article 14 of the ePD seeks to ensure the free movement of electronic communication equipment and services, in accordance with one of the two overarching objectives of the Directive. This goal, as noted above, is shared with the GDPR, although the specific reference to a prohibition on measures impeding harmonisation is more suited to a Directive than to a Regulation.
Electronic Communications Package		
Framework Directive		
Technical features and standardisation (Article 14)	Standardisation (Article 17)	The rules overlap, but are not conflicting.
Radio Equipment Directive		
Technical features and standardisation (Article 14)	- Essential requirements (Article 3) - Obligations of manufacturers (Article 10)	Paragraph 1 of Article 14 of the ePD seeks to ensure the free movement of electronic communication equipment in the Union by restricting the possibility that Member States impose mandatory requirements for specific technical features on terminal or other electronic equipment that could impede the placing of equipment on the market or affect its free circulation. Paragraph 3 of Article 14 of the ePD, on the other hand, specifically alludes to the possibility that certain technical requirements be imposed in connection with the right of users to protect and control the use of their personal data. The ePD is therefore coherent with the RED, which sets out in paragraph 3 of Article 3 that radio equipment should incorporate "*safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected*". This requirement is reinforced by paragraph 1 of Article 10 of the RED, which imposes upon manufacturers of radio equipment the obligation to "*ensure that it has been designed and manufactured in accordance with the essential requirements set out in Article 3*". The relation between these provisions can be summed up thus: the ePD permits certain specifications to be imposed for electronic equipment in the name of privacy and personal data protection, while the RED specifies that manufacturers of electronic equipment are subject to this obligation. The complementary nature of the ePD and the RED is further enhanced by the fact that the EC is empowered to adopt delegated acts specifying which categories or classes of equipment are concerned by this provision (*cf.* Article 44 of the RED), though only with respect to the categories or classes of radio equipment concerned.

Source: Deloitte.

5.14.5 EU added value

Key finding of the analysis: EU added value confirmed

The EU added value of this provision can be confirmed based on the responses received as part of the EC's public consultation. Especially responses from citizens & civil society, as well as from public bodies are largely in favour of EU rules regarding the free movement of electronic communications equipment and services. However, a small majority of businesses are not in favour of such EU rules.

Information concerning the EU added value of the ePD's provision relating to the development and free circulation of electronic communication equipment and services is available through the feedback received on the Commission's public consultation.

Neither as part of the interviews with stakeholders, nor as part of the online surveys with businesses and competent national authorities have any issues in this regard been identified.

A statistical overview of the responses is provide below.

Table 49 – Necessity of EU rules to ensure the objective of free movement of electronic communication terminal equipment and services in the EU

	Yes	No	No opinion	Yes	No	No opinion	Nr. of responses
Industry	35	87	27	23%	58%	18%	149
Citizens & civil society	115	34	34	63%	19%	19%	183
Public bodies	19	3	6	68%	11%	21%	28
Total	169	124	67	47%	34%	19%	360

Source: EC public consultation, tabulation by Deloitte

The public consultation asked if specific rules at EU level necessary to ensure the free movement of electronic communications equipment and services. Overall, 360 responses were received regarding this question. Approx. half of respondents (47%) indicated that EU rules are necessary to ensure this objective while close to one third indicated the opposite (34%). Around one in five of respondents (19%) did not have an opinion on this.

Thus, more than half of the respondents that had an opinion (58%) are in favour of EU rules concerning the free movement of electronic communications equipment and services.

Looking at the feedback in more detail, it can be seen that responses from citizens & civil society, as well as from public bodies are largely in favour of EU rules regarding the free movement of electronic communications equipment and services. Around to two thirds of these groups (63% of 183 responses from citizens and civil society organisations; 19 of 28 public bodies) replied positively to the question. Of all positive responses, 68% were provided by citizens and civil society organisations, 21% came from the industry, and 11% from public bodies.

A more detailed look at responses received from the industry shows, however, that 58% are not in favour of EU rules regarding the free movement of electronic communications equipment and services. Close to 24% replied positively while 18% did not have an opinion.

Focusing only on those responses that are either in or not in favour of EU rules, the trends identified above are being intensified with citizens and civil society organisations being heavily in favour of EU rules while the industry is against.

5.15 Enforcement (Article 15a)

The objective of Article 15a is to support the effective enforcement of the ePD.

Overview of the content

According to Article 15a Member States shall:

- Lay down the **rules on penalties**, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive. The penalties provided for must be effective, proportionate and dissuasive and effectively implemented. The relevant measures and amendments must be notified to the EC.
- Ensure that the competent national authority and, where relevant, other national bodies have the **power to order the cessation of infringements of the national provisions transposing the ePD**.
- Ensure that the competent national authority and other relevant national bodies have the **necessary investigative powers and resources**, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant to this Directive.

Article 15a(4) indicates that the relevant national regulatory authorities may adopt measures to ensure **effective cross-border cooperation** in the enforcement of the ePD. They may also create harmonised conditions for the provision of services involving cross-border data flows.

The national regulatory authorities shall provide the Commission, in good time before adopting any such measures, with a summary of the grounds for action, the envisaged measures and the proposed course of action. The Commission may, having examined such information and consulted ENISA and the Article 29 Working Party, make comments or recommendations thereupon, in particular to ensure that the envisaged measures do not adversely affect the functioning of the internal market. National regulatory authorities shall take the utmost account of the Commission's comments or recommendations when deciding on the measures.

5.15.1 Effectiveness

Key finding of the analysis: Limited effectiveness

Based on the information gathered, Article 15a does not fully achieve its objective of ensuring the effective enforcement of the ePD. A couple of specific challenges have been identified in relation to Article 15a, hindering its effectiveness. These relate to the following points:

- The ePD leaves it up to Member States to designate the national bodies for enforcement of the ePD, leading in particular to confusion for citizens, service providers and public bodies and potentially a duplication of work;
- There is insufficient guidance in relation to cross-border cases; and
- There is no recognised EU group to gather together all authorities responsible for the

enforcement of the ePD.

First, it was raised by different stakeholders as a challenge that **the ePD leaves it up to Member States to designate the national bodies for enforcement of the ePD.**[378] On this basis, the Member States have followed different approaches. Some Member States have designated DPAs (e.g. Bulgaria, Estonia, France), others the telecom national regulatory authority (NRAs) (e.g. Belgium, Finland, Denmark) and still others appointed both DPAs and NRAs (e.g. Austria, Germany, Greece) for the ePD enforcement. In some Member States, competence concerning the ePD is even shared between three or four different authorities,[379] including in addition to DPAs and NRAs e.g. consumer protection authorities. The following table presents an overview of the situation in the Member States.

Table 50 –Competent national authorities to enforce the ePrivacy Directive implementing provisions (Articles 5, 6, 9 & 13)

Country	Authorities	Provisions		
		Article 5	Articles 6 & 9	Article 13
AT	NRA	x	x	x
	Telecom office	x	x	x
	DPA			x
BE	Ministry for Economy			x
	NRA	x	x	x
	Ombudsman for telecoms	x	x	x
	Regional supervisory authorities for the media sector	x	x	x
	DPA	x		x
BG	NRA	x	x	x
	DPA	x		x
	Commission for Consumer Protection	x	x	x
HR	NRA	x	x	x
	DPA	x	x	x
	Ministry for Economic Affairs			x
	Ministry of Finance			x
CY	NRA	x	x	x
	DPA	x	x	x
CZ	DPA	x	x	x
DK	DPA	x		
	The Telecommunications Complaints Board		x	
	Competition and Consumer Authority			x
	Consumer Ombudsman			x
ES	NRA	x	x	
	DPA			x
FI	NRA	x		
	DPA		x	x
FR	NRA	x	x	x
	DPA	x	x	x
	Ministry of Economic Affairs			x
DE	NRA	x	x	x
	DPA	x	x	x
	Data Protection Commissioners of the German Lands	x		

[378] Cf. e.g. European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive), p. 11.
[379] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive), p. 11.

Country	Authorities	Provisions		
GR	NRA	x	x	x
	DPA	x	x	x
HU	NRA	x	x	x
	DPA	x	x	x
	Consumer Protection Inspectorates/National Authority			x
IE	NRA		x	
	DPA	x	x	x
IT	DPA	x	x	x
LT	NRA	x		
	DPA	x	x	x
	Ministry of Transport	x	x	x
	Consumer Protection Authority			x
LI	DPA	x	x	x
LU	DPA	x	x	x
MT	DPA	x	x	x
NL	NRA	x	x	
	DPA	x		x
	Consumer Protection Authority	x		x
PL	NRA	x	x	x
	DPA	x	x	x
	Office of Competition and Consumer Protection			x
PT	NRA	x		
	DPA	x	x	x
RO	DPA	x	x	x
SK	NRA	x	x	x
	Ministry of Transport	x	x	x
	Ministry of Finance	x		
SI	NRA	x	x	x
	DPA		x	
	Market Inspectorate			x
ES	DPA	x	x	x
SE	NRA	x	x	
	Consumer Agency			x
UK	NRA	x	x	x
	DPA	x	x	x
	Financial Authority			x

Source: Prepared by Deloitte on the basis of the 2015 European Commission study[380].

This situation potentially leads to the following problems:

- The situation may lead to confusion for citizens, service providers and public bodies and potentially a duplication of work;
- Enforcement may be hampered if responsibilities are shared between two or more authorities; and
- Authorities in charge of the enforcement of the ePD may differ in nature and have different sensibilities[381], which may lead to varying interpretations of the law.[382]

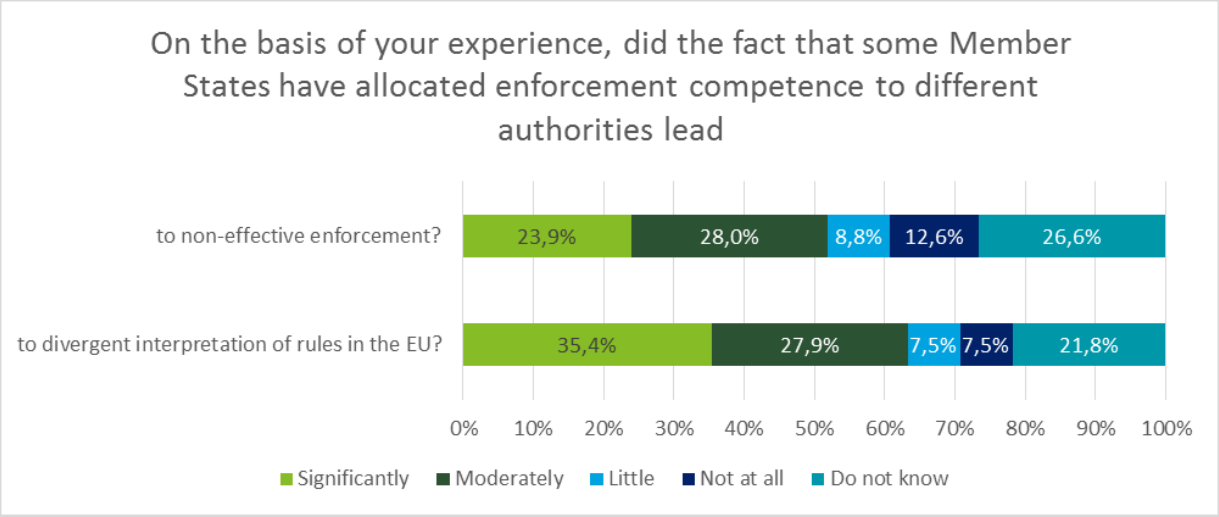
[380] European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071)
[381] For example, the DPAs will put more emphasis on data protection as such, whereas NRAs may bring in another perspective.
[382] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive), p. 11.

These points were also assessed by the EC's public consultation. First, respondents were asked, whether the fact that some Member States have allocated enforcement competence to different authorities lead to:

- Divergent interpretation of rules in the EU;
- Non-effective enforcement.

As demonstrated in the figure below, a higher share of respondents indicated that the situation significantly contributed to a divergent interpretation of the rules (35%) than to non-effective enforcement (24%). Vice versa, a higher share of respondents indicated that the situation does not at all lead to non-effective enforcement (13%) than divergent interpretation (8%).

Figure 26 – Public Consultation's results regarding fragmentation of enforcement of the ePD



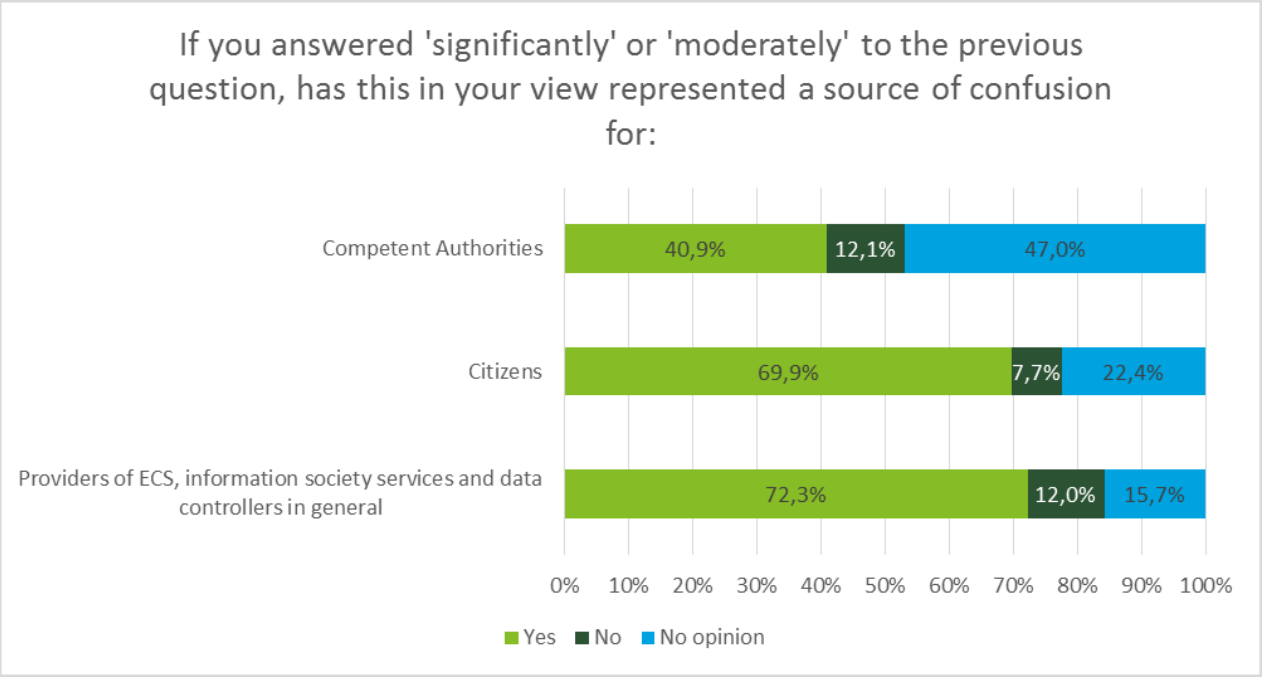
Source: EC public consultation, figure prepared by Deloitte.

Respondents who answered "significantly" or "moderately" to the previous question were also asked, whether the fact that some Member States have allocated enforcement competence to different authorities represented a source of confusion for:

- Providers of electronic communication services, information society services and data controllers in general (below referred to as providers and controllers);
- Citizens; and
- Competent authorities.

Based on the overall replies, the situation seems to be a particular source of confusion for citizens (70%) and providers/controllers (72%) (cf. the following figure).

Figure 27 – Public Consultation's results regarding confusion in relation to the enforcement of the ePD



Source: EC public consultation, figure prepared by Deloitte.

This is confirmed by the replies from the individual groups. The large majority of respondents belonging to the group of citizens and civil society (82%) indicated that the situation causes confusion for citizens. Similarly, the large majority of respondents from the industry (86%) indicated that the situation would lead to confusion for providers/controllers. This is supported by the interviews Deloitte carried out with businesses, in which some indicated that they sometimes do not know which authority to contact. Of the eleven public bodies responding to this question of the public consultation, 6 indicated that the situation would also lead to confusion for competent authorities.

The views of central authorities consulted by Deloitte are divided on this aspect. Many authorities interviewed think that the current shared institution set-up regarding the ePD is appropriate, as the authorities have specific competencies. The dialogue and cooperation between the different authorities are seen as positive.[383] However, some authorities also argued that efficiency is reduced when more than one institutions are competent on the same matter.

Details on the enforcement powers and activities of the authorities

Most of the competent authorities have **investigation powers** which include auditing. In general, it appears that the competency for auditing telecoms lies more often within the NRA rather than with the DPA. Many of the authorities vested with audit powers have specific methodologies and audit tools. In the overall, the authorities tend to audit in cases where there is a specific risk or complaint by an individual. Ex-officio audits remain a minority.

The big majority of competent authorities issues **guidelines and documentation** on the ePD. Some CA's appear to be more active than others with regard to issuing documentation. This

[383] In general, it appears that in most Member States, the DPAs and the NRAs cooperate and exchange information. In some cases, the cooperation happens more on ad hoc basis, in other cases, the cooperation is more formalised and regulated via agreements between the institutions (e.g. MoU).

depends as well on the size and resources of the authority.

The topics on which the guidance is issued vary from one Member State to another. It appears that most of the authorities focused on issuing guidance regarding Article 5.3, 6 and 9. Some issued guidance on how to obtain consent for unsolicited marketing communication. They issue as well guidance on security measures." All the interviewees believe that the guidance produced is useful.

Another challenge which has been voiced in a stakeholder workshop organised by the Commission is the fact that there is **insufficient guidance in relation to cross-border cases**. Article 15a(4) allows for the adoption of measures, but does not provide any details.[384] Depending on the types of measures national authorities have taken in this regard, this could lead to confusion amongst citizens and service providers. In addition, the cooperation between authorities across borders may be hampered e.g. based on varying practices. In Deloitte's online survey with competent authorities, the majority of respondents indicated that they consider this as a problem. Almost half consider it a serious problem (13 out of 28), six as a moderate problem and four as a minor problem. Only one authority indicated that this is not an issue. We note, however, that the interviewed authorities indicated that cross-border cases are a rarity.

A final challenge is related to the fact that **there is no recognised EU group to gather together all authorities responsible for the enforcement of the ePD.** The article refers to the Article 29 Working Party, which only represents data protection authorities and thus not all competent authorities enforcing the ePD.[385] Indeed, the authorities meet in different constellations: DPAs meet through the Article 29 Working Party and NRAs through BEREC. In addition, some consumer bodies meet through the Consumer Protection Cooperation (CPC) network. The fact that the Article 29 Working Party and the future European Data Protection Board (EDPB) only represent data protection authorities and thus not all national competent authorities is also considered as a problem by most of the competent authorities responding to Deloitte's online survey: around two thirds of the respondents consider it a serious problem (9 out of 28) or a moderate problem (8 out of 28). Another 14% consider this a minor problem. Five authorities do not regard this as a problem.

5.15.2 Efficiency

Key finding of the analysis: Insufficient information to assess

While limited information is available on the appropriateness of the costs relating to enforcement, we note that inefficiencies exist both for businesses and competent authorities due to the situation that Member States have appointed several different authorities (see section 5.15.1).

Some evidence concerning **the resources and costs associated with the work of competent authorities** in relation to the ePD was obtained as part of our online survey with competent authorities. The online survey was filled in by 34 authorities from 24 EU Member States, although not all authorities provided information on all questions. This information is patchy, as the survey has not

[384] European Commission (April 12, 2016). *Towards a future proof ePrivacy Legal Framework*. Minutes, p. 12.
[385] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive), p. 11-12; European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 5.

been filled in by all competent authorities and because many of them could not provide precise figures.

As concerns the **costs for the authorities to execute ePD-related tasks**, seven out of 28 authorities provided concrete numbers on their annual budget available. Amongst these, two provided figures in the range of around 600-700,000 Euro per year. There were four countries (some of them small) that indicated that a significantly lower budget is available (between 20,000 Euro and 70,000 Euro) and one Member State with more budget available (1 million Euro).

Two authorities specifically indicated that there is no separate budget for the ePD; only a budget for data protection activities in general. Of these, one authority indicated that they have 1.75 Mio Euro available for all aspects related to data protection legislation. Seven authorities indicated that there is no specific budget for ePD-related tasks.

In addition, competent authorities were asked about the **number of FTE assigned to ePD-related tasks**. As can be seen in the table below, in most authorities (32%) one to two FTE or even less than one FTE (28%) work on tasks related to the ePD. In around 20% of all responding authorities, three to nine FTEs work on tasks related to the ePD. One Member State indicated that a significantly higher number of persons work on tasks related to the ePD, namely around 25 FTEs.[386]

Table 51 – Number of FTEs working with tasks related to the ePD in the authorities

How many FTE[387] are working with tasks related to the ePD in your authority?		
Answer Options	**Response Percent**	**Response Count**
Less than 1 FTE	25.0%	7
1-2 FTE	32.0%	9
3-5 FTE	7.0%	2
6-9 FTE	11.0%	3
10 or more, please specify	7.0%	2
Other (please specify)	18.0%	5
	Answered question	**28**
	Skipped question	**6**

Source: Deloitte.

Turning to the **types of tasks** carried out, authorities were asked **how time consuming certain tasks are**.

Turning to the **types of tasks** carried out, authorities were asked **how time consuming certain tasks are.** As can be seen in the table below, the following items are perceived to be **most time-consuming** by the authorities carrying out these tasks:

- Preventive audits of individual service providers to check whether service providers comply with the security obligations;
- Preventive audits of individual service providers to check whether service providers comply with their notification obligations; and

[386] It was explained that this is an approximate estimate because in some areas the staff deals with both ePD and general data protection work. In those areas, the proportion of time spent on ePD issues was estimated.
[387] FTE stands for full time equivalent and equals to the hours worked by one employee on a full-time basis. In practice, one FTE position may be shared by more than one person (e.g. two persons working 20 hours per week equal one FTE).

- Developing recommendations on good practices.

Table 52 – Comparison of the time consumed for the different tasks

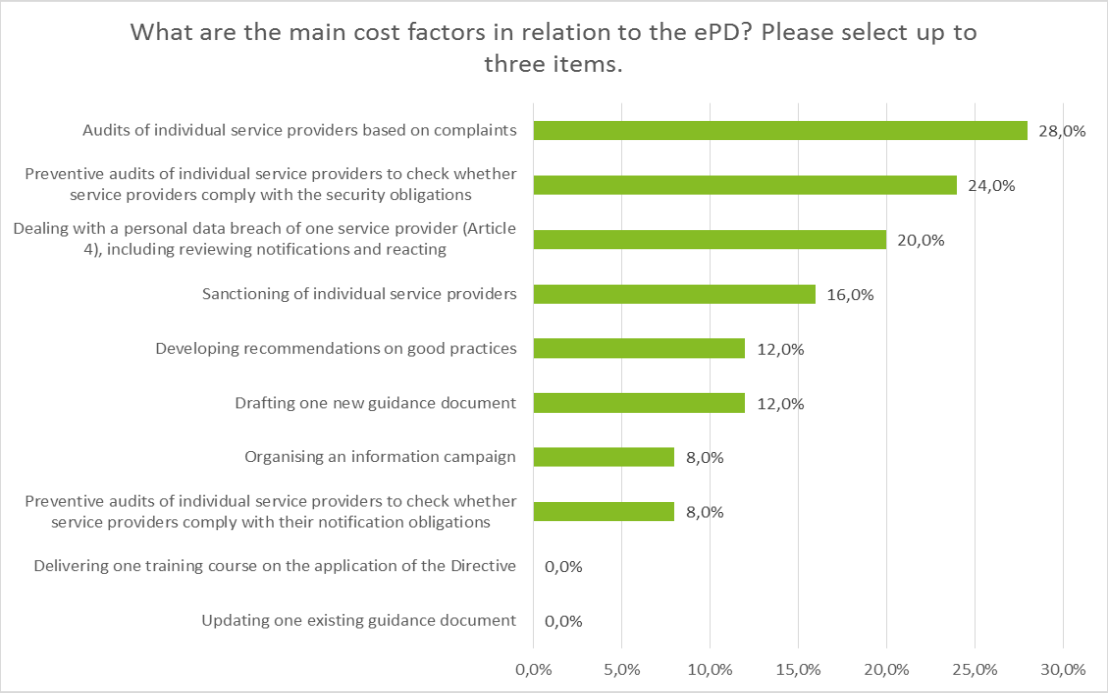
	Less than 1 working day	1 day – less than 3 days	3 days – less than a week	1 week – less than two weeks	2 weeks or more (please specify below)	Cannot answer
Preventive audits of individual service providers to check whether service providers comply with the security obligations	0	0	1	0	5	2
Preventive audits of individual service providers to check whether service providers comply with their notification obligations	0	0	1	0	3	0
Audits of individual service providers based on complaints	0	3	2	2	4	3
Dealing with a personal data breach of one service provider (Article 4), including reviewing notifications and reacting	3	3	1	2	1	3
Sanctioning of individual service providers	1	4	0	1	2	3
Drafting one new guidance document	0	2	1	2	5	0
Updating one existing guidance document	0	1	2	1	1	3
Developing recommendations on good practices	0	1	2	1	5	2
Delivering one training course on the application of the Directive	2	1	0	0	0	0
Organising an information campaign	0	0	1	2	1	1

Source: Information provided by competent authorities of the EU Member States, tabulation by Deloitte. Blue marked cells denote highest values per row.

Some authorities indicated that they carry out additional tasks. In particular, two authorities mentioned that they carry out tasks in relation to the enforcement of rules on unsolicited communications, one of them stating that this is particularly time-consuming.

The competent authorities were also asked to indicate which tasks they consider to be the **main cost factors** in relation to the ePD. As the most relevant ones, respondents named audits based on complaints, mentioned by 28%, and preventive audits, mentioned by 24%. In addition, 20% of the authorities consider dealing with personal data breaches to be one of the main cost factors.

Figure 28 – Main cost factors for competent authorities in relation to the ePD



Information provided by competent authorities of the EU Member States, presentation of data by Deloitte.

As concerns the **appropriateness of these costs,** little information is available. However, as pointed out in the previous section, the situation with several authorities appointed in each Member State may reduce efficiency.

As concerns the **business perspective,** we showed in the previous section that the current situation leads to confusion for businesses, meaning that businesses sometimes do not know which authority to contact. On this basis, it can be expected that undue costs may arise because businesses need to research the correct contact point or possibly contact the wrong authorities, causing additional work.

5.15.3 Relevance

Key finding of the analysis: Relevance tends to be confirmed

This provision gives practical guidance on how Member States should implement the ePD, which is important to ensure its consistent and effective implementation. The relevance was not questioned by any of the stakeholders consulted. However, it was questioned whether the content of this provision is fully in line with the needs of stakeholders and citizens.

No specific information was identified with regard to the relevance of this provision. However, it may be argued that this provision is important to ensure the consistent and effective implementation of the ePD. In particular, it provides guidance on enforcement measures. At the same time, none of the stakeholders consulted as part of this assignment declined the added value of this provision. However, it was questioned whether the content of this provision is fully in line with the needs of stakeholders and citizens (see section 5.15.1).

5.15.4 Coherence

Key finding of the analysis: Coherence partially ensured

Based on the evidence available, the coherence of this provision with other instruments is not fully ensured. Challenges have been identified in relation to the GDPR, as for data processing operations related to natural persons, there currently seems to be an overlap as regards the application of fines and sanctions for the breach of provisions related to the processing of personal data. At the same time, there is a positive relationship with the Framework Directive, as it reinforces the provisions in the ePD.

In the table below, we present the connection between the ePD and the GDPR as well as the Electronic Communications package. For each relevant provision[388] we provide a brief summary, using the following colour code[389]:

- Green: positive relationship (e.g. synergies);
- Grey: neutral relationship/no challenges nor positive aspects identified; and
- Yellow: potential challenges.

Further details are provided in Annex F.

The table shows that, while Article 15a works well with the Electronic Communications Package, there are potential challenges in relation to the interaction with the GDPR. For data processing operations related to natural persons, there currently seems to be an overlap as regards the application of fines and sanctions for the breach of provisions related to the processing of personal data. Legal persons are subjected only to the legal framework resulting from the ePD.

The competent authorities may also differ, as the ePD does not oblige Member States to grant competence to the data protection authorities in connection with the provisions related to these services (see transposition check, where this competence is sometimes bestowed upon telecom regulators and other agencies). On the other hand, the DPAs will be the relevant authorities for the imposition of fines and penalties resulting from the GDPR (notwithstanding certain statutory limitations in certain Member States).

Table 53 – Coherence of Article 15a with the GDPR and the Electronic Communications package

Provision in the ePD	Provision in the other instrument	Main findings
GDPR		
Implementation and Enforcement (Article 15a)	- General conditions for imposing administrative fines (Article 83) - Penalties (Article 84)	There are differences as concerns the application of fines and sanctions for the breach of provisions related to the processing of personal data and as for the competent authorities.
Electronic Communications Package		
Framework Directive		
Implementation and enforcement (Article	- National regulatory authorities (Article 3)	The provisions in the Framework Directive reinforces the provisions in the ePD.

[388] We only list those instruments and provisions that a have connection to the ePD.
[389] The summaries and colour classification are to be seen as indicative.

15a)	Implementation and enforcement (Article 13b)	

Source: Deloitte.

5.15.5 EU added value

Key finding of the analysis: EU added value confirmed

This provision gives practical guidance on how Member States should implement the ePD, which is important to ensure its consistent implementation. Consistency can only be achieved at the EU level.

This provision is important to ensure the consistent implementation of the ePD. In particular, it provides guidance on enforcement measures. Similar rules on enforcement across the EU can only be achieved by means of EU legislation. Therefore, this provision has a clear EU added value.

6 Conclusions on the REFIT evaluation of the ePD

In this section we present the conclusions for the assessment of the entire ePD towards the evaluation criteria. As this study concerns a REFIT evaluation, we took particular note of issues relating to regulatory burden, complexity, and costs. These are in particular discussed as part of the effectiveness, efficiency and coherence criteria.

6.1 Effectiveness

Although the ePD has contributed to enable more trust and confidence in the market, its effectiveness has not been fully achieved. While some of the provisions seem to function rather well, several challenges could be identified at the level of the operational objectives. In addition to the challenges identified in relation to the individual provisions (corresponding to the operational objectives), we have identified horizontal challenges, e.g. related to the complexity of the rules. Such challenges lead to difficulties in relation to the achievement of the specific and general objectives. The achievement of the operational, specific and general objectives is discussed in more detail below.

Based on the analysis presented in chapter 5, several challenges could be identified hindering the achievement of the **operational objectives** of the ePD. These findings are summarised in the following table. While the effectiveness could be achieved partially for some provisions (highlighted in green below), it was found that the effectiveness tends to be hindered in relation to the majority of provisions (highlighted in blue below).

Table 54 – Main findings in relation to the operational objectives

Operational objective of the ePD	Relevant articles	Main Findings
To ensure the security of services	Article 4	***Effectiveness not fully ensured*** The effectiveness of Article 4 does not seem to be fully ensured based on a number of challenges identified potentially hindering the achievement of the objective to ensure security of services. In particular, there are some ambiguities (e.g. to what extent the security obligations apply to non-personal data) and practical difficulties when it comes to the application of personal data breach notifications (confusion for businesses about which authority to contact, confusion based on the duplication with the GDPR, few breaches are notified hinting towards a low level of compliance, enforcement powers of authorities not always appropriate).
To ensure the confidentiality of communications as well as the related traffic data and other location data	Articles 5(1) and (2)	***Partially effective*** While Article 5(1) and (2) supported the achievement of the objective to ensure confidentiality of communications, **some issues** that potentially act as barriers in this respect have been identified. In particular, our research shows that some stakeholders faced obstacles in the practical application of this provision. Such difficulties may arise because the wording of the provisions is not sufficiently clear and potentially not in line with recent technological developments, also leading to varying implementation across Member States. Another issue raised by many stakeholders relates to the general scope of the ePD: it was criticised that in many Member States the provisions only apply to traditional telecom providers, not to OTTs. On the basis of these issues, citizens cannot rely on equal standards on the confidentiality of communications.
	Articles 6 and 9	***Not fully effective*** Based on the limited evidence available, the effectiveness of the specific provisions on traffic and location data does not seem to be fully achieved, as a number of problems seem to occur in relation to their application. First, the scope of Articles 6 and 9 only covers a small part of location based services, which is related to the general scope of the ePD which focuses on traditional telecom providers. In addition, there are ambiguities based on the interaction between Article 6 and 9 as well between the two Articles and Article 5(1) and (2), as it is difficult to distinguish between the different categories of data. Considering the exceptions under which traffic data and location data may be processed, it is questionable whether the possibility of processing traffic data for the purposes of subscriber billing and interconnection payments provided in Article 6.2 is still necessary considering that providers usually offer flat rate contracts. Turning to the consent mechanism, it was pointed out in the Commission's background paper to the public consultation that there are cases where traffic and location data might be used without consent. Finally, the provisions do not always seem to be enforced properly.
To ensure the confidentiality of information stored on the user's terminal equipment	Article 5(3)	***Partially effective*** Based on our findings, there is **room for improvement as concerns the effectiveness of this provision**. Although some strengths have been identified, several challenges were raised by various stakeholders and in the literature. These include in particular ambiguities in relation to the scope of this provision, the fact that

Operational objective of the ePD	Relevant articles	Main Findings
		the scope may be too broad, limited transparency and effectiveness of the consent mechanism as well as difficulties relating to enforcement. Based on these challenges, this provision is burdensome for businesses, while the effective added value for citizens may be improved.
To ensure that subscribers and users have a possibility to opt for non-itemised billing	Article 7	***Effectiveness tends to be confirmed*** Based on the available evidence, this provision seems to function rather effectively. However, some moderate challenges have been identified, e.g. there may be problems in relation to service contracts concluded by employers for their employees (the right to the employee's privacy may be endangered if the employer needs itemised billing). However, these issues do not appear to significantly hinder the effectiveness. There are no serious issues in relation to the transposition of this provision either.
To ensure that called and calling subscribers/users have possibilities for control over call line identification	Articles 8 and 10	***Effectiveness tends to be confirmed*** These provisions function rather well. No serious issues relating to this provision could be identified, which may imply that it is rather effective in reaching its objective. There are some minor or moderate challenges (e.g. it is unclear how providers or authorities should respond to users/subscribers who want to know who gave a call or through which line the call came in if there is a restriction to identify the calling and connected line). However, the effectiveness of these provisions does not appear to be significantly hindered based on these challenges. This is supported by the different stakeholder consultations carried out by Deloitte as well as the EC's public consultation and desk research. There are no serious issues in relation to the transposition of these provisions either.
To ensure that subscribers have the right to stop automatic call forwarding	Article 11	***Effectiveness tends to be confirmed*** The effectiveness of this provision tends to be confirmed as no serious issues have been identified. The provision appears to function rather well. The moderate challenges identified (e.g. it is unclear which safeguards should be provided for subscribers against the nuisance caused by automatic call forwarding by others) did not appear to seriously hinder the effectiveness of this provision. This is supported by the different stakeholder consultations carried out by Deloitte as well as the EC's public consultation and desk research. There are no serious issues in relation to the transposition of this provision either.
To ensure that have the right to be informed and decide about an inclusion in publicly available or printed databases of subscribers	Article 12	***Effectiveness tends to be confirmed*** This provision appears to function rather effectively, as no serious challenges have been identified. However, there are doubts whether service providers actually inform subscribers of their inclusion in a public directory or if they do so, whether they are sufficiently transparent. This implies that this provision is not effectively enforced in all Member States.
To protect citizens/consumers and legal persons against unsolicited communications	Article 13	***Limited effectiveness*** Based on the information available, it seems that Article 13 could not fully achieve its objective of protecting citizens and legal persons against unsolicited marketing communications. Based on citizens' perceptions and information (incl. statistics) provided by competent authorities, citizens still receive a high number of unsolicited marketing communications. The main reason cited by different types of stakeholders were the

Operational objective of the ePD	Relevant articles	Main Findings
		fact that the provisions allows for leeway in its implementation and that it contains several ambiguities. On this basis, the provision and is implemented in a fragmented manner in the Member States.
To avoid mandatory requirements for specific technical features that would hinder the development and free circulation of equipment/services in the internal market	Article 14	***Insufficient information to assess***
Horizontal aspect: To ensure the effective enforcement of the ePD	Article 15a	***Limited effectiveness*** Based on the information gathered, Article 15a does not fully achieve its objective of ensuring the effective enforcement of the ePD. A couple of specific challenges have been identified in relation to Article 15a, hindering its effectiveness. These relate to the following points: - The ePD leaves it up to Member States to designate the national bodies for enforcement of the ePD, leading in particular to confusion for citizens, service providers and public bodies and potentially a duplication of work; - There is insufficient guidance in relation to cross-border cases; and - There is no recognised EU group to gather together all authorities responsible for the enforcement of the ePD.

Source: *Deloitte*

In addition, horizontal observations have been made in relation to:

- The scope of the ePD;
- The transposition of the ePD;
- The complexity of the rules; and
- Stakeholders' awareness of the ePD.

As concerns the **scope of the ePD**, it was shown in section 5.4.1 that there are several challenges including ambiguities and doubts whether the scope is appropriate. In particular, it may be argued that the limitation of the scope to public or publicly available electronic communication services may not be appropriate due to the rise of new communication technologies (often internet based) and the actual needs of citizens.

The **transposition** of the ePD in the Member States varies considerably. A survey conducted in the context of the ePrivacy Study 2013/0071 on the transposition of the ePD in Member States confirmed that the provisions of the ePD[390] are not always correctly transposed in the correct national legal framework by Member States. Actually, the survey results revealed that the ePD provisions were not always transposed in the legal framework applicable to electronic communications but sometimes in in the legislation applicable to information society services, general data protection law or consumer protection.[391] Such discrepancies, typically lead to an ineffective legal framework impeding the achievement of the Digital Single Market.

The transposition check carried out for the purpose of this study showed that, while most provisions have been transposed (often literally) by most Member States, several specificities and differences could be identified. National laws vary in relation to the context, including e.g. type of legislative framework used, as well as in relation to some substantial aspects. For example, the question of whether OTT service providers and private networks are subject to the requirements of the ePD and the corresponding national implementing acts has not been uniformly addressed in the transposition of the ePD. Member States vary considerably in their approach to this topic. More importantly, the current *status quo* provides for appreciable differences in legal treatment across Member States, creating an uneven playing field for operators and a potential obstacle to the goals set out by the ePD.

Another horizontal issue relates to the **complexity of the rules**, which is based on different factors. First, some of the provisions of the ePD are complicated to interpret or apply. This relates in particular to the provisions entailing consent mechanisms, including Article 5(3) on information stored on users' terminal equipment and Article 13 on unsolicited communications. We found, for example, that it is not always clear when a consent is valid (e.g. in the case of cookie consent given via the browser). Second, the implementation of the ePD varies across Member States. In some cases this is due to differences in interpretation, e.g. some Member States included OTTs under scope of the ePD. In others it is due to the leeway given by the ePD, for instance in the case of Article 13 which gives Member States the option to choose between an opt-in or opt-out regime. This makes the situation more complex, which causes confusion to businesses and citizens. Indeed, some businesses interviewed by Deloitte indicated that they consider this to be one the most serious issues in relation to the ePD. Third, complexity may arise based on the interaction with other legal instruments. For example, several stakeholders indicated that it causes confusion that there are different notification

[390] The study did not deal with the entire ePD, but focused on the five following topics: (i) Article 1 and 3 on the scope, (ii) Article 5 on confidentiality, (iii) Article 5(3) on confidentiality of terminal equipment, (iv) Article 6 and 9 on traffic and location and (v) Article 13 on unsolicited communications.
[391] ePrivacy Study SMART 2013/0071, p.8

regimes for security and personal data breaches in different legal instruments, including the GDPR. Finally, some stakeholders reported that the fact that enforcement is in many Member States shared by different authorities hinders the application of the ePD, e.g. because it is sometimes not clear for businesses which authority to turn to or because it leads to duplication of work.

Regarding the **awareness of stakeholders** of the ePD, the big majority of the competent national authorities has confirmed in the interviews that businesses and especially large enterprises are aware of the ePD and the underlying obligations. On the contrary, however, the majority of competent national authorities have argued that consumers are not aware of the ePD and of their rights stemming from this legal instrument except for cookies and/or unsolicited marketing communication.

Some of these horizontal challenges were also discussed in Deloitte's online survey with competent authorities. Respondents were asked to assess **potential challenges hindering the success of the ePD**. As shown in the table below, i**nsufficient awareness among the users and subscribers** is viewed as the **most obstructive point** for the successful functioning of the ePD. Eleven authorities indicated that this is a moderate problem and ten that it is even a serious one. Altogether, 75% classify it as a problem. Additionally, many responded that **the scope of the ePD is too narrow**, **as well as** that **clarity of individual provisions can be improved**. In addition, several respondents consider it a serious or moderate problem that the legal framework on privacy in the electronic communications sector is too complex, as the rules are contained in different instruments (e.g. GDPR, Framework Decision).

Table 55 – Challenges hindering the success of the ePD (total n° of responses = 28)

	Not at all a problem	Minor problem	Moderate problem	Serious problem	Cannot answer
The scope of the ePD is too narrow	4	3	8	10	3
The scope of the ePD is too broad	14	6	5	0	3
The ePD is not coherent with other legal instruments, such as the GDPR	2	6	10	6	4
The legal framework on privacy in the electronic communications sector is too complex, as the rules are contained in different instruments (e.g. GDPR, Framework Decision)	4	4	11	6	3
Divergences in transposition between the Member States	1	7	10	6	4
There is lack of clarity of individual provisions	2	4	11	8	3
Enforcement are not effective	3	4	11	6	4
There is lack of awareness among service providers	2	11	8	4	3
There is lack of awareness among users/subscribers	0	4	11	10	3

Source: Information provided by competent authorities of the EU Member States, tabulation by Deloitte.

The findings at the level of the operational objectives influence the achievement of the **specific objectives**. To recall, the following specific objectives have been identified (cf. our intervention logic in section 3.3.2):

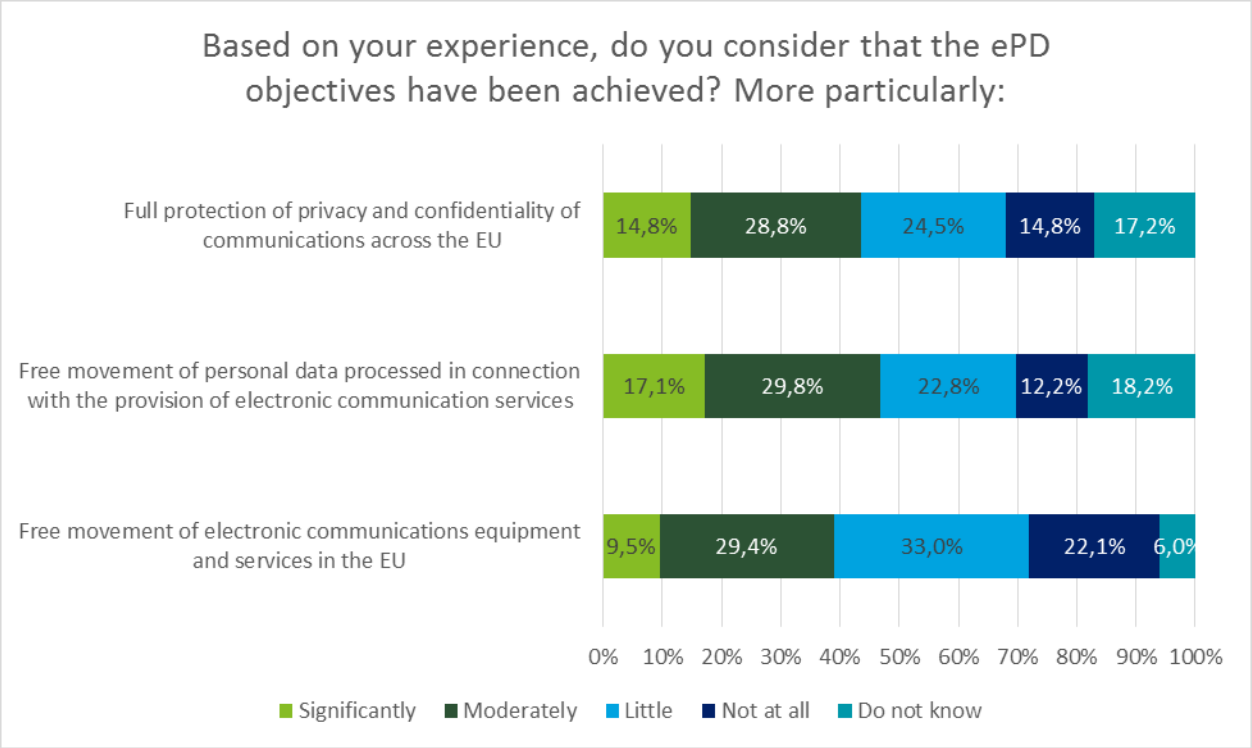
- To ensure that the right to privacy and confidentiality with respect to the processing of personal data in the electronic communications sector is respected;
- To ensure the free movement of personal data in the internal market; and
- To ensure the free movement of electronic communication terminal equipment and services in the EU.

Most challenges identified hinder the achievement of the right to privacy and confidentiality.[392] This is the case, for example, in relation to the limited effectiveness of Article 5. However, it is possible that issues relating to the right to privacy and confidentiality also hinders the free movement of personal data in the internal market. For example, if users do not trust in or understand the privacy standards applicable in other countries, they may be less inclined to make use of electronic communications services of providers that have their seat abroad.

Information in relation to the objective to ensure the free movement of electronic communication terminal equipment and services in the EU is limited. Yet, it can be noted that the effectiveness was not denied by any of the stakeholders.

The EC's public consultation also gives some insights in relation to the achievement of the specific objectives. On this basis, the picture in relation to all three objectives is mixed, as shown in the figure below. A slightly higher share of respondents thought that the free movement of personal data was "moderately" or "significantly" achieved, followed by privacy and confidentiality. As concerns the free movement of electronic equipment, fewest respondents indicated that this objective was "moderately" or "significantly" achieved.

Figure 29 – Achievement of the specific objectives of the ePD



[392] According to van Hoboken and Borgesius, "the EU lawmaker has not systematically addressed user privacy interests related to access to online content, interactive media, and the wide variety of opportunities offered by networked communications." Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. JIPITEC, Vol. 6 (2015), pp. 198-210, para. 2.

Source: EC public consultation, figure prepared by Deloitte.

As shown in our intervention logic presented in section 3.3.2, hurdles in relation to the achievement of the specific objectives influence the achievement of the following **general objectives:**

- To ensure respect for fundamental rights within the EU;
- To increase trust in electronic communication services and the market among citizens & companies; and
- To ensure the smooth functioning of the internal market.

For instance, difficulties in relation to the achievement of privacy and confidentiality may impact on the level of respect for fundamental rights in the EU as well as trust in electronic communication services. Difficulties in relation to the free movement of personal data and the free circulation of electronic equipment may impact on the smooth functioning of the internal market.

6.2 Efficiency

- This section focusses on the analysis of the efficiency of the ePD, i.e. of regulatory burden, complexity, and costs caused by it. The section provides the quantitative results of the economic analysis for the REFIT exercise as presented in Table 73Number of businesses affected (in million);
- Compliance costs (in million Euro);
- Average compliance cost per business (in Euro);
- Administrative burden (in million Euro); and
- Average costs from administrative burden per business (in Euro).

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

6.2.1 Evidence from the analysis of the individual provisions

Information based on which the efficiency of the ePD's provisions and consequently the Directive as such can be evaluated is very scarce.

The following table provides an overview of the main findings concerning the efficiency of each provision.

Table 56 – Main findings in relation to the efficiency of the provisions

Relevant articles	Main Findings
Article 4	***Partially efficient*** Overall, this provision is one of the most costly provisions, both for businesses and competent authorities. Nevertheless, some of these costs (e.g. the data breach notification) are only incurred in case of an actual breach, which is an incentive for implementing adequate security requirements. As not all of these costs seem to be justified (e.g. because duplications with other instruments exist), this provision is only considered partially efficient.
Articles 5(1) and (2)	***Tends to be efficient*** This provision has led to significant costs for businesses, including the setting up of IT infrastructure. However, these costs can be considered proportionate in light of the aim of ensuring confidentiality of communications. We also note that some of these costs may overlap with the security provisions, in case the IT solutions to ensure security and confidentiality overlap. Additional undue costs have may ensue for businesses based on the ambiguous wording of the provision and the fact that its implementation varies significantly across Member States (cf. the previous sub-section). Such costs may in particular relate to legal advice.

Relevant articles	Main Findings
	Finally, there are opportunity costs as the provisions render certain business models invalid. These costs can be considered proportionate in light of the aim of ensuring confidentiality of communications.
Article 5(3)	***Partially efficient*** The efficiency of Article 5(3) is not fully ensured. This is due to the fact that this provision tends to be the main cost factor associated by businesses with the ePD, while not all the costs appear to be justified and the benefits for citizens have been questioned. In particular, based on the ambiguities relating to the scope and consent mechanism, businesses may spend more time than needed on implementing the consent mechanism and possibly need to invest in legal advice. Furthermore, based on the fact that Article 5(3) does not make a distinction between different types of cookies, businesses that only use non-privacy invasive cookies also need to obtain consent. At the same time, users feel annoyed by the consent mechanism, which often does not provide a real choice.
Articles 6 and 9	***Insufficient information to assess*** Although businesses reported that they incurred some costs in relation to these provisions, no information is available on the magnitude of such costs. Businesses mainly incur compliance costs and opportunity costs. Compliance costs notably relate to the development / adaptation of technical infrastructure and / or software. These costs may be justified based on the added level of protection for users. Based on the ambiguities explained above (see section 5.8.1), it is also possible that businesses incur additional undue costs on legal advice, e.g. in case it is not clear under which regime a specific service falls. In addition, this may entail costs for competent authorities, as these may need to deal with unclear cases. Opportunity costs are incurred by providers of traditional telecom providers that face restrictions which do not apply to their OTT competitors.
Article 7	***Insufficient information to assess*** Stakeholders have emphasised the significant costs for the initial implementation of the provisions on non-itemised bills. However, no quantitative evidence is available. There are different opinions as to the benefits of this provision for consumers.
Articles 8 and 10	***Efficiency is limited*** In general terms, respondents to the European Commission's public consultation and interviewees indicated that significant costs were involved for the initial implementation of the provision on calling and connected line identification. Such costs related in particular to IT infrastructure. Some small recurrent costs may relate to the maintenance of such systems. As concerns the proportionality of such costs, Telecom operators explained that the services were not requested by customers.
Article 11	***Efficiency is limited*** The efficiency of this provision tends to be limited as the costs incurred by businesses to implement the possibility of stopping automatic call forwarding are much rather caused by legislative obligations than actual customer demand.
Article 12	***Insufficient information to assess***
Article 13	***Efficiency tends to be limited*** Given that ambiguities exist for all types of stakeholders concerning the substance of this provision, as well as diverging approaches by Member States (transposed into national law) – which hamper the effectiveness of the provision – the costs related to this provision do not seem to be proportionate in all cases.
Article 14	***Insufficient information to assess***
Article 15a	***Insufficient information to assess*** While limited information is available on the appropriateness of the costs relating to enforcement, we note that inefficiencies exist both for businesses and competent authorities due to the situation that Member States have appointed several different authorities (see section 5.15.1).

Source: Deloitte

The costs associated with the ePD may to some extent be justified by the **benefits** it brings:

- The ePD has limited benefits for telecom operators in the current situation as it imposes compliance costs and hinders them to pursue and develop new business models based on data (i.e. imposes opportunity costs). It can be argued that telecom operators working cross-borders benefits from the fact that the ePD makes rules more harmonised, meaning that

telecom operators do not need to adjust their policies as much as if they extent their business to another Member State. However, this benefit is limited by the fact that the ePD is a Directive and that there are still quite some differences between national implementations. A final potential benefit is increased trust by consumers based on higher privacy standards. This is rather a qualitative argument, which is hard to measure.

- Naturally, the perspective of OTT providers is a bit different. Without explicitly mentioning it, OTTs have the advantage that they are not covered by legislation and thus have all the benefits that telecom operators would like to enjoy themselves.
- This being said, the main benefits relate to consumers' privacy and confidentiality of communications. This is, however, a qualitative argument much rather than something that can be measured quantitatively.

However, there are still aspects that point to a limited efficiency of the ePD.

Horizontally across all types of stakeholders, the fragmented implementation of the ePD in the different Member States and the resulting complexity was pointed out an issue and an important source of cost. The reason is that e.g. businesses are not able to leverage existing legislative requirements and obligations for the business model but need to adapt. For instance, the transposition check showed that in some Member States the ePD was transposed in a more restrictive manner than provided by the ePD (and also compared to other Member States). In addition, some Member States have put more regulatory focus on specific areas of the ePD than others.

Business associations have pointed out that the costs related to the ePD are disproportionate. For instance, stakeholders believe that the costs related to the cookie provision are unjustified as the provision failed to accomplish its purpose. From the telecom sector perspective, the ePD legislation has disproportionate implementation costs due to the fact that different actors providing the same services are subject to different rules.

Based on the information collected as part of this study, it could be argued that there seems to be a trend towards limited efficiency of the ePD. Overall, however, the available evidence is very patchy and largely anecdotal.

Case example (horizontal): Compliance and administrative burden costs for a telecommunication service provider

The representative of a telecommunication service provider active in one South-Eastern European Member State and third countries indicated that the company would incur overall 400,000 EUR per year in relation to specific provisions of the ePD. The following high-level estimates were provided:

(1)	Submitting information to competent national authorities	25.000 €
(2)	Providing information to / communication with subscribers and users	75.000 €
(3)	Investments in technical infrastructure and related measures ensuring privacy and confidentiality to comply with the ePD.	250.000 €
(4)	Compliance with the ePD	25.000 €
(5)	Rules on spam and the rules on cookies, which are applicable beyond ECS	25.000 €
Overall		400.000 €

According to the interviewee, the estimates represent yearly annual costs calculated out of our overall annual costs (capex & opex) for IT, Security, Legal, PR/HR and other ePD relevant

streams/budgets respectively. Hence, the estimates follow rather a top-down than a bottom-up logic as the *actual* figures are not known to the company.

6.2.2 Results of the economic analysis

The Annex concerning the Economic Analysis contains information on and an explanation of the approach and methodology to get to the results referenced below.

Introduction and pre-requisites

Information on costs incurred by businesses in relation to the ePD is scarce. Businesses and business associations only have patchy, anecdotal information on the costs related to the ePD in general. Information on particular provisions is even less available. The available information has, however, been used to estimate these costs to the best extent possible.

Feedback received suggests that the majority of costs for the ePD is related to:

- Article 4 on the security of processing;
- Article 5(1) and Art. 5(2) on confidentiality of communications;
- Article 5(3) on cookie consent; and
- Article 13 on unsolicited communication.

In relation to **Article 4, as well as Articles 5(1) and 5(2)**, businesses have indicated that they have incurred a significant amount of compliance costs after the adoption of the ePD. However, businesses were not able to provide any quantitative information on this as the costs were already incurred in the past (almost 15 years ago) and have since then been written off.[393]

Article 5(3) is expected to be responsible for a significant amount of compliance costs. This is due to the extensive coverage of this provision (potentially all businesses in the EU that run a website and use cookies), as well as its importance for today's communication, marketing, advertising, and sales techniques. As businesses are increasingly developing data-driven business models, the importance of the substance of Art. 5(3) is also expected to grow over the next years. The costs associated with this provision mainly stem from the need to collect users' consent to be able to use cookies on websites, i.e. to implement the relevant technical solutions on websites.

Considering the **business perspective on Article 5(3)**, in the public consultation as well as interviews and an online survey with businesses conducted by Deloitte, several stakeholders highlighted that Article 5(3) is in fact the main cost factor relating to the ePD. As concerns the exact costs for businesses, the estimates vary widely. According to a 2014 study conducted by ITIF the average compliance costs would be around €900 per website/company, although the calculation of such costs is not demonstrated.[394] The ITIF study indicated that these costs included costs for legal advice, updates to privacy policies, and technical updates to websites and would be incurred once per website, i.e. at the time of the introduction of the new policy.[395] This study was indeed cited by different

[393] Businesses indicated in qualitative terms that they incur still today (and will in the future) costs in relation to regular updates, maintenance, and repair of the necessary hard- and software to safeguard the security and confidentiality of communications. Overall, it was not possible to obtain any quantitative information from businesses on the magnitude of such costs.
[394] The Information Technology & Innovation Foundation, Daniel Castro and Alan McQuinn, "*The Economic Costs of the European Union's Cookie Notification Policy*", November 2014 (US).
[395] The study also indicated that there could be additional recurring costs for maintenance. For instance, some companies customise their website's cookie policies to each user's preference. It is explained that these costs could lie between a few

stakeholders consulted as part of this initiative, implying that this estimate is considered realistic by these stakeholders.[396] However, there were also a few stakeholders that indicated that compliance costs would be significantly higher or lower.

In addition, Deloitte has been requested to undertake particular efforts to estimate compliance costs in relation to **Article 13** on unsolicited communications as this provision also involves the implementation of a technical solution on websites to collect users' consent to unsolicited communication.

Article 13 was one of the provisions that most businesses associated costs with.[397] The most expensive cost elements for these businesses concerned:

- Development / adaptation of technical infrastructure and / or software;
- Number of audits by competent national authorities; and
- Costs for advisory services, e.g. concerning legal interpretation of provisions.

It can be noted that three out of the five businesses that incurred significant costs in relation to Article 13 stated that they would have implemented some of the measures / the measures in a similar fashion also without the ePD in place.

In the European Commission's public consultation, several respondents specifically raised Article 13 when asked about the costs incurred in relation to the ePD. While no specific numbers were provided, it was indicated that costs are incurred in relation to adaptations in telemarketing procedures, e.g. initial costs to check opt-out registers (Robinson lists) the revision of lists, offering text-script on opt-out possibility and assistance in registering with related registers.

Finally, after the adoption of the ePD, in particular telecommunication service providers have – according to our interview results – incurred high capital costs in relation to the implementation of:

- Articles 6 and 9 on traffic data and location data other than traffic data;
- Article 7 on itemised billing;
- Article 8 on control of connected line identification (incl. Art. 10 on exception);
- Article 11 on automatic call forwarding; and
- Article 12 on directories of subscribers.

Under Art. 6 & 9, and 12 concerning directories of subscribers, businesses incur some costs regarding information obligations to consumers.

Based on the feedback received, these costs can be expected to be fairly large. However, these costs, which were incurred in the past by telecommunication service providers, can be expected to be already written off.

No quantitative / economic data was identified and / or estimated in relation to these Articles apart of what is provided in relation to each provision in chapter 5 (see the illustrative case examples in textboxes).

---

hundred or tens of thousands dollars annually per website. However, such costs are not directly based on the ePD and are, therefore, not considered further at this point.

[396] For example, eleven participants to the public consultation mentioned this study in relation to the costs for businesses stemming from the ePD. However, we note in this context that six of these were associated with the Interactive Advertisement Bureau IAB. Others included businesses or citizens.

[397] In Deloitte's business survey, it was one of the three provisions most businesses associated costs with, after the rules on confidentiality of communications (six businesses) and the rules on traffic and location data (five businesses). In addition, many businesses consulted as part of this study associated costs with Article 4.

In addition to the compliance costs related to the direct implementation of the ePD, businesses also incurred **opportunity costs** for lost business opportunities. In Deloitte's business survey, all five businesses that indicated to have incurred costs in relation to Article 13 agreed that these costs included opportunity costs. This was also raised by several respondents to the public consultation as well as in interviews carried out by Deloitte. It was explained that unsolicited communication is in some ways the backbone of the entire industry in terms of marketing and sales. The necessity of prior consent by users in order to be contacted reduces potential business opportunities in marketing and sales.

The overall quantitative results of the economic analysis in relation to the REFIT exercise are provided below.

Annex A: Economic Analysis

Further information in this regard, as well as an explanation of the approach used for the estimation of the quantitative results data is provided in the section on the basic assumptions used for the problem assessment and the establishment of the baseline scenario in Annex A concerning the Economic Analysis.

Current (and past) costs: Average annual values and changes compared to the current situation

The quantitative results of the economic analysis for the REFIT exercise are presented in Table 73:

- Number of businesses affected (in million);
- Compliance costs (in million Euro);
- Average compliance cost per business (in Euro);
- Administrative burden (in million Euro); and
- Average costs from admin. burden per business (in Euro).

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

The following table presents the quantitative findings for the current (and past situation). The table contains three columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Average annual value (2002-2015):* Denotes the average annual value of the quantitative indicator for which data has been estimated. This means, for instance, that 260,000 SMEs are affected by issues relating to the ePD per year (see the light blue cell), facing a total amount of 169.8 EURm per year (see the light green cell) at an average cost of compliance per business of 658.4 Euro (see the dark blue cell);
- *Average annual value today (2016):* Denotes the average annual value of the quantitative indicator for which data has been estimated in 2016.

A visualisation of the year-over-year development of the quantitative indicators is presented afterwards, as well as the overall values of the quantitative indicators for the timeframe 2002-2016

Table 57 – Key quantitative data estimated in relation to the REFIT exercise (2002-2016)

Quantitative indicator	Average annual value (2002-2015)	Annual value today (2016)
Number of businesses affected (in million)	2.84	3.11
Micro-enterprises	2.53	2.78
SMEs	0.26	0.25
Large enterprises	0.01	0.01
Foreign controlled enterprises	0.05	0.06
Compliance costs (in million Euro)	1,861.7 €	1,505.7 €
Micro-enterprises	1,655.8 €	1,349.0 €
SMEs	169.8 €	122.2 €
Large enterprises	5.6 €	4.2 €
Foreign controlled enterprises	30.5 €	30.3 €
Average compliance cost per business (in Euro)	658.4 €	484.5 €
Administrative burden (in million Euro)	0.28 €	0.23 €
Micro-enterprises	0.23 €	0.19 €
SMEs	0.03 €	0.03 €
Large enterprises	0.00 €	0.00 €
Foreign controlled enterprises	0.02 €	0.01 €
Average costs from admin. burden per business (in Euro)	48.9 €	36.0 €

Source: Deloitte

The analysis shows that – per year between 2002 and 2015 – around 2.8 million businesses were affected by the ePD in the EU. The majority of these businesses were micro-enterprises with less than 10 employees (2.5 million). Around 260,000 SMEs that have between 10 and 250 employees are estimated to have been affected per year while the number of large enterprises was negligible with around 10,000 per year. Approx. 50,000 foreign controlled enterprises that operated in the EU were affected per year.[398]

The businesses affected by the ePD are estimated to have incurred an annual value of 1.9 EURb to comply with Art. 5(3) and Art. 13. In addition, these businesses are expected to have incurred an unspecifiable amount of additional costs e.g. with regard to the consumer provisions. Again, micro-enterprises are expected to incur the lion share of these costs (around 1.7 EURb).

On *average*, an EU business is expected to have incurred 658 Euro per year with regard to the ePD between 2002 and 2015. This does, however, not mean that e.g. large enterprises may not have incurred significantly more costs while the costs may be significantly lower for micro-enterprises. In fact, the anecdotal evidence concerning businesses' costs presented in the text boxes in relation to each provision in chapter 5 shows otherwise. This does, however, not necessarily contradict the above but rather exemplifies the difficulties estimating such costs, as well as it should be seen as a caveat in relation to the nature of the figures as *best estimates* based on the *best data available*.

[398] The estimated numbers of affected businesses should be understood as annual values. However, the overall number of businesses affected by the ePD between 2002 and 2016 is not the sum of each annual value. The reason for this is that the majority of businesses was affected not only once but on several occasions across this time frame while some businesses were replaced by others due to the general life cycle of businesses (company birth, insolvency). This means that, in relation to the former argument, the projected value is likely underestimating the actual number of businesses affected, while the latter argument, the projection is likely to overestimate the number of affected businesses.

In relation to administrative burden, mostly stemming from the notification obligations for telecommunication service providers under Article 4, it has been estimated that an annual amount of 230,000 Euro was incurred, i.e. around 49 Euro per affected business per year.

Current (and past) costs: Visualisation of the development 2002-2016

In this section, we present visualisations of the development the following quantitative indicators between 2002 and 2016:

- The number of businesses affected;
- The compliance costs; and
- The costs from administrative burden.

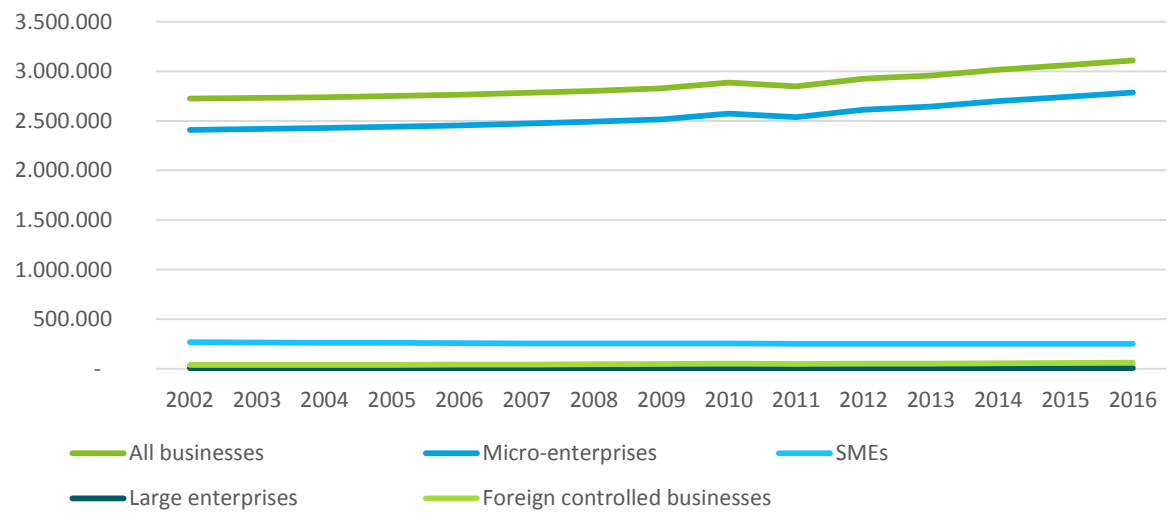
We have decided to use such a form of visualisation instead of providing the data by means of tables in order to make the sheer amount of data more accessible to the reader and to clearly be able to show the *development of the quantitative indicators over time* – which is not always easy to spot when looking at raw figures.

The graphs visualise the data per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Number of businesses affected

The following two graphs present the development of the number of businesses affected by the ePD. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

Figure 30 – Number of businesses affected by the ePD per year (2002-2016)



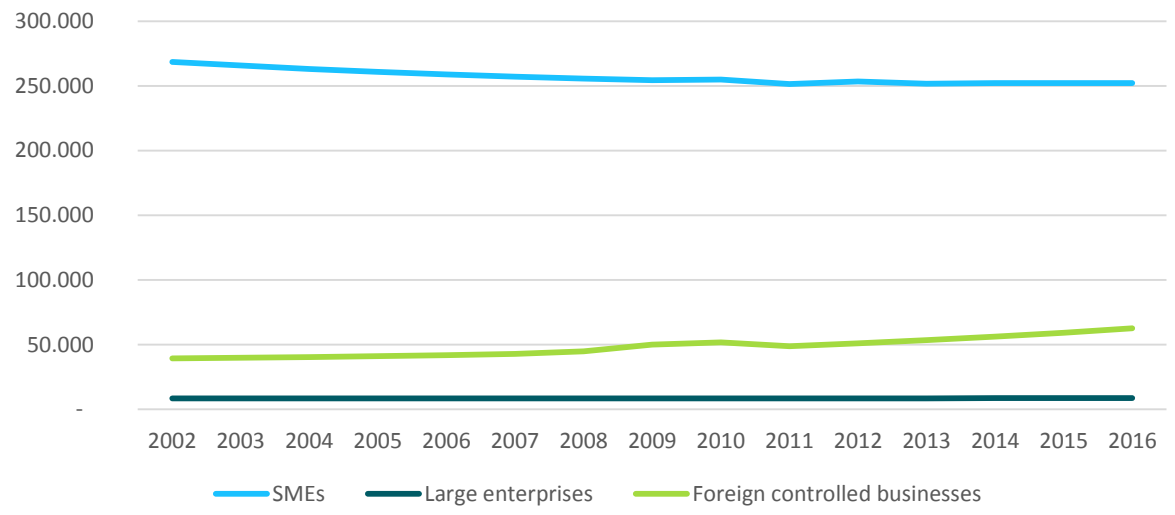
Source: Deloitte

Between 2002 and 2016, as can be seen from the graph above, the overall number of businesses affected by the ePD has increased, mostly due to growth of the micro-enterprise sector. SMEs, large enterprises, and foreign controlled enterprises were less important for the overall growth of the number of businesses affected by the ePD.

In fact, when examining the development of the number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD more closely, the following can be observed:

- The number of SMEs affected by the ePD has declined between 2002 and 2016;
- The number of large enterprises affected by the ePD has remained stable; and
- The number of foreign controlled enterprises affected by the ePD has slightly increased.

Figure 31 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (2002-2016)

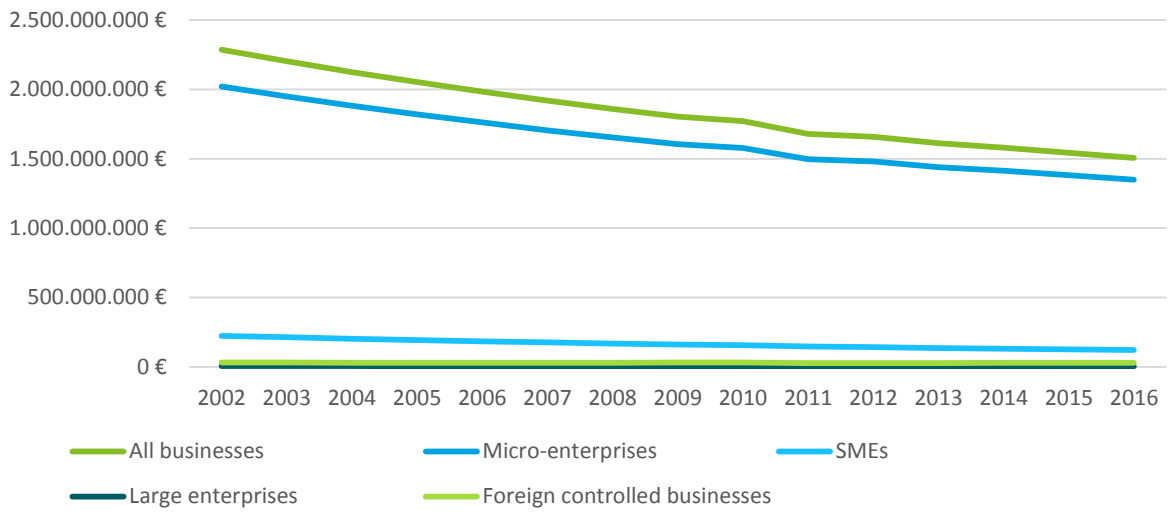


Source: Deloitte

Annual compliance costs

The following two graphs present the development of the annual compliance costs of businesses affected by the ePD. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

Figure 32 – Compliance costs of businesses affected by the ePD per year (2002-2016)

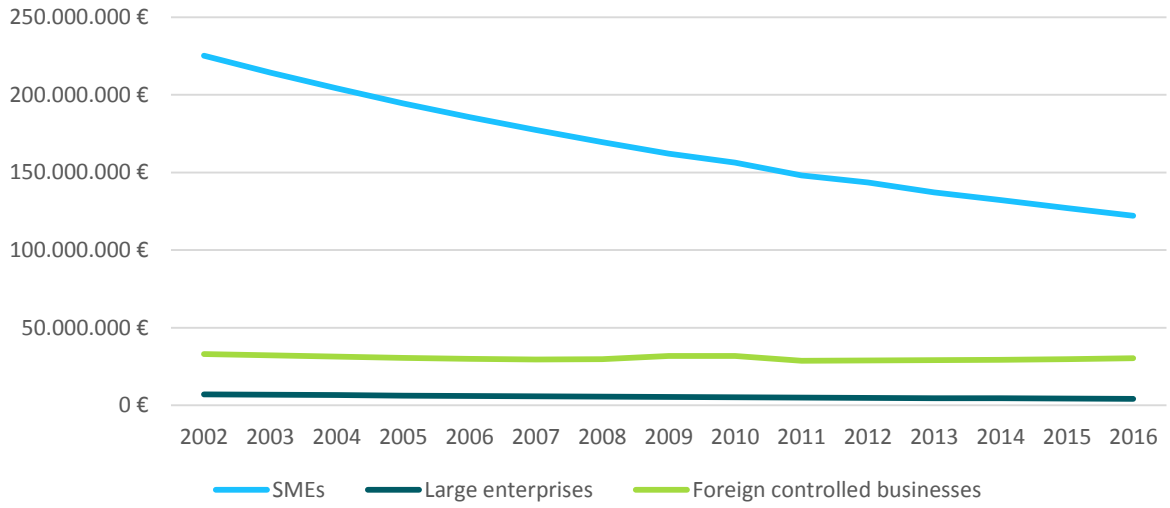


Source: Deloitte

The graph above shows the annual overall compliance costs for businesses have decreased from 2002 to 2016. Looking in more detail at annual overall compliance costs for SMEs, large enterprises, and foreign controlled enterprises (see figure below), it can be seen that – while compliance costs for

SMEs have decreased due to the decreasing number of SMEs affected over time – they have remained relatively stable for large and foreign controlled enterprises.

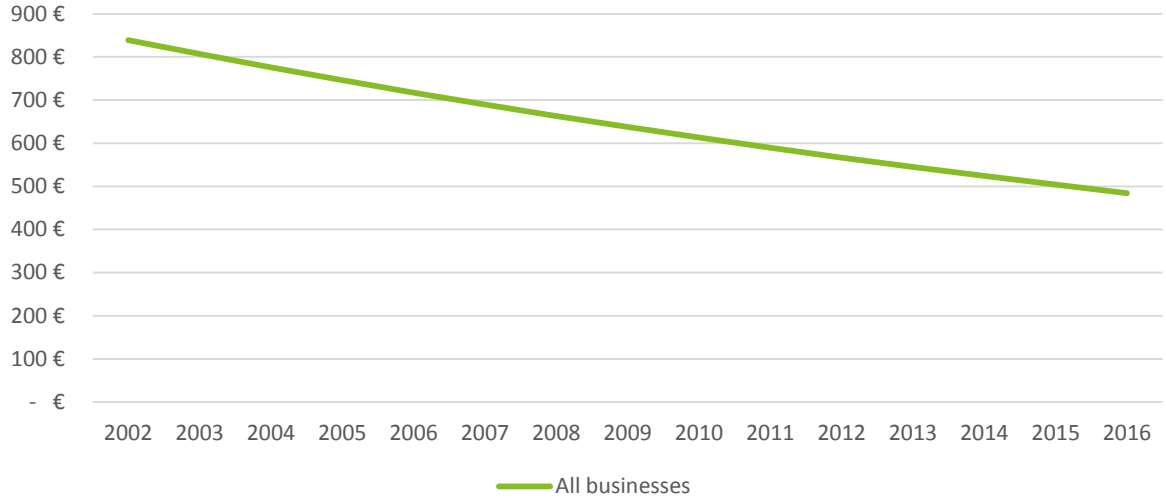
Figure 33 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (2002-2016)



Source: Deloitte

The following graph visualises the development of the average compliance costs for businesses from 2002 to 2016. No difference has been made between average costs for different size classes of businesses.

Figure 34 – Average compliance costs of per business affected by the ePD per year (2002-2016)



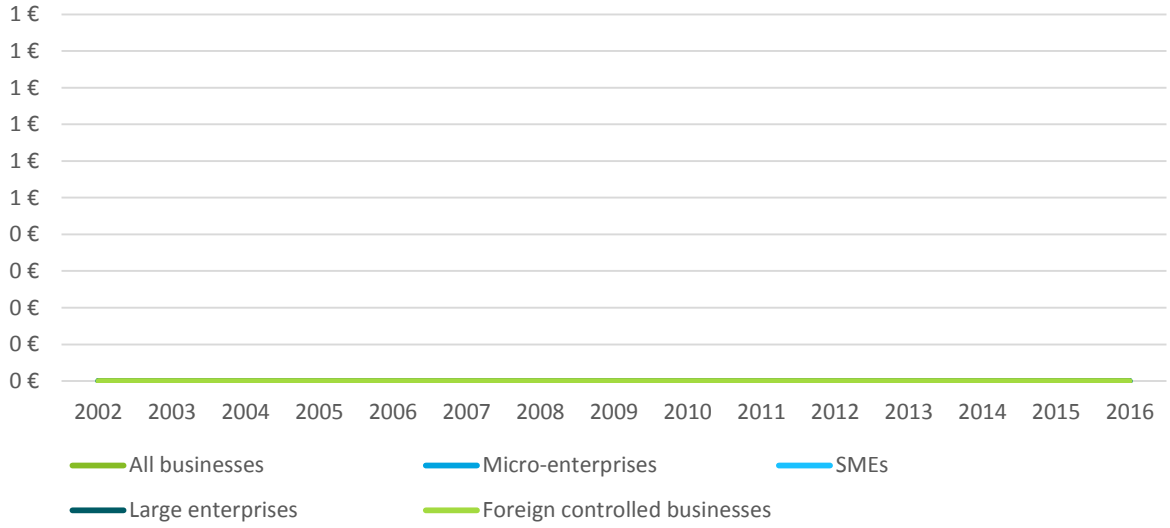
Source: Deloitte

The graph clearly shows that the average compliance costs for businesses have decreased drastically between 2002 and 2016.

Annual costs from administrative burden

The following two graphs present the development of the annual costs from administrative of businesses affected by the ePD. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

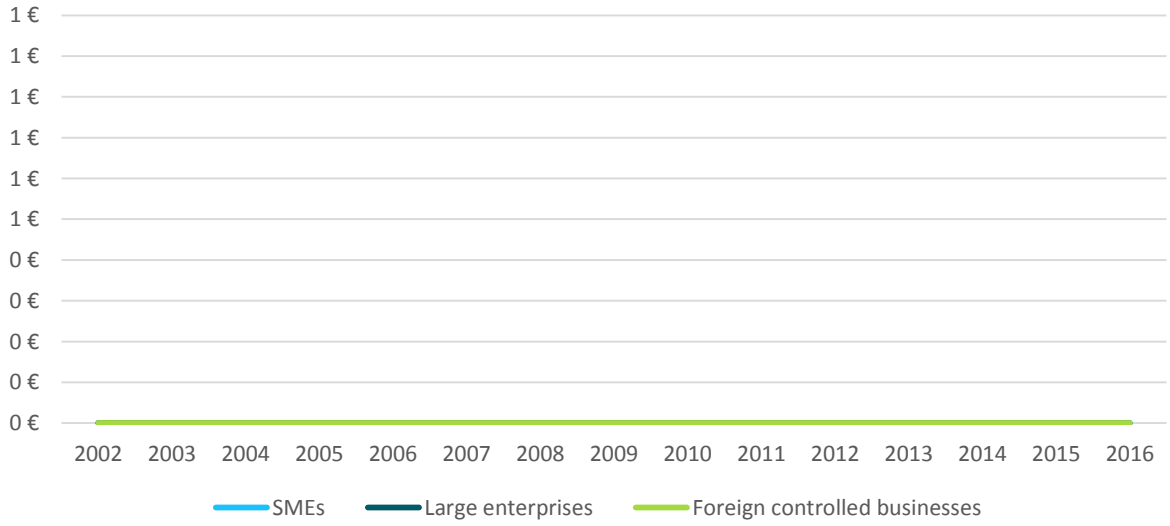
Figure 35 – Costs from administrative burden of businesses affected by the ePD per year (2002-2016)



Source: Deloitte

Similarly to the compliance costs, costs from overall annual costs from administrative burden have also decreased between 2002 and 2016 – despite some fluctuation between 2009 and 2013.

Figure 36 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (2002-2016)

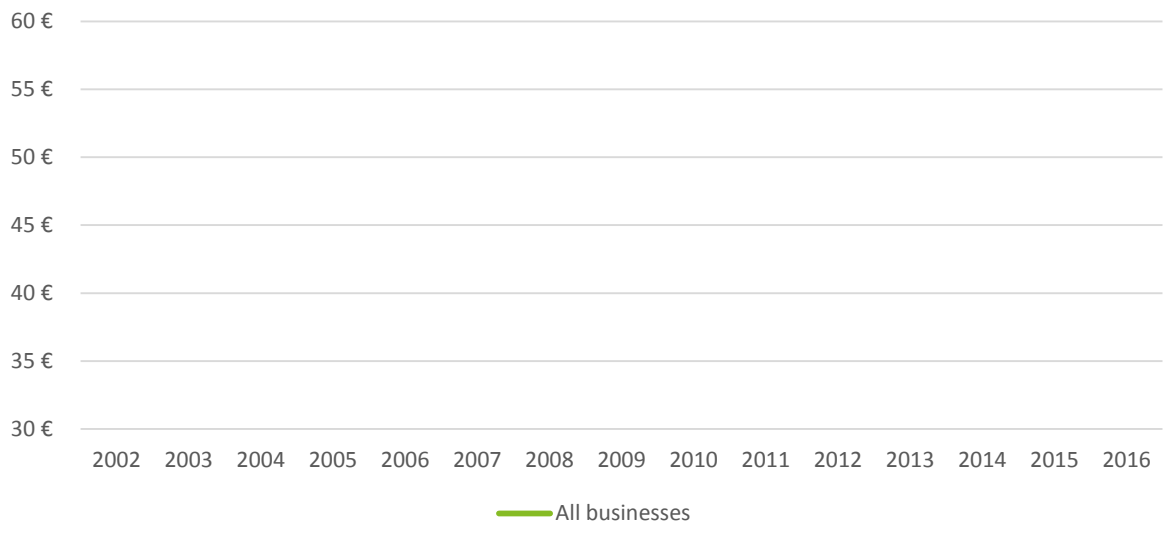


Source: Deloitte

As regards the costs from administrative burden for SMEs, large enterprises, and foreign controlled enterprises, there has been a decreasing trend since 2002. For SMEs, however, costs from administrative burden have slightly increased again in recent years.

The following graph visualises the development of the average costs from administrative burden for businesses from 2002 to 2016. No difference has been made between average costs for different size classes of businesses.

Figure 37 – Average costs from administrative burden per business affected by the ePD per year (2002-2016)



Source: Deloitte

Overall, the above graph shows that there has been a clear reduction of costs from administrative burden for across all types of businesses affected by the ePD from 2002 to today.

Current (and past) costs: Overall values 2002-2016

While the above section has presented average annual values, this section provides the key quantitative estimates for the overall time period of 2002-2016 (i.e. the sums of each individual annual value of the time period). This estimate is relevant to assess the overall costs of compliance and administrative burden stemming from the ePD for different types of businesses.

The following table contains information on:

- Compliance costs (in million Euro); and
- Administrative burden (in million Euro).

The number of businesses affected is not presented as this number is – over the entire time period – subject to double counting.[399] Compared to the above section, average compliance cost per business, as well as average costs from administrative burden per business are not relevant to present in this section as they are *average* values and not *overall* values.

The table contains two columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business; and
- *Overall value (2002-2016):* Denotes the overall annual value of the quantitative indicator for which data has been estimated. This means, for instance, that all SMEs in the EU together

[399] This is due to the fact that businesses are affected by the ePD over longer time frames than just one year. An alternative way of phrasing this is that the ePD does not affect an entirely different set of businesses each and every year.

have incurred compliance costs of 2,499.4 EURm over the entire time period of 2002-2016 (see the light green cell).

Table 58 – Key quantitative data estimated in relation to the REFIT exercise (2002-2016)

Quantitative indicator	Overall value (2002-2016)
Compliance costs (in million Euro)	27,569.8 €
Micro-enterprises	24,530.4 €
SMEs	2,499.4 €
Large enterprises	83.1 €
Foreign controlled enterprises	457.0 €
Administrative burden (in million Euro)	4.1 €
Micro-enterprises	3.4 €
SMEs	0.4 €
Large enterprises	0.0 €
Foreign controlled enterprises	0.2 €

Source: Deloitte

The table above shows that businesses have incurred around 28 EURb of compliance costs related to the ePD over the entire time frame of 2002 to 2016. The vast majority of costs was incurred by micro-enterprises. Although this overall amount may look dramatic at first glance, it should be kept in mind that this cost is incurred by businesses from all types of industries across the entire EU. Thus, the share of compliance costs of the overall EU GDP between 2002 and 2016 is marginal. According to Eurostat, the overall EU28 GDP between 2002 and 2015 was 175,948,834.7 EURm. Thus, the share of 27,569.8 EURm of compliance costs is only 0.016% of the entire EU economy.

Compared to compliance costs, costs from administrative burden were insignificant between 2002 and 2016. Overall, 4.1 EURm have been incurred between 2002 and 20016, again mostly by micro-enterprises.

6.3 Relevance

Under this evaluation criterion, the relevance of the ePD's provisions in view of problems faced by stakeholders (in particular businesses and citizens) is assessed. This includes an assessment of the relevance of the ePD's provisions in the light of how the initial problems at the time of the adoption of the ePD have evolved until today. **We found that the relevance of the ePD and its specific objectives tends to be confirmed overall. However, its scope and some of its individual provisions do not seem to be relevant any longer or are no longer in line with the needs of citizens/businesses. On this basis, not all the operational objectives appear to be fully relevant.**

Considering first the **overall relevance of the ePD**, we note at the outset that, while Directive 95/46/EC and the GDPR are elaborations of the right to personal data protection, the ePD is the only instrument in the EU to contain specific privacy and confidentiality rules for electronic communications.[400].

[400] Article 29 Working Party, Opinion 3/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC) [2016] WP240, p 4.

The existence of such rules may be considered relevant in light of general policy objectives of the EU: In 2015, the Commission issued its Communication on ***A Digital Single Market Strategy for Europe***.[401] Achieving the DSM is considered to enable EU businesses to grow globally, as well as to promote modern open government. Therefore, in order to unleash the full potential of the digitalisation of the EU economy and society, it is crucial according to the Commission to remove barriers to the achievement of a DSM. A typical and major barrier to the accomplishment of the Digital Single Market stems from legal fragmentation and enforcement discrepancies among Member States. Thus, creating the right conditions for digital networks services to flourish is one of the main objectives of the DSM Strategy. This implies the provision of the right regulatory conditions for innovation, investment, fair competition and level playing field. One of the identified solutions is developing strong European Data Protection rules to boost the digital economy. Likewise, the DSM Communication sets as objective to create the right conditions and level playing field for advanced digital networks and innovative services, e.g. by strengthening the standards of the protection granted by Article 8 of the Charter namely the right to the protection of personal data. Thus, in light of the DSM, the ePD appears to be still relevant.

Based on our analysis of the scope of the ePD, the need to have specific rules for data protection in the electronic communications sector is also confirmed. However, the scope is not considered to be fully appropriate in light of the needs of consumers, notably because it does not cover services that are increasingly used by citizens as substitutes for traditional electronic communication services. This shortcoming is in particular based on the fact that OTTs are excluded from the scope of the ePD. On this basis, a large part of consumers uses services every day that are not covered by the ePD. According to Eurobarometer:

- Email is used by 46% of consumers every day;
- OTTs for the purpose of instant messaging (e.g. WhatsApp) are used by 41% every day[402]; and
- Online social networks are used by 38% every day.

These types of services are very important from a societal perspective as they are an integral part of today's (and very likely future) communication, especially within the group of younger citizens. Therefore, although the scope of ePD is relevant for one part of today's communication means (i.e. browsing the Internet, mobile telecommunication), another part of today's communication is not within the scope of the ePD.

This technological backwardness (or lack of technological neutrality) is considered to be an important impediment to the relevance of the ePD as such (and was also emphasised by almost all stakeholders). This being said, it appears that some Member States have extended while implementing the ePD locally to include in its scope OTT services.

This issue also impedes on the achievement of the DSM. A fully functioning Digital Single Market requires a level playing field between all the market players in the Internet value chain. The unequal

[401] Communication (COM(2015) 192 final: A Digital Single Market Strategy for Europe.

[402] Interestingly, the Eurobarometer data shows that for instant messaging OTTs, two large groups of consumers seem to exist: Those that use instant messaging every day and those that never use it. The proportion of consumers that uses it a few times per week / month is comparatively small. It can be assumed that age is an important factor with regard to the take-up of such services. While younger generations use instant messaging every day, the majority of older consumers do not use it at all. Therefore, it can be expected that the share of consumers who use instant messaging on a daily basis will increase over the next years.

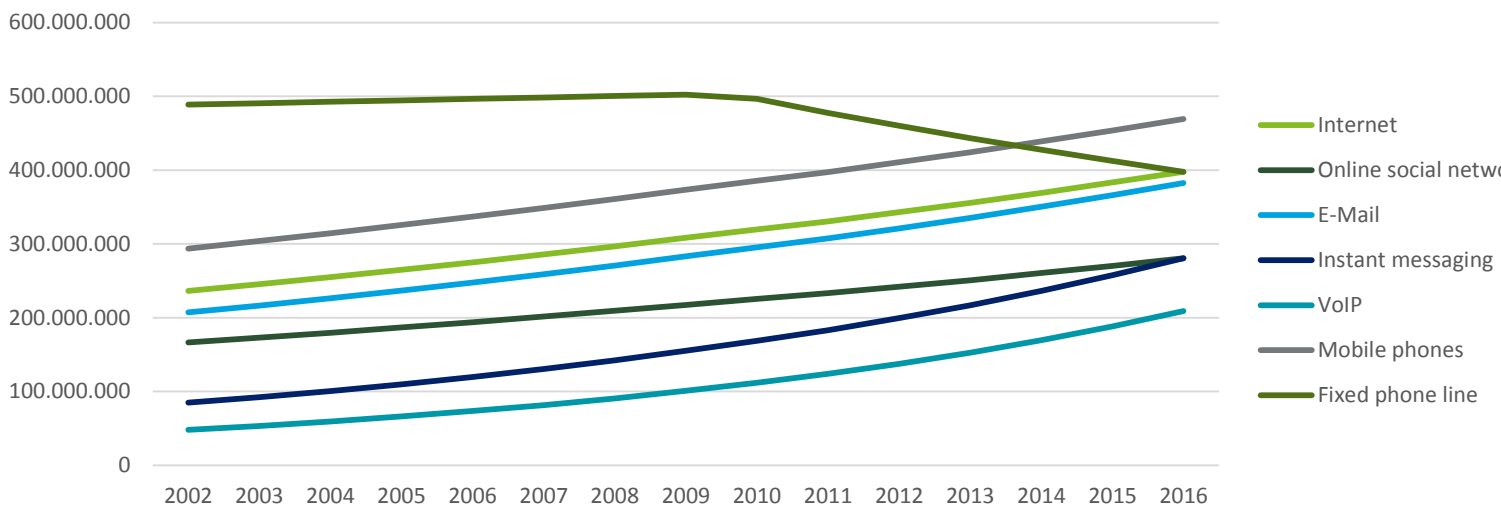
treatment of telecommunication services and OTT services allows for the existence of an uneven playing field for customers, governments, and generates competition distortion.

In this context it is also important to note that the number of citizens potentially affected by the ePD has been steadily increasing over the past years. In the following, we present the number of citizens affected each year by the ePD in relation to the different types of communication services (some of which are covered by the ePD):

- Internet to browse online;
- Online social networks;
- Email;
- Instant messaging (e.g. WhatsApp);
- Voice of IP;
- Mobile phones to make calls or send texts; and
- Fixed phone lines.

The graph visualises the years 2002 to 2016.

Figure 38 – Number of citizens affected by communication services per year (2002-2016)



Source: Deloitte

As can be seen from above figure, the number of users affected by all types of communication services has been growing since 2002. Today, almost all EU citizens make use of mobile phones while e.g. VoIP is used by fewer citizens. While fixed line phones have been used by (almost) all EU citizens until a few years ago, the number of users has started to decline. Today, more citizens make use of mobile phones than of fixed line phones. Interestingly, services not covered by the ePD such as instant messaging have seen a steady increase in usage numbers.

Therefore, in principle, the ePD is relevant today with a view to both achieving the DSM and strengthening the right to the protection of confidentiality of communications and personal data. This supported the relevance of its specific objectives "to ensure that the right to privacy and confidentiality with respect to the processing of personal data in the electronic communications sector is respected" and "to ensure the free movement of personal data in the internal market". With respect to the specific objective "to ensure the free movement of electronic communication terminal

equipment and services in the EU", information is only available to a limited extent. **However, although its objectives are still relevant, its scope is not fully in line with society's needs.**

Turning to the **individual provisions**, we found that some of them are no longer relevant or are no longer in need with the needs of citizens and businesses. The following table provides an overview of the main findings concerning the relevance of each provision.

Table 59 – Main findings in relation to the relevance of the provisions

Relevant articles	Main Findings
Article 4	***Partially relevant*** There are doubts as to the relevance of all parts of this provision, notably because there are some overlaps with other legal instruments, in particular most of the provision overlaps with the GDPR. Stakeholders were most critical of Article 4(3), whereas there is some support to retain Article 4(1) and 4(2).
Articles 5(1) and (2)	***Relevance tends to be confirmed*** Overall, the relevance of specific rules on the confidentiality of communications tends to be confirmed. This is in particular based on the fact that citizens regard this as an important issue, while no similar rules are contained in the in Directive 95/46/EC or the GDPR. However, the relevance of these provisions is weakened by its restriction to traditional telecom providers in most Member States.
Article 5(3)	***Relevance tends to be confirmed*** From the perspective of citizens, it may be argued that the provisions are relevant to safeguard the privacy of users. We also note that this provision does not have any legal equivalent in other instruments. The relevance is also supported by the competent authorities responding to Deloitte's online survey. However, while Article 5(3) is considered important to retain, the content is not considered to be fully in line with businesses' and consumers' needs. In particular, as shown in the previous sub-sections, based on the ambiguities relating to the scope and consent mechanism, the implementation is burdensome for businesses with limited added value for citizens.
Articles 6 and 9	***Relevance tends to be confirmed*** While it is confirmed that it is relevant to keep rules on the processing of traffic and location data, the format of the current rules is questioned. In particular, a number of ambiguities relating to the application of these provisions has been identified.
Article 7	***Relevance tends to be confirmed*** There are no similar rules in any other EU legal instrument, e.g. the GDPR, supporting the relevance of this provision. The relevance of this provision is also largely supported by the stakeholders consulted. However, we note that the support of this provision was overall stronger among citizens and civil society, while the industry seems to be more critical, arguing e.g. that customers do not demand these services.
Articles 8 and 10	***Relevance tends to be limited*** The relevance of this provision can be confirmed as no similar rules are contained in the GDPR. However, concerns were voiced that calling line identification would have most probably been replaced by alternative solutions in line with the technological developments if not for the existing legal obligation to have it in place. Indeed, the presentation and restriction of calling and connected line identification is a feature that is today built in by design by device manufacturers. However, this is so far mostly valid for modern mobile phones, but not necessarily for fixed phones.
Article 11	***Insufficient information to assess*** It is difficult to draw a conclusion on the relevance of this provision due to the mixed data available. On the one hand, ensuring a possibility of stopping automatic call forwarding by a third party theoretically contributes to ensuring citizens' privacy while on the other hand, the responses to the public consultation do not give a clear picture in this matter. Moreover, telecom operators have emphasised that customers have not demanded such a feature.
Article 12	***Relevance tends to be confirmed*** The relevance of this provision tends to be confirmed, based on the fact that there are no similar rules in any other EU legal instrument and that directories of subscribers are a pre-requisite for unsolicited marketing communications sent and received through the Internet, as well as through calls. This is confirmed by competent authorities and citizens. However, doubts were voiced by businesses: Telecom operators do not necessarily see the relevance of a legal obligation due to customer demand and competition driven market.
Article 13	***Relevance confirmed*** As part of the EC's public consultation, the majority citizens and civil society organisation, as well as public bodies have supported the relevance of this provision. By contrast, the majority

Relevant articles	Main Findings
	of respondents from the industry does not confirm an added value of specific rules on unsolicited marketing communications.
Article 14	***Insufficient information to assess***
Article 15a	***Relevance tends to be confirmed*** This provision gives practical guidance on how Member States should implement the ePD, which is important to ensure its consistent and effective implementation. The relevance was not questioned by any of the stakeholders consulted. However, it was questioned whether the content of this provision is fully in line with the needs of stakeholders and citizens.

Source: Deloitte

These findings also reflect the relevance of the ePD's operational objectives. While most of them appear to be still relevant, the relevance of the following operational objectives may be questioned:

- To ensure the security of services;
- To ensure that called and calling subscribers/users have possibilities for control over call line identification;
- To ensure that subscribers have the right to stop automatic call forwarding; and
- To ensure that have the right to be informed and decide about an inclusion in publicly available or printed databases of subscribers.

6.4 Coherence

The analysis focused on the coherence of the ePD with the GDPR, the Electronic Communications Package, the RED as well as the EU's aim to achieve the DSM. On this basis, the ePD does not seem to be fully coherent with the relevant instruments. Notably, while the ePD is largely coherent with the Electronic Communications Package and the RED, there are potential challenges in relation to the GDPR and the DSM.

Considering the individual provisions, we note that the coherence has been confirmed for most of them, while issues exist mainly in relation to Article 4 and Articles 6 and 9. The following table provides an overview of the main findings concerning the coherence of each provision.

Table 60 – Main findings in relation to the coherence of the provisions

Relevant articles	Main Findings
Article 4	***Limited coherence in the light of recent legal developments*** While Article 4 works rather well with the Electronic Communications Package and the RED, there are several overlaps with the GDPR. Notably, the GDPR also contains rules on security and personal data breaches as laid down in Article 4(1)-(3) of the ePD. However, the GDPR is even more detailed in some aspects. On this basis, the coherence is proved to be limited.
Articles 5(1) and (2)	***Coherence tends to be confirmed*** The external coherence of Article 5(1) and (2) can be confirmed, as no challenges have been identified. In contrast, while no similar rules are contained in the GDPR, there is a noteworthy synergy between the ePD and the Radio Equipment Directive, to the extent that the equipment covered by the latter must be able to support the safeguards for the protection of privacy and personal data set out by the ePD. As concerns the internal coherence, some lack of clarity was identified in relation to other articles of the ePD, including Article 3 as well as Articles 6 and 9.

Relevant articles	Main Findings
Article 5(3)	***Coherence tends to be confirmed*** No significant challenges hindering the internal coherence have been identified. As concerns the external coherence, there may be potential ambiguities based on the interaction of Article 5(3) and the GDPR, notably that it is not clear what level of information has to be provided to a subscriber who is not a natural person. On the other hand, the relationship with the RED allows for synergies, as the RED provides for radio equipment which is constructed in such a way as to support the prevention of the unlawful access to information stored in communication terminals. With respect to the interaction with general policy goals of the EU, the provision is in line with EU's goal to safeguard fundamental rights. While it may be argued that it does not support the establishment of the internal market by restricting the tracking of users, this restriction can be justified based on the rationale to protect citizens' privacy.
Articles 6 and 9	***Partially coherent*** While Articles 6 and 9 work rather well with other instruments, notably the GDPR, challenges have been identified in relation to the **internal coherence**. In particular, the distinction between the different types of data covered by Article 6, 9 and 5 may not always be clear in practice.
Article 7	***Coherence confirmed*** The coherence of this provision is confirmed as there are no similar or contradictory rules contained in any of the instruments studied.
Articles 8 and 10	***Coherence confirmed*** The analysis has shown that, as a lex specialis that particularises a specific situation, the provision is coherent with the GDPR and the Electronic Communications Package.
Article 11	***Coherence confirmed*** The coherence of this provision is confirmed as no issues have been identified vis-à-vis the GDPR and the Electronic Communications Package.
Article 12	***Coherence confirmed*** The coherence of this provision is confirmed as no issues have been identified vis-à-vis the GDPR and the Electronic Communications Package.
Article 13	***Coherence partially confirmed*** Based on the evidence available, there are no challenges in relation to the external coherence of this provision. However, there could be potential challenges in relation to the internal coherence. This is due to the leeway for Member States to decide about the specificities of their national regimes (opt-in vs. opt-out, see Table 45), as well as the incoherence of the regimes under Art. 13(1) and 13(3) perceived by different types of stakeholders.
Article 14	***Coherence confirmed*** The coherence of this provision is confirmed as no issues have been identified vis-à-vis the GDPR and the Electronic Communications Package. A positive relationship has been established in relation to the RED, as the ePD and the RED complement each other.
Article 15a	***Coherence partially ensured*** Based on the evidence available, the coherence of this provision with other instruments is not fully ensured. Challenges have been identified in relation to the GDPR, as for data processing operations related to natural persons, there currently seems to be an overlap as regards the application of fines and sanctions for the breach of provisions related to the processing of personal data. At the same time, there is a positive relationship with the Framework Directive, as it reinforces the provisions in the ePD.

Source: Deloitte

In the following sub-sections we present our observations in relation to the different instruments/policy areas analysed.

6.4.1 Coherence with the GDPR

In general terms, the objectives of the ePD and the GDPR are coherent. Both instruments aim at achieving a high level of privacy within the internal market. The ePD acts as a *lex specialis* in relation to the GDPR in that it provides more specific rules for the electronic communications sector.

This said, some potential challenges in relation to specific provisions have been identified. Notably, these relate to the following topics:

- **Services concerned (Article 3)**: There may be a lack of clarity as when the ePD and when the GDPR applies, as the distinction of "public or publicly available electronic communications services";
- **Notification of personal data breaches (Article 4.3 and 4.4)**: The procedures for personal data breaches vary considerably; thus, the same business may need to follow different procedures in case it offers electronic communications and other services;
- **Confidentiality of the Communications (Article 5.3)**: From the interplay between the provisions in the ePD and the GDPR, it is not clear what level of information has to be provided to a subscriber who is not a natural person; and
- **Implementation and Enforcement (Article 15a)**: There are differences as concerns the application of fines and sanctions for the breach of provisions related to the processing of personal data and as for the competent authorities.

Challenges in relation to the interaction between the ePD and the GDPR have also been raised by many of the stakeholders consulted as part of this assignment.

Further details are provided in Annex F.

6.4.2 Coherence with the Electronic Communications Package

The ePD is largely coherent with the other pieces of the Electronic Communications Package. This is not surprising given that it was adopted at the same time as the Framework Directive and the other Specific Directives. Although there are certain overlapping areas, no challenges have been identified.

Further details are provided in Annex F.

6.4.3 Coherence with the Radio Equipment Directive

The ePD is coherent with the Radio Equipment Directive. The two instruments have distinct scopes: while the Radio Equipment Directive establishes a framework for placing and marketing radio and telecommunications terminal equipment on the single market, the ePD is concerned with the protection of privacy and personal data protection of electronic communications, regardless of whether they are carried out by way of such radio equipment.

The two instruments converge, however, whenever a particular radio equipment can be used for the purposes of carrying out an electronic communication under the scope of the ePD. Such equipment must then be designed in such a way as to comply with the protections set out by the ePD, which entails the design and production of ePD-compliant devices. The same requirement can be found in the R&TTE for wired telecommunications terminal equipment.

This is a significant finding since communication through radio equipment (as opposed to fixed line equipment) is currently widespread. When overlaid with the provisions of the ePD, the Radio Equipment Directive effectively requires that all radio equipment be compliant with the requirements provided in the former. More accurately, the construction of radio equipment must take into account and enable the incorporation of such safeguards. This strong synergy may have important consequences for the construction of radio equipment, particularly with regard to the provisions of the

ePD related to the security of processing of data, confidentiality of communications, presentation and restriction of calling and connected line identification, and automatic call forwarding.

6.4.4 Coherence with the DSM

In general terms, the objectives of the ePD are coherent with the goal to establish the DSM.

Indeed, the DSM Communication sets as objective to create the right conditions and level playing field for advanced digital networks and innovative services. To achieve this objective, the DSM Communication clarifies that it is necessary to build *"on reliable, trustworthy, high-speed, affordable networks and services that safeguard consumers' fundamental rights to privacy and personal data protection while also encouraging innovation".*[403] In light of these considerations, the EU committed to strengthen the standards of the protection granted by Articles 7 and 8 of the Charter of Fundamental Rights[404], namely the right to respect for private life and family and the right to the protection of personal data.

Yet, it is a potential challenge to the aims of the DSM that the scope of the ePD is limited to public or publicly available electronic communication services (cf. the section on effectiveness). Indeed, the European regulatory landscape with regard to the **online environment** still operates on the basis of the distinction between three differently regulated legal concepts:

- Information society services (E-Commerce Directive);
- Electronic communications services (Telecoms package); and
- Audio-visual media services (Audio-visual Media Service Directive).[405]

6.5 EU added value

The EU added value of harmonised rules on privacy and confidentiality can be confirmed.

It was already recognised at the time of the adoption of Directive 95/46/EC and the ePD itself that there is a **need to address data protection, including in the electronic communications sector, at the EU level**. It was argued that the establishment of the internal market as well as the introduction of new telecommunications networks would necessarily lead to a substantial increase in cross-border flows of personal data. A potential difference in levels of protection was expected to constitute a barrier to the functioning of the internal market, as data exchanges may be hindered.[406]

This assessment is still valid today, as also pointed out in the recent Impact Assessment on the GDPR. The EU is best placed to ensure an effective and consistent protection for individuals, in particular when personal data is transferred across borders, as common standards are required for this purpose.[407]

[403] Communication COM(2015) 192 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, p. 9 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN.

[404] Charter of Fundamental Rights of The European Union http://www.europarl.europa.eu/charter/pdf/text_en.pdf

[405] Sandfeld Jakobsen, S. (2014). *EU Internet law in the era of convergence: the interplay with EU telecoms and media law*. In. Savin, A. & Trzaskowski, J. (eds.) (2014). Research Handbook on EU Internet Law, Cheltenham, UK: Edward Elgar, p. 60.

[406] Recitals (5), (6), (7), and (8) of Directive 95/46/EC; Recital (8) of the ePD.

[407] Impact Assessment Accompanying the document "Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 10 final, p. 37.

Harmonised standards in this field, ensuring an equivalent level of protection for all EU citizens, cannot be achieved by Member States alone since communications are not bound by borders (in particular within the internal market) and Member States' standards on this varied before the introduction of the ePD.

This is reflected in the **assessment of the individual provisions** (see Table 61). It can be seen that most of the ePD's provisions have a clear EU added value. For other provisions, the EU added value is, however less pronounced or absent. Although the provision on itemised billing of invoices, for instance, is expected to contribute to ensure that citizens have the same rights across the EU, the share of citizens that makes use of itemised billing today – in particular in a cross-border context – is expected to be fairly small compared to the overall number of users.

Moreover, the provisions on automatic call forwarding as well as on the presentation and restriction of calling and connected line identification relate to technical features that are today built in by design by device manufacturers – that are not necessarily (only) bound by EU law when designing their products. Thus, the EU added value of having legal obligations on such features is limited.

The following table provides an overview of the main findings concerning the EU added value of each provision.

Table 61 – Main findings in relation to the EU added value of the provisions

Relevant articles	Main Findings
Article 4	***EU added value tends to be confirmed*** Personal data and security breaches are not an issue that is bound by Member States' borders. Therefore, there is an added value of having a specific provision concerning the security of processing and notification of personal data breaches at the EU level. This was not denied by any of the stakeholders consulted.
Articles 5(1) and (2)	***EU added value confirmed*** As communications are not bound by borders, a clear EU added value of harmonised rules on the confidentiality of communications can be seen. This is supported by the stakeholder consultations carried out as part of this project and the EC's public consultation.
Article 5(3)	***EU added value tends to be confirmed*** The confidentiality of communications and the use of websites is a transnational issue that is not restricted by Member States' borders, as also recognised by stakeholders. If this matter were solved at the national level, businesses would need to adjust their approach for every EU Member State and consumers would face a lack of transparency. On this basis, there is an added value to have common standards in place.
Articles 6 and 9	***EU added value confirmed*** As communications and location-based services are not bound by borders, a clear EU added value of harmonised rules on the protection of traffic data and location data can be seen.
Article 7	***Limited EU added value*** Itemised billing of invoices is considered to be an issue that does have limited EU added value. The provision is expected to contribute to ensure that citizens have the same rights across the EU. At the same time, however, the share of citizens that makes use of itemised billing today – in particular in a cross-border context – is expected to be fairly small compared to the overall number of users. Although difference exist in how the Member States have transposed this provision, citizens still benefit from having equal rights across the EU in this matter.
Articles 8 and 10	***Limited EU added value*** Although differences exist in how the Member States have transposed this provision, citizens still benefit from having equal rights across the EU in this matter. The presentation and restriction of calling and connected line identification is a feature that is today often built in by design by device manufacturers (in particular for mobile phones) that are not necessarily (only) bound by EU law when designing their products.
Article 11	***Limited EU added value*** Automatic call forwarding is a feature that is today built in by design by device manufacturers

Relevant articles	Main Findings
	that are not necessarily (only) bound by EU law when designing their products. Thus, it is not the provision that enables citizens to make use of their rights but much rather the manufacturers of devices that apply international (not EU) standards in their product design. Although difference exist in how the Member States have transposed this provision, citizens still benefit from having equal rights across the EU in this matter.
Article 12	***EU added value tends to be confirmed*** Although difference exist in how the Member States have transposed this provision, citizens still benefit from having equal rights across the EU in this matter.
Article 13	***EU added value confirmed*** There is a clear EU added value of this provision as both businesses and citizens potentially benefit from a set of similar rules and rights across the EU. However, the ePD leaves leeway for Member States to differ in their national transposition from EU law which is considered to be a barrier for achievement of the *full* EU added value of the provision.
Article 14	***EU added value confirmed*** The EU added value of this provision can be confirmed based on the responses received as part of the EC's public consultation. Especially responses from citizens & civil society, as well as from public bodies are largely in favour of EU rules regarding the free movement of electronic communications equipment and services. However, a small majority of businesses are not in favour of such EU rules.
Article 15a	***EU added value confirmed*** This provision gives practical guidance on how Member States should implement the ePD, which is important to ensure its consistent implementation. Consistency can only be achieved at the EU level.

Source: Deloitte

The EU added value also tends to be confirmed by stakeholders' views.

In general terms, consumers tend to support common rules for data protection in the EU: A 2015 Special Eurobarometer study on Data Protection revealed that nearly 90% of the respondents wish to have the same influence over their own personal information, regardless of the country the service provider is established in. Beyond that, a majority of 45% sees the responsibility of enforcing such rules on personal data protection at the European level.[408]

Responses received as part of the European Commission's public consultation have showed that, from the stakeholders' perspective, the ePD has a clear EU added value to *increase* the confidentiality of electronic communications in Europe (52% all responses). Almost half of respondents think that the ePD had a clear EU added value to *harmonise* the confidentiality of electronic communications in Europe (48% of all responses). Less than 40%, however, agreed that the ePD had a clear EU added value in relation to ensuring the free flow of data and equipment.

[408] European Commission (2015). *Special Eurobarometer (EB) 431 on Data Protection.* Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_fact_de_en.pdf .

Task 2: Assessment of Options

7 Problem assessment

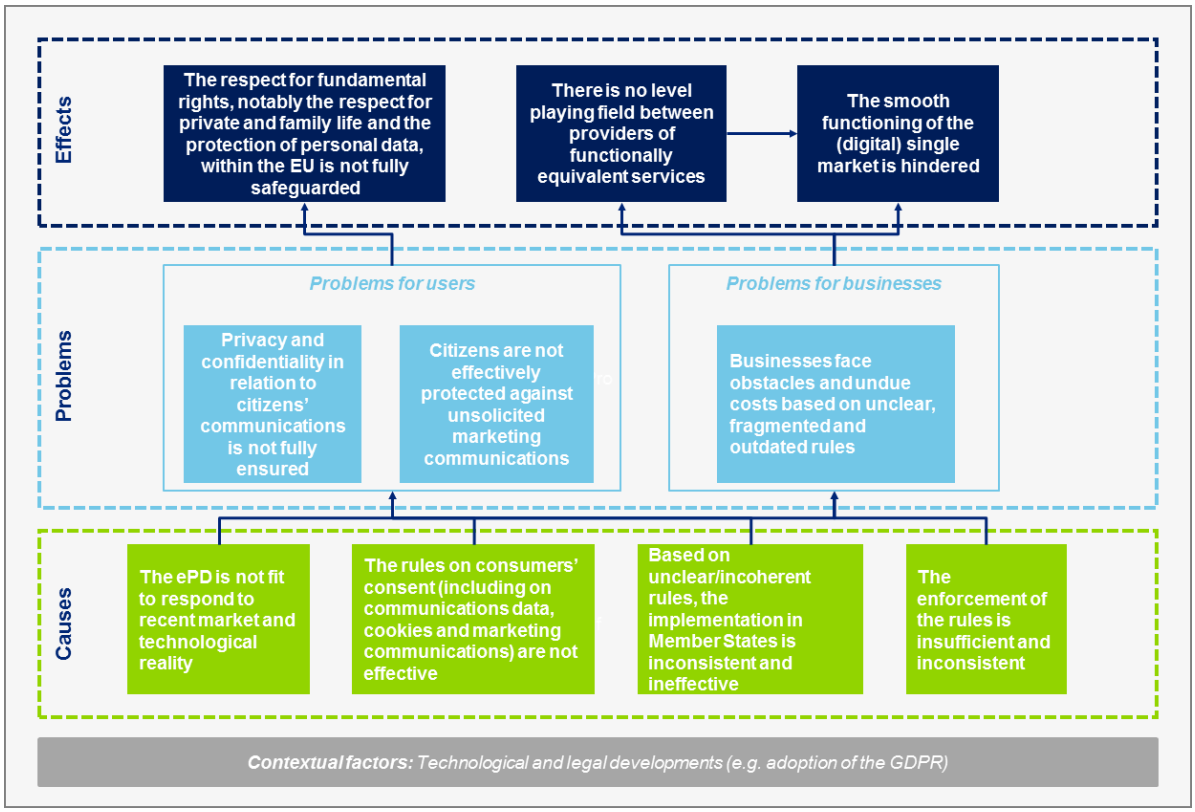
In this section we present our assessment of the problems, including our problem tree and a summary of the identified problems, their causes and effects.

7.1 Introduction

The starting point of the impact assessment consists of an assessment of the current problems. In this context, we identified and analysed the **problems, their causes and their effects / impacts, taking into account how different stakeholder groups are affected**. For preparing the problem assessment, we have taken into account the information gathered as part of the REFIT assessment. For further information, please see chapter 2.

Our understanding of the problems covered by the present assignment, as clarified in discussions with Commission services, their causes and effects is presented below by means of a problem tree. Problem trees are usually a good way to illustrate the relevant causal relationships. The problem tree should be read from the bottom to the top.

Figure 39 - Problem tree



Source: Deloitte

The following sections are devoted to the problems, their causes, and effects and provide information in relation to each of the respective boxes presented in the problem tree. At the end of this chapter, we provide an assessment of the likely development of the identified problems in case no policy action is taken.

7.2 Assessment of the Causes

The "causes" are presented at the bottom of the problem tree. In general terms, causes are at the operational level, reflecting e.g. issues relating to the current legal framework. They represent barriers that may be addressed e.g. through legislative or non-legislative action.

The following causes have been identified (see Figure 39):

- The ePD is not fit to respond to recent market and technological reality;
- The rules on consumers' consent (including on communications data, cookies and marketing communications) are not effective;
- Based on unclear rules, the implementation in Member States is inconsistent and ineffective; and
- The enforcement of the rules is insufficient and inconsistent.

We explain each of these causes below.

7.2.1 The ePD is not fit to respond to recent market and technological reality

The evaluation found that the ePD is not well adapted to the market and technological reality. This relates to the scope and some of the substantial provisions. Both of these aspects are further discussed below.

The **types of services within the scope of the ePD** based on Articles 1 and 3 include public or publicly available electronic communication services. However, there are certain provisions that have an atypical scope. The following table presents the scope of the different provisions, giving examples of specific types of services based on the definitions of the ePD.[409]

Table 62 – Overview of the scope in relation to the types of services covered per provision

Provisions of the ePD	Explanation
Articles with a typical scope	
Security of processing (Article 4)	- These provisions follow the scope as defined in Articles 1 and 3 of the ePD and thus apply to **public or public available electronic communications services**. - Examples of **included services**: o Internet providers o Telephone providers - Examples of **excluded services**: o Private networks and services (such as purely corporate networks) o OTT services, including communications (WhatsApp, Skype, Facetime), providers of online television and video services (Netflix, YouTube, Google play), other applications (social
Traffic data and other location data (Article 6 and 9)	
Itemised billing (Article 7)	
Presentation and restriction of calling and connected line identification (Articles 8 and 10)	
Automatic call forwarding (Article 11)	
Directories of subscribers	

[409] Some of these services may still be covered in some Member States, depending on the transposition (see chapter 4).

Provisions of the ePD	Explanation
(Article 12)	networks, online baking, e-Health). One notable exception are VoIP services offering fixed inbound and outbound phone numbers for users, which are therefore regarded as ECS in the Universal Service Directive.[410] ○ Webmail providers ○ Advertising networks (e.g. online marketing company, providers of smart phone apps)
Articles with an atypical scope	
Security of communications (Article 5.1 and 5.2)	- There are different opinions on the scope of these provisions. According to the EDPS, the scope of this provision is broader than what is set out in Articles 1 and 3, covering not only public or publicly electronic communications services.[411] It may also be argued based on the wording of the article that it aims at protecting communications in general.[412]
Confidentiality of information stored on users' terminal equipment (Article 5.3)	- This provision is broader in scope compared to what is set out in Article 1 and 3. It applies to anyone storing or accessing information (e.g. cookies) on a user's device.[413]
Unsolicited communications (Article 13)	- This provision is broader in scope compared to what is set out in Article 1 and 3. It applies to anyone potentially sending out spam using electronic communication services, including e.g. online shops.

Source: Deloitte

Several **challenges** have been identified in relation to the scope of the ePD. The following are considered the most relevant issues:

- **The ePD does not cover all online communication services (OTTs)**: As indicated in Table 62, the ePD only applies, for the most part, to **traditional telecommunication service providers**, i.e. those providers that are responsible for carrying signals over an electronic communications network.[414] Most provisions do not apply to the delivery of audio, video, and other media over the Internet without the involvement of a multiple-system operator in the control or distribution of the content, the so-called **over-the-top services (OTT)**.[415] On this basis, various stakeholders have criticised that the scope of the ePD in relation to the types of services covered in their view is **too narrow** considering the increased use of such services as substitutes for traditional ECS.[416] A lack of protection of substitutable services via the ePD

[410] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p. 80
[411] European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Proposal for a Directive on privacy and electronic communications', Brussels, (2008/C 181/01), 10 April 2008, par 33.
[412] Cf. Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 25.
[413] Cf. Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 27.
[414] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15039), p. 5; European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, p. 4.
[415] Ibid, p. 4.
[416] For example, of the respondents to Deloitte's online survey with competent authorities this was regarded as the most serious problem: 56.7% (17 out of 30) authorities indicated that the fact that OTTs are not covered is a serious problem and another 26.7% (8 out of 30) considered this to be a moderate problem. No authority indicated that this was a minor problem or not at all a problem.

might result in a **void of protection for citizens and an uneven playing field**.[417] These aspects are discussed in more detail in section 7.3.

- **The ePD does not cover private or closed networks**: In this context, there is a lack of clarity which services qualify as a publicly available electronic communications services in public communications networks. For example, not all Member States agree that cases such as **Wi-Fi access offered by an airport or internet access provided in internet cafes and shopping malls** qualify as publicly available electronic communications services in public communications networks.[418] Indeed, it was noted by the Article 29 Working Party that the distinction between public and private networks is not always clear, as private and public elements are increasingly intertwined.[419] Furthermore, some stakeholders argue that it is a weakness of the ePD that private networks are excluded, as this hampers the achievement of the ePD's privacy related objectives.[420]
- **There are ambiguities relating to the coverage of certain new technologies**: For example, it was raised by some stakeholders responding to the public consultation that it is not clear to what extent the ePD applies to IoT devices. We note in this context that the 2009 review clarified that the ePD applies to RFID devices connected to a network and that an analogy could be made.

In addition to these issues on the scope, the evaluation found that some of the substantial provisions are not in line with recent market and technological developments or are no longer relevant altogether. Doubts exist in particular in relation to the following provisions:

- **Article 5(1) and 5(2) on the confidentiality of communications**: According to national enforcement authorities the **wording of the provisions is not sufficiently clear and potentially not in line with recent technological developments.** For example, 13 out of 29 (45%) of the competent authorities responding to Deloitte's online survey considered it a serious problem that it is not sufficiently clear what type of communications data is in scope. Another five authorities considered this as a moderate problem. In addition, eight out of 29 (26%) considered it a serious problem that the wording of this provision is not in line with modern technologies, while another eight considered this a moderate problem.
- **Article 5(3) on the confidentiality of information stored on the user's terminal equipment**: Although Article 5(3) is meant to be technology neutral, it has been raised by different stakeholders that **not all relevant techniques may be covered**. According to some

[417] European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, p. 4; Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 2; Communication COM(2015) 192 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, p. 9 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

[418] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15039), p. 5.

[419] Article 29 Working Party, 'Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)' (WP150), p. 4. See also: Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 16; European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, pp. 24 ff.

[420] European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, p. 4.

stakeholders, there is at least a lack of clarity relating to the coverage of some techniques. Examples of aspects that are not explicitly covered include **Wi-Fi tracking, near field communication (NFC), and Bluetooth**.[421]

- **Article 8 on the presentation and restriction of calling and connected line identification:** This provision does not yet take into account that there are alternative technological solutions to achieve the same purpose (e.g. to block numbers directly in the cell phone instead of via the service provider). Stakeholders consulted by Deloitte and BEREC voiced concerns in this respect, indicating that the provision is not fully in line with such new developments.

7.2.2 The rules on consumers' consent are not effective

The ePD includes several rules that include the users' consent as a precondition for certain actions. Issues have been identified in relation to some of these rules notably:

- Article 5(3) on the confidentiality of communications;
- Article 6 and 9 on traffic and location data; and
- Article 13 on unsolicited communication.

We discuss the relevant issues identified in relation to these three provisions below.

One point of criticism on **Article 5(3) on the confidentiality of communications** relates to the **transparency of the consent mechanism.** There seems to be a lack of clarity in relation to the modalities of giving consent and the information that should be given to the users.[422] Indeed, for some users and subscribers it may not be clear that giving mere consent can provide a justification to comprehensively track their behaviour in the online environment ("profiling").[423] On this basis, giving consent might trigger that users get a false sense of protection.[424] Similarly, it was pointed out at the workshop the Commission held with competent authorities that there is a danger of an information overload and too much complexity.[425] In addition, there is a lack of clarity under which circumstances consent given via the configuration of browser settings is valid and effective.[426] Furthermore, the effectiveness of fending off cookies via browser settings may be hindered. In particular, default browser settings do not provide the consumer with a granularity of choice and it may only work in 10% of app cases.[427]

Furthermore, critics argue that the provision does not ensure that users have a real choice when it comes to cookies. Although users seemingly have a choice, they are in fact sometimes **not able to**

[421] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 1.
[422] European Commission (2015). *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*. Final Report, (https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data), p. 13.
[423] Ibid, p. 13.
[424] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15039), p. 8.
[425] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 1.
[426] See e.g. European Commission (2015). *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*. Final Report, (https://ec.europa.eu/digital-s; European Commission (April 12, 2016). *Towards a future proof ePrivacy Legal Framework*. Minutes, p. 11.ngle-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data), p. 12.
[427] European Commission (April 12, 2016). *Towards a future proof ePrivacy Legal Framework*. Minutes, p. 11.

access the content of a website if consent to the use of cookies is not given.[428] This is particularly critical if they are **really in need of the requested service (e.g. a website with health or traffic jam information)** resulting in *de facto* "market power" of website providers.[429] On this basis, the confidentiality of information stored on users' terminal equipment may be safeguarded. However, users arguably do not have a real choice if the use of certain websites depends on their consent to cookies.

Turning to **Article 6 and 9 on traffic and location data**, several challenges that relate to the effectiveness of the consent mechanism have been identified.

In particular, there are still **situations in which traffic and location data may be used without consent**. For example, it was argued in the Commission's 2015 study on the ePD that only a fraction of location based services is regulated by Articles 6 and 9: The ePD only covers those services which rely on the processing of location data other than traffic data offered via a public communications network. On this basis, location based services that are offered to members of a private network (e.g. data transmitted via infrared signals or GPS) do not fall under the ePD.[430]

An additional barrier for the effectiveness of the consent mechanism is based on ambiguities associated with these provisions. For example, ambiguities have been identified in relation to the **interaction of Articles 6 and 9 with other provisions and legal instruments**. In particular, it was pointed out by several competent authorities that it is not clear what type of data falls under Article 9, as most type of location data actually falls under Article 6. The authorities explained that the difference between "traffic data" and "location data, other than traffic data" is difficult to ascertain and apply in practice. A few authorities indicated that they do not consider this an issue. Similarly, some businesses and competent authorities indicated that the separation between Article 5(1) and (2) via-a-vis Articles 6 and 9 causes confusion, as the separation between communication data and traffic/location data is not always clear cut. This increases the risk for misapplication of the provision, which renders the consent mechanism ineffective.

Finally, some challenges have been raised in relation to the **enforcement** of these provisions. For example, in relation to Article 6(3) it has been pointed out on different occasions that in practice some mobile operators mention the possibility of processing user and traffic data in their general terms and conditions, without further information. Some of these terms and conditions grant the operator a right to process the data for a duration of two years after the end of the contract.[431]

Article 13 on unsolicited communications contains rules on users' consent, which give Member States the possibility to choose between an opt-in or an opt-out regime. On this basis, **the rules in the Member States vary significantly**. The ensuing fragmentation of rules was raised as one of the

[428] European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 2.
[429] Ibid, p. 8.
[430] European Commission (2015). *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation.* Final Report, (https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data), p. 12. Additional situations in which traffic and location may be processed without consent are mentioned in: European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15039), p. 9.
[431] This has for example been reported by the Belgian consumers' organisation "Test-Achats" in a report of October 2014, summarised in their magazine "Budget & Droit", January-February 2014, p. 10-11. See also European Commission (2015). *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*. Final Report, (https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data), p. 81.

biggest concerns in relation to Article 13 by stakeholders consulted by Deloitte[432] and as part of the EC's public consultation.[433] The table below presents the situation in the Member States.

Table 63 – Opt-in and opt-out regimes per Member State

Member States	Number of businesses	Fixed-line phones		Mobile phones	
		Opt-in	Opt-out	Opt-in	Opt-out
Austria	321,661	X		X	
Belgium	593,421		X	X	
Bulgaria	319,856	X		X	
Croatia	147,337		X		X
Cyprus	46,938	X		X	
Czech Republic	995,754		X		X
Denmark	212,740	X[1]	X[2]	X[1]	X[2]
Estonia	64,040		X		X
Finland	229,248		X		X
France	3,188,138		X	X	
Germany	2,193,135	X[1]	X[3]	X[1]	X[3]
Greece	700,166		X		X
Hungary	514,537	X		X	
Ireland	146,741		X	X	
Italy	3,715,164		X		X
Latvia	100,491	X		X	
Lithuania	174,611	X		X	
Luxembourg	31,385	X		X	
Malta	26,193		X		X
Netherlands	1,054,562		X		X
Poland	1,549,326		X		X
Portugal	781,823	X		X	
Romania	455,852	X		X	
Slovakia	400,683	X[1]	X[3]	X[1]	X[3]
Slovenia	130,088		X		X
Spain	2,377,191		X	X	
Sweden	673,218		X		X
United Kingdom	1,841,715		X		X
		11	19	15	15
Number / share of businesses affected	22,986,014	4,771,889	20,238,860	11,077,380	13,933,369
		21%	88%	48%	61%

Source: European Commission, tabulation by Deloitte. [1]For 'consumers'; [2] For 'businesses'; [3] For 'other market players'. Statistical data from taken from Eurostat (most recent data from 2014).

Furthermore, we identified **ambiguities** in relation to Article 13, which may also hinder the effectiveness of the consent mechanism. Article 13(2) provides a possibility for retailers to send marketing communications to their own customers, but only for similar products than the ones previously bought by the customers. Available evidence suggests that there are a number of

[432] This was, for example, raised by businesses, business associations and competent authorities.
[433] According to the responses received as part of the European Commission's public consultation, two thirds of respondents (63.6%) indicate that Member States should not retain the possibility to choose between an opt-in and opt-out regime for direct marketing telephone calls (with human interaction) directed toward individual citizens. Similarly, 61% of respondents indicate that Member States should not retain the possibility to choose between and opt-in and opt-out regime for direct marketing communications to legal persons (automatic calling machines, fax, e-mail and telephone calls with human interactions). This is valid across the stakeholders from industry, citizens and civil society organisations, as well as public bodies.

ambiguities in relation to the application of this paragraph. These relate, for instance, to questions such as:

- Is browsing products and services on a website already part of a sale or its negotiations respectively and accordingly sufficient to allow for sending spam afterwards?[434]
- Is sending spam allowed in relation to similar products and services to those that were bought?[435]

Furthermore, it is not clear if spam is in practice only sent on the basis of identity details given away in a sale or also by simple browsing in an online shop, clicking on cookies, having access to exclusive sites or subscribing to a newsletter/voucher.[436]

7.2.3 Based on unclear/incoherent rules, the implementation in Member States is inconsistent and ineffective

The **transposition** of the ePD in the Member States varies considerably, as shown both by the 2015 Study and Deloitte's transposition check. The identified variations can lead to legal uncertainty for businesses and consumers. In addition, in some cases the transposition does not facilitate the effective application of the rules. We provide a summary of the findings of the two relevant analyses below.

A survey conducted in the context of the ePrivacy Study 2013/0071[437] on the transposition of the ePD in Member States dealt with the following provisions of the ePD:

- Articles 1 and 3 on the scope;
- Article 5 on confidentiality;
- Article 5(3) on confidentiality of terminal equipment;
- Articles 6 and 9 on traffic and location; and
- Article 13 on unsolicited communications.

This study found that these provisions of the ePD are not always correctly transposed in the correct national legal framework by Member States. In addition, the survey results revealed that the ePD provisions were not always transposed in the legal framework applicable to electronic communications but sometimes in in the legislation applicable to information society services, general data protection law or consumer protection.[438] Such discrepancies, typically lead to an ineffective legal framework impeding the achievement of the Digital Single Market.

The transposition check carried out for the purpose of this study dealt with the following provisions:

- Articles 1, 2 and 3 on the scope and definitions;
- Article 4 on the security of processing; and
- Articles 7, 8, 10, 11, 12 on users' rights and exceptions.

[434] Edwards, L. (ed.) (2005). The New Legal Framework for E-Commerce in Europe. Oxford and Portland, Oregon: Hart Publishing, p. 47.
[435] Ibid, p. 47.
[436] Ibid, p. 47.
[437] European Commission, ePD Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, 2015, (https://ec.europa.eu/digital-single-market/news/ePD-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data).
[438] ePrivacy Study SMART 2013/0071, p.8

The analysis showed that, while most provisions have been transposed (often literally) by most Member States, several specificities as well as substantial differences could be identified. National laws vary in relation to the context, including e.g. type of legislative framework used, as well as in relation to some substantial aspects. For example, the question of whether OTT service providers and private networks are subject to the requirements of the ePD and the corresponding national implementing acts has not been uniformly addressed in the transposition of the ePD. Member States vary considerably in their approach to this topic. It is reasonable to conclude, based on this uneven transposition of the ePD, that the current situation obscures the level of legal certainty by obliging operators and users to consult secondary sources of law, some of which might not always be readily accessible or drafted with the principal concern of clarity. More importantly, the current *status quo* provides for appreciable differences in legal treatment across Member States, creating an uneven playing field for operators and a potential obstacle to the goals set out by the ePD.

7.2.4 The enforcement of the rules is insufficient and inconsistent

Insufficient an inconsistent enforcement has been identified as a horizontal challenge impacting on the functioning of the ePD. Weaknesses in relation to enforcement were also identified in the 2015 Study, which pointed for instance to the fact that Article 6 is often not properly enforced.[439]

One of the main reasons for these challenges is the fact that **the ePD leaves it up to Member States to designate the national bodies for enforcement of the ePD**.[440] On this basis, the Member States have followed **inconsistent approaches**. Some Member States have designated DPAs (e.g. Bulgaria, Estonia, France), others the telecom national regulatory authority (NRAs) (e.g. Belgium, Finland, Denmark) and still others appointed both DPAs and NRAs (e.g. Austria, Germany, Greece) for the ePD enforcement. In some Member States, competence concerning the ePD is even shared between three or four different authorities,[441] including in addition to DPAs and NRAs e.g. consumer protection authorities.

This situation potentially leads to the following problems:

- **Ineffective and/or inefficient enforcement**: This question was dealt with in the EU public consultation. The majority of respondents supported the statement that the fact that Member States appointed different authorities can lead to ineffective enforcement.[442] It was also pointed out by some of the authorities consulted by Deloitte that this situation can lead to a duplication of work. We note, however, that the views of the competent authorities were divided on this aspect.
- **Confusion for citizens, service providers and public bodies**: Based on EC's public consultation, the situation seems to be a particular source of confusion for citizens (70% of the respondents thought so) and providers/controllers (72% thought so). This was also raised by some of the businesses and authorities consulted by Deloitte.

[439] See p. 120.
[440] Cf. e.g. European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive), p. 11.
[441] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive), p. 11.
[442] 24% indicated that this is significantly the case, 28% moderately, and 9% little. 13% did not support this statement at all.

- **Different interpretations of the law**: Authorities in charge of the enforcement of the ePD may differ in nature and have different sensibilities[443], which may lead to varying interpretations of the law.[444] This was also confirmed by the replies to the EC's public consultation, in which a majority of the respondents supported the statement that the fact that Member States appointed different authorities can lead to different interpretations of EU law.

Another challenge which has been voiced in a stakeholder workshop organised by the Commission is the fact that there is **insufficient guidance in relation to cross-border cases**. Article 15a(4) allows for the adoption of measures, but does not provide any details.[445] Depending on the types of measures national authorities have taken in this regard, this could lead to confusion amongst citizens and service providers. In addition, the cooperation between authorities across borders may be hampered e.g. based on varying practices. In Deloitte's online survey with competent authorities, the majority of respondents indicated that they consider this as a problem. Almost half consider it a serious problem (13 out of 28), six as a moderate problem and four as a minor problem. Only one authority indicated that this is not an issue. We note, however, that the interviewed authorities indicated that cross-border cases are a rarity.

A final challenge potentially hindering the consistency is related to the fact that **there is no recognised EU group to gather together all authorities responsible for the enforcement of the ePD.** Article 15 of the ePD refers to the Article 29 Working Party, which only represents data protection authorities and thus not all competent authorities enforcing the ePD.[446] Indeed, the authorities meet in different constellations: DPAs meet through the Article 29 Working Party and NRAs through BEREC. In addition, some consumer bodies meet through the Consumer Protection Cooperation (CPC) network. The fact that the Article 29 Working Party and the future European Data Protection Board (EDPB) only represent data protection authorities and thus not all national competent authorities is also considered as a problem by most of the competent authorities responding to Deloitte's online survey: around two thirds of the respondents consider it a serious problem (9 out of 28) or a moderate problem (8 out of 28). Another 14% consider this a minor problem. Five authorities do not regard this as a problem.

7.3 Assessment of the Problems

The barriers identified in the previous sections potentially lead to the following problems (cf. our problem tree in Figure 39):

- Citizens' private life when communicating online is not effectively protected;
- Citizens are not effectively protected against unsolicited marketing communications; and
- Businesses face obstacles and undue costs based on unclear, fragmented and outdated rules.

These are discussed in the following sub-sections.

[443] For example, the DPAs will put more emphasis on data protection as such, whereas NRAs may bring in another perspective.
[444] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive), p. 11.
[445] European Commission (April 12, 2016). *Towards a future proof ePrivacy Legal Framework*. Minutes, p. 12.
[446] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive), p. 11-12; European Commission (April 19, 2016). *Meeting with Competent National Authorities on the review of the e-Privacy Directive*. Minutes, p. 5.

7.3.1 Privacy and confidentiality in relation to citizens' communications is not fully ensured

This problem relates to two different user groups:

- The users of traditional electronic communications services, i.e. the services explicitly covered by the current ePD; and
- The users of OTTs, which are not explicitly covered by the ePD.

The problems for these two groups are discussed separately in the following two sub-sections.

Users of traditional electronic communications services

One of the reasons for this problem is the **limited effectiveness of Articles 4, 5, 6, and 9**, which aim to ensure data security and the confidentiality of communications:

- **Article 4 on the security of processing:** The evaluation identified practical difficulties relating to the application of Article 4. For example, there are doubts whether all security or personal data breaches are in fact notified based on several issues identified in relation to this provision. In particular, there are some ambiguities, for example it is not clear to what extent the security obligations apply to non-personal data. In addition, there are practical difficulties when it comes to the application of personal data breach notifications: some businesses are confused about which authority to contact in case of breaches and due to the duplication with the GDPR. Furthermore, few breaches are notified hinting towards a low level of compliance and the enforcement powers of authorities are not always appropriate.[447] On this basis, there may be situations in which breaches are not properly fixed and users' data may thus not be fully protected.
- **Articles 5(1) and 5(2) on the confidentiality of communications:** While Article 5(1) and (2) supported the achievement of the objective to ensure confidentiality of communications, some issues that potentially act as barriers in this respect have been identified. In particular, our research shows that some stakeholders faced obstacles in the practical application of this provision. Such difficulties may arise because the wording of the provisions is not sufficiently clear and potentially not in line with recent technological developments, also leading to varying implementation across Member States. On this basis, **consumers do not face equal standards in this regard across all Member States.**
- **Article 5(3) on the confidentiality of communications stored on the user's terminal equipment:** The evaluation found that there are several challenges relating to the practical application of this provision by businesses and citizens. These include in particular

[447] According to some authorities, the breach notification provision is good on theoretical level but ineffective in practice. This is confirmed by the inexistent or very low numbers of breach notifications in many Member States. Out of 10 Member States that provided input on the number of personal breaches, two indicated that there was no breach between 2010 and 2015. In three Member States, the annual number of breaches ranged between 1 and 5. Of the five Member States that reported more than that, Ireland reported most breaches (between 410 in 2010 and 2317 in 2015). An overview is provided in Table 21. Some authorities explained that the lack of criteria makes it difficult to determine which breaches need to be notified and not. Correspondingly, some authorities responding to Deloitte's online survey indicated that businesses in some cases fail to report personal data breaches.

ambiguities relation to the scope of this provision, the fact that the scope may be too broad, limited transparency and usefulness of the consent mechanism as well as difficulties relating to enforcement. This has different consequences for citizens. Based on the lack of transparency of the consent mechanism, it is **possible that users do not know exactly how far-reaching the consent is**. It was also criticised that users do not have a real choice. This further impedes on the confidentiality of information stored on the users' terminal equipment, because **consumers may feel forced to give their consent**.

- **Articles 6 and 9 on traffic and location data:** Based on the evidence available, the effectiveness of the specific provisions on traffic and location data does not seem to be fully achieved, as a number of problems seem to occur in relation to their application. First, lack of clarity for businesses and competent authorities may lead to a wrong application of the rules. On this basis, **users may not benefit from the envisaged equal standards**. In relation to the consent mechanism, there are still cases where traffic and location data may be used without consent. This is in particular based on the scope of the provisions: For example, location based services offered in the context of private networks may process traffic and location data without asking the users' consent.[448] Finally, the provisions do not always seem to be enforced properly. For example, in relation to Article 6(3) it has been pointed out on different occasions that in practice some mobile operators mention the possibility of processing user and traffic data in their general terms and conditions, without further information. Some of these terms and conditions grant the operator the right to process the data for a duration of two years after the end of the contract.[449]

Additional reasons include **horizontal challenges**, in particular the diverging transposition of the rules in the Member States (see section 7.2.3) and ineffective and inconsistent enforcement (see section 7.2.4). As a consequence of these challenges, **users do not benefit from equal standards** in relation to privacy and the confidentiality of communications in the electronic communications sector. On this basis, the **privacy and confidentiality may not be fully ensured**, e.g. because rules are not at all or not properly applied.

The following table presents the number of citizens using the services covered by the ePD. These numbers equal the **number of citizens potentially affected by this problem**.

Table 64 – Number of citizens potentially affected based on the usage rates of relevant services

Average number of citizens affected per year (in million)	2002-2015	2016 snap shot
Internet to browse online	304.8	397.7
Mobile phone to make calls or send texts	369.1	469.1

[448] European Commission (2015). *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation.* Final Report, (https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data), p. 12. Additional situations in which traffic and location may be processed without consent are mentioned in: European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15039), p. 9.

[449] This has for example been reported by the Belgian consumers' organisation "Test-Achats" in a report of October 2014, summarised in their magazine "Budget & Droit", January-February 2014, p. 10-11. See also European Commission (2015). *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*. Final Report, (https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data), p. 81.

Fixed phone line	477.2	397.7

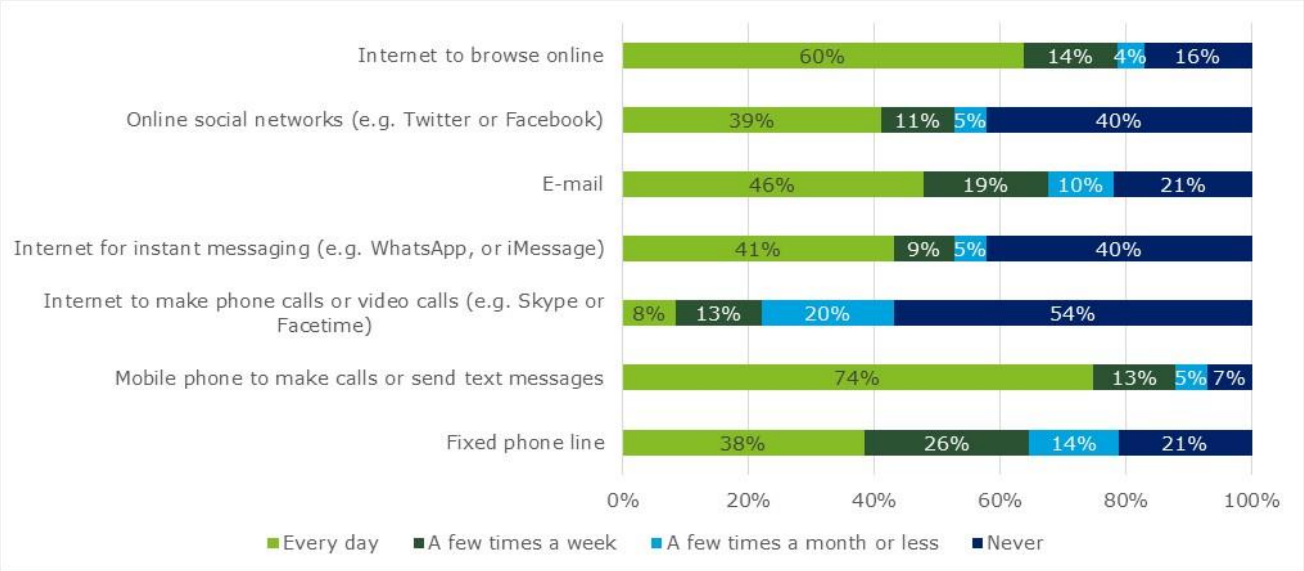
Source: Deloitte based on data gathered as part of the Eurobarometer on ePrivacy.

Users of OTTs

As explained in section 7.2.1, OTTs are not explicitly covered by the scope of the ePD. This results in a **void of protection, as users of OTTs do not face as high standards on privacy and confidentiality compared to traditional electronic communication services**.[450] From a user's perspective, this is difficult to understand since the service-centric approach of the ePD "can lead to – from a user perspective – arbitrary differences between protections for different but functionally equivalent services."[451]

This problem becomes especially relevant based on the increased use of OTTs by citizens. Available Eurobarometer data[452] shows that that the services covered by the ePD are generally used by consumers (see Figure 14).

Figure 40 – Usage patterns of citizens regarding different types of telecom services



Source: Eurobarometer, graphical representation by Deloitte.

The **ePD covers important parts of consumers' everyday communication means**. However, **very important parts are also excluded from its scope** – in particular communication means that are expected to become more important over the next couple of years (both societal, as well as financially in terms of businesses' turnover) and that are especially used by younger generations:

- Email is used by 46% of consumers every day;

[450] European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, p. 4; Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 2; Communication COM(2015) 192 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, p. 9 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

[451] Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 33. It was also pointed out that users may in some cases not even aware whether they use electronic communications services or other, e.g. VoIP, services.

[452] Flash Eurobarometer 443 (2016): e-Privacy. Data on 26,526 consumers collected between 6 and 8 July 2016. At this stage, the Eurobarometer results are only of provisional character.

- OTTs for the purpose of instant messaging (e.g. WhatsApp) are used by 41% every day[453]; and
- Online social networks are used by 38% every day.

The notable exception here is the usage of the Internet to make phone calls or video calls (e.g. via Skype or Facetime). More than half of consumers never use this type of service. However, it can reasonably expected that this figure is going to decrease over the upcoming years with take-up rates for Internet based audio and video communication increasing.

This shows that communication means that are used by, typically, younger consumers on a daily basis are excluded from the ePD. In practice, this means that an important segment of users (i.e. data subjects) are deprived, possibly unknowingly, of the confidentiality of communications offered to users of more traditional means of communications under the current ePD. This is a critical point, not only from the perspective of the market players, but also in light of the young consumers within the user group that may not be fully aware of the privacy risks involved in this type of electronic communication services.

This said, the interpretation and implementation of the scope of the ePD varies across Member States. Indeed, some Member States have extended the ePD provisions to OTT services.[454] An overview is presented in the table below.

Table 65 – The coverage of OTTs within the scope of national implementing legislation

Country	OTTs covered	OTTs not covered	Case-by-case	No information/ unclear
Austria	X			
Belgium				X
Bulgaria	X			
Croatia				X
Cyprus				X
Czech Republic		X		
Denmark				X
Estonia		X		
Finland				X
France	X			
Germany			X	
Greece	X			
Hungary				X
Ireland		X		
Italy			X	
Latvia	X			

[453] Interestingly, the Eurobarometer data shows that for instant messaging OTTs, two large groups of consumers seem to exist: Those that use instant messaging every day and those that never use it. The proportion of consumers that uses it a few times per week / month is comparatively small. It can be assumed that age is an important factor with regard to the take-up of such services. While younger generations use instant messaging every day, the majority of older consumers do not use it at all. Therefore, it can be expected that the share of consumers who use instant messaging on a daily basis will increase over the next years.

[454] European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, p. 4.

Country	OTTs covered	OTTs not covered	Case-by-case	No information/ unclear
Lithuania				X
Luxembourg		X		
Malta				X
Netherlands		X		
Poland		X		
Portugal		X		
Romania		X		
Slovakia		X		
Slovenia	X			
Spain	X			
Sweden				X
UK				X
Overall	7	9	2	10

Source: Deloitte – Transposition check.

On this basis, the citizens in the seven Member States in which OTTs are covered are not affected by this problem. Citizens in the other 21 Member States are potentially affected.[455]

The following table presents the number of citizens using OTTs in the 21 Member States in which OTTs are not clearly covered based on data gathered as part of the Eurobarometer on ePrivacy. These numbers equal the **number of citizens potentially affected by this problem**.

Table 66 – Number of citizens potentially affected based on the usage rates of relevant services

Average number of citizens affected per year in the 21 Member States not clearly covering OTTs(in million)	2002-2015	2016 snap shot
Online social networks	154.6	201.1
E-Mail	201.6	274.3
Instant messaging (e.g. WhatsAppWhatsApp)	112.8	201.1
VoIP	74.8	149.9

Source: Deloitte based on data gathered as part of the Eurobarometer on ePrivacy.[456]

7.3.2 Citizens are not effectively protected against unsolicited marketing communications

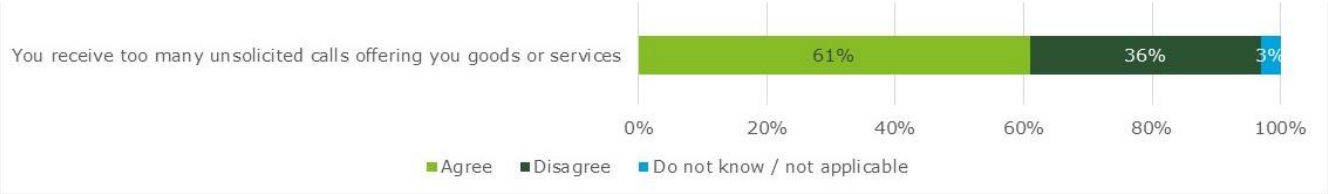
Based on a number of challenges identified in relation to Article 13, it appears that the ePD has not managed to effectively protect citizens against unsolicited marketing communications.

Indeed, in the Eurobarometer 61% of EU consumers have indicated that they receive too many unsolicited calls offering them goods or services.

[455] While it is clear that citizens in Member States in which OTTs are not covered are affected, citizens in Member States that apply a case-by-case approach may be affected depending on the exact service they use. They may also face an increased level of uncertainty, as the matter may depend on ad hoc decisions by the competent authorities. For the Member States we do not have information, we assume that the citizens are potentially affected as it is not clear whether OTTs are covered. In any case, citizens in these Member States may face uncertainty.

[456] Flash Eurobarometer 443 (2016): e-Privacy. Data on 26,526 consumers collected between 6 and 8 July 2016. At this stage, the Eurobarometer results are only of provisional character.

Figure 41 – Consumers' assessment of the amount of unsolicited calls



Source: Eurobarometer, graphical representation by Deloitte.

This is further confirmed by data from Statista, indicating that 42% of the Germans believe that there is a high possibility of receiving unsolicited marketing while 43% think receiving spam e-mails is certain through the use of internet[457]. Furthermore, 71% people in Germany have already made negative experience with unsolicited marketing[458]. Statistics from the UK show that the actual numbers of calls can be quite high. So far in 2016 one of the concerned authorities in the UK, the Information Commissioner's Office (ICO), has received more than 93.000 complaints from people affected by nuisance calls[459]. Data by the UK authority Ofcom indicates that each year UK consumers receive around 4.8 billion nuisance calls: 1.7 billion live sales calls, 1.5 billion silent calls, 940 million recorded sales messages, and 200 million abandoned calls.[460]

This recent increment of unsolicited marketing is seen to be a serious issue to deal with by the responsible national authorities, as it causes significant distress to the consumers. Consumer complaints reported to the ICO range from bothering of disabled and the exploitation of the elderly to upsetting relatives and frustration in general – all issues caused by different forms of unsolicited marketing[461]. As a result of such calls, citizens most likely feel annoyed, as shown in a survey commissioned by the UK authority Ofcom. Participants in this survey were requested to keep track of actual calls they received in a four-week period. As concerns nuisance calls, 80% of these were perceived as annoying and 5% as distressing. Rather few (12%) were considered as being not a problem and very few were considered useful (1%). Participants who considered calls as being annoying or distressing commonly indicated that this was the case because they had received a lot of nuisance calls already, the call interrupted what they were doing, or there was no reply when answering the phone.[462]

Furthermore, it needs to be noted that citizens spend time on dealing with unsolicited communications. As concerns calls, the time spent depending on how citizens deal with such calls. For one call, this could e.g. be between 15 seconds in case the citizen hangs up directly after

[457] https://de.statista.com/statistik/daten/studie/499845/umfrage/einschaetzung-von-risiken-bei-der-internetnutzung-in-deutschland/
[458] https://de.statista.com/statistik/daten/studie/467041/umfrage/umfrage-zu-den-erfahrungen-mit-datenmissbrauch-in-deutschland/
[459] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/08/cold-call-crooks-hit-with-10k-a-day-in-fines-by-regulator/

[460] ICO-OFCOM, *Tackling Nuisance Calls and messages* (December 2015): http://stakeholders.ofcom.org.uk/binaries/consultations/silentcalls/JAP_Update_Dec2015.pdf.
[461] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/08/cold-call-crooks-hit-with-10k-a-day-in-fines-by-regulator/
[462] OFCOM (April 2015): Landline nuisance calls panel Wave 3 (January- February 2015), http://stakeholders.ofcom.org.uk/binaries/telecoms/nuisance-calls-2015/Nuisance_calls_W3_report.pdf, p. 9.

realising that they are not interested in the call[463] up to several minutes in case the citizens first listens to the caller and perhaps tries to persuade them not to call anymore.

As a consequence of the high number of calls received and the negative effects for citizens, the number of people registering to do-not-call lists is constantly growing[464].

The seriousness of this issue is confirmed by statistics gathered from the Member States as part of this initiative. The table below provides an overview of complaints by citizen received per Member State, including only Member States for which data was available at the time of the analysis.[465] For the Member States reflected, the number of complaints has increased between 2010 and 2015. UK and Germany received the highest number of complaints.

Table 67 – Complaints by citizens concerning Article 13 by Member State and year

Member State	2010	2011	2012	2013	2014	2015
Belgium	170	284	453	289	316	218
Bulgaria	0	0	0	87	100	45
Croatia	N/A	N/A	N/A	0	0	0
Cyprus	660	465	251	332	122	128
France				1071	932	2057
Germany	55,778	35,829	24,063	59,018	60,953	72,099
Greece	87	118	229	193	211	117
Ireland	231	253	606	204	176	104
Poland						91
Slovakia	128	91	132	288	155	95
Sweden				46	49	66
United Kingdom			79,018	199,376	175,248	166,663
Total	**57,054**	**37,040**	**104,752**	**260,904**	**238,262**	**241,683**

Source: Deloitte based on data made available by the competent authorities.

In comparison with the other provisions of the ePD, most competent authorities received the highest number of complaints for Article 13. For example, the Greek DPA estimates that around 90% of all complaints received in relation to the ePD relate to Article 13.

[463] This is an estimate, assuming that it is necessary to get the telephone (e.g. go to another room in case of fixed line or search in a purse for a mobile phone), potentially move to a quiet place in case the call is accepted in loud surroundings and listed to the introduction of the caller.

[464] Step Change Debt Charity, *Combating Nuisance Calls and Texts*, by Claire Milne, https://www.stepchange.org/Portals/0/documents/media/reports/additionalreports/Nuisance_Calls_Report_FINAL.pdf.

[465] BE, BG, CY, DE, FR, GR, HR, IE, PL, SK, SE, UK.

7.3.3 Businesses face obstacles and undue costs based on unclear, fragmented and outdated rules

The difficulties identified in relation to the functioning of the individual provisions of the ePD has led to concrete obstacles for businesses, resulting also in undue costs. This in particular due to the following horizontal issues:

- **Some of the provisions are not clear**: Businesses may need to spend more time interpreting the rules, including e.g. to decide whether they fall within the scope of certain provisions and/or to decide how they should be applied. This may also involve costs for (external) legal advice. In some cases, they may need to contact the competent authorities and discuss certain issues with them. For example, in some Member States it is decided on a case-by-case basis when OTTs are covered by the rules or not. Companies for which it is not clear whether they are covered usually engage in exchanges with the competent authorities to solve this question.
- **The implementation of the rules is fragmented**: Based on ambiguities and legal leeway in the ePD, the implementation of the rules varies considerably. In addition, the rules are not always consistently and effectively enforced. On this basis, businesses engaging in cross-border activities still face varying legal frameworks in the Member States. On this basis, they may incur additional costs for legal advice as they need to understand the rules in different Member States. In addition, they may incur additional costs for implementing the rules, as they will need to follow different legal regimes. For example, they may need to apply different marketing strategies if they are active in a Member State that uses an opt-in regime for unsolicited communications and one that uses an opt-out regime. Horizontally across all types of stakeholders, the fragmented implementation of the ePD in the different Member States and the resulting complexity was pointed out an issue and an important source of cost.
- **Some of the rules are outdated**: Businesses incur costs because they need to implement provisions that are no longer needed, e.g. because they are covered in other legal instruments (Article 4) or are no longer requested by consumers (Article 8). In addition, some of the rules only bring limited use for citizens as they are no longer in line with new technologies, whereas businesses still incur costs. This concerns in particular Article 5(3).

Overall, business associations have pointed out that the costs related to the ePD are disproportionate. For instance, stakeholders believe that the costs related to the cookie provision are unjustified as the provision failed to accomplish its purpose. The text box below presents an example of the types and magnitude of costs that could be incurred by a telecom provider based on the ePD.

Case example (horizontal): Compliance and administrative burden costs for a telecommunication service provider

The representative of a telecommunication service provider active in one South-Eastern European Member State and third countries indicated that the company would incur overall 400,000 EUR per year in relation to specific provisions of the ePD. The following high-level estimates were provided:

(1) Submitting information to competent national authorities	25.000 €
(2) Providing information to / communication with subscribers and users	75.000 €
(3) Investments in technical infrastructure and related measures ensuring privacy and confidentiality to comply with the ePD.	250.000 €

(4) Compliance with the ePD	25.000 €
(5) Rules on spam and the rules on cookies, which are applicable beyond ECS	25.000 €
Overall	400.000 €

According to the interviewee, the estimates represent yearly annual costs calculated out of our overall annual costs (capex & opex) for IT, Security, Legal, PR/HR and other ePD relevant streams/budgets respectively. Hence, the estimates follow rather a top-down than a bottom-up logic as the *actual* figures are not known to the company.

In the following sub-sections we first present the types of costs associated with the individual provisions. Then we present the results of Deloitte's economic analysis, including the estimated magnitude of costs businesses faced as well as the number of businesses affected.

Evidence from the analysis of the individual provisions

The following table provides an overview of the main findings concerning the efficiency of each provision.

Table 68 – Main findings in relation to the costs for businesses generated by the individual provisions

Relevant articles	Main Findings
Article 4	Overall, this provision is one of the most costly provisions, both for businesses and competent authorities. Nevertheless, some of these costs (e.g. the data breach notification) are only incurred in case of an actual breach, which is an incentive for implementing adequate security requirements. As not all of these costs seem to be justified (e.g. because duplications with other instruments exist), this provision is only considered partially efficient.
Articles 5(1) and (2)	This provision has led to significant costs for businesses, including the setting up of IT infrastructure. However, these costs can be considered proportionate in light of the aim of ensuring confidentiality of communications. We also note that some of these costs may overlap with the security provisions, in case the IT solutions to ensure security and confidentiality overlap. Additional undue costs have may ensue for businesses based on the ambiguous wording of the provision and the fact that its implementation varies significantly across Member States (cf. the previous sub-section). Such costs may in particular relate to legal advice. Finally, there are opportunity costs as the provisions render certain business models invalid. These costs can be considered proportionate in light of the aim of ensuring confidentiality of communications.
Article 5(3)	The efficiency of Article 5(3) is not fully ensured. This is due to the fact that this provision tends to be the main cost factor associated by businesses with the ePD, while not all the costs appear to be justified and the benefits for citizens have been questioned. In particular, based on the ambiguities relating to the scope and consent mechanism, businesses may spend more time than needed on implementing the consent mechanism and possibly need to invest in legal advice. Furthermore, based on the fact that Article 5(3) does not make a distinction between different types of cookies, businesses that only use non-privacy invasive cookies also need to obtain consent. At the same time, users feel annoyed by the consent mechanism, which often does not provide a real choice.
Articles 6 and 9	Although businesses reported that they incurred some costs in relation to these provisions, no information is available on the magnitude of such costs. Businesses mainly incur compliance costs and opportunity costs. Compliance costs notably relate to the development / adaptation of technical infrastructure and / or software. These costs may be justified based on the added level of protection for users. Based on the ambiguities explained above (see section 5.8.1), it is also possible that businesses incur additional undue costs on legal advice, e.g. in case it is not clear under which regime a specific service falls. In addition, this may entail costs for competent authorities, as these may need to deal with unclear cases. Opportunity costs are incurred by providers of traditional telecom providers that face restrictions which do not apply to their OTT competitors.
Article 7	Stakeholders have emphasised the significant costs for the initial implementation of the

Relevant articles	Main Findings
	provisions on non-itemised bills. However, no quantitative evidence is available. There are different opinions as to the benefits of this provision for consumers.
Articles 8 and 10	In general terms, respondents to the European Commission's public consultation and interviewees indicated that significant costs were involved for the initial implementation of the provision on calling and connected line identification. Such costs related in particular to IT infrastructure. Some small recurrent costs may relate to the maintenance of such systems. As concerns the proportionality of such costs, Telecom operators explained that the services were not requested by customers.
Article 11	The efficiency of this provision tends to be limited as the costs incurred by businesses to implement the possibility of stopping automatic call forwarding are much rather caused by legislative obligations than actual customer demand.
Article 12	***Insufficient information to assess***
Article 13	***Efficiency tends to be limited*** Given that ambiguities exist for all types of stakeholders concerning the substance of this provision, as well as diverging approaches by Member States (transposed into national law) – which hamper the effectiveness of the provision – the costs related to this provision do not seem to be proportionate in all cases.
Article 14	***Insufficient information to assess***
Article 15a	***Insufficient information to assess*** While limited information is available on the appropriateness of the costs relating to enforcement, we note that inefficiencies exist both for businesses and competent authorities due to the situation that Member States have appointed several different authorities (see section 5.15.1).

Source: Deloitte

Results of the economic analysis

Introduction and pre-requisites

Information on costs incurred by businesses in relation to the ePD is scarce. Businesses and business associations only have patchy, anecdotal information on the costs related to the ePD in general. Information on particular provisions is even less available. The available information has, however, been used to estimate these costs to the best extent possible.

Feedback received suggests that the majority of costs for the ePD is related to:

- Article 4 on the security of processing;
- Article 5(1) and Art. 5(2) on confidentiality of communications;
- Article 5(3) on cookie consent; and
- Article 13 on unsolicited communication.

In relation to **Article 4, as well as Articles 5(1) and 5(2)**, businesses have indicated that they have incurred a significant amount of compliance costs after the adoption of the ePD. However, businesses were not able to provide any quantitative information on this as the costs were already incurred in the past (almost 15 years ago) and have since then been written off.[466]

Article 5(3) is expected to be responsible for a significant amount of compliance costs. This is due to the extensive coverage of this provision (potentially all businesses in the EU that run a website and use cookies), as well as its importance for today's communication, marketing, advertising, and sales techniques. As businesses are increasingly developing data-driven business models, the importance

[466] Businesses indicated in qualitative terms that they incur still today (and will in the future) costs in relation to regular updates, maintenance, and repair of the necessary hard- and software to safeguard the security and confidentiality of communications. Overall, it was not possible to obtain any quantitative information from businesses on the magnitude of such costs.

of the substance of Art. 5(3) is also expected to grow over the next years. The costs associated with this provision mainly stem from the need to collect users' consent to be able to use cookies on websites, i.e. to implement the relevant technical solutions on websites.

Considering the **business perspective on Article 5(3)**, in the public consultation as well as interviews and an online survey with businesses conducted by Deloitte, several stakeholders highlighted that Article 5(3) is in fact the main cost factor relating to the ePD. As concerns the exact costs for businesses, the estimates vary widely. According to a 2014 study conducted by ITIF the average compliance costs would be around €900 per website/company, although the calculation of such costs is not demonstrated.[467] The ITIF study indicated that these costs included costs for legal advice, updates to privacy policies, and technical updates to websites and would be incurred once per website, i.e. at the time of the introduction of the new policy.[468] This study was indeed cited by different stakeholders consulted as part of this initiative, implying that this estimate is considered realistic by these stakeholders.[469] However, there were also a few stakeholders that indicated that compliance costs would be significantly higher or lower.

In addition, Deloitte has been requested to undertake particular efforts to estimate compliance costs in relation to **Article 13** on unsolicited communications as this provision also involves the implementation of a technical solution on websites to collect users' consent to unsolicited communication.

Article 13 was one of the provisions that most businesses associated costs with.[470] The most expensive cost elements for these businesses concerned:

- Development / adaptation of technical infrastructure and / or software;
- Number of audits by competent national authorities; and
- Costs for advisory services, e.g. concerning legal interpretation of provisions.

It can be noted that three out of the five businesses that incurred significant costs in relation to Article 13 stated that they would have implemented some of the measures / the measures in a similar fashion also without the ePD in place.

In the European Commission's public consultation, several respondents specifically raised Article 13 when asked about the costs incurred in relation to the ePD. While no specific numbers were provided, it was indicated that costs are incurred in relation to adaptations in telemarketing procedures, e.g. initial costs to check opt-out registers (Robinson lists) the revision of lists, offering text-script on opt-out possibility and assistance in registering with related registers.

Finally, after the adoption of the ePD, in particular telecommunication service providers have – according to our interview results – incurred high capital costs in relation to the implementation of:

- Articles 6 and 9 on traffic data and location data other than traffic data;

[467] The Information Technology & Innovation Foundation, Daniel Castro and Alan McQuinn, "*The Economic Costs of the European Union's Cookie Notification Policy*", November 2014 (US).
[468] The study also indicated that there could be additional recurring costs for maintenance. For instance, some companies customise their website's cookie policies to each user's preference. It is explained that these costs could lie between a few hundred or tens of thousands dollars annually per website. However, such costs are not directly based on the ePD and are, therefore, not considered further at this point.
[469] For example, eleven participants to the public consultation mentioned this study in relation to the costs for businesses stemming from the ePD. However, we note in this context that six of these were associated with the Interactive Advertisement Bureau IAB. Others included businesses or citizens.
[470] In Deloitte's business survey, it was one of the three provisions most businesses associated costs with, after the rules on confidentiality of communications (six businesses) and the rules on traffic and location data (five businesses). In addition, many businesses consulted as part of this study associated costs with Article 4.

- Article 7 on itemised billing;
- Article 8 on control of connected line identification (incl. Art. 10 on exception);
- Article 11 on automatic call forwarding; and
- Article 12 on directories of subscribers.

Under Art. 6 & 9, and 12 concerning directories of subscribers, businesses incur some costs regarding information obligations to consumers.

Based on the feedback received, these costs can be expected to be fairly large. However, these costs, which were incurred in the past by telecommunication service providers, can be expected to be already written off.

No quantitative / economic data was identified and / or estimated in relation to these Articles apart of what is provided in relation to each provision in chapter 5 (see the illustrative case examples in textboxes).

In addition to the compliance costs related to the direct implementation of the ePD, businesses also incurred **opportunity costs** for lost business opportunities. In Deloitte's business survey, all five businesses that indicated to have incurred costs in relation to Article 13 agreed that these costs included opportunity costs. This was also raised by several respondents to the public consultation as well as in interviews carried out by Deloitte. It was explained that unsolicited communication is in some ways the backbone of the entire industry in terms of marketing and sales. The necessity of prior consent by users in order to be contacted reduces potential business opportunities in marketing and sales.

The overall quantitative results of the economic analysis in relation to the REFIT exercise are provided below.

Annex A: Economic Analysis

Further information in this regard, as well as an explanation of the approach used for the estimation of the quantitative results data is provided in the section on the basic assumptions used for the problem assessment and the establishment of the baseline scenario in Annex A concerning the Economic Analysis.

Current (and past) costs: Average annual values and changes compared to the current situation

The quantitative results of the economic analysis for the REFIT exercise are presented in Table 73:

- Number of businesses affected (in million);
- Compliance costs (in million Euro);
- Average compliance cost per business (in Euro);
- Administrative burden (in million Euro); and
- Average costs from administrative burden per business (in Euro).

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

The following table presents the quantitative findings for the current (and past situation). The table contains three columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Average annual value (2002-2015):* Denotes the average annual value of the quantitative indicator for which data has been estimated. This means, for instance, that 260,000 SMEs are affected by issues relating to the ePD per year (see the light blue cell), facing a total amount of 169.8 EUR million per year (see the light green cell) at an average cost of compliance per business of 658.4 Euro (see the dark blue cell);
- *Average annual value today (2016):* Denotes the average annual value of the quantitative indicator for which data has been estimated in 2016.

A visualisation of the year-over-year development of the quantitative indicators is presented afterwards, as well as the overall values of the quantitative indicators for the timeframe 2002-2016

Table 69 – Key quantitative data estimated in relation to the REFIT exercise (2002-2016)

Quantitative indicator	Average annual value (2002-2015)	Annual value today (2016)
Number of businesses affected (in million)	2.84	3.11
Micro-enterprises	2.53	2.78
SMEs	0.26	0.25
Large enterprises	0.01	0.01
Foreign controlled enterprises	0.05	0.06
Compliance costs (in million Euro)	1,861.7 €	1,505.7 €
Micro-enterprises	1,655.8 €	1,349.0 €
SMEs	169.8 €	122.2 €
Large enterprises	5.6 €	4.2 €
Foreign controlled enterprises	30.5 €	30.3 €
Average compliance cost per business (in Euro)	658.4 €	484.5 €
Administrative burden (in million Euro)	0.28 €	0.23 €
Micro-enterprises	0.23 €	0.19 €
SMEs	0.03 €	0.03 €
Large enterprises	0.00 €	0.00 €
Foreign controlled enterprises	0.02 €	0.01 €
Average costs from admin. burden per business (in Euro)	48.9 €	36.0 €

Source: Deloitte

The analysis shows that – per year between 2002 and 2015 – around 2.8 million businesses were affected by the ePD in the EU. The majority of these businesses were micro-enterprises with less than 10 employees (2.5 million). Around 260,000 SMEs that have between 10 and 250 employees are estimated to have been affected per year while the number of large enterprises was negligible with around 10,000 per year. Approx. 50,000 foreign controlled enterprises that operated in the EU were affected per year.[471]

[471] The estimated numbers of affected businesses should be understood as annual values. However, the overall number of businesses affected by the ePD between 2002 and 2016 is not the sum of each annual value. The reason for this is that the majority of businesses was affected not only once but on several occasions across this time frame while some businesses were replaced by others due to the general life cycle of businesses (company birth, insolvency). This means that, in relation to the

The businesses affected by the ePD are estimated to have incurred an annual value of 1.9 EURb to comply with Art. 5(3) and Art. 13. In addition, these businesses are expected to have incurred an unspecifiable amount of additional costs e.g. with regard to the consumer provisions. Again, micro-enterprises are expected to incur the lion share of these costs (around 1.7 EURb).

On *average*, an EU business is expected to have incurred 658 Euro per year with regard to the ePD between 2002 and 2015. This does, however, not mean that e.g. large enterprises may not have incurred significantly more costs while the costs may be significantly lower for micro-enterprises. In fact, the anecdotal evidence concerning businesses' costs presented in the text boxes in relation to each provision in chapter 5 shows otherwise. This does, however, not necessarily contradict the above but rather exemplifies the difficulties estimating such costs, as well as it should be seen as a caveat in relation to the nature of the figures as *best estimates* based on the *best data available*.

In relation to administrative burden, mostly stemming from the notification obligations for telecommunication service providers under Article 4, it has been estimated that an annual amount of 230,000 Euro was incurred, i.e. around 49 Euro per affected business per year.

Current (and past) costs: Visualisation of the development 2002-2016

In this section, we present visualisations of the development the following quantitative indicators between 2002 and 2016:

- The number of businesses affected;
- The compliance costs; and
- The costs from administrative burden.

We have decided to use such a form of visualisation instead of providing the data by means of tables in order to make the sheer amount of data more accessible to the reader and to clearly be able to show the *development of the quantitative indicators over time* – which is not always easy to spot when looking at raw figures.

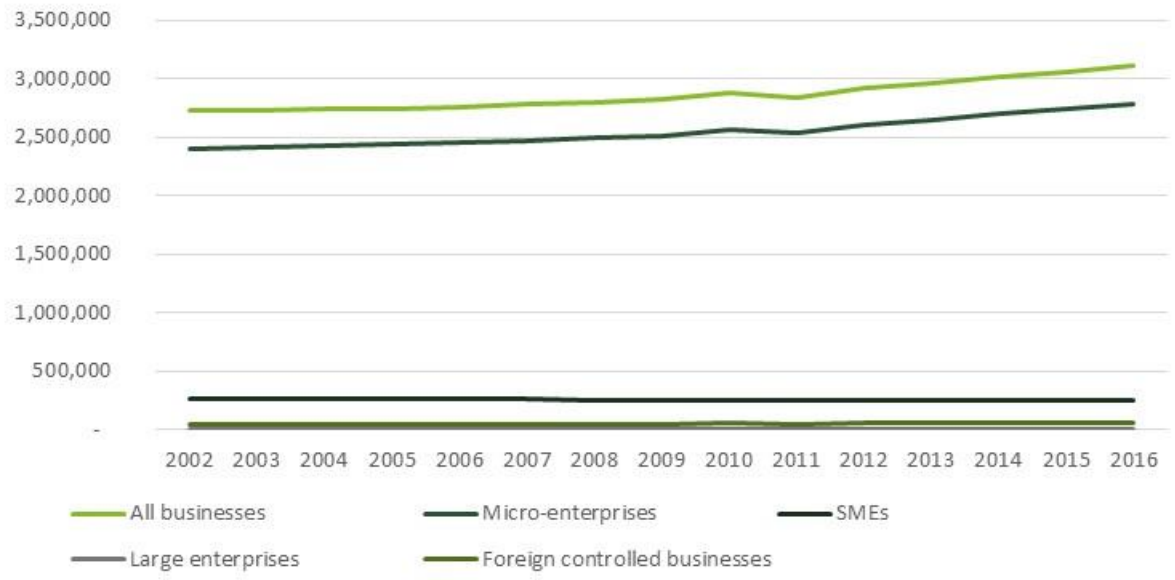
The graphs visualise the data per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Number of businesses affected

The following two graphs present the development of the number of businesses affected by the ePD. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

former argument, the projected value is likely underestimating the actual number of businesses affected, while the latter argument, the projection is likely to overestimate the number of affected businesses.

Figure 42 – Number of businesses affected by the ePD per year (2002-2016)



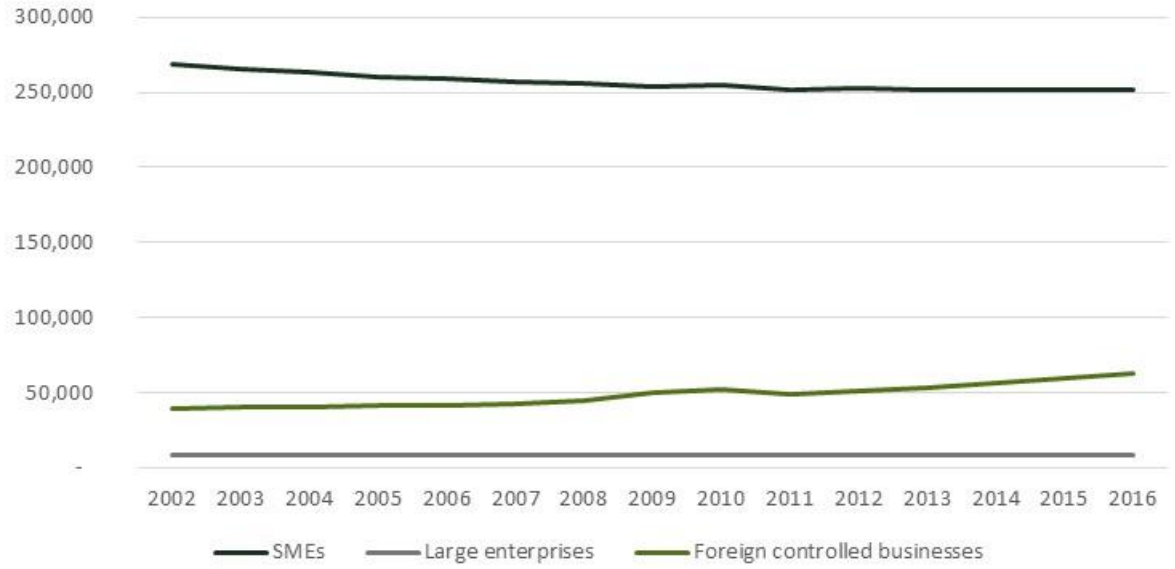
Source: Deloitte

Between 2002 and 2016, as can be seen from the graph above, the overall number of businesses affected by the ePD has increased, mostly due to growth of the micro-enterprise sector. SMEs, large enterprises, and foreign controlled enterprises were less important for the overall growth of the number of businesses affected by the ePD.

In fact, when examining the development of the number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD more closely, the following can be observed:

- The number of SMEs affected by the ePD has declined between 2002 and 2016;
- The number of large enterprises affected by the ePD has remained stable; and
- The number of foreign controlled enterprises affected by the ePD has slightly increased.

Figure 43 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (2002-2016)

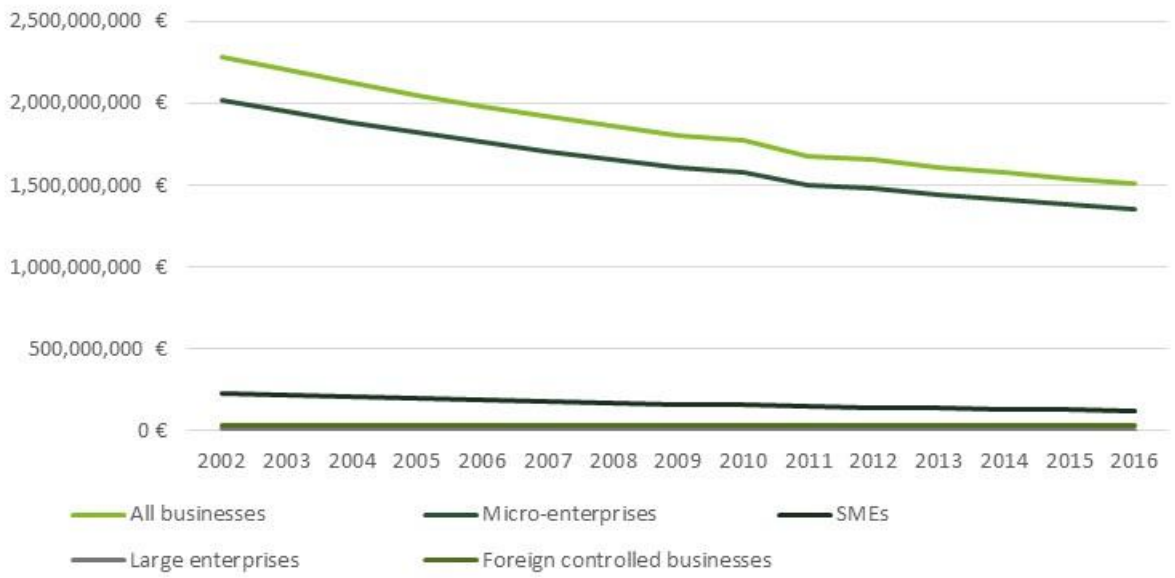


Source: Deloitte

Annual compliance costs

The following two graphs present the development of the annual compliance costs of businesses affected by the ePD. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

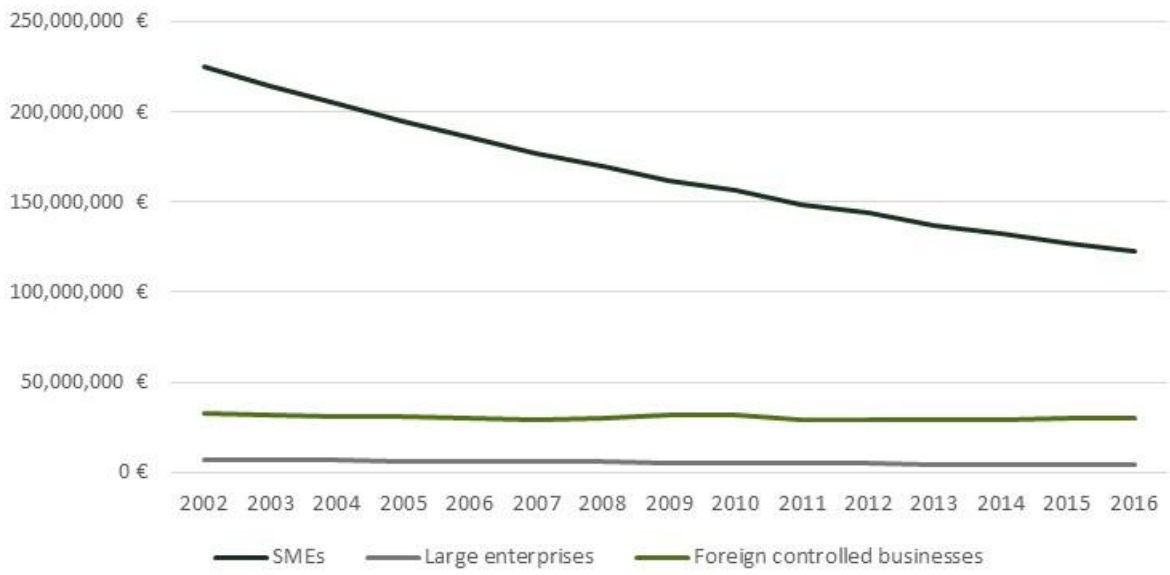
Figure 44 – Compliance costs of businesses affected by the ePD per year (2002-2016)



Source: Deloitte

The graph above shows the annual overall compliance costs for businesses have decreased from 2002 to 2016. Looking in more detail at annual overall compliance costs for SMEs, large enterprises, and foreign controlled enterprises (see figure below), it can be seen that – while compliance costs for SMEs have decreased – the have remained relatively stable for large and foreign controlled enterprises.

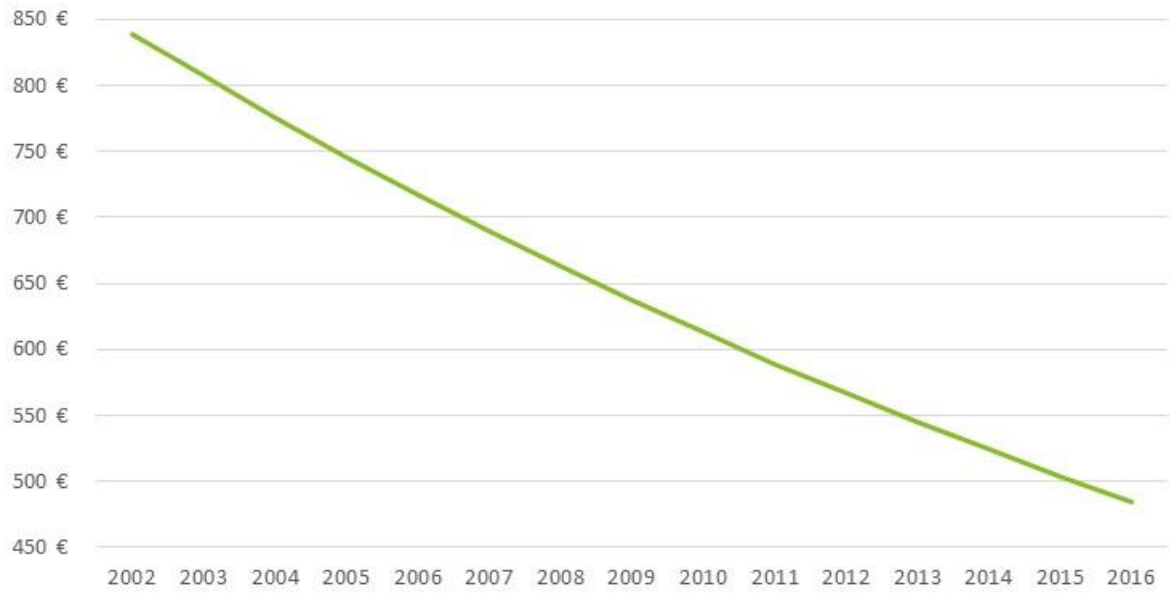
Figure 45 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (2002-2016)



Source: Deloitte

The following graph visualises the development of the average compliance costs for businesses from 2002 to 2016. No difference has been made between average costs for different size classes of businesses.

Figure 46 – Average compliance costs of per business affected by the ePD per year (2002-2016)



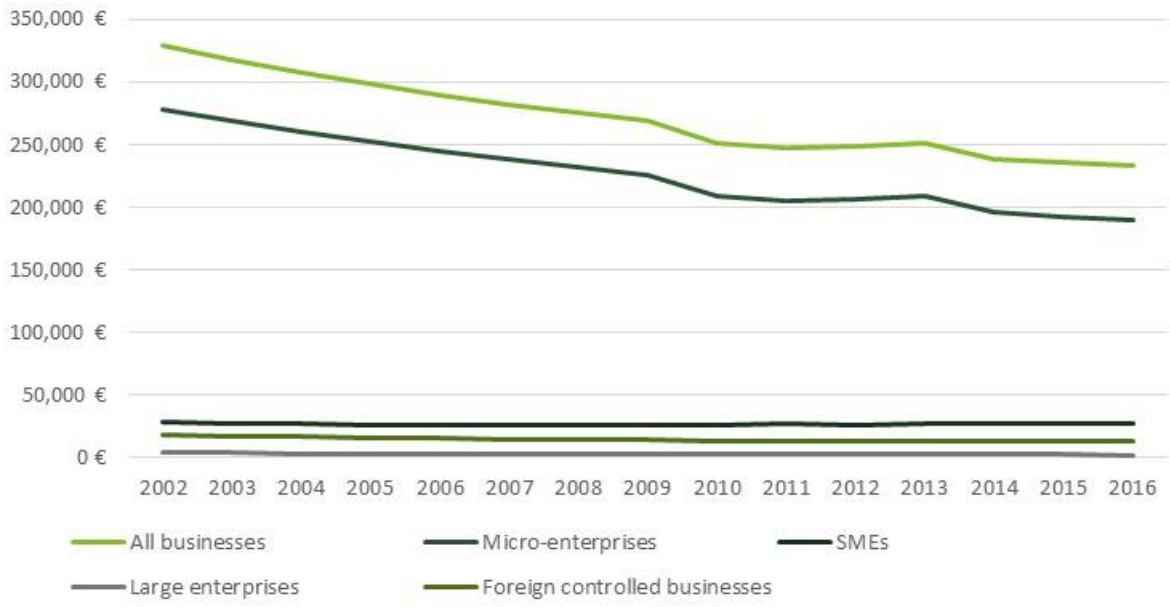
Source: Deloitte

The graph clearly shows that the average compliance costs for businesses have decreased drastically between 2002 and 2016.

Annual costs from administrative burden

The following two graphs present the development of the annual costs from administrative of businesses affected by the ePD. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

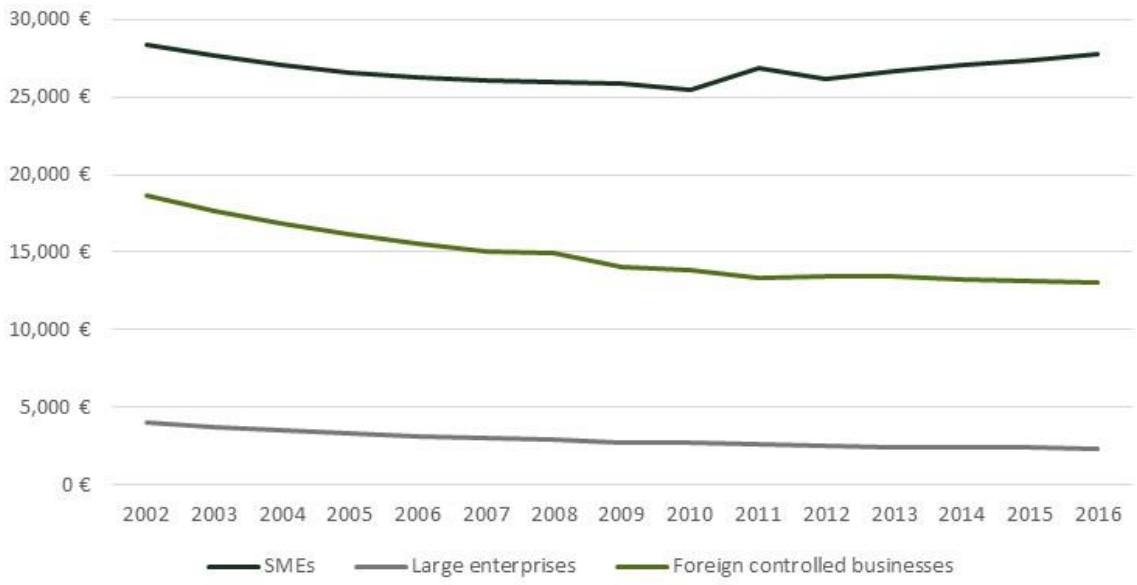
Figure 47 – Costs from administrative burden of businesses affected by the ePD per year (2002-2016)



Source: Deloitte

Similarly to the compliance costs, costs from overall annual costs from administrative burden have also decreased between 2002 and 2016 – despite some fluctuation between 2009 and 2013.

Figure 48 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (2002-2016)

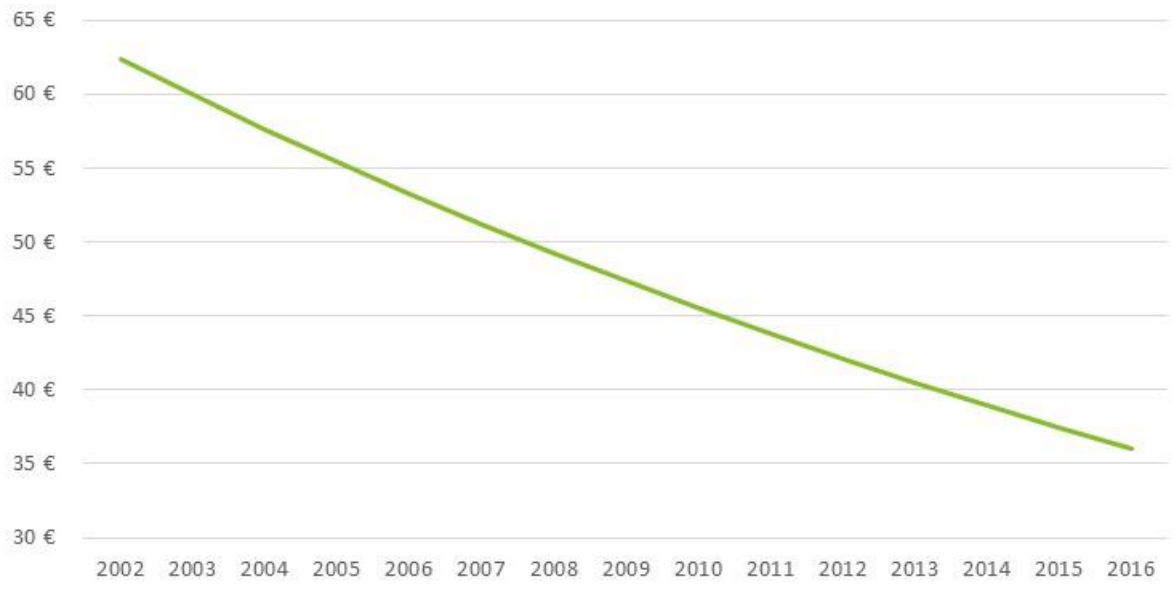


Source: Deloitte

As regards the costs from administrative burden for SMEs, large enterprises, and foreign controlled enterprises, there has been a decreasing trend since 2002. For SMEs, however, costs from administrative burden have slightly increased again in recent years.

The following graph visualises the development of the average costs from administrative burden for businesses from 2002 to 2016. No difference has been made between average costs for different size classes of businesses.

Figure 49 – Average costs from administrative burden per business affected by the ePD per year (2002-2016)



Source: Deloitte

Overall, the above graph shows that there has been a clear reduction of costs from administrative burden for across all types of businesses affected by the ePD from 2002 to today.

Current (and past) costs: Overall values 2002-2016

While the above section has presented average annual values, this section provides the key quantitative estimates for the overall time period of 2002-2016 (i.e. the sums of each individual annual value of the time period). This estimate is relevant to assess the overall costs of compliance and administrative burden stemming from the ePD for different types of businesses.

The following table contains information on:

- Compliance costs (in million Euro); and
- Administrative burden (in million Euro).

The number of businesses affected is not presented as this number is – over the entire time period – subject to double counting.[472] Compared to the above section, average compliance cost per business, as well as average costs from administrative burden per business are not relevant to present in this section as they are *average* values and not *overall* values.

The table contains two columns:

[472] This is due to the fact that businesses are affected by the ePD over longer time frames than just one year. An alternative way of phrasing this is that the ePD does not affect an entirely different set of businesses each and every year.

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business; and
- *Overall value (2002-2016):* Denotes the overall annual value of the quantitative indicator for which data has been estimated. This means, for instance, that all SMEs in the EU together have incurred compliance costs of 2,499.4 EURm over the entire time period of 2002-2016 (see the light green cell).

Table 70 – Key quantitative data estimated in relation to the REFIT exercise (2002-2016)

Quantitative indicator	Overall value (2002-2016)
Compliance costs (in million Euro)	27,569.8 €
Micro-enterprises	24,530.4 €
SMEs	2,499.4 €
Large enterprises	83.1 €
Foreign controlled enterprises	457.0 €
Administrative burden (in million Euro)	4.1 €
Micro-enterprises	3.4 €
SMEs	0.4 €
Large enterprises	0.0 €
Foreign controlled enterprises	0.2 €

Source: Deloitte

The table above shows that businesses have incurred around 28 EURb of compliance costs related to the ePD over the entire time frame of 2002 to 2016. The vast majority of costs was incurred by micro-enterprises. Although this overall amount may look dramatic at first glance, it should be kept in mind that this cost is incurred by businesses from all types of industries across the entire EU. Thus, the share of compliance costs of the overall EU GDP between 2002 and 2016 is marginal. According to Eurostat, the overall EU28 GDP between 2002 and 2015 was 175,948,834.7 EURm. Thus, the share of 27,569.8 EURm of compliance costs is only 0.016% of the entire EU economy.

Compared to compliance costs, costs from administrative burden were insignificant between 2002 and 2016. Overall, 4.1 EURm have been incurred between 2002 and 20016, again mostly by micro-enterprises.

7.4 Assessment of the Effects

The problems for citizens and businesses identified in the previous sub-section may have wider effects. The following potential effects have been identified (cf. our problem tree in Figure 39):

- The respect for fundamental rights, notably the respect for private and family life and the protection of personal data, within the EU is not fully safeguarded;
- There is no level playing field between providers of functionally equivalent services; and
- The smooth functioning of the (digital) single market is hindered.

We discuss these three points in the following sub-sections.

7.4.1 The respect for fundamental rights, notably the respect for private and family life and the protection of personal data, within the EU is not fully safeguarded

The EU aims to safeguard fundamental rights in line with the EU Charter of Fundamental Rights and recognises the rights contained in the European Convention for the Protection of Human Rights and Fundamental Freedoms as general principles of EU law (cf. Article 6 TEU). In addition, it aims to set up an "area of freedom, security and justice with respect for fundamental rights and the different legal systems and traditions of the Member States" (Article 67 TFEU). In this context, the rights to privacy and the protection of personal data as enshrined in article 7 and 8 of the Charter are of particular relevance.

As noted in the previous sub-sections, the evaluation has found certain difficulties in relation to the functioning of the ePD, which impact on the rights privacy and the protection of personal data. In particular, it has been found that the protection of privacy and the confidentiality of communications is hindered by the scope of the ePD (non-coverage of OTTs) shortcomings in relation to Article 4, 5, 6 and 9. Details are presented in section 7.3.1.

These difficulties in relation to the achievement of privacy and confidentiality may impact on the level of respect for fundamental rights in the EU, as they are directly connected to the rights of privacy and the protection of personal data.

7.4.2 There is no level playing field between providers of functionally equivalent services

As explained in section 7.2.1, OTTs are not explicitly covered by the scope of the ePD. Since OTT service providers are not themselves responsible for the conveyance of signals over an electronic communications network, they do not fall under the ePD and its obligations. On this basis, OTTs are subject to more general regulatory frameworks, including the European data and consumer protection framework, which do not include specific obligations relating to communication services.

The difference in treatment leads to an **uneven playing field,** as businesses providing similar services are covered by different legal regimes.[473] On this basis, the fact that OTTs are not covered by the ePD were in particular considered to be problematic by Telecom providers interviewed by Deloitte. It was argued that the legal treatment is currently not symmetrical vis-à-vis similar services. Most other types of businesses took a slightly different perspective. For example, an OTT provider argued that there are important differences between traditional Telecoms and OTT provider that justify a different treatment: they highlighted in this context that users are dependent on the services of traditional Telecom providers, whereas they can freely choose which OTT providers they want to use or not.

[473] European Commission (2016). *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*, SMART 2016/0080, Terms of Reference, p. 4; Van Hoboken, J. and Zuiderveen Borgesius, F. (2015). Scoping Electronic Communication Privacy Rules: Data, Services and Values. *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 2; Communication COM(2015) 192 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, p. 9 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

In general, OTT services have broader opportunities to use user data, e.g. on traffic and location, apart from simply enabling communications.[474] Due to the obligations under Art. 6, 9 and 13 of the ePD, ECS are prevented from using certain assets to develop new business models in order to compete with OTTs and generate new revenue streams: This is most obvious in the case of the (personalised) **advertisement revenue model**[475]**,** which can be seen as a central OTT business model. ECS cannot engage in storing, analysing and selling or sharing user data on traffic and location with third party advertisers to deliver ads.[476] With regard to unsolicited communications for the purpose of direct marketing, ECS need to obtain prior consent from users and are only allowed to use this consent for offering similar services.[477] Unsolicited communications sent via OTT platforms like social networks are so far not assumed to be affected or restricted by Art. 13 of the ePD.[478]

This is reflected in the business models employed by ECS and OTTs, which vary considerably. ECS providers mostly follow direct payment revenue models for their services, demanding subscription fees and pre- or post-payment of services. OTTs are able to pursue a more diverse array of revenue models, for example offer their services through selling/placing (personalised) advertisement, demand one-time or recurring software licenses, or selling devices through which users can access the full service or a dedicated store with apps.[479] These models tend to rely more on use of customer data than direct reimbursement.

Several ECS providers have attempted to launch OTT services, for example social network apps like Libon (Orange) or Tuenti (Telefonica).[480] While they offer services similar to OTT competitors (WhatsApp, Skype, etc.) they apparently fail to attract users, possibly due to their late start, but also potentially because they initially only offered package deals (direct payment) rather than freemium models (e.g. ad financed services).[481] Thus, although ECS and OTTs offer increasingly functionally equivalent services, the sector-specific restrictions create boundary problems in the development of new products by ECS and prevent competition between ECS and OTT providers on equal terms.[482]

A detailed description of the telecommunications and OTT markets in the EU is presented in section 3.5.

7.4.3 The smooth functioning of the (digital) single market is hindered

It is one of the EU's goals to establish an internal market comprising "an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured" (Article 3.3 TEU, Article 26.2 TFEU).

[474] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p.129.
[475] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. ch. 5.4.2.
[476] Mentioned in stakeholder interviews with EU ECS providers, also: Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p.128,
[477] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p.129.
[478] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p.128, 130.
[479] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p. 102.
[480] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. p. 99.
[481] Ecorys (2016): Study on future trends and business models in communication services. FINAL REPORT. A study prepared for the European Commission DG Communications Networks, Content & Technology. ch. 5.4.1.
[482] DLA Piper 2016: ETNO. Study on the revision of the ePrivacy Directive, p. 16.

Some of the difficulties identified as part of the evaluation of the ePD may act as obstacles to the functioning of the internal market. The main cause for these obstacles lies in the fragmented application of the ePD. The transposition check carried out as part of this project as well as the ePrivacy Study 2013/0071[483] showed that the transposition of the ePD varies considerably across Member States. In some cases this may be due to leeway left by the ePD (e.g. Article 13.3), ambiguities in the text of the ePD or differences in the legal frameworks and market realities of the Member States. Details in relation to the transposition of the ePD are presented in chapter 4 and section 7.2.3.

On this basis, **businesses may face obstacles when engaging in cross-border activities**, as they still face varying legal frameworks in the Member States. On this basis, they may incur additional costs for legal advice as they need to understand the rules in different Member States. In addition, they may incur additional costs for implementing the rules, as they will need to follow different legal regimes. For example, they may need to apply different marketing strategies if they are active in a Member State that uses an opt-in regime for unsolicited communications and one that uses an opt-out regime. Horizontally across all types of stakeholders, the fragmented implementation of the ePD in the different Member States and the resulting complexity was pointed out an issue and an important source of cost. See also section 7.3.3.

7.5 The likely development of the problems without policy action (baseline scenario)

Without policy action, the identified problems are likely to remain in place.

From the **citizens' perspective**, the problems relating to the respect for privacy and confidentiality as well as unsolicited marketing communications are relevant. These are based on shortcomings relating to the legal framework (including ambiguities and inappropriate rules), which would not be addressed in case no policy action is taken. As concerns the **confidentiality for users of OTTs**, we note that some OTT providers have already put in place rules to strengthen confidentiality of communications. For example, many ask for the consent of their users to process certain information, strengthened the rules on security e.g. by introducing end-to-end encryption for communications (e.g. *WhatsApp*) or increased the transparency (e.g. *Wire*[484]) and control of users (e.g. *Threema*[485]). It may, therefore, be expected that some improvement may be introduced based on market forces. However, if such regulation is largely left to the voluntary initiative of the industry, citizens will not face equal transparent standards. The situation in relation to **tracking** may even deteriorate, as technologies improve. The situation in relation to **unsolicited communications** is not expected to change significantly.

Turning to the **business perspective**, problems (in particular undue costs) arise in particular based the fact that some of the provisions are not clear or outdated and because the implementation of the rules is fragmented. The **shortcomings in relation to the individual provisions of the ePD** would

[483] European Commission, ePD Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, 2015, (https://ec.europa.eu/digital-single-market/news/ePD-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data).

[484] The privacy focused messenger *Wire* places strong emphasis on informing users on their website with regard to how their services function and how data is processed. In addition to disclosing their approach in white papers on privacy and security, the company publishes transparency reports on a regular basis. See: https://wire.com/privacy/

[485] *Threema* enables users to sign up without providing a phone number and matching their phone books with servers to add contacts (this may be changed later if the customer chooses to do so). Furthermore, *Threema* enables users to add additional features like voice-messages as plug-in extensions, further increasing the user control over the services used. See: https://threema.ch/de/

not be addressed in case of no policy action and would thus not change significantly. The situation in relation to outdated provisions may even deteriorate in light of new technological developments. The **fragmentation of implementation** would not be addressed either. While it may be possible that Member States would cooperate on their own initiative, this would probably not lead to a fully harmonised situation.

A more detailed assessment of the baseline scenario is presented as part of the assessment of the options in section 9.2.

8 Policy Objectives and Policy Options

In this section we present the policy objectives and policy options (as prepared by the European Commission until 10 September 2016).

8.1 Policy objectives

The policy objectives set out the political priorities and aims for action in the relevant field.[486] The definition of policy objectives is an essential step of each Impact Assessment as they, in accordance with the *Better Regulation Guidelines*, support:

- The creation of a logical link between the identified problems and the solutions considered;
- The clarification of the relationship between the specific goals of the initiative considered and the horizontal EU objectives and/or any other relevant agreed political goals;
- The explanation of any trade-off between different policy objectives;
- The definition of the criteria for comparing the different policy options and the indicators to measure performance and progress towards the objectives; and
- The establishment of the criteria to be considered as part of the proposed monitoring and evaluation framework for the implemented policy measure.

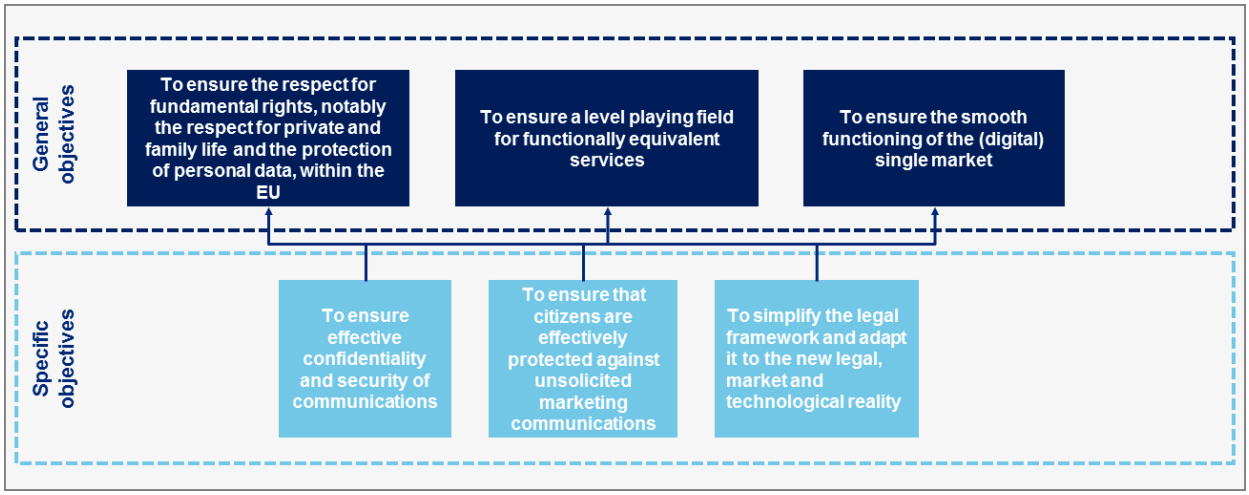
Policy objectives are normally identified at the following levels:

- **General objectives** refer to Treaty-based goals and constitute a link with the existing policy-setting.
- **Specific objectives** relate to the specific domain and set out what the Commission wants to achieve with the intervention in detail.
- **Operational objectives** concern deliverables or objectives of actions. Operational objectives tend to “pre-empt” the solution. Therefore, it is generally not suitable to define the operational objectives directly after the analysis of the problems, but rather after identifying the preferred option. The operational objectives are thus not identified.

The following figure presents our understanding of the general and specific objectives.

[486] European Commission, Better Regulation Guidelines, 19 May 2015, SWD(2015) 111 final, pp. 21-22 (http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm); European Commission, Better Regulation "Toolbox", complementing the Better Regulation Guidelines presented in in SWD(2015) 111, pp. 80-81 (http://ec.europa.eu/smart-regulation/guidelines/docs/br_toolbox_en.pdf).

Figure 50 – Objectives tree



Source: Deloitte

8.2 Policy options

In line with the Terms of Reference, the policy options have been developed by the Commission.

In this chapter, we present the five Policy Options received from the Commission on 10 September 2016:

- *Policy Option 1:* Non-legislative ("soft law") measures;
- *Policy Option 2:* Limited reinforcement of privacy/confidentiality and simplification;
- *Policy Option 3:* Measured reinforcement of privacy/confidentiality and simplification;
- *Policy Option 4:* Far reaching reinforcement of privacy/confidentiality and simplification; and
- *Policy Option 5:* Repeal of the ePD.

Table 71 presents the Policy Options as suggested by the European Commission.

Table 71 –Policy Options suggested by the European Commission

Name of Policy Option	Description of Policy Option	Elements of the Policy Option
Policy Option 1		
Non-legislative ("soft law") measures	Under this option, the Commission would make extensive use of its implementing powers and use soft policy instruments in order to improve the protection of the users. The specific contents of the individual measures cannot be delineated with precision at this stage, as they will emerge as a result of the overall process within the Commission and with the stakeholders.	Objective 1: *Ensuring effective confidentiality and security of communications* 1. **Increased use of interpretative communications.** The Commission would provide more detailed guidance on the interpretation of certain aspects of the ePD which are unclear or open to different interpretations. 2. **Support EU-wide self-regulatory initiatives** building on the existing *ePrivacy acquis* ("co-regulation").[487] 3. **Specify privacy by design requirements of terminal electronic equipment through EU standards**.[488] 4. **Research and awareness-raising activities**. The Commission would significantly increase the funds related to R&D projects in the field of online privacy and security by 25%. In addition, it would engage in awareness-raising activities.[489] Objective 2: *Ensuring effective protection against unsolicited commercial communications* 5. **Interpretative communications**, clarifying the interpretation of unclear or ambiguous concepts.[490] 6. **Awareness-raising initiatives** instructing citizens on how to defend themselves, how to seek redress from national supervisory authorities *Objective 3: Simplifying the legal framework and adapting it to the new legal, market and technological reality* 7. Issue **interpretative communications** to promote an application of the current rules, which is business friendly, while preserving the essence of the protection of confidentiality of communications.[491] 8. Work closely with **industry** in order to encourage the adoption of **common best practices**.[492] 9. **Support MS cooperation** to improve enforcement in cross-border cases as well as harmonised interpretation by organising meetings and workshops with authorities
Policy Option 2		
Limited reinforcement of privacy rights and	Under this option the Commission would propose minimum changes to the current	Objective 1: *Ensuring effective confidentiality and security of communications* 1. Extension of the scope of the ePD to OTTs providing communications functions, such as webmail, Internet messaging, VoIP.

[487] The Commission would lead and coordinate industry efforts to promote standards and codes of conduct in crucial areas such standard information notices related to the use of location data by ECS providers, online tracking, standardised icons and labels, an EU-wide OBA code of conduct and/or an EU DNT standard.
[488] Article 14(3).
[489] Such as setting-up an ad-hoc website and an Internet based advertising campaign, ad-hoc conferences, events (e.g., online communications day) and training for national officials
[490] For example, the issues around the scope of the provision, silent or abandoned calls, the implementation of Robinson lists.
[491] This would cover issues such as the scope of the ePD (e.g., publicly available WiFi networks, IoT devices); modalities to provide consent for tracking, the exceptions to the consent rules under the ePD.
[492] Concerning, for instance, the provision of information and consent mechanisms, thus facilitating a uniform and clear implementation of the current rules.

Name of Policy Option	Description of Policy Option	Elements of the Policy Option
simplification	Directive with a view to adjust privacy and confidentiality provisions and to improve harmonisation and simplification of the current rules.	2. Clarify that the ePD applies to publicly available communications networks, such as in particular commercial Wi-Fi networks in stores, hospitals, airports, etc. Only services which occur in an official or employment situation solely for work-related or official purposes, as well as use of services for exclusively domestic purposes, may be exempted. 3. On the protection of terminal equipment devices: Specify that the protection applies to any machine that is connected to the network (including M2M communications, such as for example, a refrigerator connected to a grocery store web site). Objective 2: *Ensuring effective protection against unsolicited commercial communications* 4. Clarify the scope of the provision and make it technologically neutral: clarify that it applies to any form of unsolicited electronic communication, irrespective of the technological means used. The provision would apply, for example, also to advertisings messages sent on OTT platforms. 5. Mandate the use of a special prefix distinguishing direct marketing calls from other calls. Objective 3: *Simplifying the legal framework and adapting it to the new legal, market and technological reality* 6. Reinforce cooperation obligations among the competent authorities, including for cross-border enforcement. 7. Repeal of the security rules leaving the matter to be regulated by the corresponding rules in the Telecom Framework and the GDPR.
Policy Option 3		
Measured reinforcement of privacy/confidentiality and simplification	Under this option, the Commission would propose **a new ePrivacy instrument,** complementing and particularising the GDPR.	Objective 1: *Ensuring effective confidentiality and security of communications* 1. The new instrument would propose a technology neutral definition of electronic communications, encompassing all the additional elements under **Option 2** (1, 2 and 3). It would specify a general principle of confidentiality of communications (i.e. nobody can process data relating electronic communications), except with the consent of the parties to a communication. 2. Clarify that **consent can be given by means of the appropriate settings** of a browser or other application. Consent under this option will be in line with the concept of consent under the GDPR[493]. Require browsers and/or other similar platforms to provide their products and services with **privacy friendly settings to reinforce user's control** over the flow of data from and into their terminal equipment. This may also entail addressing the interactions between web sites, advertisers and users regarding whether they accept to be tracked, for example there may be a situation where a user may have set a default privacy setting rejecting third party cookies and thus disallowing the tracking but the user is ready to accept third party cookies/tracking from a particular tracking. This option does not provide for a **prohibition of the practice of denying access to a website** or an **online service** in case users do not provide

[493] See Recital 32 of the GDPR: "*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website,* ***choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data****. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided*."

Name of Policy Option	Description of Policy Option	Elements of the Policy Option
		consent to third party cookies/tracking. Under the new instrument, the Commission would be empowered to issue delegated acts or to mandate industry standards under EU rules (e.g. Radio Equipment Directive) to impose these requirements.[494] 3. Impose enhanced transparency requirements on entities processing communications data (e.g., websites, mobile apps and Wi-Fi), by obliging them to display a concise privacy warning message (e.g. informing users accessing free online services that "the service is financed by OBA and the users' browsing data will be used for this purpose"). The Commission would have implementing powers to specify the exact form and content of the message to be displayed. 4. Reinforce and streamline enforcement powers: The new instrument would lay down effective investigation end enforcement powers of national competent authorities. This would address the problems of ineffective and inconsistent enforcement. Objective 2: *Ensuring effective protection against unsolicited commercial communications* 5. All the measures from 4 to 5 under **Option 2**. 6. Require **opt-in consent for all types of unsolicited communications covered by the current rules**, including advertising messages sent to unique users in social media and voice-to-voice marketing calls, while keeping the existing business relationships exception for email.[495] 7. Clarify the provision on **presentation of calling line identification** to include the right of users to reject calls from specific numbers (or categories of numbers). Objective 3: *Simplifying the legal framework and adapting it to the new legal, market and technological reality* 8. Propose changes aimed at **clarifying and minimising the margin of manoeuvre of certain provisions** identified by stakeholders as a source of confusion and legal uncertainty.[496] 9. Consider introducing consistency mechanisms for the ePrivacy rules. 10. Repeal provisions on security, automatic call forwarding and the provisions on itemised billing. 11. Repeal the provisions on traffic data and location data to reflect the fact that the traffic and location data are more and more a homogeneous category, both in terms of privacy intrusiveness and technological availability. The processing of traffic and location data will be regulated under the general provision of confidentiality of communications. 12. Specify that service providers can only process communications data with the consent of the users, although they are allowed to refuse access to the services in the absence of consent. Providing for additional/broadened exceptions to the consent and enhanced transparency rules (points 1, 2 and 3 above) for specific purposes which give rise to little or no privacy risks: a. Transmission or service: the processing of communications data is necessary for the purpose of the transmission of the communication or for providing a service requested by the user. b. Security: the processing of traffic data is necessary to protect, maintain and manage the technical security of

[494] Regulation 1025/2012/EU, OJ L 316, 14.11.2012, p. 12–33.
[495] Article 13(2).
[496] This would cover in particular more detailed rules on the scope of the ePrivacy instrument, the exceptions to the consent requirements and the scope of the unsolicited communications provisions.

Name of Policy Option	Description of Policy Option	Elements of the Policy Option
		a network or service, with appropriate privacy safeguards. c. Billing: in line with the current provision on traffic data, communications data may be retained insofar as necessary for billing or network management purposes. d. For a lawful business practice provided that there are no significant risks for the privacy of individuals. In particular, the data collection is performed solely by the entity concerned or third-parties on behalf of the ECS for the purpose of web analytics and web measurement.
Policy Option 4		
Far reaching reinforcement of privacy/confidentiality and simplification	Under this option, the Commission would propose a new ePrivacy legal instrument with more far reaching measures reinforcing the protection of privacy/confidentiality and guaranteeing greater simplification/harmonisation.	Objective 1: *Ensuring effective confidentiality and security of communications* 1. All the measures under No 1, 2, 3 and 4 of Option 3. 2. Explicitly prohibit the practice of denying access to a website or an online service in case users do not provide consent to tracking (so-called cookie-wall). Objective 2: *Ensuring effective protection against unsolicited commercial communications* 3. All the measures under No 5, 6 and 7 of Option 3. 4. Under this option, the Commission would repeal the provision allowing direct marketers to send communications to subscribers and users when they have received their contact details in the context of a previous business relationship Objective 3: *Simplifying the legal framework and adapting it to the new legal, market and technological reality* 5. Measures under No 8 - 12 of Option 3. 6. Commission's implementing powers for deciding on the correct application of the ePD instrument where there is an issue of consistency or coherence with EU law. 7. Repeal the provisions on calling line identification and directories of subscribers.
Policy Option 5		
Repeal of the ePD	Under this option, the Commission would propose the repeal of the ePD.	Objective 1: *Ensuring effective confidentiality and security of communications* 1. The GDPR provides for reinforced rights of individuals and the obligations of data controllers, which are in keeping with the challenges of the digital age. The consent rule under the GDPR has been in particular substantially strengthened with a view to ensure that it is freely-given. The GDPR addressed the issue of unbalance of economic power between the controller and the processor, requesting that this aspect be taken into account in the assessment of the validity of consent. 2. The GDPR would guarantee more effective enforcement in view of the reinforced powers conferred on data protection authorities Objective 2: *Ensuring effective protection against unsolicited commercial communications* 3. Unsolicited communications would be essentially regulated under a general opt-out regime across 28 MS. Objective 3: *Simplifying the legal framework and adapting it to the new legal, market and technological reality* 4. All providers of electronic communications will be subject to the same rules without discrimination based on the technology used. 5. There would be no duplication of rules in the security area and all the ePD provisions related to specific issues in the

Name of Policy Option	Description of Policy Option	Elements of the Policy Option
		electronic communications sector (e.g. directories of subscribers) would be dealt with on the basis of the general data protection rules.

Source: European Commission

9 Assessment of the Impacts of the Options

This section presents the assessment of the impacts of the options (inc. the baseline scenario).

9.1 Introduction

It was agreed with the Commission that the assessment of the impacts of the options would include the following types of impacts[497]:

- Economic impacts[498];
- Effectiveness in reaching the policy objectives; and
- Social impacts.

We briefly discuss our approach in relation to these three aspects below.

As part of the assessment of the **economic impacts** vis-à-vis the baseline scenario, the compliance costs, as well as the costs from administrative burden for businesses (of different size classes, incl. SMEs and micro-enterprises) are assessed, as well as the costs for public administrations. More specifically, the respective sections contain the following:

- Detailed qualitative assessment tables regarding the impact of each element of the policy options on compliance costs and administrative burden for businesses and public administrations;
- A table providing the key quantitative findings from the economic analysis, relating to the impacts on compliance costs and administrative burden for businesses; and
- A section on other economic impacts, e.g. on competiveness and opportunity costs.

The qualitative assessment tables on impacts on businesses contain the qualitative reasoning used for the quantitative assessments of the impacts of the policy options on compliance costs and costs related to administrative burden. In addition, they contain:

- An indication of the types of businesses affected by each element;
- Qualitative rating / colour coding of the expected impacts of each element of the options;
- An indication whether or not businesses would incur compliance costs or costs related to administrative burden from each specific element; and
- The frequency of costs (as far as information is available).

The qualitative assessment tables on impacts on public administrations contain the qualitative assessment of the types of costs that would be incurred by EU and national public administrations. We

[497] This means that the European Commission has confirmed that legal impacts of the policy options (incl. on the coherence, as well as on Fundamental Rights) are excluded from the scope of the assessment. This is also valid for the assessment of the proportionality of the policy options.

[498] The assessment of the impacts is focused on the assessment of the economic impacts as this was prioritised by the European Commission. This priority was not only set out in the Terms of Reference but also confirmed throughout the entire project (lastly during a meeting on 22 September 2016).

also a qualitative rating / colour coding of the expected impacts of each element of the options on public administrations. However, no calculations on the magnitude of the costs have been carried out.

The quantitative tables contain the number of businesses affected (in million), the compliance costs (in million Euro), the average compliance cost per business (in Euro), as well as the costs from administrative burden (in million Euro), and the average costs from admin. burden per business (in Euro). Furthermore, the tables contain the absolute and relative changes of the average annual value compared to the baseline scenario.

As concerns the sections on other economic impacts, these contain qualitative descriptions of any economic impacts other than compliance costs, including e.g. impacts on competitiveness or opportunity costs. We have also provided qualitative ratings to allow for a comparison of the different policy options. However, we have not provided calculations for these types of costs, as such calculations would not have been robust based on the limited information available on the magnitude of such costs.

For further information on the approach and methodology used for the quantitative assessment of economic impacts, please see Annex A.

The assessment of the **effectiveness** is related to the contributions of the policy options to effectively achieve the policy objectives (see section 8.1). This assessment focuses on the specific policy objectives:[499]

- To ensure effective confidentiality and security of communications;
- To ensure that citizens are effectively protected against unsolicited marketing communications; and
- To simplify the legal framework and adapt it to the new legal, market and technological reality.

The assessment of the effectiveness is mainly qualitative and includes a qualitative rating of the different policy options vis-à-vis the baseline scenario.

In line with the Better Regulation Guidelines, the assessment of the **societal impacts** is focused on impacts on employment and labour markets. Issues such as effects on income, its distribution and social inclusion have been excluded from the analysis.

For all three aspects, a **qualitative rating** is used, supporting the comparability of the options. The rating scale used ranges from -3 (significantly positive contribution) to +3 (significantly negative contribution) and compares the situation envisaged under the policy options to the status quo:

Significantly positive contribution (-3)	Medium positive contribution (-2)	Slight positive contribution (-1)	Neutral contribution (0)	Slight negative contribution (+1)	Medium negative impact (+2)	Significantly negative contribution (+3)

The scale is applied either to all individual elements of the options (economic impacts) or to the overall policy options (effectiveness, societal impacts).

This chapter is structured according to the different policy options (starting with the baseline scenario). For each policy option, separate sub-sections have been prepared in relation to each Impact

[499] Specific objectives relate to the specific domain and set out what the Commission wants to achieve with the intervention in detail. General objectives refer to Treaty-based goals and constitute a link with the existing policy-setting.

Assessment criterion. Where relevant, we have used assessment tables that include the qualitative ratings.

The chapter closes with the comparison of policy options, including a summary and overview of the ratings of the impacts of the policy options vis-à-vis the baseline scenario based on which the best performing policy option is highlighted.

9.2 Baseline scenario: No policy change

In the baseline scenario, no changes to the current policy would be introduced.

9.2.1 Overview of assessments

In the following table we present an overview of our assessment of the baseline scenario. The detailed assessment according to the individual assessment criteria can be found in the following sub-sections.

Table 72 – Qualitative rating of the impacts of the baseline scenario

Assessment criteria	Rating	Brief explanation of the rating
Economic impacts		
Impacts on costs for businesses	0	Businesses would continue to face the same compliance costs and costs related to administrative burden.
Impacts on costs for public authorities	0	The competent authorities dealing with the ePD would continue to incur the same types of costs as in the current situation.
Other economic impacts	0	Telecom providers may incur additional losses, as consumers further shift to OTTs which still have a competitive advantage as they face less strict rules. Providers of new technologies, e.g. IoT, may incur additional costs as ambiguities as to the coverage of such technologies will continue to exist.
Effectiveness in reaching the policy objectives		
Objective 1: To ensure effective confidentiality and security of communications	0	The problems identified in relation to the confidentiality of communications are likely to remain in place or even deteriorate, including based on the development of new technologies.
Objective 2: To ensure that citizens are effectively protected against unsolicited marketing communications	0	The situation is not expected to change significantly. Citizens will continue to receive similar numbers of unsolicited marketing calls.
Objective 3: To simplify the legal framework and adapt it to the new legal, market and technological reality	0	The legal framework will remain complex based on the relationship with other legal instruments and the fragmented implementation in the Member States. Based on further technological developments, it may get less adapted to the technological reality.
Social impacts	0	No significant social impacts are expected.
Total	0	

Source: Deloitte

9.2.2 Economic impacts

Within this section on the assessment of the economic impacts, we are focusing on three key aspects: (1) The costs for businesses (incl. SMEs and micro-enterprises), and (2) public authorities; as well as (3) other impacts such as on competiveness and competition in the Digital Single Market.

Impacts on compliance costs and administrative burden for businesses

In this section, we provide the key quantitative findings from the economic analysis in relation to the baseline scenario. No detailed qualitative assessment table has been prepared as this is not necessary for the baseline scenario.

Baseline scenario: Average annual values and changes compared to the current situation

The overall quantitative results of the analysis concerning the baseline scenario are presented in Table 73:

- Number of businesses affected (in million)
- Compliance costs (in million Euro)
- Average compliance cost per business (in Euro)
- Administrative burden (in million Euro)
- Average costs from admin. burden per business (in Euro)

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Annex A: Economic Analysis

Further information in this regard, as well as an explanation of the approach used for the estimation of the quantitative results data is provided in the section on the basic assumptions used for the problem assessment and the establishment of the baseline scenario in Annex A concerning the Economic Analysis.

The following table presents the quantitative findings for the baseline scenario. The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Average annual value:* Denotes the average annual value of the quantitative indicator for which data has been estimated. This means, for instance, that 260,000 SMEs are affected by issues relating to the ePD per year (see the light blue cell), facing a total amount of 97 EURm per year (see the light green cell) at an average cost of compliance per business of 373.5 Euro (see the dark blue cell);
- *Absolute Δ to 2002-2016:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the average annual value compared to the current and past situation (i.e. 2002-2016); and
- *Relative Δ to 2002-2016:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the average annual value compared to the current and past situation (i.e. 2002-2016).

Visualisations of the year-over-year development of the quantitative indicators are presented afterwards, as well as overall values for the timeframe 2016-2030.

Table 73 – Key quantitative data estimated in relation to the baseline scenario (2016-2030)

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to 2002-2016	Relative Δ to 2002-2016
Number of businesses affected (in million)	3.70	0.86	30.2%
Micro-enterprises	3.31	0.78	30.9%
SMEs	0.26	0.00	1.6%
Large enterprises	0.01	-	0.0%
Foreign controlled enterprises	0.12	0.07	157.4%
Compliance costs (in million Euro)	1,355.4 €	-506.3 €	-27.2%
Micro-enterprises	1,213.0 €	-442.8 €	-26.7%
SMEs	97.0 €	-72.8 €	-42.9%
Large enterprises	3.3 €	-2.3 €	-40.9%
Foreign controlled enterprises	42.1 €	11.6 €	38.0%
Average compliance cost per business (in Euro)	373.5 €	-284.9 €	-43.3%
Administrative burden (in million Euro)	0.23 €	-0.04 €	-16.0%
Micro-enterprises	0.18 €	-0.05 €	-21.3%
SMEs	0.03 €	0.01 €	25.9%
Large enterprises	0.00 €	0.00 €	-33.3%
Foreign controlled enterprises	0.01 €	0.00 €	-6.7%
Average costs from admin. burden per business (in Euro)	27.8 €	-21.2 €	-43.3%

Source: Deloitte

The analysis shows that – per year between 2016 and 2030 – around 3.7 million businesses will be affected by the ePD in the EU. The majority of these businesses will be micro-enterprises with less than 10 employees (3.3 million). Around 260,000 SMEs that have between 10 and 250 employees are estimated to be affected per year until 2030 while the number of large enterprises is negligible with around 10,000 per year. Approx. 120,000 foreign controlled enterprises that operate in the EU will be affected.[500]

The businesses affected by the ePD are estimated to incur an annual value of 1.4 EURb to comply with Art. 5(3) and Art. 13. In addition, these businesses are expected to incur an unspecifiable amount of additional costs with regard to other provisions such as the consumer provisions. Again, micro-enterprises are expected to incur the lion share of these costs (around 1.2 EURb).

On *average*, an EU business is expected to incur 374 Euro per year with regard to the ePD until 2030. This does, however, not mean that e.g. large enterprises may not incur significantly more costs while the costs may be significantly lower for micro-enterprises.

[500] The estimated numbers of affected businesses should be understood as annual values. However, the overall number of businesses affected by the ePD between 2016 and 2030 is not the sum of each annual value. The reason for this is that the majority of businesses will be affected not only once but on several occasions across this time frame while some businesses will be replaced by others due to the general life cycle of businesses (company birth, insolvency). This means that, in relation to the former argument, the projected value is likely underestimating the actual number of businesses affected, while the latter argument, the projection is likely to overestimate the number of affected businesses.

In addition to the compliance costs related to the direct implementation of the ePD, businesses will also incur significant opportunity costs for lost business opportunities.

In relation to administrative burden, mostly stemming from the notification obligations for telecommunication service providers under Article 4, it has been estimated that an annual amount of 230,000 Euro is incurred, i.e. around 28 Euro per affected business per year.

Baseline scenario: Visualisation of the development 2016-2030

In this section, we present visualisations of the development the following quantitative indicators between 2016 and 2030:

- The number of businesses affected;
- The compliance costs; and
- The costs from administrative burden.

We have decided to use such a form of visualisation instead of providing the data by means of tables in order to make the sheer amount of data more accessible to the reader and to clearly be able to show the *development of the quantitative indicators over time* – which is not always easy to spot when looking at raw figures.

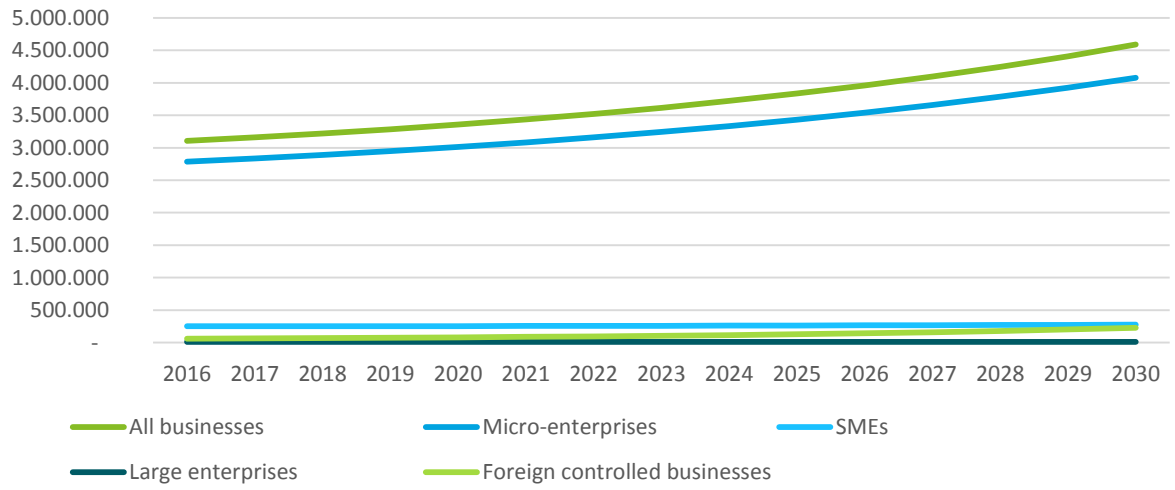
The graphs visualise the data per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Graphical comparisons of the quantitative indicators under each policy option with the baseline scenario are provided in section 9.8.1.

Number of businesses affected in the baseline scenario

The following two graphs present the development of the number of businesses affected by the ePD. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

Figure 51 – Number of businesses affected by the ePD per year (baseline scenario, 2016-2030)



Source: Deloitte

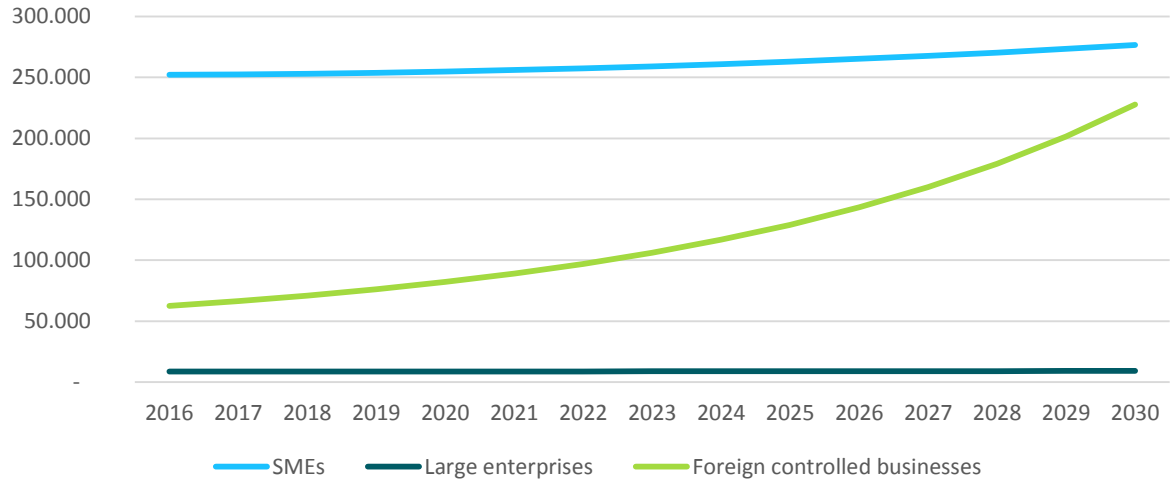
In the baseline scenario, as can be seen from the graph above, the overall number of businesses affected by the ePD is expected to grow from 2016 to 2030 in line with the general economic trend. Most of this growth is expected to stem from the growth of the number of micro-enterprises while

SMEs, large enterprises, and foreign controlled enterprises are of less importance for the overall growth of the number of businesses affected by the ePD.

Looking in more detail at the growth of the number of SMEs, large enterprises, and foreign controlled enterprises, it can be seen that – while the number of SMEs affected is expected to increase slightly and the number of large enterprises is expected to remain stable until 2030 – the number of foreign controlled enterprises affected by the ePD is expected to increase comparatively strong until 2030 vis-à-vis 2016.

This trend is slightly different compared to what was observed between 2002 and 2016.

Figure 52 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (baseline scenario, 2016-2030)

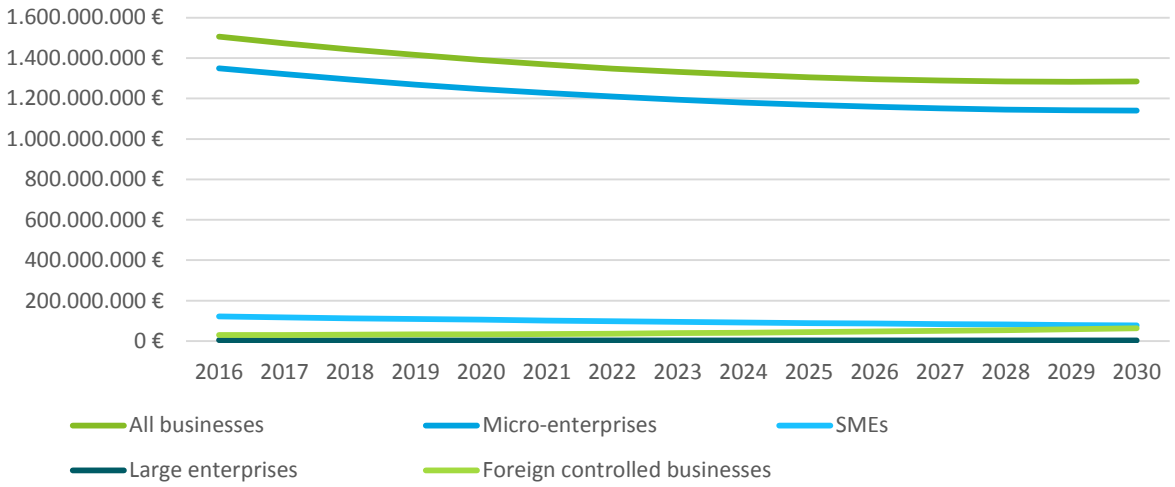


Source: Deloitte

Annual compliance costs in the baseline scenario

The following two graphs present the development of the annual compliance costs of businesses affected by the ePD. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

Figure 53 – Compliance costs of businesses affected by the ePD per year (baseline scenario, 2016-2030)

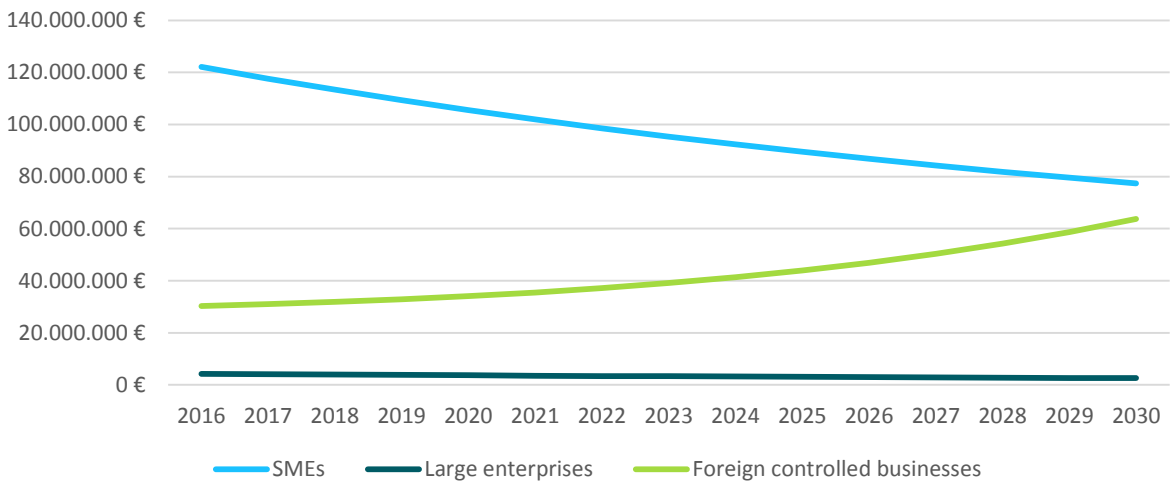


Source: Deloitte

The graph above shows the annual overall compliance costs for businesses can be expected to decrease between 2016 and 2030. Looking in more detail at annual overall compliance costs for SMEs, large enterprises, and foreign controlled enterprises (see figure below), it can be seen that – while compliance costs for SMEs are expected to decrease – they are expected to remain relatively stable for large enterprises and are expected to increase for foreign controlled enterprises.

This trend is slightly different compared to what was observed between 2002 and 2016.

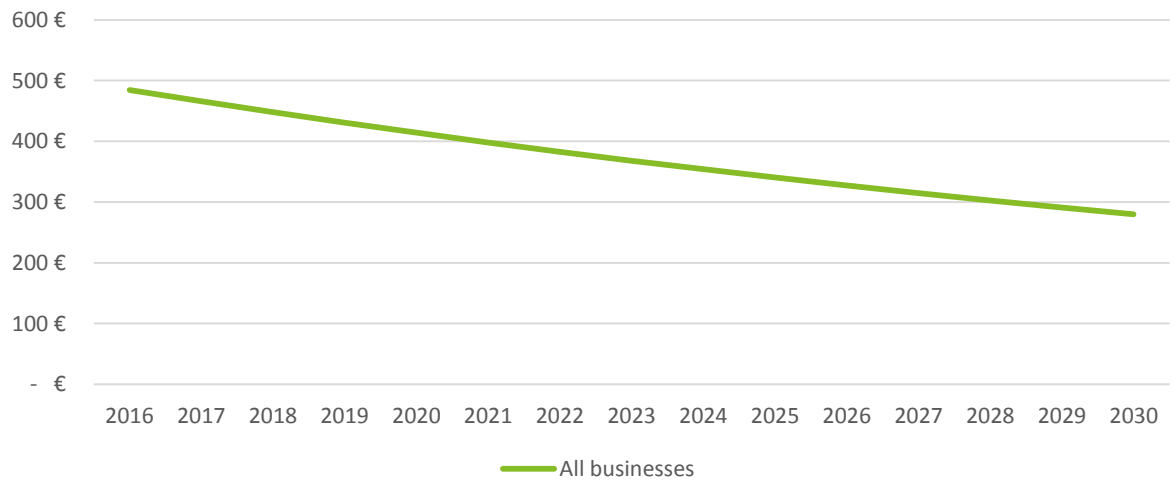
Figure 54 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (baseline scenario, 2016-2030)



Source: Deloitte

The following graph visualises the development of the average compliance costs for businesses from 2016 to 2030. No difference has been made between average costs for different size classes of businesses.

Figure 55 – Average compliance costs of per business affected by the ePD per year (baseline scenario, 2016-2030)



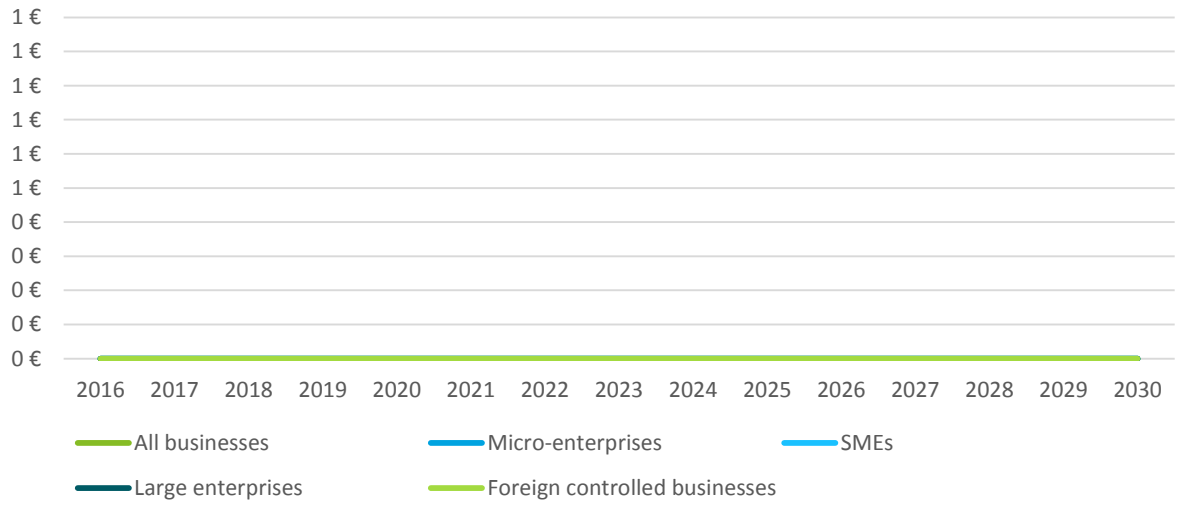
Source: Deloitte

The graph clearly shows that the average compliance costs for businesses are expected to decrease between 2016 and 2030. This decrease is a continuation of the trend already seen between 2002 and 2016.

Annual costs from administrative burden in the baseline scenario

The following two graphs present the development of the annual costs from administrative of businesses affected by the ePD. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

Figure 56 – Costs from administrative burden of businesses affected by the ePD per year (baseline scenario, 2016-2030)

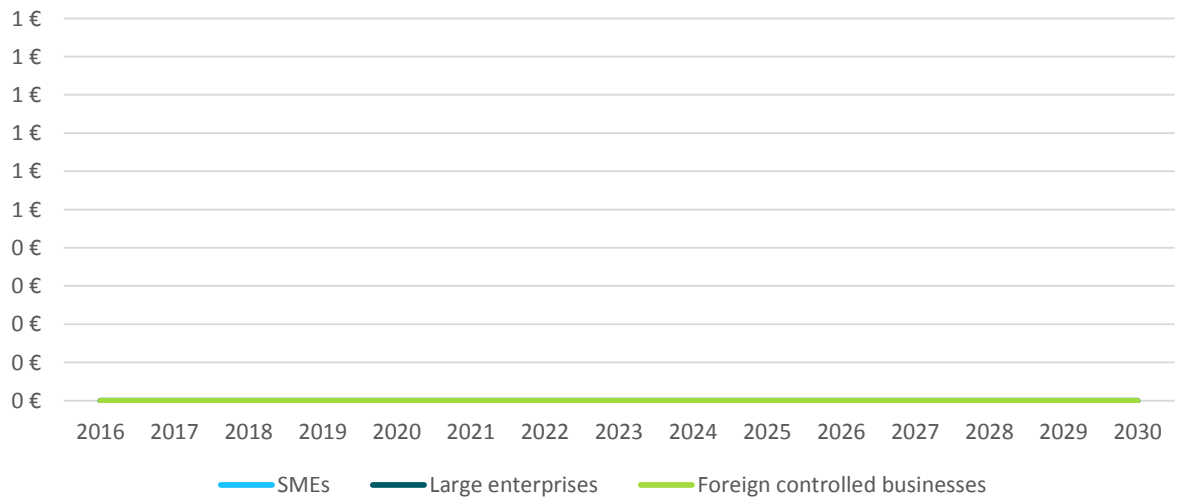


Source: Deloitte

The costs stemming from administrative burden are expected to increase slightly in the baseline scenario. While costs for micro- and large enterprises are expected to remain fairly stable, the costs for SMEs and foreign controlled enterprises are expected to increase (see also the graph below).

This trend is different compared to what was observed between 2002 and 2016.

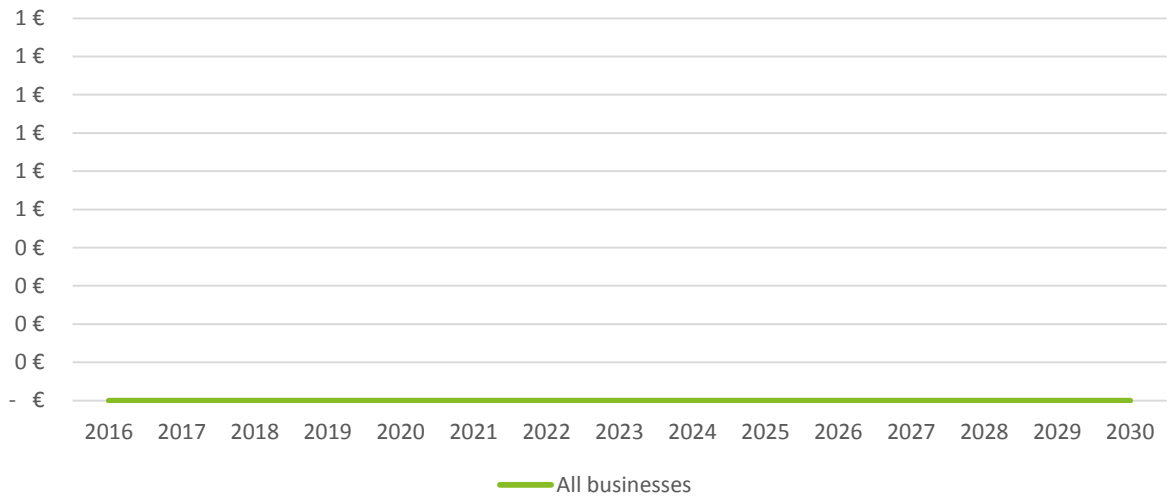
Figure 57 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (baseline scenario, 2016-2030)



Source: Deloitte

The following graph visualises the development of the average costs from administrative burden for businesses from 2016 to 2030. No difference has been made between average costs for different size classes of businesses.

Figure 58 – Average costs from administrative burden per business affected by the ePD per year (baseline scenario, 2016-2030)



Source: Deloitte

Overall, however, the average costs per business from administrative burden are expected to decrease (see the figure above). This is due to the number of businesses affected by the ePD strongly increasing between 2016 and 2030, while costs are expected to increase for a comparatively small share of businesses only (SMEs and foreign controlled enterprises).

Baseline scenario: Overall values 2016-2030

While the above section has presented average annual values, this section provides the key quantitative estimates for the overall time period of 2016-2030 (i.e. the sums of each individual annual value of the time period). This estimate is relevant to assess the overall costs of compliance and administrative burden stemming from the ePD for different types of businesses.

The following table contains information on:

- Compliance costs (in million Euro); and
- Administrative burden (in million Euro).

The number of businesses affected is not presented in terms of overall values relating to the whole period 2016-2020, as it would not be possible to simply add up the businesses affected each year. This would lead to double-counting, due to the fact that businesses are affected by the ePD over longer time frames than just one year.[501] On this basis, it is more appropriate to examine the number of businesses affected on an annual basis. Compared to the above section, average compliance cost per business, as well as average costs from administrative burden per business are not relevant to present in this section as they are *average* values and not *overall* values.

The table contains four columns:

[501] An alternative way of phrasing this is that the ePD does not affect an entirely different set of businesses each and every year.

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business; and
- *Overall value (2016-2030):* Denotes the overall annual value of the quantitative indicator for which data has been estimated. This means, for instance, that all SMEs in the EU together have will incur compliance costs of 1,455.3 EURm over the entire time period of 2016-2030 (see the light green cell).
- *Absolute Δ to 2002-2016:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the average annual value under the baseline scenario compared to the current and past situation (i.e. REFIT, 2002-2016); and
- *Relative Δ to 2002-2016:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the average annual value compared to the current and past situation (i.e. REFIT, 2002-2016).

Table 74 – Key quantitative data estimated in relation to the baseline scenario (overall 2016-2030)

Quantitative indicator	Overall value (2016-2030)	Absolute Δ to 2002-2016	Relative Δ to 2002-2016
Compliance costs (in million Euro)	20,330.7 €	-7,239.1 €	-26.3%
Micro-enterprises	18,194.6 €	-6,335.8 €	-25.8%
SMEs	1,455.3 €	-1,044.1 €	-41.8%
Large enterprises	50.0 €	-33.2 €	-39.9%
Foreign controlled enterprises	630.9 €	173.9 €	38.1%
Administrative burden (in million Euro)	3.5 €	-0.6 €	-15.0%
Micro-enterprises	2.7 €	-0.7 €	-20.4%
SMEs	0.5 €	0.1 €	26.9%
Large enterprises	0.0 €	0.0 €	-22.7%
Foreign controlled enterprises	0.2 €	0.0 €	-5.0%

Source: Deloitte

As can be seen from the table above, businesses are expected to incur less compliance costs and costs from administrative burden between 2016 and 2030 than they have between 2002 and 2016. This is logical, as organisations adapt and learn over time (also get more acquainted to a specific set of rules). This is closely linked to economies of scale (i.e. a solution is fairly cheap to be replicated once it is developed at relatively high investment). Stakeholders consulted as part of this study explained that they incurred more costs when the rules were new, as they had to invest in equipment and develop new procedures. Afterwards, they can implement the rules increasingly efficient. In absolute terms, compliance costs are expected to decrease by 7,239 EURm to 20,331 EURm compared to the overall amount incurred between 2002 and 2016. This equals a reduction of roughly 26%. In the baseline scenario, SMEs are expected to benefit most from reductions of compliance costs (-42%).

As argued in the REFIT section 6.2.2, the magnitude of the compliance costs should be seen in relation to the overall value of EU GDP. This way, the magnitude of compliance costs is marginal compared to the overall value of the economy.

As regards the costs from administrative burden, reductions are expected to be less pronounced. Overall, it is expected that 600,000 Euro can be saved between 2016 and 2030 at EU level. This is expected to result in an overall amount of 3.5 EURm of costs from administrative burden. The reduction is expected to be 15% compared to the overall amount incurred between 2002 and 2016.

Impacts on costs for public authorities

Without policy action, there would be no significant impacts on the costs for public authorities. The competent authorities dealing with the ePD would continue to incur the same types of costs as in the current situation.

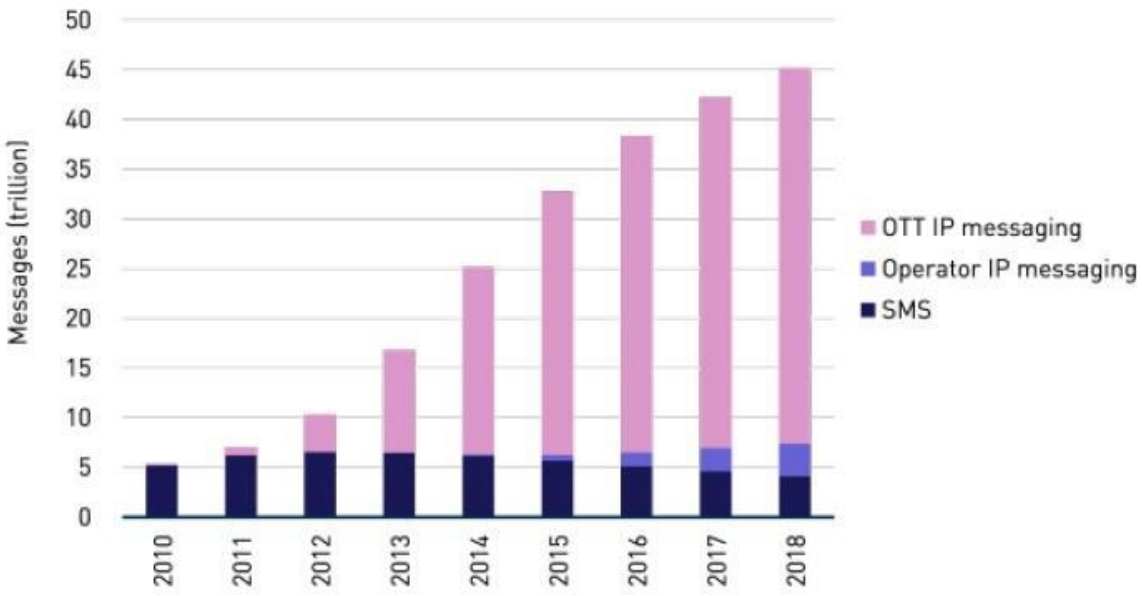
Other economic impacts

There would be no direct impacts on other economic aspects, including e.g. opportunity costs incurred by businesses in the electronic communications sector.

On this basis, **telecom service providers would continue to incur opportunity costs** vis-à-vis their OTT competitors. As pointed out in section 7.3.3, the fact that OTTs are excluded from the scope of the ePD leads to an unequal situation between OTTs and telecom providers.

Telecom providers may further incur losses, as **citizens are expected to rely increasingly on OTT services** as a substitute for traditional electronic communications services. This was, for example, shown in a study commissioned by the European Parliament estimated the potential developments in this field.

Figure 59 – Estimated developments relating to the use of messaging services



Source: DG for Internal Policies, "Over-the-Top players (OTTs), Study for the IMCO Committee", 2015, 31.

Further costs may ensue for **providers of new communication technologies**, including e.g. players in the context of the IoT. As the current uncertainties would not be addressed while technologies would continue to develop, there will a higher number of businesses that may not be sure whether or not they fall under the scope of (specific provisions of) the ePD. This uncertainty would lead to higher costs for legal advice.

9.2.3 Effectiveness in reaching the policy objectives

There would be no direct impact on the achievement of the policy objectives, as no policy action is taken. On this basis, it is expected that the situation in relation to the specific objectives would remain stable or deteriorate. Our analysis relating to the specific objectives is presented in the following sub-sections.

Specific Objective 1: To ensure effective confidentiality and security of communications

The problems identified in relation to the confidentiality of communications are likely to remain in place or even deteriorate. To recall, the following main issues were identified (see section 7.3.1):

- The confidentiality of users of traditional electronic communications services and the internet to browse online is not ensured based on shortcomings relating to Articles 4, 5, 6 and 9; and
- The confidentiality of users of OTTs in most EU Member States is not ensured because OTTs are excluded from the scope of the ePD or are only covered on a case-by-case basis.

As concerns the first point, the identified shortcomings will remain if no policy action is taken. On this basis, the limitations in relation to privacy and confidentiality for users of traditional electronic communications services are expected to persist. They may even become worse, for example because further ambiguities may arise based on the development of new technologies. The same is valid for privacy concerns related to online browsing. As demonstrated in the problem assessment, the current rule on information stored on users' terminal equipment (Article 5.3) is not fully effective in protecting users. It can be expected that the risks for users will grow. It was, for example, pointed out by the WP29 that more and more websites experiment with alternatives to cookies in order to circumvent the consent rule of the ePD.[502] This may negatively impact on citizens' trust in the digital economy, who may feel that their online activities are not sufficiently protected by law.

In relation to the second bullet point related to users of OTTs, no direct impacts are expected. As concerns the **likely future development of privacy standards for OTTs**, we note that it is **possible that these will improve** based on different factors.

First, some OTT providers have already put in place rules to strengthen confidentiality of communications. For example, many ask for the consent of their users to process certain information, strengthened the rules on security e.g. by introducing end-to-end encryption for communications (e.g. WhatsApp) or increased the transparency and control of users. It may, therefore, be expected that some improvement may be introduced based on market forces. However, there are currently still important differences between the standards of OTTs and ECS, as further described under the assessment of option 2.

Second, OTTs will be governed by stricter rules (including e.g. clearer conditions on consent) based on the entry into force of the GDPR in 2018. Third, in some Member States the rules of the ePD are already applied to OTTs (cf. Table 65). However, they represent a minority and it is not clear whether other Member States would take similar paths.

Thus, while there may be certain improvements, **citizens will still not be able to rely on consistent standards for OTTs** that are comparable to those valid for traditional electronic communications

[502] WP29 Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting.

services. OTTs will in most EU Member States still face less restrictive regulatory conditions to process communications data. The number of citizens affected by these issues is expected to grow, as an increasing number of persons will make use of OTTs.

Specific Objective 2: To ensure that citizens are effectively protected against unsolicited marketing communications

It was shown in the problem assessment that there are shortcomings in relation to Article 13, which is why citizens are not effectively protected against unsolicited marketing communications (see section 7.3.2).

In case no action is taken, it can be expected that this situation will remain similar. **Citizens will still face different legal regimes (opt-in or opt-out) depending on the Member State** they are in. In the Member States with an opt-out regime, they will still need to register with Robinson lists to report an opt-out for unsolicited marketing calls. It can be expected that nuisance calls will remain at a similar level, at least in the short term,[503] meaning that citizens will still feel that they receive too many of such calls.

Specific Objective 3: To simplify the legal framework and adapt it to the new legal, market and technological reality

One of the results of the evaluation was that the current legal framework is complex and not well adapted to current market and technological developments. This is based on various reasons, which will not be affected significantly without policy change:

- **Complexity in relation to other EU instruments**: For example, it was criticised by several stakeholders that there is a duplication of notification schemes between Article 4 of the ePD and other legal instruments, including the GDPR. This will not change without policy intervention. Businesses and competent authorities will continue to face different schemes.
- **Complexity based on the fragmented implementation of the ePD in Member States:** Based on ambiguities and legal leeway in the ePD, the implementation of the rules varies considerably. In addition, the rules are not always consistently and effectively enforced. On this basis, businesses engaging in cross-border activities still face varying legal frameworks in the Member States. On this basis, they may incur additional costs for legal advice as they need to understand the rules in different Member States. In addition, they may incur additional costs for implementing the rules, as they will need to follow different legal regimes. For example, they may need to apply different marketing strategies if they are active in a Member State that uses an opt-in regime for unsolicited communications and one that uses an opt-out regime. While it is possible that Member States may cooperate to exchange good practices, it is not expected that the situation would change significantly.
- **Some of the rules are outdated**: Businesses incur costs because they need to implement provisions that are no longer needed, e.g. because they are covered in other legal instruments (Article 4) or are no longer requested by consumers (Article 8). In addition, some of the rules only bring limited use for citizens as they are no longer in line with new technologies, whereas businesses still incur costs. This concerns in particular Article 5(3). Without policy intervention,

[503] For example, in its latest panel Ofcom noted that the number of nuisance calls remained relatively stable compared to previous years. https://www.ofcom.org.uk/__data/assets/pdf_file/0025/49471/Nuisance_calls_2016.pdf

the ePD will remain ill-adapted and the situation may deteriorate based on the development of new technologies in the future.

Thus, this objective would not be achieved without policy intervention.

9.2.4 Social impacts

No significant social impacts are expected.

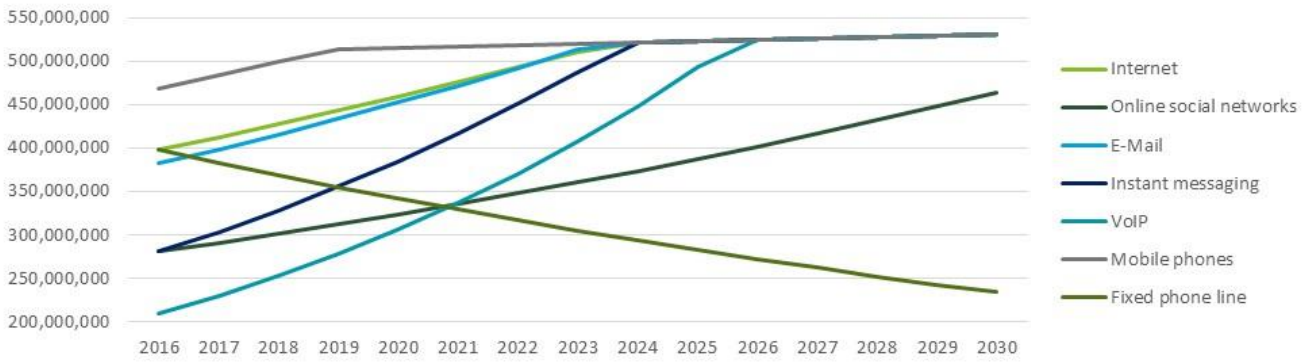
9.2.5 Number of citizens affected in the baseline scenario (2016-2030)

In this section, we present the number of citizens affected each year by the ePD in relation to the different types of communication services (some of which are covered by the ePD):

- Internet to browse online;
- Online social networks;
- Email;
- Instant messaging (e.g. WhatsApp);
- Voice of IP;
- Mobile phones to make calls or send texts; and
- Fixed phone lines.

The graph visualises the years 2016 to 2030.

Figure 60 – Number of citizens affected by communication services per year (baseline scenario, 2016-2030)



Source: Deloitte

As can be seen from above figure, the number of users affected by all types of communication services is expected to grow in the baseline scenario until (almost) all EU citizens make use of the different services (this explains the flat line at the top of the figure). The sole exception from this trend is the use of fixed line telephone which is expected to lose subscribers until 2030. It is expected that the use of innovative communication means will still increase over the next eight to ten years, incl. services that are currently not covered by the ePD.

Under the policy options 1-5, we assume that the number of citizens affected will remain equal, as it is always based on the usage of certain communication services. This is largely independent of the ePD and the policy options for its amendment. This means that the policy option will not have an impact on the number of citizens affected because the take-up of communication services is a rather an overall macro-trend than a steered by EU legislation (unless of course the use of a service is prohibited).

9.3 Policy Option 1: Non-legislative ("soft law") measures

Under this option, the Commission would make extensive use of its implementing powers and use soft policy instruments in order to improve the protection of the users. The specific contents of the individual measures cannot be delineated with precision at this stage, as they will emerge as a result of the overall process within the Commission and with the stakeholders.

The specific elements of the policy option can be found in chapter 8.2.

9.3.1 Overview of assessments

In the following table we present an overview of our assessment of policy option 1. The detailed assessment according to the individual assessment criteria can be found in the following sub-sections.

Table 75 – Qualitative rating of the impacts of Policy Option 1

Assessment criteria	Rating	Brief explanation of the rating
Economic impacts		
Impacts on costs for businesses	1	Business may incur some additional compliance cost savings as the interpretative communications and awareness raising activities would contribute to clarifying the legal framework. However, there would be additional costs, e.g. to participate in standard-setting activities. There would be no impact on administrative burden.
Impacts on costs for public authorities	14	Both EU and national administrations would incur high costs to implement this policy options. Costs relate in particular to the drafting of guidance documents, the funding of projects and the coordination of industry activities.
Other economic impacts	0	No significant other impacts are expected.
Effectiveness in reaching the policy objectives		
Objective 1: To ensure effective confidentiality and security of communications	-1	While this policy option would contribute slightly to the achievement of all policy objectives via introducing additional guidance, awareness raising activities and cooperation, it does not address all problems identified
Objective 2: To ensure that citizens are effectively protected against unsolicited marketing communications	-1	
Objective 3: To simplify the legal framework and adapt it to the new legal, market and technological reality	-1	
Social impacts	0	No significant other impacts are expected.
Total	12	

Source: Deloitte

9.3.2 Economic impacts

In this section on the assessment of the economic impacts of policy option 1, we are focusing on three key aspects: (1) The impacts on compliance costs and administrative burden for businesses (incl. SMEs and micro-enterprises), and (2) on costs for public authorities; as well as (3) other economic impacts such as on competiveness and competition in the Digital Single Market.

Impacts on compliance costs and administrative burden for businesses

In this section, we provide the following:

- ***Part A:*** A detailed qualitative assessment table regarding the impact of each element of the policy option 1; and
- ***Part B:*** The key quantitative findings from the economic analysis in relation to the impact of policy option 1.

The former will feed into the latter with regard to the assessment of the economic impact of the policy option.

Part A: Detailed qualitative assessment tables

A more **detailed qualitative assessment table** regarding the impact of each element of policy option 1 is provided below. The table contains:

- Qualitative reasoning used for the quantitative assessments of the impacts of the policy options on businesses (in particular on compliance costs and costs related to administrative burden);
- An indication of the types of businesses affected by each element;
- Qualitative rating / colour coding of the expected impacts of each element of the options;
- An indication whether or not businesses would incur compliance costs or costs related to administrative burden from each specific element;
- The frequency of costs (as far as information is available); and
- The existence / emergence of opportunity costs in relation to each of the elements of the policy options.

As described in Annex A on the *general approach used to translate qualitative reasoning into quantitative assumptions*, the ratings contained in the below table of this Part B have been used as a qualitative basis for the quantitative assessment of the impacts of the policy options in Part A above.

Table 76 – Qualitative classification of the impacts of policy option 1 on costs for businesses

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin. burden	Frequency
Objective 1: Ensuring effective confidentiality and security of communications						
1. **Increased use of interpretative communications.** The Commission would provide more detailed guidance on the interpretation of certain aspects of the ePD which are unclear or open to different interpretations.	Business may need to spend less time on interpreting the provisions. Potentially, this also decreases the need for legal advice. At the same time, there may be more businesses applying the ePD (e.g. those that previously did not consider their WiFi network or IoT devices to be covered).	ECS	0	x		
2. **Support EU-wide self-regulatory initiatives** building on the existing *ePrivacy acquis* ("co-regulation").[504].	Businesses may be more inclined to participate in standard-setting activities. The increase of costs would be moderate, however, as the participation would be voluntary, normally only a small number of businesses actually actively participate in such activities, and there are already some efforts in this direction.	ECS	1	x		Recurring
3. **Specify privacy by design requirements of terminal electronic equipment through EU standards**.[505]	Businesses would need to implement the new standards. The exact increase would depend on the standards proposed and the number of companies that need to be compliant. For individual companies, the costs may be significant. For instance, a large IT equipment manufacturer indicated that they incur annual costs of between 5 and 10 million Euros.[506] However, the number of such companies is limited compared to the overall number of businesses complying with the ePD. On this basis, the overall increase is assumed to be moderate.	ECS	1	x		

[504] The Commission would lead and coordinate industry efforts to promote standards and codes of conduct in crucial areas such standard information notices related to the use of location data by ECS providers, online tracking, standardised icons and labels, an EU-wide OBA code of conduct and/or an EU DNT standard.
[505] Article 14(3).
[506] They indicated that 200 or more FTEs work on implementing such standards.

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin. burden	Frequency
4. **Research and awareness-raising activities**. The Commission would significantly increase the funds related to R&D projects in the field of online privacy and security by 25%. In addition, it would engage in awareness-raising activities.[507]	This does not have a direct implication for businesses. It may be considered, however, that businesses may apply for this funding.		0	x		
Objective 2: Ensuring effective protection against unsolicited commercial communications						
5. **Interpretative communications**, clarifying the interpretation of unclear or ambiguous concepts.[508]).	Business may need to spend less time on interpreting the provisions. Potentially, this also decreases the need for legal advice. In addition, they may save costs based on the promotion of a business-friendly application of the ePD.	All businesses	-1	x		
6. **Awareness-raising initiatives** instructing citizens on how to defend themselves, how to seek redress from national supervisory authorities.	No direct costs for businesses are involved. It may be possible that the campaigns would lead to businesses being more inclined to apply the ePD. However, as this depends on the effectiveness of the campaigns and the willingness of businesses, it is not possible to estimate the impact.	All businesses	0	x		
Objective 3: Simplifying the legal framework and adapting it to the new market and technological reality						
7. Issue **interpretative communications** to promote an application of the current rules, which is business friendly, while preserving the essence of the protection of confidentiality of communications.[509]	Business may need to spend less time on interpreting the provisions. Potentially, this also decreases the need for legal advice. In addition, they may save costs based on the promotion of a business-friendly application of the ePD.		-1	x		

[507] Such as setting-up an ad-hoc website and an Internet based advertising campaign, ad-hoc conferences, events (e.g., online communications day) and training for national officials
[508] For example, the issues around the scope of the provision, silent or abandoned calls, the implementation of Robinson lists.
[509] This would cover issues such as the scope of the ePD (e.g., publicly available WiFi networks, IoT devices); modalities to provide consent for tracking, the exceptions to the consent rules under the ePD.

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin. burden	Frequency
8. Work closely with **industry** in order to encourage the adoption of **common best practices**.[510]	Businesses may be more inclined to participate in activities supporting the adoption of best practices. The increase of costs would be moderate, however, as the participation would be voluntary, normally only a small number of businesses actually actively participate in such activities, and there are already some efforts in this direction.		1	x		
9. **Support MS cooperation** to improve enforcement in cross-border cases as well as harmonised interpretation by organising meetings and workshops with authorities	This element does not have any significant impact on businesses.		0			
Overall implications (Compliance)			**1**			
Overall implications (Admin burden)			**1**			
Overall implications on the number of businesses affected	This option does not entail any changes that impact on the number of businesses affected by the ePD.		**0**			

Source: Deloitte

[510] Concerning, for instance, the provision of information and consent mechanisms, thus facilitating a uniform and clear implementation of the current rules.

Part B: Key quantitative findings from the economic analysis

Policy option 1: Average annual values and changes compared to the current situation

The overall quantitative results of the analysis concerning policy option 1 are presented in Table 73:

- Number of businesses affected (in million);
- Compliance costs (in million Euro);
- Average compliance cost per business (in Euro);
- Administrative burden (in million Euro); and
- Average costs from administrative burden per business (in Euro).

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Annex A: Economic Analysis

Further information in this regard, as well as an explanation of the approach used for the estimation of the quantitative results data is provided in the section on the basic assumptions used for the assessment of the impacts of the policy options in Annex A concerning the Economic Analysis.

The following table presents the quantitative findings for policy option 1. The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Average annual value:* Denotes the average annual value of the quantitative indicator for which data has been estimated. This means, for instance, that 260,000 SMEs are affected by issues relating to the ePD per year (see the light blue cell), facing a total amount of 102 EURm per year (see the light green cell) at an average cost of compliance per business of 392 Euro (see the dark blue cell);
- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the average annual value compared to the baseline scenario (2016-2030); and
- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the average annual value compared to the baseline scenario (i.e. 2016-2030).

Visualisations of the year-over-year development of the quantitative indicators are presented afterwards, as well as overall values for the timeframe 2016-2030.

Table 77 – Key quantitative data estimated in relation to policy option 1 (2016-2030)

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Number of businesses affected (in million)	3.70	0	0%
Micro-enterprises	3.31	0	0%
SMEs	0.26	0	0%
Large enterprises	0.01	0	0%
Foreign controlled enterprises	0.12	0	0%

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Compliance costs (in million Euro)	1,423.15 €	67.8 €	5.0%
Micro-enterprises	1,273.6 €	60.6 €	5.0%
SMEs	101.9 €	4.9 €	5.0%
Large enterprises	3.5 €	0.2 €	5.0%
Foreign controlled enterprises	44.2 €	2.1 €	5.0%
Average compliance cost per business (in Euro)	392.2 €	18.7 €	5.0%
Administrative burden (in million Euro)	0.23 €	0.002 €	0.9%
Micro-enterprises	0.18 €	0.002 €	1.1%
SMEs	0.03 €	0.000 €	0.0%
Large enterprises	0.00 €	0.000 €	0.0%
Foreign controlled enterprises	0.01 €	0.000 €	0.0%
Average costs from admin. burden per business (in Euro)	28.0 €	0.278 €	1.0%

Source: Deloitte

Under policy option 1, the analysis shows that – per year between 2016 and 2030 – around 3.7 million businesses will be affected by the ePD in the EU. The majority of these businesses will be micro-enterprises with less than 10 employees (3.3 million). Around 260,000 SMEs that have between 10 and 250 employees are estimated to be affected per year until 2030 while the number of large enterprises is negligible with around 10,000 per year. Approx. 120,000 foreign controlled enterprises that operate in the EU will be affected.[511]

The businesses affected by the ePD are estimated to incur an annual value of 1.4 EURb to comply with Art. 5(3) and Art. 13. In addition, these businesses are expected to incur an unspecifiable amount of additional costs with regard to other provisions such as the consumer provisions. Again, micro-enterprises are expected to incur the lion share of these costs (around 1.3 EURb).

On *average*, an EU business is expected to incur 392 Euro per year with regard to the ePD until 2030. This does, however, not mean that e.g. large enterprises may not incur significantly more costs while the costs may be significantly lower for micro-enterprises.

In relation to administrative burden, mostly stemming from the notification obligations for telecommunication service providers under Article 4, it has been estimated that an annual amount of 230,000 Euro is incurred, i.e. around 28 Euro per affected business per year.

Policy option 1: Visualisation of the development 2016-2030

In this section, we present visualisations of the development of the following quantitative indicators between 2016 and 2030 under policy option 1:

- The number of businesses affected;
- The compliance costs; and
- The costs from administrative burden.

[511] The estimated numbers of affected businesses should be understood as annual values. However, the overall number of businesses affected by the ePD between 2016 and 2030 is not the sum of each annual value. The reason for this is that the majority of businesses will be affected not only once but on several occasions across this time frame while some businesses will be replaced by others due to the general life cycle of businesses (company birth, insolvency). This means that, in relation to the former argument, the projected value is likely underestimating the actual number of businesses affected, while the latter argument, the projection is likely to overestimate the number of affected businesses.

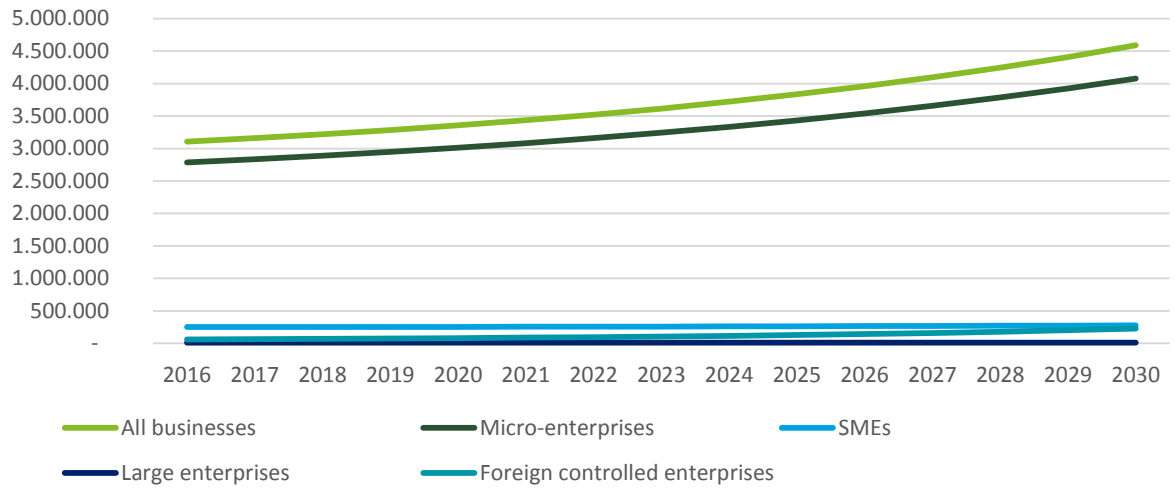
It has been decided to use such a form of visualisation instead of providing the data by means of tables in order to make the sheer amount of data more accessible to the reader and to clearly be able to show the *development of the quantitative indicators over time* – which is not always easy to spot when looking at raw figures.

The graphs visualise the data per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Number of businesses affected under policy option 1

The following two graphs present the development of the number of businesses affected by the ePD under policy option 1. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

Figure 61 – Number of businesses affected by the ePD per year (policy option 1, 2016-2030)

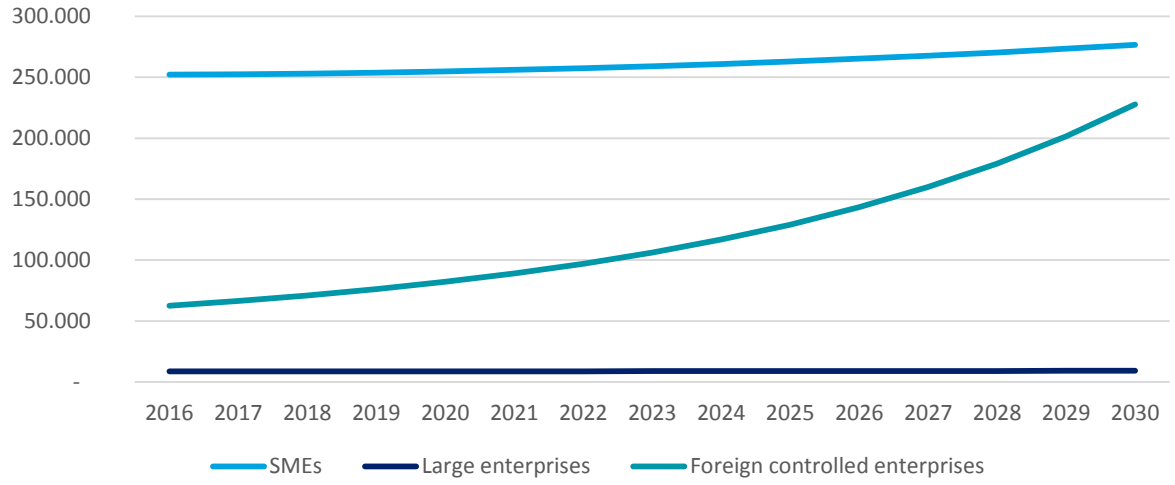


Source: Deloitte

The trends that can be seen from the graphs above and below in relation to the growth of the number of businesses affected by the ePD are equal to those in the baseline scenario.

- The overall number of businesses affected by the ePD is expected to grow from 2016 to 2030
- SMEs, large enterprises, and foreign controlled enterprises are of less importance for the overall growth of the number of businesses affected by the ePD;
- The number of SMEs affected is expected to increase slightly
- The number of large enterprises is expected to remain stable
- The number of foreign controlled enterprises affected by the ePD is expected to increase comparatively strong until 2030 vis-à-vis 2016.

Figure 62 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 1, 2016-2030)

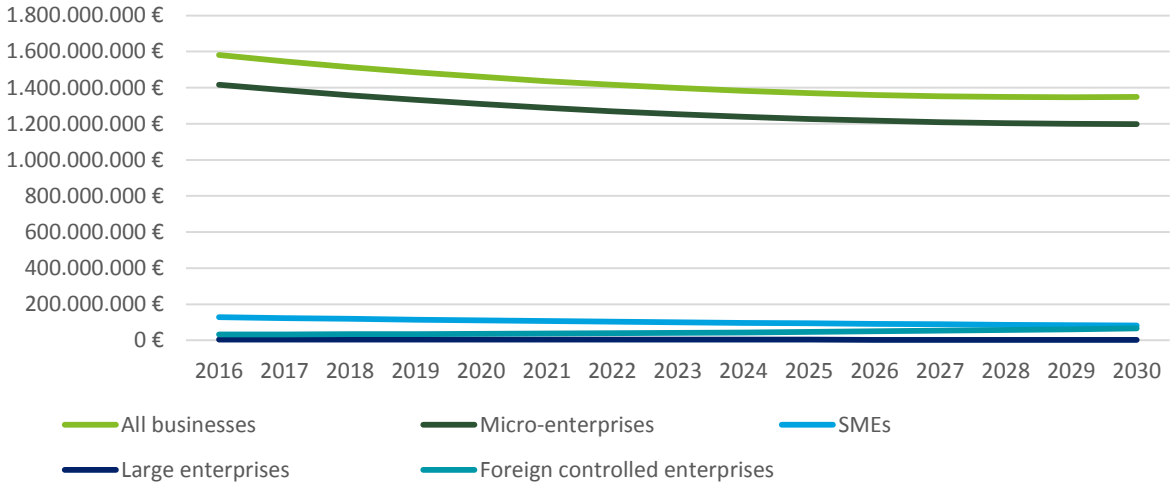


Source: Deloitte

Annual compliance costs under policy option 1

The following two graphs present the development of the annual compliance costs of businesses affected by the ePD under policy option1. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

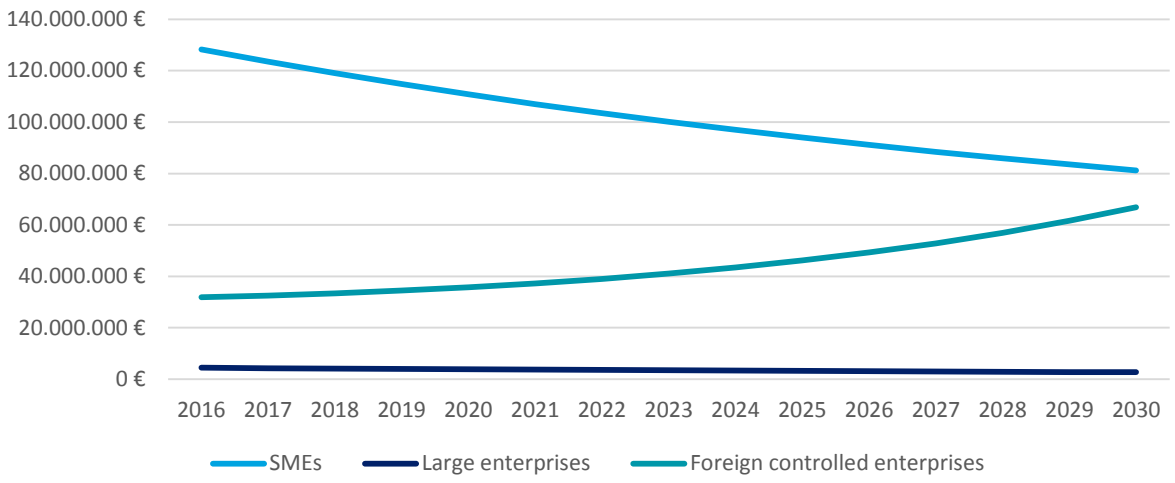
Figure 63 – Compliance costs of businesses affected by the ePD per year (policy option 1, 2016-2030)



Source: Deloitte

As can be seen above, the annual overall compliance costs for businesses are expected to decrease under policy option 1 until 2030. While the decrease is expected to be mostly driven by micro-enterprises, compliance costs for SMEs and large enterprises are also expected to decrease under policy option 1. Conversely, an increase of compliance costs for foreign controlled enterprises is expected until 2030 (see below).

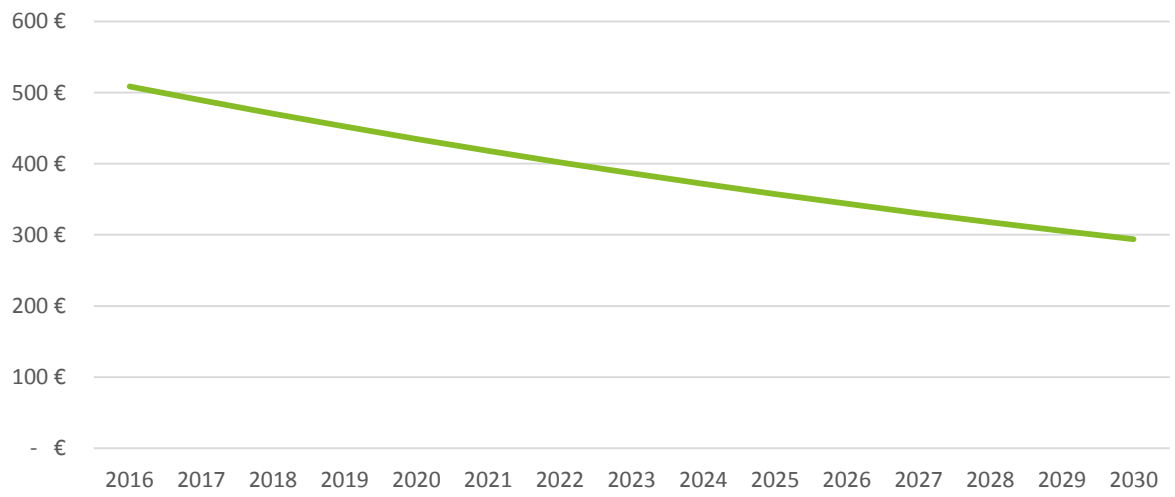
Figure 64 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 1, 2016-2030)



Source: Deloitte

The following graph visualises the development of the average compliance costs for businesses from 2016 to 2030 under policy option 1. No difference has been made between average costs for different size classes of businesses.

Figure 65 – Average compliance costs of per business affected by the ePD per year (policy option 1, 2016-2030)



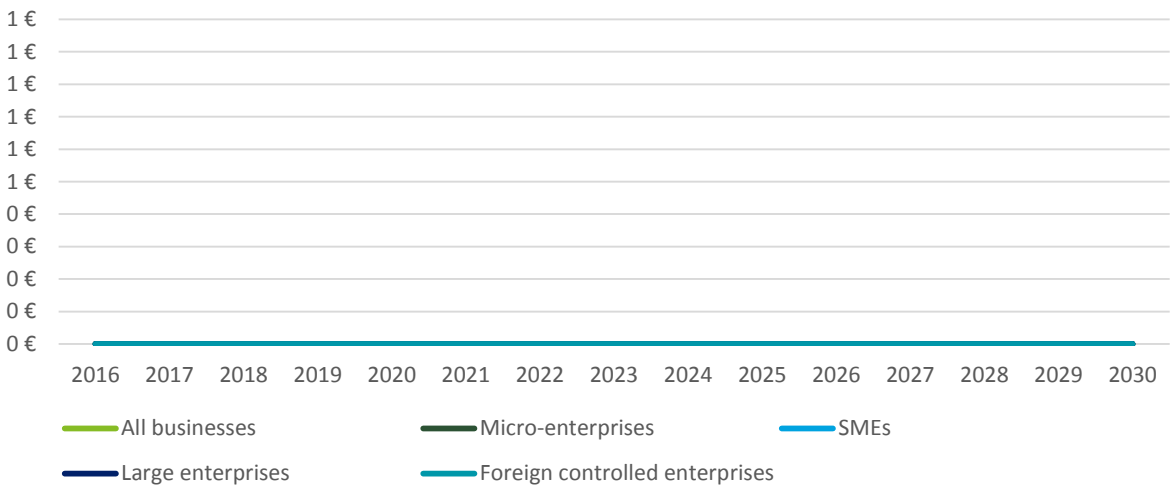
Source: Deloitte

The graph clearly shows that the average compliance costs for businesses are expected to decrease between 2016 and 2030.

Annual costs from administrative burden under policy option 1

The following two graphs present the development of the annual costs from administrative of businesses affected by the ePD under policy option 1. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

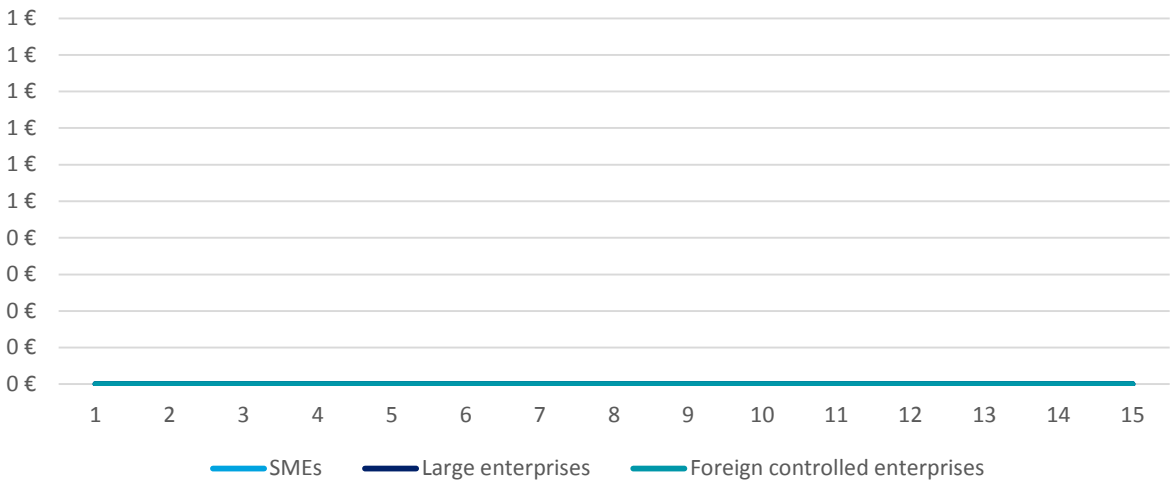
Figure 66 – Costs from administrative burden of businesses affected by the ePD per year (policy option 1, 2016-2030)



Source: Deloitte

Conversely to the compliance costs, costs from administrative burden are expected to increase slightly between 2016 and 2030 in line with the increasing number of businesses affected over time. The trends is equal to the baseline scenario as policy option 1 does not touch upon those provisions that cause costs from administrative burden.

Figure 67 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 1, 2016-2030)

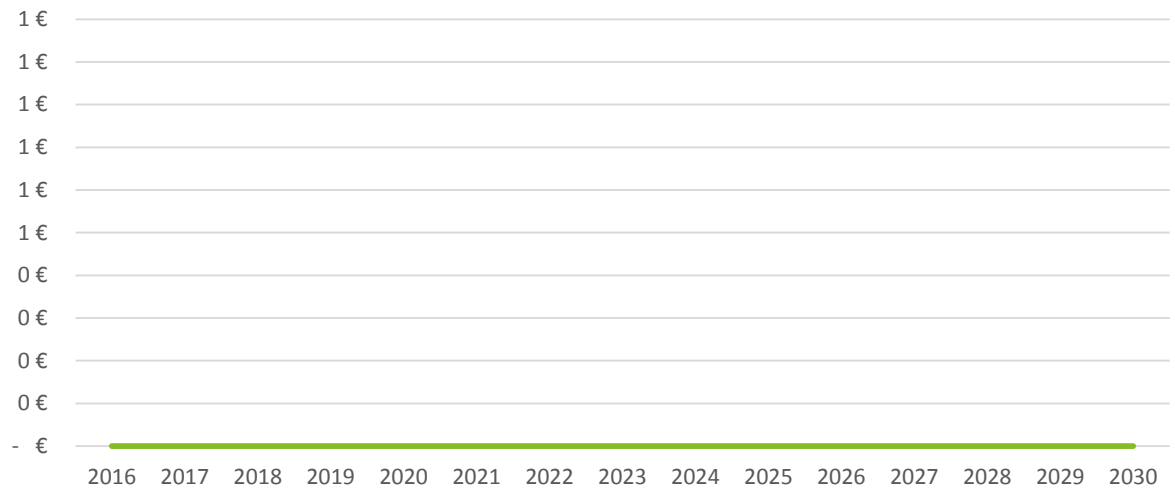


Source: Deloitte

The figure above shows that administrative burden costs increase for SMEs and foreign controlled enterprises while staying more or less stable for large enterprises until 2030.

The following graph visualises the development of the average costs from administrative burden for businesses from 2016 to 2030 under policy option 1. No difference has been made between average costs for different size classes of businesses.

Figure 68 – Average costs from administrative burden per business affected by the ePD per year (policy option 1, 2016-2030)



Source: Deloitte

Overall, the above graph shows that a reduction of average costs from administrative burden per business can be expected over time.

Policy option 1: Overall values 2016-2030

While the above section has presented average annual values, this section provides the key quantitative estimates for the overall time period of 2016-2030 (i.e. the sums of each individual annual value of the time period) under policy option 1. This estimate is relevant to assess the overall costs of compliance and administrative burden stemming from the ePD for different types of businesses.

The following table contains information on:

- Compliance costs (in million Euro); and
- Administrative burden (in million Euro).

The number of businesses affected is not presented as this number is – over the entire time period – subject to double counting.[512] Compared to the above section, average compliance cost per business, as well as average costs from admin. burden per business are not relevant to present in this section as they are *average* values and not *overall* values.

The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Overall value (2016-2030):* Denotes the overall annual value of the quantitative indicator for which data has been estimated. This means, for instance, that all SMEs in the EU together have will incur compliance costs of 1,528 EURm over the entire time period of 2016-2030 (see the light green cell);
- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the overall value between 2016 and 2030 under policy option 1 compared to the overall value under the baseline scenario; and

[512] This is due to the fact that businesses are affected by the ePD over longer time frames than just one year. An alternative way of phrasing this is that the ePD does not affect an entirely different set of businesses each and every year.

- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the overall value between 2016 and 2030 under policy option 1 compared to the overall value under the baseline scenario.

Table 78 – Key quantitative data estimated in relation to policy option 1 (overall 2016-2030)

Quantitative indicator	Overall value (2016-2030)	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Compliance costs (in million Euro)	21,347.2 €	1,016.5 €	5.0%
Micro-enterprises	19,104.3 €	909.7 €	5.0%
SMEs	1,528.1 €	72.8 €	5.0%
Large enterprises	52.5 €	2.5 €	5.0%
Foreign controlled enterprises	662.4 €	31.5 €	5.0%
Administrative burden (in million Euro)	3.50 €	0.04 €	1.0%
Micro-enterprises	2.74 €	0.03 €	1.0%
SMEs	0.51 €	0.01 €	1.0%
Large enterprises	0.03 €	0.00 €	0.0%
Foreign controlled enterprises	0.21 €	0.00 €	0.9%

Source: Deloitte

Under policy option 1, as can be seen from the table above, businesses are expected to incur more compliance costs and costs from administrative burden between 2016 and 2030 than they would in the baseline scenario.

In absolute terms, compliance costs are expected to increase by 1,016 EURm to 21,347 EURm compared to the overall amount incurred in the baseline scenario. This equals an increase of roughly 5%. Under policy option 1.

As argued in the REFIT section 6.2.2, the magnitude of the compliance costs should be seen in relation to the overall value of EU GDP. This way, the magnitude of compliance costs is marginal compared to the overall value of the economy.

As regards the costs from administrative burden, no significant reductions are expected under this policy option as it does not touch upon the provisions that are considered the drivers of the costs. Thus, the overall amount is expected to be equal to the baseline scenario in which 3.5 EURm of costs from administrative burden are incurred overall.

Impacts on costs for public authorities

In the tables below, we provide an assessment of the impacts of policy option 1 on public administrations. The table contains:

- Qualitative reasoning used for the quantitative assessments of the impacts of the policy options on businesses (in particular on compliance costs and costs related to administrative burden) complemented where possible with exact cost estimates;
- A rating of the magnitude of these costs, according to the scheme portrayed below, serving to make the impacts of the options comparable; and
- The frequency of costs (as far as information is available).

The general approach used for these qualitative ratings is outlined in Annex A on the Analysis of the impacts of the policy options on the costs for public administrations.

Table 79 – Qualitative classification of the impacts of policy option 1 on costs for public administrations

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
Objective 1: Ensuring effective confidentiality and security of communications				
1. **Increased use of interpretative communications.** The Commission would provide more detailed guidance on the interpretation of certain aspects of the ePD which are unclear or open to different interpretations.	The Commission would need to slightly increase the time spent on issuing guidance on the ePD. It may be assisted by ENISA or the JRC on these matters. It can be assumed that it would need to devote slightly more resources to this in the beginning. Updates or additional guidance may then become necessary at a later stage as well.	EU	1	One-off and recurring
	National authorities would need to get familiar with the new implementing/soft law measures. It can be assumed that this would involve around one day of training per authority. On this basis, it can be assumed that costs would be around EUR 870 per authority[513]. Some limited time may be spent in case of any updates at a later stage.	MS	1	One-off and recurring
2. **Support EU-wide self-regulatory initiatives** building on the existing *ePrivacy acquis* ("co-regulation").[514].	The Commission would need to follow the standardisation efforts and coordinate industry led-initiatives. This could, for example, entail the attendance of meetings and preparations for such meetings. It may be assisted by ENISA or the JRC on these matters.	EU	1	Recurring
	National authorities would be involved in the co-regulatory efforts. This cost will vary according to the number of meetings and the degree of cooperation requested by national authorities. Assuming that many issues may be steered by the Commission and national authorities would attend 3 meetings a year for 3 years, the annual cost per authority may be estimated to be between 2,500 and 7,000.[515]	MS	3	Recurring
3. **Specify privacy by design requirements of terminal electronic equipment through EU standards**.[516]	The Commission would need to bear costs related to the launching and following the standardisation process. It can be assumed that it would need to devote slightly more resources to this in the beginning. Updates or additional	EU	1	One-off and recurring

[513] Familiarisation/training costs= 3 staff-members per authority needing training *hours spent on training per staff (8 hours) *staff costs per hour (hourly wage rate EUR 41.5, Eurostat data 2012).

[514] The Commission would lead and coordinate industry efforts to promote standards and codes of conduct in crucial areas such standard information notices related to the use of location data by ECS providers, online tracking, standardised icons and labels, an EU-wide OBA code of conduct and/or an EU DNT standard.

[515] This is based on assuming that between one and two persons per MS might join, that they need to spend time on travel, the meeting itself and preparation (between 12 and 16 hours) considering the hourly salary of 41.5 EUR and that they need to pay for flight (on average between 350 and 400 Euro) and in some cases for one night accommodation (on average 100 Euro).

[516] Article 14(3).

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
	guidance may then become necessary at a later stage as well. It may be assisted by ENISA or the JRC on these matters.			
4. **Research and awareness-raising activities**. The Commission would significantly increase the funds related to R&D projects in the field of online privacy and security by 25%. In addition, it would engage in awareness-raising activities.[517]	Currently, the funding of projects under the Secure societies chapter of H2020, covering awareness raising and other activities amounts to 1,694.6 Mio. Euro.[518] Of these, 19.04 Mio. Euro are specifically dedicated to the topic "Privacy"[519]. It is not possibly to estimate the exact impact, without knowing the planned increased magnitude. Assuming, for example, that the funding dedicated to "Privacy" would be increased by 25%, it would amount to 4.76 Mio. Euro for the period 2014-2020. This would equal an average annual increase of 680,000 Euro.	EU	2	Recurring
Objective 2: Ensuring effective protection against unsolicited commercial communications				
5. **Interpretative communications**, clarifying the interpretation of unclear or ambiguous concepts.[520]).	This seems to overlap with point 2 above, which would entail the same type of involvement by the Commission and national authorities and also mentions an EU-wide OBA code of conduct. Therefore, it is assumed that there would be no additional separate impact from this point.	EU/MS	0	Recurring
6. **Awareness-raising initiatives** instructing citizens on how to defend themselves, how to seek redress from national supervisory authorities.	The launching of an awareness raising campaign may require the help of an external contractor; the cost may be estimated to be in the region of EUR 250-400,000 depending on the tools employed.[521] The overall impact would also depend on the frequency with which such campaigns may be launched.	EU	1	Recurring
Objective 3: Simplifying the legal framework and adapting it to the new market and technological reality				
7. Issue **interpretative communications** to promote an application of the current rules, which is business friendly, while preserving the essence of the protection of confidentiality of communications.[522]	This seems to overlap with point 1 above, which already indicates that guidance would be issued. As it is not clear whether this point would entail any additional measures, it is assumed that there would be no additional separate impact from this point.	EU/MS	0	One-off and recurring

[517] Such as setting-up an ad-hoc website and an Internet based advertising campaign, ad-hoc conferences, events (e.g., online communications day) and training for national officials
[518] Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC, ANNEX II, O.J. L 347, 20.12.2013, p. 104.
[519] See: http://ec.europa.eu/rea/pdf/2_security_societies_calls.pdf
[520] For example, the issues around the scope of the provision, silent or abandoned calls, the implementation of Robinson lists.
[521] This means that costs will be lower in case e.g. only and online campaign will be launched. In case e.g. an EU-wide awareness-raising campaign is launched with printed materials, informative events, discussion rounds etc., the costs would likely be higher than this estimate.
[522] This would cover issues such as the scope of the ePD (e.g., publicly available WiFi networks, IoT devices); modalities to provide consent for tracking, the exceptions to the consent rules under the ePD.

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
8. Work closely with **industry** in order to encourage the adoption of **common best practices**.[523]	The Commission would need to coordinate the efforts of the industry to adopt common standards. This could, for example, entail the attendance of meetings and preparations for such meetings. It may be assisted by ENISA or the JRC on these matters.	EU	1	Recurring
9. **Support MS cooperation** to improve enforcement in cross-border cases as well as harmonised interpretation by organising meetings and workshops with authorities	The Commission would need to coordinate the efforts by Member States. This may, e.g. entail the organisation and attendance of meetings and workshops, the development of guidance/good practices in cooperation with national authorities.	EU	1	Recurring
	National authorities would need to attend (and potentially prepare) the workshops and meetings and would need to be involved in the development of guidance/good practices. Assuming that many issues may be steered by the Commission and national authorities would attend 2 meetings a year, the annual cost per authority may be estimated to be between 1,700 and 4,700.[524]	MS	2	Recurring
Overall implications (EU)	It is estimated that it would require two administrators and one assistant working full time on different elements of this option. However, most of these measures could be undertaken by redistribution and refocusing of existing personnel and with the contribution of ENISA and the JRC.		**8**	
Overall implications (MS)	Member States would mainly be involved in the efforts to support co-regulation initiatives of the industry and to coordinate enforcement of cross-border cases. Some limited efforts would need to be undertaken to get acquainted with the new guidance documents prepared by the Commission.		**6**	

Source: Deloitte

[523] Concerning, for instance, the provision of information and consent mechanisms, thus facilitating a uniform and clear implementation of the current rules.
[524] This is based on assuming that between one and two persons per MS might join, that they need to spend time on travel, the meeting itself and preparation (between 12 and 16 hours) considering the hourly salary of 41.5 EUR and that they need to pay for flight (on average between 350 and 400 Euro) and in some cases for one night accommodation (on average 100 Euro).

Other economic impacts

There would be no direct impacts on other economic aspects, including e.g. opportunity costs incurred by businesses in the electronic communications sector.

On this basis, **telecom service providers would continue to incur** opportunity costs vis-à-vis their OTT competitors, as in the baseline scenario. As pointed out in section 7.3.3, the fact that OTTs are excluded from the scope of the ePD leads to an unequal situation between OTTs and telecom providers.

As this policy option does not change this situation, Telecom providers may further incur losses, as **citizens are expected to rely increasingly on OTT services** as a substitute for traditional electronic communications services (cf. the section on other economic impacts under the baseline scenario). This was, for example, shown in a study commissioned by the European Parliament estimated the potential developments in this field.[525]

9.3.3 Effectiveness in reaching the policy objectives

In this section, the effectiveness of policy option 1 in reaching the policy objectives is assessed. It is shown in the following sub-sections that the effectiveness of this option is limited in relation to all specific objectives.

Specific Objective 1: To ensure effective confidentiality and security of communications

The **increased use of interpretative communications**, i.e. providing more detailed guidance on certain provisions of the ePD, would have small positive impacts. It was demonstrated in the problem assessment that one of the horizontal issues hindering the functioning of the ePD was the fragmented implementation of its rules in the Member States. An increased use of interpretative communications would likely increase harmonisation, meaning that citizens are more likely to benefit from comparable standards across the EU. However, as additional guidance does not present binding interpretations for Member States, effective harmonisation in the enforcement ePD provisions is not expected.

Based on insights from stakeholder interviews and the consultation process, the effectiveness of **specifying privacy by design requirements** of terminal electronic equipment through EU standards is expected to have a small positive impact. Stakeholders reported that they strongly consider EU standards in their development efforts because of the size of the EU market and the cost of regional adaptions. The positive effect is expected to be limited, given that common standards:

- Are limited to aspects of communication equipment; and
- Require a challenging negotiation process in cooperation with stakeholders until they are adopted.

Similarly, the effectiveness **industry self-regulation initiatives** has to be considered as ambiguous. ECS providers from various Member States repeatedly mentioned that the privacy and security requirements are not recognised as a unique selling point by users. Thus, even though a small segment of users strictly favours services with a focus on privacy and security features (e.g. in

[525] DG for Internal Policies, "Over-the-Top players (OTTs), Study for the IMCO Committee", 2015, 31.

messaging or email services), the incentive for business to compete via higher privacy and security standards (which increase operational costs) is low. Thus, the effectiveness of increasing privacy and confidentiality through self-regulation initiatives is expected to be limited.

Awareness-raising might produce a small positive impact in the long run. On the one hand, businesses targeted by this measure might in some cases recognise and remediate prior mistakes in the application of rules. This positive effect is expected to be small, as actual effects depend on the reach of campaigns adopted and the willingness of businesses to comply. On the other hand, raising awareness and knowledge of national officials, e.g. through campaigns or trainings could have a small positive impact on the future application of existing rules. Citizens, as well as businesses and national officials, may gain a deeper understanding of:

- Possible privacy differences between functionally equivalent services; and
- Legal and practical instruments to prevent privacy intrusions at their disposal.

On this basis, some consumers may e.g. make more informed decisions about which types of OTT services they use, forcing OTT providers to reflect on their policies. Still, the expected effects of enhanced awareness in relation to this objective are expected to be very limited. Awareness does not preclude that:

- Users face different levels of privacy and security when using OTT and ECS services, due to the limits of the ePD; and
- Users cannot provide meaningful consent to the use of their data or might even feel forced to give consent in order to access services in the context of the confidentiality of communications stored on the user's terminal equipment (Article 5.3).
- Users may nevertheless choose services out of indifference or lack of choice in their social environment, thereby displaying indifference to privacy and security aspects.[526]

Increasing funds related to **research and development** in the field of online privacy and security might result in security tools which are simpler to use for citizens than those presently available (e.g. encryption tools for a majority of communications). Yet, the effectiveness of awareness-raising and R&D measures crucially depends on the ability and willingness of citizens to protect their online privacy and security. By emphasising informed actions of consumers, they bear the sole responsibility for the confidentiality of communications.

Although there would be small improvements in relation to the achievement of this objective, the main problems identified in relation to the confidentiality of communications are likely to remain in place or even deteriorate. To recall, the following main issues were identified (see section 7.3.1):

- The confidentiality of users of traditional electronic communications services and the internet to browse online is not ensured based on shortcomings relating to Articles 4, 5, 6 and 9; and
- The confidentiality of users of OTTs in most EU Member States is not ensured because OTTs are excluded from the scope of the ePD or are only covered on a case-by-case basis.

This policy option does not address the shortcomings identified in relation to the provision mentioned nor the scope of the ePD. Therefore, communications via OTT services will continue to differ from ECS communication with respect to confidentiality and security standards in several Member States.

[526] In academic discussions. this has been discussed as the *privacy paradox*: "Based on the warning message, it is possible that some consumers may refrain from using the website/service concerned. At the same time, the behaviour of most consumers is not based solely on privacy risks but to a great extent also on benefits associated with a current service. On this basis, the likelihood that they use another service may depend on the existence of valid alternatives." Source: https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Liu_Privacy-paradox_v10.pdf

Hence, this measure is not expected to result in significant changes from the situation observed under the baseline scenario.

Specific Objective 2: To ensure that citizens are effectively protected against unsolicited marketing communications

With regard to Article 13, **interpretative communications** were considered as at least partially helpful by stakeholders during phone interviews conducted by Deloitte. For example, stakeholders indicated that guidance on the following points may be useful:

- what constitutes unsolicited communications in practice;
- the scope of the content of communications permitted under the present regulation; and
- the timing and adequate format of user consent;

Based on such clarifications, it may be possible that nuisances from unsolicited communications would be slightly decreased. In order to effectively protect citizens from these communications while enabling B2C interaction, guidance would need to specify the boundaries for new formats of communications under the present rules (like customer service chats functions found on websites). Nevertheless, despite additional guidance, citizens still face the same multitude of different opt-in or opt-out regimes across Member States as in the baseline scenario.

Awareness-raising initiatives, that provide information on the Member State regime or promote Robinson lists providing opt-outs from phone marketing, may thus enhance protection from unsolicited communications for citizens. Given that opt-out options are presently dispersed (often depending on standards varying by sectors, marketing channels and compliance of directory service providers), the effectiveness of this measure depends on citizens' willingness and ability for action. Similar to the observations for the specific objective 1, citizens themselves are responsible for their protection in this situation.

Specific Objective 3: To simplify the legal framework and adapt it to the new legal, market and technological reality

As explained in the context of specific objective 1, an increased use of **interpretative communications** would likely to increase harmonisation of standards across the EU. However, as additional guidance does not present binding interpretations for Member States, effective harmonisation in the enforcement ePD provisions is not expected. Even with additional guidance, businesses would still incur costs due to these reasons while citizens would still face the same complex legal environment. Further guidance will not be able to effectively address challenges due to technological developments with regard to the definitions of different types of data (e.g. whether traffic and location data are different data types) and outdated services (e.g. itemised billing in contexts of flat rate models) either.

Common best practices developed in cooperation with industries are expected be experience similar challenges with regard to effectiveness as mentioned for the EU-wide self-regulation initiatives assessed for specific policy objective 1.

Although these measures could produce small improvements of the present situation, neither issuing interpretative communications nor encouraging the adoption of common best practices is likely to reduce:

- The presently existing regulatory gap between ECS and OTT service;

- Challenges for citizens' with regard to unsolicited communication via new communication formats mentioned in the previous section;
- The complexity in relation to other EU instruments; and
- The fact that some of the rules remain outdated and are no longer in line with new technologies.

Supporting **Member State cooperation** might result in a more harmonised legal approach towards services covered by the ePD. The effectiveness of this measure strongly depends on Member States' willingness for cooperation and the forum for this exchange. In the present situation, where for example some Member States have already tried to cover OTT and ECS services under similar national laws while others have not, cooperation might at least enhance common understanding of potential challenges and different approaches to solutions. Nevertheless, this does not necessarily result in a simplified framework. Therefore, some differences in treatment of different technologies within the Digital Single Market are likely to remain. Businesses will thus still incur costs for legal advice and the development of different marketing strategies across Member States in the Single Market.

9.3.4 Social impacts

No significant other impacts are expected.

9.4 Policy Option 2: Limited reinforcement of privacy/confidentiality and simplification

Under this option the Commission would propose minimum changes to the current Directive with a view to adjust privacy and confidentiality provisions and to improve harmonisation and simplification of the current rules.

The specific elements of the policy option can be found in chapter 8.2.

9.4.1 Overview of assessments

In the following table we present an overview of our assessment of policy option 2. The detailed assessment according to the individual assessment criteria can be found in the following sub-sections.

Table 80 – Qualitative rating of the impacts of Policy Option 2

Assessment criteria		Rating	Brief explanation of the rating
Economic impacts			
	Impacts on costs for businesses	1	Business would incur an increase of compliance costs (rated 3) and a decrease in costs for administrative burden (rated -2).
	Impacts on costs for public authorities	0	There would be some additional costs for the European Commission, essentially coinciding with the conduct of the legislative process. Member States would incur some additional costs, which would be countered by some cost savings.
	Other economic impacts	1	This option would have positive impacts on competition, notably based on the extension of the scope to OTTs. At the same time, some stakeholders would incur opportunity

Assessment criteria	Rating	Brief explanation of the rating
		costs (OTTs and other businesses based on the change to Article 13). The impact on SMEs would be mixed.
Effectiveness in reaching the policy objectives		
Objective 1: To ensure effective confidentiality and security of communications	-2	This option brings important improvements, e.g. based on the extension of the scope. However, not all problems are addressed.
Objective 2: To ensure that citizens are effectively protected against unsolicited marketing communications	-2	The clarification of the provision and introduction of a special prefix would bring would bring important improvements. This policy option would, however, not address the varying implementation and enforcement in Member States.
Objective 3: To simplify the legal framework and adapt it to the new legal, market and technological reality	-2	This option would have a positive impact on this objective, notably by clarifying certain provisions, reinforcing the cooperation between competent authorities and repealing the security rules.
Social impacts	0	No significant social impact is expected.
Total	-1	

Source: Deloitte

9.4.2 Economic impacts

In this section on the assessment of the economic impacts of policy option 2, we are focusing on three key aspects: (1) The impacts on compliance costs and administrative burden for businesses (incl. SMEs and micro-enterprises), and (2) on costs for public authorities; as well as (3) other economic impacts such as on competiveness and competition in the Digital Single Market.

Impacts on compliance costs and administrative burden for businesses

In this section, we provide the following:

- ***Part A:*** A detailed qualitative assessment table regarding the impact of each element of the policy option 2; and
- ***Part B:*** The key quantitative findings from the economic analysis in relation to the impact of policy option 2.

The former will feed into the latter with regard to the assessment of the economic impact of the policy option.

Part A: Detailed qualitative assessment tables

A more **detailed qualitative assessment table** regarding the impact of each element of policy option 2 is provided below. The table contains:

- Qualitative reasoning used for the quantitative assessments of the impacts of the policy options on businesses (in particular on compliance costs and costs related to administrative burden);
- An indication of the types of businesses affected by each element;
- Qualitative rating / colour coding of the expected impacts of each element of the options;

- An indication whether or not businesses would incur compliance costs or costs related to administrative burden from each specific element;
- The frequency of costs (as far as information is available); and
- The existence / emergence of opportunity costs in relation to each of the elements of the policy options.

As described in Annex A on the *general approach used to translate qualitative reasoning into quantitative assumptions*, the ratings contained in the below table of this Part B have been used as a qualitative basis for the quantitative assessment of the impacts of the policy options in Part A above.

Table 81 – Qualitative classification of the impacts of policy option 2 on costs for businesses

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
Objective 1: Ensuring effective confidentiality and security of communications						
1. Extension of the scope of the ePD to OTTs providing communications functions, such as webmail, Internet messaging, VoIP.	OTT providers would need to implement the entire ePD. This would entail a review and adaptation of their current data processing practices, which would be based on thorough legal review of the new rules, potentially with external support. Ongoing compliance would also increase.[527] While the costs associated with Art. 5.3 and 13 should already apply to these players now, additional costs would ensue based on the implementation of other provisions (e.g. confidentiality of communications).	OTT	2	x		One-off and recurring
	Administrative burden would not increase significantly, as the main cause of administrative burden (Article 4) will be removed. Some costs may ensue in relation to audits. We note in this context that these businesses will already face some costs in relation to audits based on the new requirements of the General Data Protection Regulation. Thus, while the costs based on the ePD would increase, the actual costs that these business will incur at the end may not change significantly.	OTT	1		x	Recurring
2. Clarify that the ePD applies to publicly available communications networks, such as in particular commercial Wi-Fi networks in stores, hospitals, airports, etc. Only services which occur in an official or employment situation solely	Business may need to spend less time on interpreting the provisions. Potentially, this also decreases the need for legal advice. At the same time, there may be more businesses applying the ePD (e.g. those that previously did not consider their Wi-Fi network or IoT devices	All businesses	0	x		Recurring

[527] Although they may follow some of the requirements, e.g. relating to confidentiality of communications, already now voluntarily, these would then be because of the ePD.

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
for work-related or official purposes, as well as use of services for exclusively domestic purposes, may be exempted.	to be covered).					
3. On the protection of terminal equipment devices: Specify that the protection applies to any machine that is connected to the network (including M2M communications, such as for example, a refrigerator connected to a grocery store web site).	Business may need to spend less time on interpreting the provisions. Potentially, this also decreases the need for legal advice. At the same time, there may be more businesses applying the ePD (e.g. those that previously did not consider their Wi-Fi network or IoT devices to be covered).	All businesses	0	x		Recurring
Objective 2: Ensuring effective protection against unsolicited commercial communications						
4. Clarify the scope of the provision and make it technologically neutral: clarify that it applies to any form of unsolicited electronic communication, irrespective of the technological means used. The provision would apply, for example, also to advertisings messages sent on OTT platforms.	Business may need to spend less time on interpreting the provisions. Potentially, this also decreases the need for legal advice. At the same time, there may be more businesses applying the ePD.	All businesses	0	x		Mainly one-off
5. Mandate the use of a special prefix distinguishing direct marketing calls from other calls.	Some costs may ensue from the obligation to use a specific prefix in order to distinguish direct marketing calls from other calls. These costs relate to (1) the subscription to having such a number; (2) paying the calls issued to customers; and (3) registering such a number with the national telecommunication authority. For one business, this may cause costs of around 500 Euro yearly. We provide further details on this cost estimate in the text box below this table.	All businesses	1	x		One-off & recurring
Objective 3: Simplifying the legal framework and adapting it to the new market and technological reality						
6. Reinforce cooperation obligations among the competent authorities,	This would have no impact on businesses.		0			

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
including for cross-border enforcement						
7. Repeal of the security rules leaving the matter to be regulated by the corresponding rules in the Telecom Framework and the GDPR.	Business would no longer need to deal with personal data breach notifications under the ePD (only under the GDPR).	ECS	-3		x	Recurring
Overall implications (Compliance)			**3**			
Overall implications (Admin burden)			**-2**			
Overall implications on the number of businesses affected	Although OTTs would apply additional provisions compared to the current situation, no significant impact on the overall number of businesses is expected. This is due to the fact that we calculated the number of businesses applying the ePD based on Article 5(3), i.e. all businesses with an active website using cookies. This number is not influenced by this policy option, as Article 5(3) is not changed. At the same time, there will be more businesses applying the provisions directed to electronic communications provider, as the scope of these provisions is extended to OTTs. In addition, Point 4 may lead to a moderate increase of businesses applying the ePD, as it is clarified that the scope of Article 13 is technologically neutral and e.g. also applies to OTTs.		**2**			

Source: Deloitte

Case example (Art. 13): Costs for businesses relating to the use of a special prefix for telephone calls

The use of special prefixes for businesses telephone numbers when they are calling (potential) customers for marketing purposes is associated with costs. These costs relate to (1) the subscription to having such a number; (2) paying the calls issued to customers; and (3) registering such a number with the national telecommunication authority.

In Germany, for instance, there are several businesses that offer solutions regarding the use of special prefixes for marketing communications (so called 0800-numbers). Consumers can call such numbers for free but the operator of the number must pay for the use of this service. Three typical service offerings could, for example, look like this:[528]

Small solution	*Medium solution*	*Large solution*
• 9.90 Euro / month for subscription; • 250 min. / month incl. • Afterwards: 4.5 cent / min. for landline; 14 cent / min. for mobile • One-off cost for registration with service provider: 9.90 Euro • One-off cost for registration with federal agency: 25 Euro	• 19.90 Euro / month for subscription; • 750 min. / month incl. • Afterwards: 4.3cent / min. for landline; 13.5 cent 7 min. for mobile • One-off cost for registration with service provider: 9.90 Euro • One-off cost for registration with federal agency: 25 Euro	• 34.90 Euro / month for subscription; • 1,250 min. / month incl. • Afterwards: 4.1 cent / min. for landline; 13 cent 7 min. for mobile • One-off cost for registration with service provider: 9.90 Euro • One-off cost for registration with federal agency: 25 Euro

To exemplify the costs per for one business that wants / is obliged to make use of a special prefix for marketing communications, it could for instance be assumed that one FTE is working roughly two working weeks (i.e. ten days) on marketing calls. This equals about 4,800 minutes of marketing telephone communication (40 hours per week for two weeks equals 4,800 minutes). For illustrative purposes, we assume that half of these minutes refer to landline calls and the other half to mobile calls. Given the pricing opportunities indicated above, the business would have to incur the following costs for the first year of usage:

Small solution	*Medium solution*	*Large solution*
= 9.90 € * 12 months + (4,800 min. – 250 min.) / 2 * 0.045 € + (4,800 min. – 250 min.) / 2 * 0.14 € + 9.90 € + 25 € = ***574.58 €***	= 19.90 € * 12 months + (4,800 min. – 750 min.) / 2 * 0.043 € + (4,800 min. – 750 min.) / 2 * 0.135 € + 9.90 € + 25 € = ***514.15 €***	= 34.90 € * 12 months + (4,800 min. – 1,250 min.) / 2 * 0.041 € + (4,800 min. – 1,250 min.) / 2 * 0.13 € + 9.90 € + 25 € = ***457.23 €***

Thus, in this illustrative example, the business would choose the „large solution“ as it is less costly than the small solution (457 € vs. 574 €). This estimate only concerns the first year of usage of the special prefix number. Each year afterwards would be a bit less expensive for this illustrative business as costs relating to the one-off registration would not be incurred anymore.

As concerns the types of businesses affected, we note that not all businesses carry out unsolicited marketing calls. Rather, this may be outsourced to specialised businesses with call centres, which would be mainly affected by these costs.

[528] See e.g.: https://www.dtms.de/0800/

Part B: Key quantitative findings from the economic analysis

Policy option 2: Average annual values and changes compared to the current situation

The overall quantitative results of the analysis concerning policy option 2 are presented in Table 73:

- Number of businesses affected (in million);
- Compliance costs (in million Euro);
- Average compliance cost per business (in Euro);
- Administrative burden (in million Euro); and
- Average costs from admin. burden per business (in Euro).

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Annex A: Economic Analysis

Further information in this regard, as well as an explanation of the approach used for the estimation of the quantitative results data is provided in the section on the basic assumptions used for the assessment of the impacts of the policy options in Annex A concerning the Economic Analysis.

The following table presents the quantitative findings for policy option 2. The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Average annual value:* Denotes the average annual value of the quantitative indicator for which data has been estimated. This means, for instance, that 270,000 SMEs are affected by issues relating to the ePD per year (see the light blue cell), facing a total amount of 112 EURm per year (see the light green cell) at an average cost of compliance per business of 409 Euro (see the dark blue cell);
- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the average annual value compared to the baseline scenario (2016-2030); and
- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the average annual value compared to the baseline scenario (i.e. 2016-2030).

Visualisations of the year-over-year development of the quantitative indicators are presented afterwards, as well as overall values for the timeframe 2016-2030.

Table 82 – Key quantitative data estimated in relation to policy option 2 (2016-2030)

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Number of businesses affected (in million)	3.89	0.19	5.0%
Micro-enterprises	3.48	0.166	5.0%
SMEs	0.27	0.013	5.0%
Large enterprises	0.01	-	0.0%
Foreign controlled enterprises	0.13	0.006	5.0%
Compliance costs (in million Euro)	1,558.7 €	203.3 €	15.0%

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Micro-enterprises	1,394.9 €	181.9 €	15.0%
SMEs	111.6 €	14.6 €	15.0%
Large enterprises	3.8 €	0.5 €	15.0%
Foreign controlled enterprises	48.4 €	6.3 €	15.0%
Average compliance cost per business (in Euro)	409.1 €	35.6 €	9.5%
Administrative burden (in million Euro)	0.21 €	-0.02 €	-10.0%
Micro-enterprises	0.16 €	-0.02 €	-9.9%
SMEs	0.03 €	0.00 €	-8.8%
Large enterprises	0.00 €	0.00 €	0.0%
Foreign controlled enterprises	0.01 €	0.00 €	-7.1%
Average costs from admin. burden per business (in Euro)	23.8 €	-4.0 €	-14.3%

Source: Deloitte

Under policy option 2, the analysis shows that – per year between 2016 and 2030 – around 3.9 million businesses will be affected by the ePD in the EU. The majority of these businesses will be micro-enterprises with less than 10 employees (3.5 million). Around 270,000 SMEs that have between 10 and 250 employees are estimated to be affected per year until 2030 while the number of large enterprises is negligible with around 10,000 per year. Approx. 130,000 foreign controlled enterprises that operate in the EU will be affected.[529]

The businesses affected by the ePD are estimated to incur an annual value of 1.56 EURb to comply with Art. 5(3) and Art. 13. In addition, these businesses are expected to incur an unspecifiable amount of additional costs with regard to other provisions such as the consumer provisions. Again, micro-enterprises are expected to incur the lion share of these costs (around 1.39 EURb).

On *average*, an EU business is expected to incur 409 Euro per year with regard to the ePD until 2030. This does, however, not mean that e.g. large enterprises may not incur significantly more costs while the costs may be significantly lower for micro-enterprises.

In addition to the compliance costs related to the direct implementation of the ePD, businesses will also incur significant opportunity costs for lost business opportunities.

In relation to administrative burden, mostly stemming from the notification obligations for telecommunication service providers under Article 4, it has been estimated that an annual amount of 210,000 Euro is incurred, i.e. around 24 Euro per affected business per year.

Policy option 2: Visualisation of the development 2016-2030

In this section, we present visualisations of the development of the following quantitative indicators between 2016 and 2030 under policy option 2:

- The number of businesses affected;
- The compliance costs; and

[529] The estimated numbers of affected businesses should be understood as annual values. However, the overall number of businesses affected by the ePD between 2016 and 2030 is not the sum of each annual value. The reason for this is that the majority of businesses will be affected not only once but on several occasions across this time frame while some businesses will be replaced by others due to the general life cycle of businesses (company birth, insolvency). This means that, in relation to the former argument, the projected value is likely underestimating the actual number of businesses affected, while the latter argument, the projection is likely to overestimate the number of affected businesses.

- The costs from administrative burden.

It has been decided to use such a form of visualisation instead of providing the data by means of tables in order to make the sheer amount of data more accessible to the reader and to clearly be able to show the *development of the quantitative indicators over time* – which is not always easy to spot when looking at raw figures.

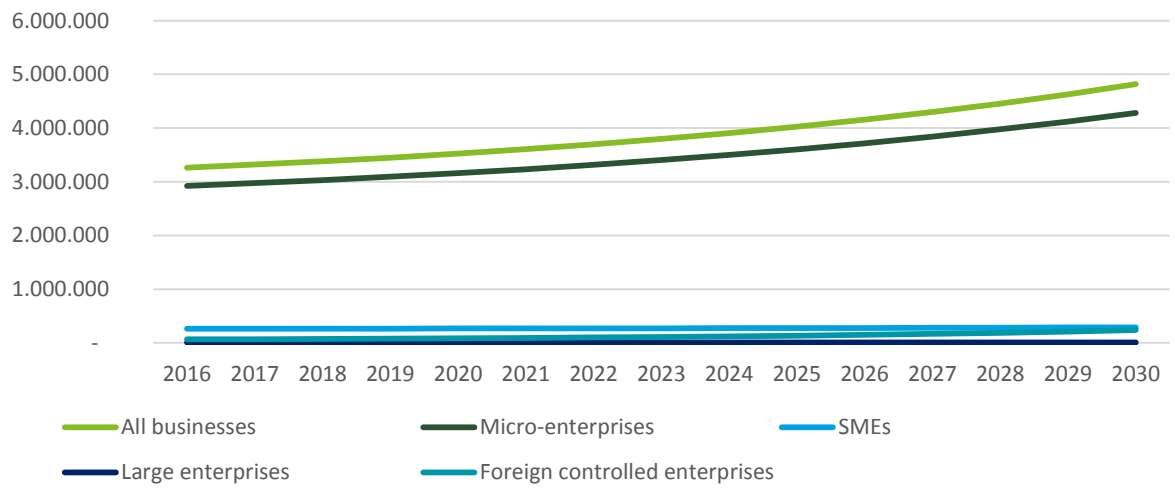
The graphs visualise the data per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Graphical comparisons of the quantitative indicators under each policy option with the baseline scenario are provided in section 9.8.1.

Number of businesses affected under policy option 2

The following two graphs present the development of the number of businesses affected by the ePD under policy option 2. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

Figure 69 – Number of businesses affected by the ePD per year (policy option 2, 2016-2030)

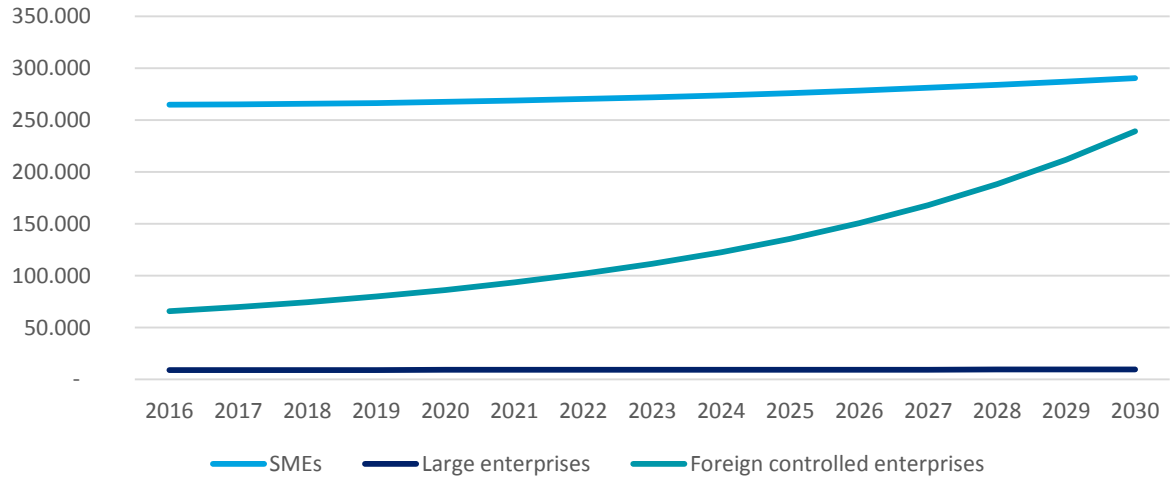


Source: Deloitte

The trends that can be seen from the graphs above and below in relation to the growth of the number of businesses affected by the ePD are similar to those in the baseline scenario:

- The overall number of businesses affected by the ePD is expected to grow from 2016 to 2030
- SMEs, large enterprises, and foreign controlled enterprises are of less importance for the overall growth of the number of businesses affected by the ePD;
- The number of SMEs affected is expected to increase slightly
- The number of large enterprises is expected to remain stable
- The number of foreign controlled enterprises affected by the ePD is expected to increase significantly until 2030

Figure 70 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 2, 2016-2030)

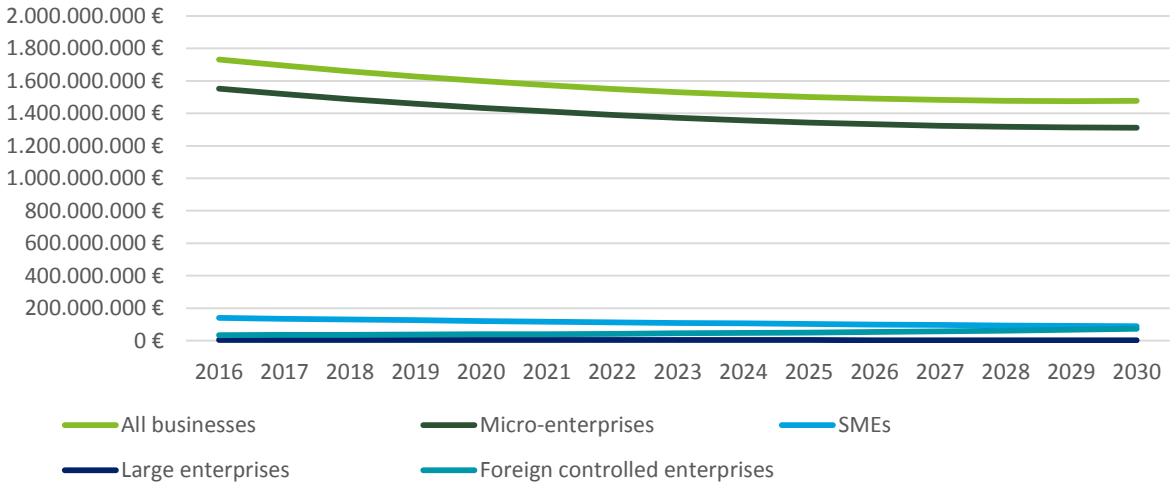


Source: Deloitte

Annual compliance costs under policy option 2

The following two graphs present the development of the annual compliance costs of businesses affected by the ePD under policy option 2. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

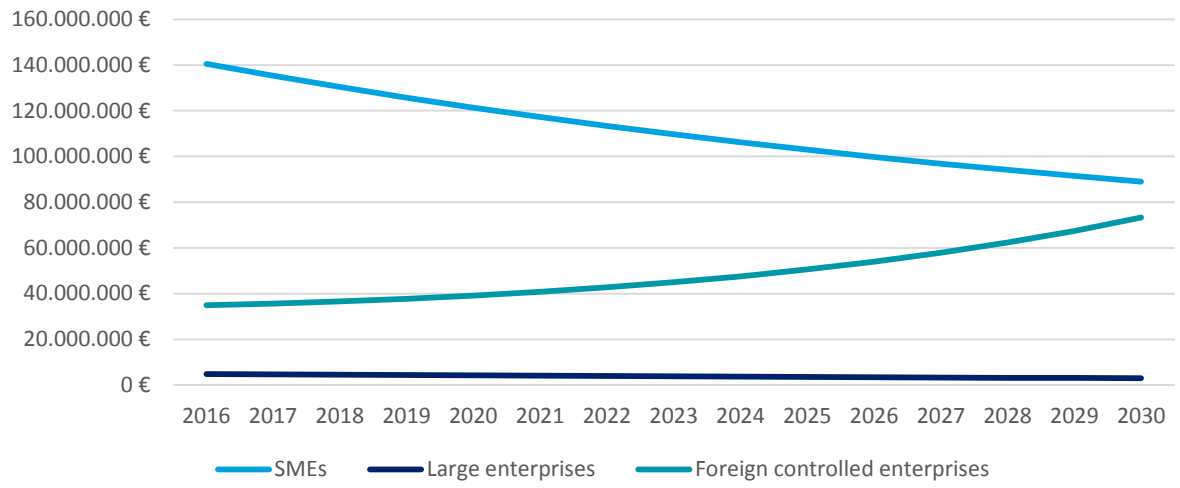
Figure 71 – Compliance costs of businesses affected by the ePD per year (policy option 2, 2016-2030)



Source: Deloitte

The graph above shows the annual overall compliance costs for businesses are expected to decrease until 2030. Looking in more detail at annual overall compliance costs for SMEs, large enterprises, and foreign controlled enterprises (see figure below), it can be seen that – while compliance costs for SMEs are decreasing – they are expected to rise for foreign controlled enterprises and remain relatively stable for large enterprises.

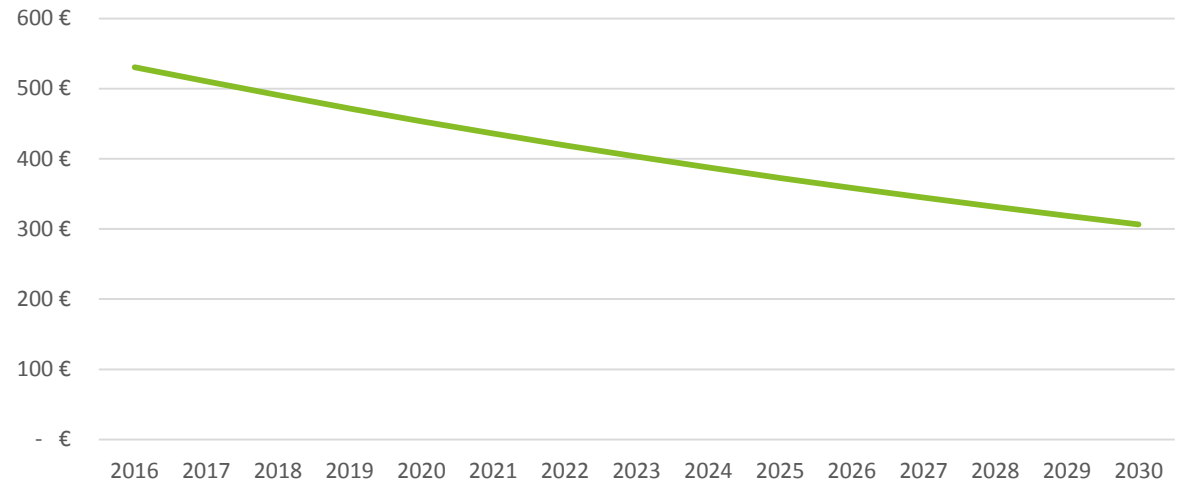
Figure 72 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 2, 2016-2030)



Source: Deloitte

The following graph visualises the development of the average compliance costs for businesses from 2016 to 2030 under policy option 2. No difference has been made between average costs for different size classes of businesses.

Figure 73 – Average compliance costs of per business affected by the ePD per year (policy option 2, 2016-2030)



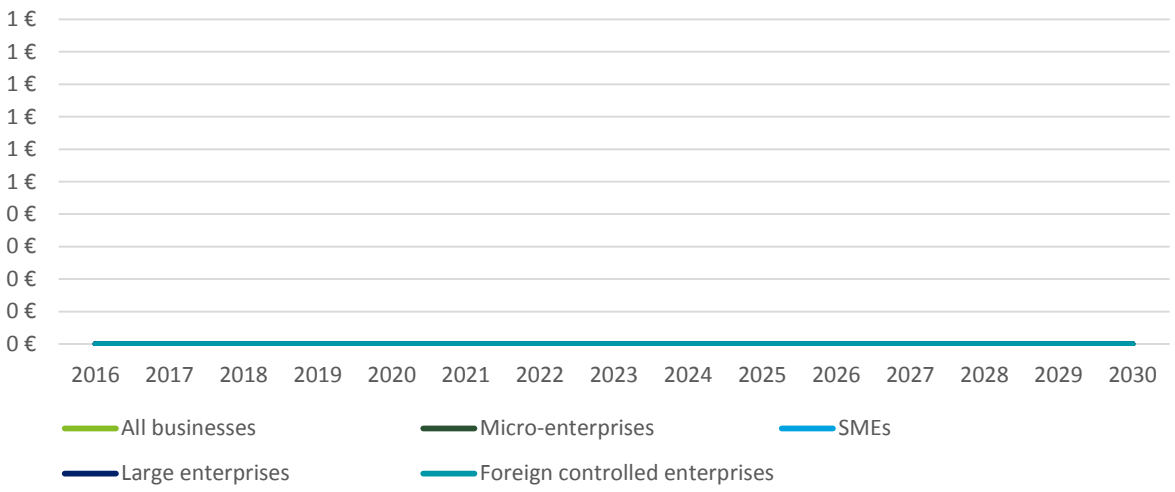
Source: Deloitte

The graph clearly shows that the average compliance costs for businesses are expected to decrease drastically between 2016 and 2030, as at the same time the number of businesses affected by the ePD increases.

Annual costs from administrative burden under policy option 2

The following two graphs present the development of the annual costs from administrative of businesses affected by the ePD under policy option 2. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

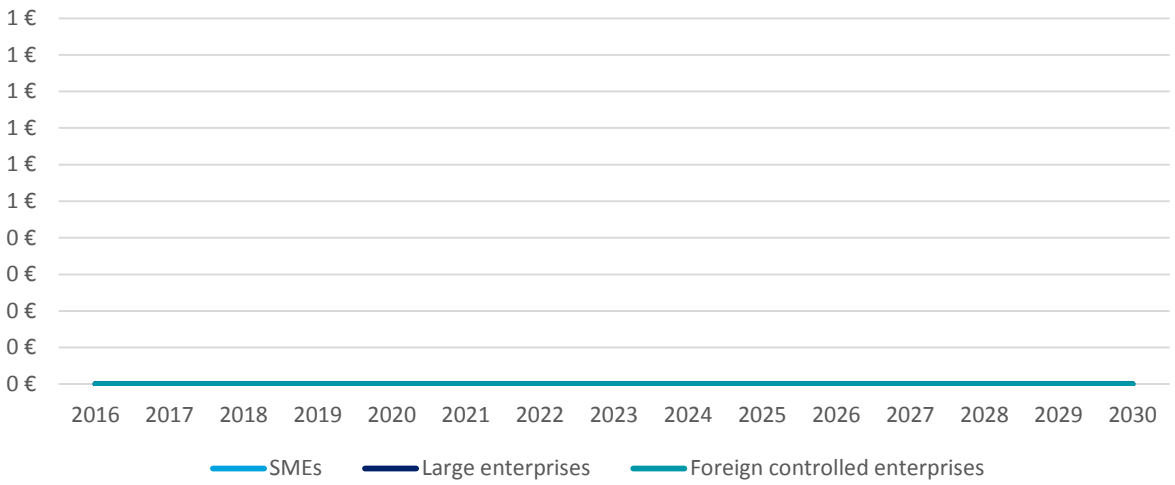
Figure 74 – Costs from administrative burden of businesses affected by the ePD per year (policy option 2, 2016-2030)



Source: Deloitte

Unlike the compliance costs, the costs from overall annual administrative burden are expected to slightly increase over the selected period of time.

Figure 75 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 2, 2016-2030)

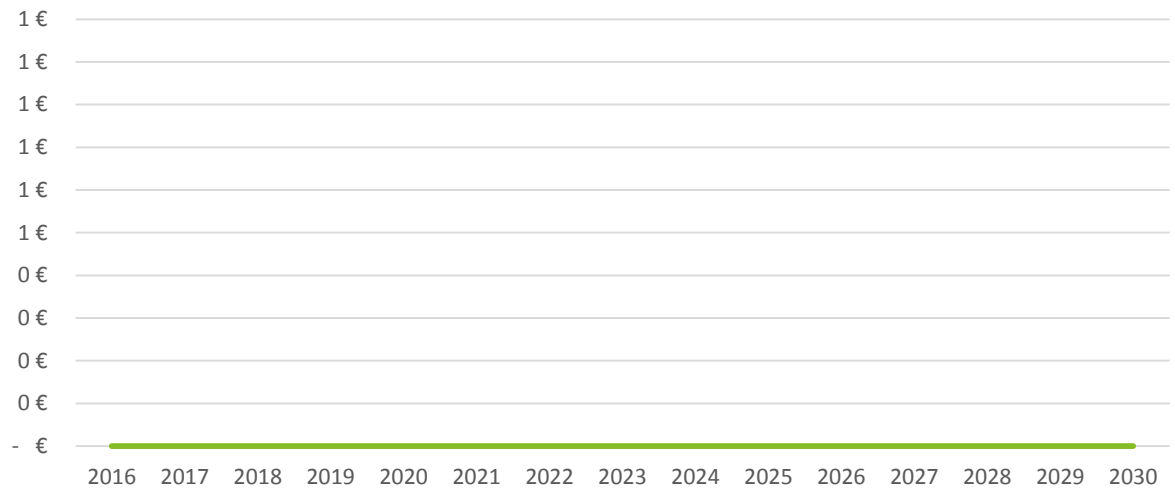


Source: Deloitte

As regards the costs from administrative burden for SMEs, large enterprises, and foreign controlled enterprises, an increase is expected until 2030. For large enterprises the costs are expected to remain stable.

The following graph visualises the development of the average costs from administrative burden for businesses from 2016 to 2030 under policy option 2. No difference has been made between average costs for different size classes of businesses.

Figure 76 – Average costs from administrative burden per business affected by the ePD per year (policy option 2, 2016-2030)



Source: Deloitte

Overall, the above graph shows that a clear reduction of costs from administrative burden is expected across all types of businesses affected by the ePD from 2016 to 2030, as at the same time the number of businesses affected by the ePD increases.

Policy option 2: Overall values 2016-2030

While the above section has presented average annual values, this section provides the key quantitative estimates for the overall time period of 2016-2030 (i.e. the sums of each individual annual value of the time period) under policy option 2 This estimate is relevant to assess the overall costs of compliance and administrative burden stemming from the ePD for different types of businesses.

The following table contains information on:

- Compliance costs (in million Euro); and
- Administrative burden (in million Euro).

The number of businesses affected is not presented as this number is – over the entire time period – subject to double counting.[530] Compared to the above section, average compliance cost per business, as well as average costs from admin. burden per business are not relevant to present in this section as they are *average* values and not *overall* values.

The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Overall value (2016-2030):* Denotes the overall annual value of the quantitative indicator for which data has been estimated. This means, for instance, that all SMEs in the EU together have will incur compliance costs of 1,674 EURm over the entire time period of 2016-2030 (see the light green cell);
- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the overall value between 2016 and 2030 under policy option 2 compared to the overall value under the baseline scenario; and

[530] This is due to the fact that businesses are affected by the ePD over longer time frames than just one year. An alternative way of phrasing this is that the ePD does not affect an entirely different set of businesses each and every year.

- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the overall value between 2016 and 2030 under policy option 2 compared to the overall value under the baseline scenario.

Table 83 – Key quantitative data estimated in relation to policy option 2 (overall 2016-2030)

Quantitative indicator	Overall value (2016-2030)	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Compliance costs (in million Euro)	23,380.3 €	3,049.6 €	15.0%
Micro-enterprises	20,923.7 €	2,729.2 €	15.0%
SMEs	1,673.6 €	218.3 €	15.0%
Large enterprises	57.5 €	7.5 €	15.0%
Foreign controlled enterprises	725.5 €	94.6 €	15.0%
Administrative burden (in million Euro)	3.12 €	-0.3 €	-10.0%
Micro-enterprises	2.44 €	-0.3 €	-10.0%
SMEs	0.46 €	-0.1 €	-10.0%
Large enterprises	0.03 €	0.0 €	-8.8%
Foreign controlled enterprises	0.19 €	0.0 €	-10.0%

Source: Deloitte

Under policy option 2, as can be seen from the table above, businesses are expected to incur more compliance costs and costs from administrative burden between 2016 and 2030 than they would in the baseline scenario.

In absolute terms, compliance costs are expected to increase by 3,050 EURm to 23,380 EURm compared to the overall amount incurred in the baseline scenario. This equals an increase of 15%.

As argued in the REFIT section 6.2.2, the magnitude of the compliance costs should be seen in relation to the overall value of EU GDP. This way, the magnitude of compliance costs is marginal compared to the overall value of the economy.

As regards the costs from administrative burden, reductions are expected to be less pronounced. Overall, it is expected that 300,000 Euro can be saved under policy option 2 between 2016 and 2030 at EU level. This is expected to result in an overall amount of 3.12 EURm of costs from administrative burden. The reduction is expected to be 10% compared to the overall amount incurred in the baseline scenario.

Impacts on costs for public authorities

In the tables below, we provide an assessment of the impacts of policy option 2 on public administrations. The table contains:

- Qualitative reasoning used for the quantitative assessments of the impacts of the policy options on businesses (in particular on compliance costs and costs related to administrative burden) complemented where possible with exact cost estimates;
- A rating of the magnitude of these costs, according to the scheme portrayed below, serving to make the impacts of the options comparable; and
- The frequency of costs (as far as information is available).

The general approach used for these qualitative ratings is outlined in Annex A on the Analysis of the impacts of the policy options on the costs for public administrations.

Table 84 – Qualitative classification of the impacts of policy option 2 on costs for public administrations

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
Objective 1: Ensuring effective confidentiality and security of communications				
1. Extension of the scope of the ePD to OTTs providing communications functions, such as webmail, Internet messaging, VoIP.	As the number of businesses applying the ePD would increase, national authorities may have slightly more to do in terms of correspondence with businesses and carrying out audits. On the other hand, there would be savings based on the clarification provided. For example, one authority indicated that they spend a lot of time (equalling according to their estimate around 2 FTE) on examining questions around the scope. This includes e.g. cases in which OTT providers approach the authority to ask whether the rules of the ePD apply to them or not. Such cases are usually examined by different authorities and thus entail several exchanges and meetings.	MS	-1	Recurring
2. Clarify that the ePD applies to publicly available communications networks, such as in particular commercial Wi-Fi networks in stores, hospitals, airports, etc. Only services which occur in an official or employment situation solely for work-related or official purposes, as well as use of services for exclusively domestic purposes, may be exempted.				
3. On the protection of terminal equipment devices: Specify that the protection applies to any machine that is connected to the network (including M2M communications, such as for example, a refrigerator connected to a grocery store web site).	No specific impact on public administrations is expected.	EU/MS	0	
Objective 2: Ensuring effective protection against unsolicited commercial communications				
4. Clarify the scope of the provision and make it technologically neutral: clarify that it applies to any form of unsolicited electronic communication, irrespective of the technological means used. The provision would apply, for example, also to advertisings messages sent on OTT platforms.	Currently, national authorities spend a significant share of time devoted to the ePD on the rules on unsolicited communications. It is possible that this option would slightly increase this time, for the following reasons: - The number of businesses applying the ePD may slightly increase by the clarification in point 4, possibly leading to a higher number of complaints, and more time spent on audits and correspondence with businesses; and - The number of complaints could increase based on the stricter rules. At the same time, the harmonisation may make the situation easier for businesses, as businesses would face only one legal regime across the EU. This may lead to a lower number of requests from businesses to authorities and a higher compliance rate. An opt-in situation would also be less prone to error. On this basis, it is possible that the number of complaints would decrease. Therefore, overall it is expected that these elements would not	MS	0	Recurring
5. Mandate the use of a special prefix distinguishing direct marketing calls from other calls.				

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
	entail significant impacts on costs.			
Objective 3: Simplifying the legal framework and adapting it to the new market and technological reality				
6. Reinforce cooperation obligations among the competent authorities, including for cross-border enforcement	The impact is expected to be moderate, as the W29 has in the past already dealt with the ePD[531] and authorities are already involved in activities relating to the WP29. Between 2007 and 2015, there were on average around 4 plenary sessions per year. It is expected that the issues relating to the ePD would be discussed at these sessions. It is possible that a bit more time may be spent on working groups relating to the ePD.	MS	1	
	It is possible that some additional resources would be required at the EDPS to coordinate the additional efforts of the European Data Protection Board.	EU	1	
7. Repeal of the security rules leaving the matter to be regulated by the corresponding rules in the Telecom Framework and the GDPR.	The data breach provisions are the only provisions that explicitly require the involvement of authorities. Authorities need to deal with the data breach notifications of businesses, which includes correspondence as well as potentially checking that the service providers implemented appropriate technological protection measures. The actual number of data breaches dealt with varies significantly per Member State.[532] In the Online survey carried out by Deloitte with competent authorities, tasks related to Article 4 were considered among the most time-consuming tasks. Yet, again the actual time spent depends very much on the Member State. For example, as concerns the time to deal with one personal data breach, three authorities indicated that this takes less than one working day, 4 indicated that it takes between 1 day and less than a week and three authorities indicated that takes 1 week or more. On this basis, the overall impact is assumed to be medium.	MS	-2	Recurring
Horizontal aspects				
Drafting legislation	The Commission would need to assign staff to drafting the new piece of legislation and to follow the legislative process. We note that no budget	EU	1	One-off

[531] For example, it adopted opinions in relation to the ePD.
[532] For example, in 2015, the highest number of complaints was reported for Ireland (2317), followed by the UK (550). Sweden (24), Greece (15), Estonia (5), Romania (3) and Belgium (1) followed with significantly less. Cyprus and Croatia reported that no breaches occurred. No information is available for the other Member States.

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
	change is foreseen for this.			
Overall implications (EU)	The costs for the Commission are low and essentially coinciding with the conduct of the legislative process. Costs for the Commission to oversee the functioning of the new instrument would not change significantly compared to the current situation.	**2**		
Overall implications (MS)		**-2**		

Source: Deloitte

Other economic impacts

Based on the **extension of the scope to OTTs**, this option would impact the **competitive relationship between ECS and OTT providers**. While ECS currently face stricter standards, creating a disadvantage vis-à-vis their OTT competitors, this option would ensure that both would be covered by the same standards. This way, competition would be strengthened as ECS providers would no longer be disadvantaged in comparison to OTTs.

At the same time, **OTTs would face stricter standards compared to the current situation**. On this basis, they may need to revise their current business models and data processing practices. In particular, they will no longer be able to rely on other legal bases under this option than consent. In addition to the costs for complying with the new standards (discussed in the section on compliance costs for businesses), this may cause **opportunity costs** in case they need to restrict their business models and practices. These opportunity costs would only be incurred by the OTT providers in Member States that do not yet apply the rules of the ePD to OTTs or only on a case by case basis. An overview of the situation in Member States is provided in the problem assessment in Table 65. In the other Member States, there are some OTT providers which already operate on the basis of consent and transparent practices. For these, the opportunity costs are expected to be smaller, as it is less likely that their business models are not in line with the ePD. Opportunity costs would be higher for those that do not operate on the basis of consent. However, the magnitude of these costs would depend on the circumstances and business models employed by individual businesses.

For example, an ever-increasing number of OTT communication providers has moved to offer end-to-end encryption of messages and calls for users of their service (thus demonstrating basic compatibility with Article 5).[533] While a study by the *Electronic Frontier Foundation* reveals that 35 out of 36 OTT services have implemented this feature to some extent, this does not entail implicit compatibility with all ePD provisions.[534] Indeed, different providers of messaging services may need to implement changes to their privacy policies if the scope of the ePD was extended to them. For example, depending on the design of the privacy policies, the following provisions may require changes:

- **Article 8:** It may be necessary to include features that allow users to hide their number on a per call basis.
- **Article 9:** Additional information may be needed, e.g. in relation to how long location data is stored and it may be necessary to provide for possibilities to refuse the processing of location data.
- **Article 12:** In some messaging services, users upload their phonebooks to servers to establish connections with other users.[535] The data of non-users may be processed as well. In such cases, citizens are thus included in semi-public directories. Citizens are not informed that their number is processed, neither are they able to protect their identity in these quasi-public directories.

[533] A 2015 study conducted by Zang et al. reveals that encryption does not preclude that sensitive data is nevertheless shared with third parties through messaging apps. See: Zang J, Dummit K, Graves J, Lisker P, Sweeney L. (30.10.2015): Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps. *Technology Science*. 2015103001, http://techscience.org/a/2015103001

[534] Electronic Frontier Foundation (2016): Secure Messaging Scorecard, https://www.eff.org/de/node/82654; The EFF is currently revising the scorecard, emphasizing that the list should not be used to guide decisions for using a service. Nevertheless, the outdated version (last update posted on April 5th 2016) serves as a snapshot of trends in the market.

[535] This is e.g. the policy of *WhatsApp*.

With regard to **consent**, OTT providers would need to check their policies and potentially adjust them to ensure they are in line with the provisions of the ePD. We note in this context that the conditions for a valid consent would need to be in line with the GDPR. Although some players have already introduced certain consent mechanisms, these may not be in line with the conditions.[536] On this basis, OTT providers may incur opportunity costs as users may be less inclined to give their consent if they have a more obvious choice. The magnitude of these costs depends on the extent to which the relevant players already comply with the rules of the ePD and the behaviour of users.

Based on the **clarification of the scope of Article 13 on unsolicited communications**, additional businesses may incur opportunity costs. As it would be clarified that Article 13 does not only apply to marketing communications via traditional electronic communications services but also e.g. to ads sent via OTT platforms, an additional number of marketing activities could only be carried out based on consent (either opt-in or opt-out depending on the Member State in question).

Finally, this option would have mixed impacts on **SMEs**. On the one hand, SMEs which qualify as ECS would benefit from a more equal playing ground between ECS and OTTs. SMEs that qualify as OTTs would be affected by the more restrictive rules and namely from the reduced flexibility in the application of the legal grounds for processing personal data other than consent, unless they apply already comparable rules voluntarily.

9.4.3 Effectiveness in reaching the policy objectives

In this section, the effectiveness of policy option 2 in reaching the policy objectives is assessed. It is shown in the following sub-sections that this option would contribute to some extent to the achievement of all specific objectives.

Specific Objective 1: To ensure effective confidentiality and security of communications

The **extension of the scope of the ePD to OTTs** would significantly improve privacy and confidentiality. Citizens would on this basis benefit from equal standards disregarding what type of communication service they use, which would also increase legal certainty and transparency. On this basis, one of the main problems identified hindering privacy and confidentiality (see section 7.3.1) would be addressed.

In addition, the **clarifications** (Points 2 and 3) would have a small positive effect on privacy and confidentiality as the ePD would be applied in additional situations (e.g. publicly available networks and M2M communications).

However, this option does not effectively address all the problems identified in relation to privacy and confidentiality. In particular, the issues identified in relation to Articles 5, 6 and 9 would remain. In addition, while this option aims at improving cross-border enforcement, it does not address the issue

[536] For example, *Facebook* interpreted a simple log-in interpreted as consent to changes to the privacy policy required to expand the business model in 2015 (Shore J., Steinman J. (11.08.2015): Did You Really Agree to That? The Evolution of Facebook's Privacy Policy. Technology Science. 2015081102. http://techscience.org/a/2015081102). *WhatsApp* on the other hand, explicitly asked for user consent to changes in their privacy policy in order to expand their business model in 2016, yet relied on pre-ticked boxes and an expiry date for withdrawing consent for sharing data with affiliated Facebook (WhatsApp FAQ (26.10.2016): How do I choose not to share my account information with Facebook to improve my Facebook ads and products experiences? https://www.WhatsApp.com/faq/general/26000016). In both cases, even though consent is given by users, neither the format nor the implications appear to be in line with the concept of consent employed by the GDPR.

of fragmented implementation of the ePD. On this basis, option 2 would **partially contribute to achieving this objective**.

Specific Objective 2: To ensure that citizens are effectively protected against unsolicited marketing communications

The **clarification of the scope of the provision** would positively contribute to achieving this objective. It would ensure all forms of unsolicited electronic marketing communications would need to be based on consent (opt-in or opt-out). Thus, citizens may receive a reduced number of unsolicited marketing communications via channels previously not explicitly covered, such as email or OTTs.

The **introduction of a special prefix** would also contribute positively to achieving this objective. It would potentially increase transparency for citizens as they would be able to directly recognise a marketing call, giving them e.g. the option of not answering. It may also support the effectiveness of enforcement as it would be easier to distinguish unsolicited marketing calls. We note in this context that the actual usefulness of this change would require citizens to use a phone and contract allowing them to see the number calling them. For example, some fixed phones do not have this feature. It is, however, assumed that the majority of citizens do use the relevant equipment/contract and are thus able to see the number of a caller. Considering the example of telephones, the vast majority of telephones on the market nowadays do have a display allowing for the identification of the caller ID, including for example phones specifically designed for the elderly. There are only very few phones that do not have a display to show the caller's ID. These are usually special vintage phones, which citizens buy because of their style. Thus, it can be assumed that citizens who do not have a phone with a display usually made an aware choice to get a vintage phone or to try and evade digitalisation. There may also be some citizens who simply did not see the need in buying a new phone for a very long time. It can reasonably be assumed that these groups are not are not likely to acquire the relevant equipment/contract because of the change of the ePD and to better distinguish marketing calls. Indeed, if they would find this matter important, they may also change their equipment in the current situation. The same applies to citizens who do not have a phone contract offering this function or who have so far not chosen to make use of this service, e.g. because their service provider does not offer this function for free. On this basis, while citizens can only benefit from this measure if they have the right equipment and contract, this measure would not cause any additional costs for citizens.

This policy option would, however, not address the varying implementation and enforcement in Member States.

Specific Objective 3: To simplify the legal framework and adapt it to the new legal, market and technological reality

The **clarification of the rules** (Points 2, 3 and 4) would reduce the risk of divergent transposition and implementation by Member States, which was considered by stakeholders as one of the most serious problems. In addition, it helps adapting the legal framework to the technological reality, as the coverage of specific technologies is explicitly regulated.

In addition, **reinforcing the cooperation between competent authorities** would have positive effects as it may lead to a more consistent enforcement, including on cross-border cases. The actual effect of this option would depend on the type of rules introduced.

The **repeal of the security rules** would further contribute to reducing complexities of the legal framework, in particular the duplication of notification scheme.

9.4.4 Social impacts

No significant social impact is expected.

9.5 Policy Option 3: Measured reinforcement of privacy/confidentiality and simplification

Under this option, the Commission would propose **a new ePrivacy legal instrument,** complementing and particularising the GDPR.

The specific elements of the policy option can be found in chapter 8.2.

In relation to changes to Article 5(3), Policy option 3 consists of three sub-options in relation to which alternative quantitative and qualitative assessments were carried out:

- *"Browser solution":* Consent for the storing of information on users' terminal equipment would be organised via browsers. The affected businesses are the browser operators, as well as additional businesses of different size classes that would have to implement any technical solutions e.g. in order for their websites to be able to communicate with the browser.
- *"Tracking companies solution":* Consent for the storing of information on users' terminal equipment would be organised by the companies placing tracking cookies. The affected businesses are the browser operators and those companies that place tracking cookies, as well as additional businesses of different size classes that would have to implement any technical solutions in order for their websites to comply.
- *"Publisher solution":* Consent for the storing of information on users' terminal equipment would be organised by the publishers. All businesses of different size classes would be affected, similarly to the baseline scenario.

For each of these different solutions, separate sections have been prepared in relation to the key quantitative findings from the economic analysis.

9.5.1 Overview of assessments

In the following table we present an overview of our assessment of policy option 3. The detailed assessment according to the individual assessment criteria can be found in the following sub-sections.

Table 85 – Qualitative rating of the impacts of Policy Option 3

Assessment criteria	Rating			Brief explanation of the rating
	"Browser solution"	"Tracking company solution"	"Publisher solution"	
Economic impacts				
Impacts on costs for businesses	-8	-6	-5	While some new cost elements would apply, businesses would overall incur less compliance costs and administrative burden compared to the baseline scenario. Significant savings would in particular be incurred due to the changes to Article 5(3) and the introduction of additional exceptions. Cost savings would be largest in the browser solution.
Impacts on costs for public authorities	3	3	3	This option would entail some additional costs for the EU, e.g. related to the drafting of standards (rated at 3) and some cost savings for the Member States, e.g. related to the

Assessment criteria	Rating			Brief explanation of the rating
	"Browser solution"	"Tracking company solution"	"Publisher solution"	
				repeal of the security provisions (rated at -1).
Other economic impacts	1	1	1	This option would have positive impacts on competition, notably based on the extension of the scope to OTTs. At the same time, some stakeholders would incur opportunity costs (OTTs and other businesses based on the change to Article 13). The impact on SMEs would be mixed.
Effectiveness in reaching the policy objectives				
Objective 1: To ensure effective confidentiality and security of communications	-3	-3	-3	This option brings important improvements, e.g. based on the extension of the scope and the proposed changes to Article 5(3).
Objective 2: To ensure that citizens are effectively protected against unsolicited marketing communications	-3	-3	-3	The clarification of the provision and introduction of a special prefix would bring would bring important improvements. In addition, the imposition of the opt-in consent would increase the protection of users who would benefit from more transparent and effective rules across the EU.
Objective 3: To simplify the legal framework and adapt it to the new legal, market and technological reality	-3	-2	-2	This option would have a positive impact on this objective, notably by clarifying certain provisions, reinforcing the cooperation between competent authorities and repealing the security rules. An additional significant supporting factor for this objective is the fact that the new instrument would be a Regulation.
Social impacts	0	0	0	No significant social impacts are expected.
Total	-13	-10	-9	

Source: Deloitte

9.5.2 Economic impacts

Within this section on the assessment of the economic impacts of policy option 3, we are focusing on three key aspects: (1) The impacts on compliance costs and administrative burden for businesses (incl. SMEs and micro-enterprises), and (2) on costs for public authorities; as well as (3) other economic impacts such as on competiveness and competition in the Digital Single Market.

Impacts compliance costs and administrative burden for businesses

In this section, we provide the following:

- ***Part A:*** Detailed qualitative assessment tables regarding the impact of each element of all three solutions of the policy options.
- ***Part B:*** The key quantitative findings from the economic analysis in relation to the impact of policy option 3:
  - Part B*1:* "Browser solution"
  - Part B2: "Tracking company solution";
  - Part B3: "Publishers solution"; and

The former will feed into the latter with regard to the assessment of the economic impact of the policy option.

Part A: Detailed qualitative assessment tables

A more **detailed qualitative assessment table** regarding the impact of each element of policy option 3 is provided below. The table contains:

- Qualitative reasoning used for the quantitative assessments of the impacts of the policy options on businesses (in particular on compliance costs and costs related to administrative burden);
- An indication of the types of businesses affected by each element;
- Qualitative rating / colour coding of the expected impacts of each element of the options;
- An indication whether or not businesses would incur compliance costs or costs related to administrative burden from each specific element;
- The frequency of costs (as far as information is available); and
- The existence / emergence of opportunity costs in relation to each of the elements of the policy options.

As described in Annex A on the *general approach used to translate qualitative reasoning into quantitative assumptions*, the ratings contained in the below table of this Part B have been used as a qualitative basis for the quantitative assessment of the impacts of the policy options in Part A above.

Table 86 – Qualitative classification of the impacts of policy option 3 on costs for businesses

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
Objective 1: Ensuring effective confidentiality and security of communications						
1. The new instrument would propose a technology neutral definition of electronic communications, encompassing all the additional elements under **Option 2** (1, 2 and 3). It would specify a general principle of confidentiality of communications (i.e. nobody can process data relating electronic communications), except with the consent of the parties to a communication.	See below.					
i. Extension of the scope of the ePD to OTTs providing communications functions, such as webmail, Internet messaging, VoIP.	OTT providers would need to implement the entire ePD. This would entail a review and adaptation of their current data processing practices, which would be based on thorough legal review of the new rules, potentially with external support. Ongoing compliance would also increase.[537] While the costs associated with Art. 5.3 and 13 should already apply to these players now, additional costs would ensue based on the implementation of other provisions (e.g. confidentiality of communications).	OTT	1	x		One-off and recurring
	Administrative burden would not increase significantly, as the main cause of administrative burden (Article 4) will be removed. Some costs may ensue in relation to audits. We note in this context that these businesses will already face some costs in relation to audits based on the new	OTT	1		x	Recurring

[537] Although they may follow some of the requirements, e.g. relating to confidentiality of communications, already now voluntarily, these would then be because of the ePD.

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
	requirements of the General Data Protection Regulation. Thus, while the costs based on the ePD would increase, the actual costs that these business will incur at the end may not change significantly.					
ii. Clarify that the ePD applies to publicly available communications networks, such as in particular commercial Wi-Fi networks in stores, hospitals, airports, etc. Only services which occur in an official or employment situation solely for work-related or official purposes, as well as use of services for exclusively domestic purposes, may be exempted.	Business may need to spend less time on interpreting the provisions. Potentially, this also decreases the need for legal advice. At the same time, there may be more businesses applying the ePD (e.g. those that previously did not consider their Wi-Fi network or IoT devices to be covered).	All businesses	0	x		Recurring
iii. On the protection of terminal equipment devices: Specify that the protection applies to any machine that is connected to the network (including M2M communications, such as for example, a refrigerator connected to a grocery store web site).	Business may need to spend less time on interpreting the provisions. Potentially, this also decreases the need for legal advice. At the same time, there may be more businesses applying the ePD (e.g. those that previously did not consider their Wi-Fi network or IoT devices to be covered).	All businesses	0	x		Recurring
2. Clarify that **consent can be given by means of the appropriate settings** of a browser or other application. Consent under this option will be in line with the concept of consent under the GDPR[538]. Require browsers	The businesses concerned need to implement privacy-friendly settings. We note that at least some browsers already offer such functions. The extent to which these would have to be updated depends on the exact specifications mandated by the Commission and the solution	Providers of browsers	1	x		Mainly one-off

[538] See Recital 32 of the GDPR: "*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website,* ***choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed***

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
and/or other similar platforms to provide their products and services with **privacy friendly settings to reinforce user's control** over the flow of data from and into their terminal equipment. This may also entail addressing the interactions between web sites, advertisers and users regarding whether they accept to be tracked, for example there may be a situation where a user may have set a default privacy setting rejecting third party cookies and thus disallowing the tracking but the user is ready to accept third party cookies/tracking from a particular tracking. This option does not provide for a **prohibition of the practice of denying access to a website** or an **online service** in case users do not provide consent to third party cookies/tracking. Under the new instrument, the Commission would be empowered to issue delegated acts or to mandate industry standards under EU rules (e.g. Radio Equipment Directive) to impose these requirements.[539]	taken with respect to settings for individual websites. Slightly higher costs for providers of browsers would emerge if solution 1 is adopted, i.e. if all communication would run via the browsers. Browsers would then need to implement functions that enable the users to diverge from their default settings for individual websites. However, such solutions already exist, which is why it can be expected that they would be relatively easy to implement. In general, this element only concerns a small fraction of all businesses applying the ePD. The browser market itself is highly concentrated in Europe: Users of *Google*'s *Chrome* browser account for a half of all website visitors, while close to a third of all users relies on Safari and Firefox. Four major companies dominate the market of browsers used by consumers: 94% of all website visitors in Europe rely on software from *Google* (*Chrome*, *Android browser*), *Apple* (*Safari*), *Microsoft* (*IE*, *Edge*, *IEMobile*) and *Mozilla* (*Firefox*). There are some additional browser operators with smaller market shares, including e.g. *Opera* and *Yandex*.[540] On this basis, an overall moderate increase for browsers may be expected for all three solutions.					
NB: There are different potential technical solutions to facilitate users to diverge from their default setting for individual websites,	***Additional impacts for solution 1 (browser solution)***					
	Assuming that the communication would exclusively run via the browsers, all the costs	Website operators	-3	x		

***processing of his or her personal data**. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided*."

[539] Regulation 1025/2012/EU, OJ L 316, 14.11.2012, p. 12–33.

[540] Data for geographic Europe only, based on visitors of a sample of 3 million websites globally accessible on http://gs.statcounter.com/

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
all with different implications on costs. The following scenarios exist: (1) All communication runs centralised via the browsers ("browser solution"); (2) The party placing the cookie is responsible for asking the consent ("tracking company solution"); (3) Individual websites are responsible for asking the consent ("publishers solution").	would lie with the browser providers (as reflected above). Websites on the other hand, would have no specific costs. Thus, in comparison to the current situation, websites would save the costs they incur now to implement the cookie banner. As this is considered the main cost associated for businesses with the ePD, this would be a significant decrease.					
In agreement with the Commission, we provide alternative assessments for these three points.	***Additional impacts for solution 2 (tracking company solution)***					
	Websites would have no specific costs. Thus, in comparison to the current situation, websites would save the costs they incur now to implement the cookie banner. As this is considered the main cost associated for businesses with the ePD, this would be a significant decrease.	Website operators	-3	x		
	In this scenario, the costs would lie with the companies placing the data. It is expected that this would be slightly more expensive compared to solution 1, as a higher number of businesses would be concerned. Although most tracking cookies are placed by few main players, other smaller players will be affected as well. Furthermore, this solution would require the development of new practical and technical solutions to implement the option.	The parties placing the cookie	2	x		
	Additional impacts for solution 3 (publisher solution)					
	In this case, there would be no significant changes for website operators, as they would in principle still employ cookie banners (or a similar technical solution).	Website operators	0			
3. Impose enhanced transparency requirements on entities processing	All businesses would need to check whether this provision applies to them. Those	All businesses	1	x		Mainly one-off

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
communications data (e.g., websites, mobile apps and Wi-Fi), by obliging them to display a concise privacy warning message (e.g. informing users accessing free online services that "the service is financed by OBA and the users' browsing data will be used for this purpose"). The Commission would have implementing powers to specify the exact form and content of the message to be displayed.	businesses processing or monitoring the usage of terminal equipment would need to update their website to implement the new message. As it is just a notification and not a consent mechanism, this should be relatively easy to implement. In addition, it is assumed that the number of businesses concerned would be smaller compared to the status quo, as not all websites using cookies would need to implement this banner, but only specific types of websites.	processing or monitoring the usage of terminal equipment				
4. Reinforce and streamline enforcement powers: The new instrument would lay down effective investigation and enforcement powers of national competent authorities. This would address the problems of ineffective and inconsistent enforcement.	There are no direct costs stemming from this element. There may be small savings based on the increased clarity as to the competent authority. The costs associated with penalties cannot be estimated as these would occur only in case of breaches. We also note that some penalties already exist in Member States.	All businesses	0	x	x	One-off & recurring
Objective 2: Ensuring effective protection against unsolicited communications						
5. All the measures from 4 to 5 under **Option 2**.	See below.					
i. Clarify the scope of the provision and make it technologically neutral: clarify that it applies to any form of unsolicited electronic communication, irrespective of the technological means used. The provision would apply, for example, also to advertisings messages sent on OTT platforms.	Business may need to spend less time on interpreting the provisions. Potentially, this also decreases the need for legal advice. At the same time, there may be more businesses applying the ePD.	All businesses	0	x		Mainly one-off
ii. Mandate the use of a special prefix distinguishing direct	Some costs may ensue from the obligation to use a specific prefix in order to distinguish	All businesses	1	x		One-off & recurring

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
marketing calls from other calls.	direct marketing calls from other calls. These costs relate to (1) the subscription to having such a number; (2) paying the calls issued to customers; and (3) registering such a number with the national telecommunication authority. For one business, this may cause costs of around 500 Euro yearly. We provide further details on this cost estimate in the text box below Table 81.					
6. Require opt-in consent for all types of unsolicited communications, while keeping the existing business relationships exception for email.[541]	The businesses in Member States that currently apply the opt-out regime would need to revise their practices and update the mechanisms they use to obtain consent. This would entail e.g. the technical implementation of consent boxes on their websites. However, the practices would only change in some of the Member States. In Member States that already apply the opt-in regime, no additional costs would ensue. As concerns the ongoing costs, it is expected that they are similar under both regimes. Furthermore, some cost savings may be expected as the situation will be simplified due to harmonisation. Therefore, businesses operating in different Member States would no longer need to implement different regimes. On this basis, an overall moderate increase is expected.	All businesses	1	x		One-off & recurring
7. Clarify the provision on presentation of calling line identification to include the right of users to reject calls from specific numbers (or categories of	No costs for businesses are expected to be associated with this element as it does not entail changing the current technical systems in place with regard to calling line identification		0			

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
numbers).	and there is no need to introduce a new system.					
Objective 3: Simplifying the legal framework and adapting it to the new market and technological reality						
8. Propose changes aimed at **clarifying and minimising the margin of manoeuvre of certain provisions** identified by stakeholders as a source of confusion and legal uncertainty.[542]	There would be cost savings in relation to legal advice for businesses operating cross-border, as they would no longer need to deal with different legal framework. There would also be savings, as businesses would no longer need to implement different rules.	All businesses	-3	x		Recurring
9. Consider introducing consistency mechanisms for the ePrivacy rules.	There may be some small cost savings as it may be clearer for businesses which authority they need to contact and as interchanges with authorities may be simplified.	All businesses	-1		x	
10. Repeal provisions on security, automatic call forwarding and the provisions on itemised billing.	Business would no longer need to deal with personal data breach notifications under the ePD (only under the GDPR).	ECS	-3		x	
	Small savings for businesses already applying Article 4. These savings would e.g. relate to the maintenance of systems. However, we note that similar costs may be incurred based on the GDPR. There would be no significant cost savings relating to the provision on itemised billing, as recurring costs are negligible based on feedback received from businesses.	Mainly ECS	-1	x		Recurring
11. Repeal the provisions on traffic data and location data to reflect the fact that the traffic and location data are more and more a homogeneous category, both in terms of privacy intrusiveness and technological availability. The processing of traffic and location data will be regulated	Possibly, there would be some small time savings / savings of legal advice due to simplifications. At the same time, the practices would need to be checked.	All businesses	0	x		

[542] This would cover in particular more detailed rules on the scope of the ePrivacy instrument, the exceptions to the consent requirements and the scope of the unsolicited communications provisions.

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
under the general provision of confidentiality of communications.						
12. Specify that service providers can only process communications data with the consent of the users, although they are allowed to refuse access to the services in the absence of consent. Providing for additional/broadened exceptions to the consent and enhanced transparency rules (points 1, 2 and 3 above) for specific purposes which give rise to little or no privacy risks:	See below.					
a. Transmission or service: the processing of communications data is necessary for the purpose of the transmission of the communication or for providing a service requested by the user.	No significant costs would occur, as this is similar to the current exceptions.		0	x		One-off & recurring
b. Security: the processing of traffic data is necessary to protect, maintain and manage the technical security of a network or service, with appropriate privacy safeguards.	This would lead a simplification, resulting in fewer businesses that need to apply the provisions mentioned.	All businesses	-1	x		One-off & recurring
c. Billing: in line with the current provision on traffic data, communications data may be retained insofar as necessary for billing or network management purposes.	No cost-related impact is expected.	All businesses	0	x		

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
d. For a lawful business practice provided For a lawful business practice provided that there are no significant risks for the privacy of individuals. In particular, the data collection is performed solely by the entity concerned or third-parties on behalf of the ECS for the purpose of web analytics and web measurement.	On this basis, the number of businesses that need to obtain consent for using cookies would decrease significantly. On average, the businesses falling under this exception may thus be assumed to save 300 Euro per year.		-3	x		
Aspect common to all above exceptions.	In case of an audit, providers would need to be able to demonstrate compliance with the exceptions. This could lead to high compliance costs in relation to legal advice.	All businesses	1		x	One-off & recurring
Overall implications (Compliance)	**Scenario 1 (Browsers)**		**-6**			
	Scenario 2 (Parties placing the cookies)		**-4**			
	Scenario 3 (Websites)		**-3**			
Overall implications (Admin burden)			**-2**			
Overall implications on the number of businesses affected	Based on the new exceptions, the website that use non-privacy invasive cookies would no longer be affected by the consent rule. Based on current statistics, this would lead to a 30% decrease. In addition, depending on the selected technical implementation (scenario 1-3), the number could be reduced in addition. A further decrease is possible based on the possibility to introduce adequate safeguards. The magnitude of this impact is unknown, as it depends on the types of safeguards employed and the willingness of businesses to implement these. The selected value is the result of the exceptions, as well as the implementation of a specific technical solution, and the possibility to introduce adequate safeguards.		**-8**			

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
	At the same time, Point 5(i) may lead to a moderate increase of businesses applying the ePD, as it is clarified that the scope of the provision is technologically neutral and e.g. also applies to advertisings on OTT platforms. In addition, it can be expected that a larger number of businesses would have to implement Art. 5(1) due to the extension of the ePD to OTTs. Overall, however, the number of businesses is still expected to decrease significantly.-					

Source: Deloitte

Part B1: "Browser solution" – Key quantitative findings from the economic analysis

Policy option 3 ("Browser solution"): Average annual values and changes compared to the current situation

The overall quantitative results of the analysis concerning policy option 3 ("browser solution") are presented in Table 73:

- Number of businesses affected (in million);
- Compliance costs (in million Euro);
- Average compliance cost per business (in Euro);
- Administrative burden (in million Euro); and
- Average costs from administrative burden per business (in Euro).

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Annex A: Economic Analysis

Further information in this regard, as well as an explanation of the approach used for the estimation of the quantitative results data is provided in the section on the basic assumptions used for the assessment of the impacts of the policy options in Annex A concerning the Economic Analysis.

The following table presents the quantitative findings for policy option 3 ("browser solution"). The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Average annual value:* Denotes the average annual value of the quantitative indicator for which data has been estimated. This means, for instance, that 13,000 SMEs are affected by issues relating to the ePD per year (see the light blue cell), facing a total amount of 406.6 EURm per year (see the light green cell) at an average cost of compliance per business of 2,241 Euro (see the dark blue cell);
- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the average annual value compared to the baseline scenario (2016-2030); and
- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the average annual value compared to the baseline scenario (i.e. 2016-2030).

Visualisations of the year-over-year development of the quantitative indicators are presented afterwards, as well as overall values for the timeframe 2016-2030.

Table 87 – Key quantitative data estimated in relation to policy option 3 ("browser solution", 2016-2030)

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Number of businesses affected (in million)	0.185	-3.52 €	-95.0%
Micro-enterprises	0.166	-3.15 €	-95.0%

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
SMEs	0.013	-0.25 €	-95.0%
Large enterprises	0	-0.01 €	-100.0%
Foreign controlled enterprises	0.006	-0.12 €	-95.0%
Compliance costs (in million Euro)	406.6 €	-948.8 €	-70.0%
Micro-enterprises	363.9 €	-849.1 €	-70.0%
SMEs	29.1 €	-67.9 €	-70.0%
Large enterprises	1.0 €	-2.3 €	-70.0%
Foreign controlled enterprises	12.6 €	-29.4 €	-70.0%
Average compliance cost per business (in Euro)	2,240.9 €	1,867.4 €	500.0%[543]
Administrative burden (in million Euro)	0.208 €	-0.023 €	-10.0%
Micro-enterprises	0.163 €	-0.018 €	-9.9%
SMEs	0.031 €	-0.003 €	-8.8%
Large enterprises	0.002 €	0.000 €	0.0%
Foreign controlled enterprises	0.013 €	-0.001 €	-7.1%
Average costs from admin. burden per business (in Euro)	499.5 €	471.8 €	1700.0%

Source: Deloitte

Under policy option 3 ("browser solution"), the analysis shows that – per year between 2016 and 2030 – around 185,000 businesses will be affected by the ePD in the EU. The majority of these businesses will be micro-enterprises with less than 10 employees (166,000). Around 13,000 SMEs that have between 10 and 250 employees are estimated to be affected per year until 2030 while the number of large enterprises is negligible with. Approx. 6000 foreign controlled enterprises that operate in the EU will be affected.[544]

The businesses affected by the ePD are estimated to incur an annual value of 407 EURm to comply with Art. 5(3) and Art. 13. In addition, these businesses are expected to incur an unspecifiable amount of additional costs with regard to other provisions such as the consumer provisions. Again, micro-enterprises are expected to incur the lion share of these costs (around 364 EURm).

On *average*, an EU business is expected to incur 2,241 Euro per year with regard to the ePD until 2030.

In addition to the compliance costs related to the direct implementation of the ePD, businesses will also incur significant opportunity costs for lost business opportunities.

[543] This increase of the average compliance cost per business (in Euro) by 500% is explained by the following reasoning: While it is expected that the policy option reduces the number of affected businesses by 95%, the overall costs are only expected to decrease by 70%. This means that the financial burden would have to be shouldered by less businesses (in relative terms) compared to the baseline scenario. This means that each business is expected to incur, on average, more costs under this policy option than in the baseline scenario. Overall, however, the compliance costs are still expected to be lower under this policy option than in the baseline scenario.

[544] The estimated numbers of affected businesses should be understood as annual values. However, the overall number of businesses affected by the ePD between 2016 and 2030 is not the sum of each annual value. The reason for this is that the majority of businesses will be affected not only once but on several occasions across this time frame while some businesses will be replaced by others due to the general life cycle of businesses (company birth, insolvency). This means that, in relation to the former argument, the projected value is likely underestimating the actual number of businesses affected, while the latter argument, the projection is likely to overestimate the number of affected businesses.

In relation to administrative burden, mostly stemming from the notification obligations for telecommunication service providers under Article 4, it has been estimated that an annual amount of 210,000 Euro is incurred, i.e. around 500 Euro per affected business per year.

Policy option 3 ("browser solution"): Visualisation of the development 2016-2030

In this section, we present visualisations of the development of the following quantitative indicators between 2016 and 2030 under policy option 3 ("browser solution"):

- The number of businesses affected;
- The compliance costs; and
- The costs from administrative burden.

It has been decided to use such a form of visualisation instead of providing the data by means of tables in order to make the sheer amount of data more accessible to the reader and to clearly be able to show the *development of the quantitative indicators over time* – which is not always easy to spot when looking at raw figures.

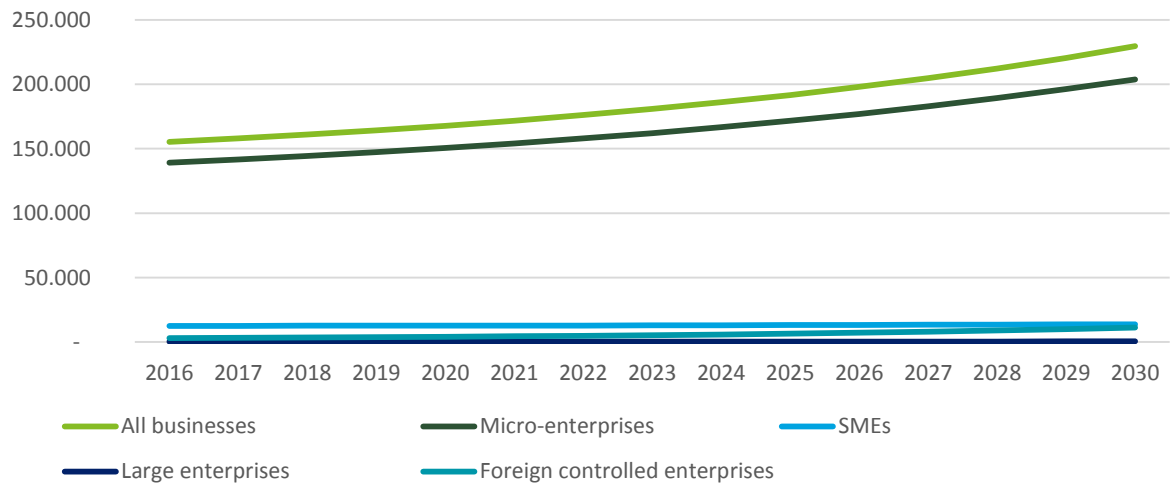
The graphs visualise the data per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Graphical comparisons of the quantitative indicators under each policy option with the baseline scenario are provided in section 9.8.1.

Number of businesses affected under policy option 3 ("Browser solution)

The following two graphs present the development of the number of businesses affected by the ePD under policy option 3 ("Browser solution"). While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

Figure 77 – Number of businesses affected by the ePD per year (policy option 3, "Browser solution" 2016-2030)



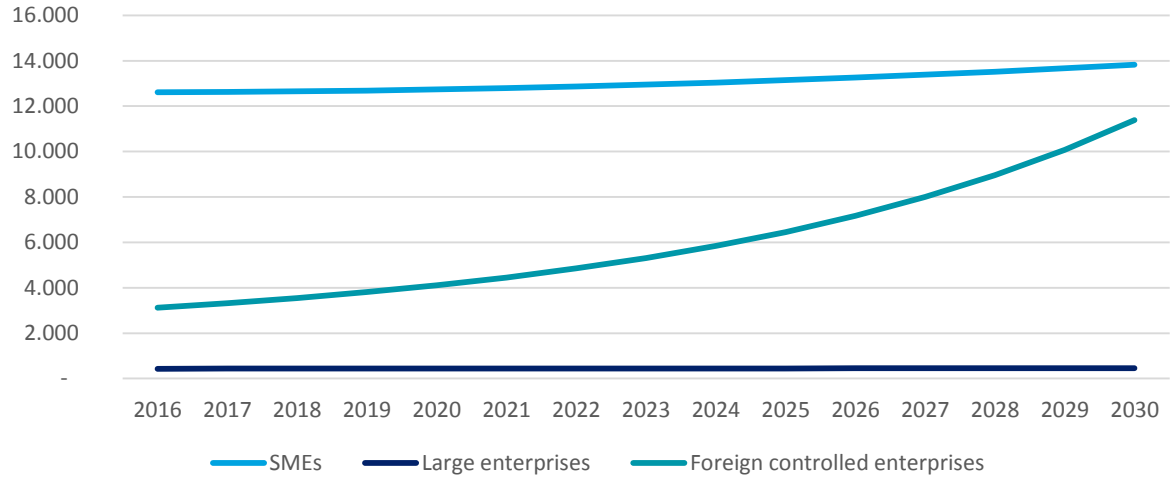
Source: Deloitte

The trends that can be seen from the graphs above and below in relation to the growth of the number of businesses affected by the ePD are similar to those in the baseline scenario:

- The overall number of businesses affected by the ePD is expected to grow from 2016 to 2030
- SMEs, large enterprises, and foreign controlled enterprises are of less importance for the overall growth of the number of businesses affected by the ePD;

- The number of SMEs affected is expected to increase slightly
- The number of large enterprises is expected to remain stable
- The number of foreign controlled enterprises affected by the ePD is expected to increase significantly until 2030

Figure 78 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Browser solution" 2016-2030)

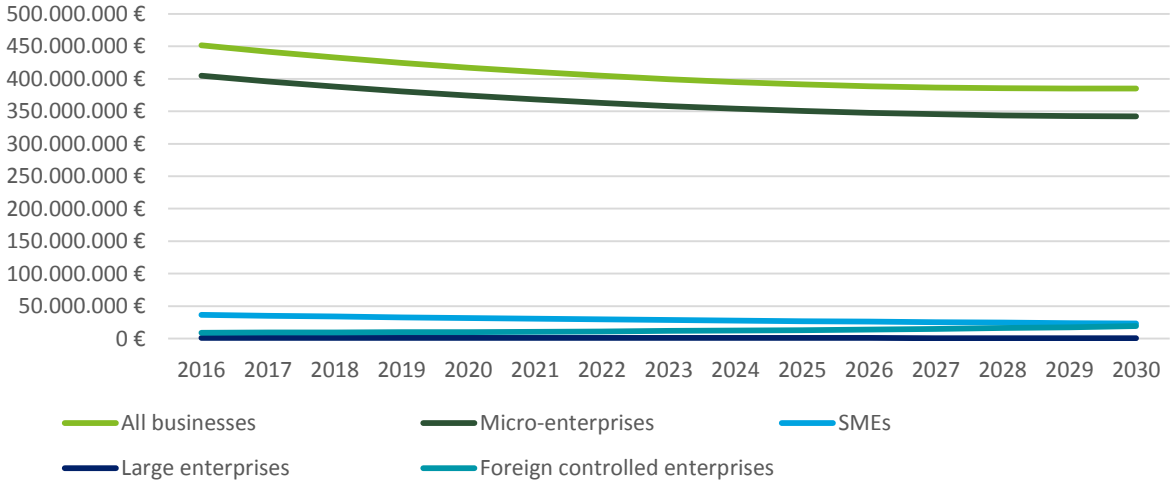


Source: Deloitte

Annual compliance costs under policy option 3 ("Browser solution")

The following two graphs present the development of the annual compliance costs of businesses affected by the ePD under policy option 3 ("Browser solution"). While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

Figure 79 – Compliance costs of businesses affected by the ePD per year (policy option 3, "Browser solution" 2016-2030)

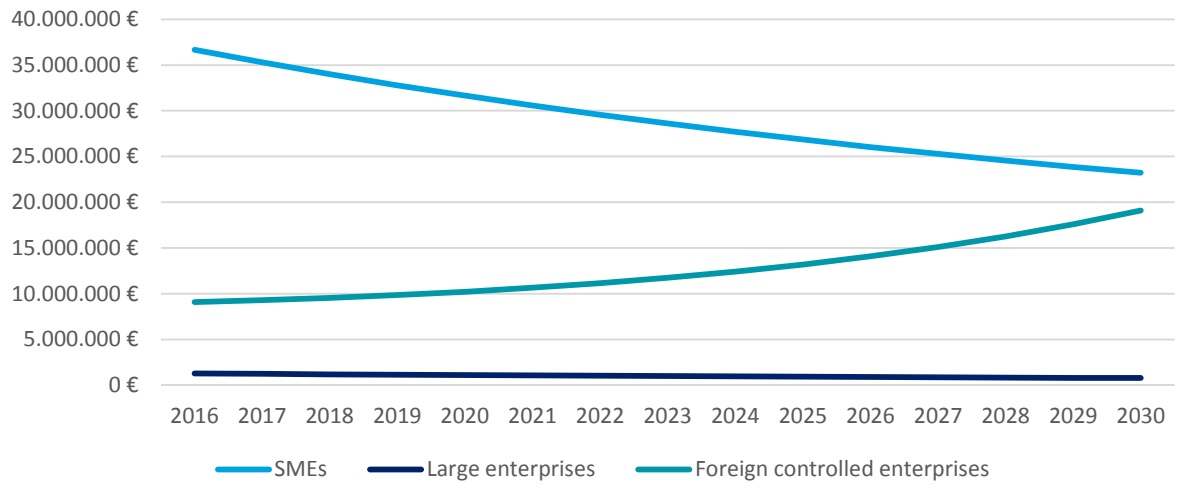


Source: Deloitte

The graph above shows a slight increase in the annual overall compliance costs for businesses from 20016 to 2030. Looking in more detail at annual overall compliance costs for SMEs, large enterprises, and foreign controlled enterprises (see figure below), it can be seen that – while compliance costs for

SMEs are expected to decrease – they are expected to remaine relatively stable for large and foreign controlled enterprises.

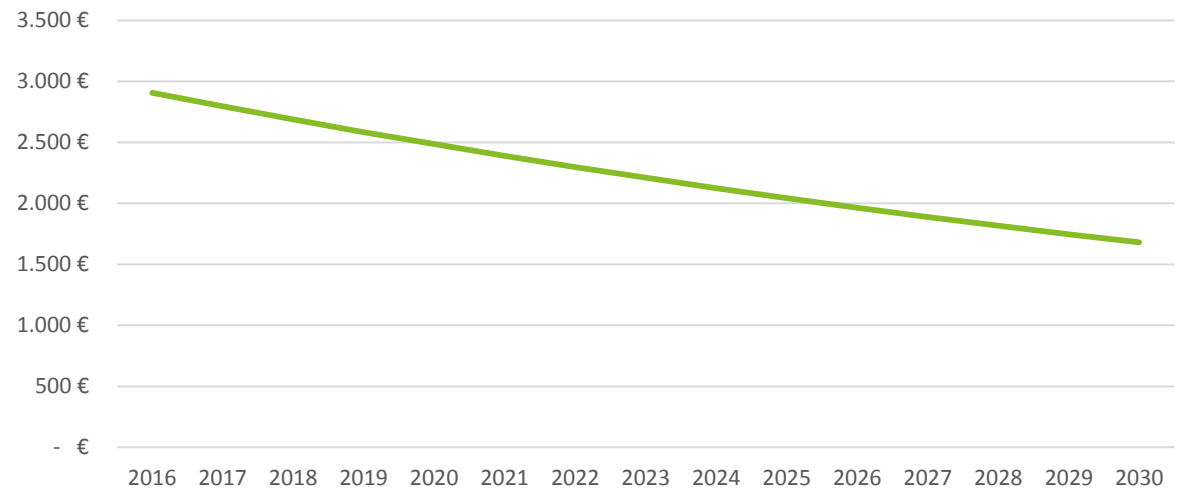
Figure 80 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Browser solution" 2016-2030)



Source: Deloitte

The following graph visualises the development of the average compliance costs for businesses from 2016 to 2030 under policy option 3 ("Browser solution"). No difference has been made between average costs for different size classes of businesses.

Figure 81 – Average compliance costs of per business affected by the ePD per year (policy option 3, "Browser solution" 2016-2030)



Source: Deloitte

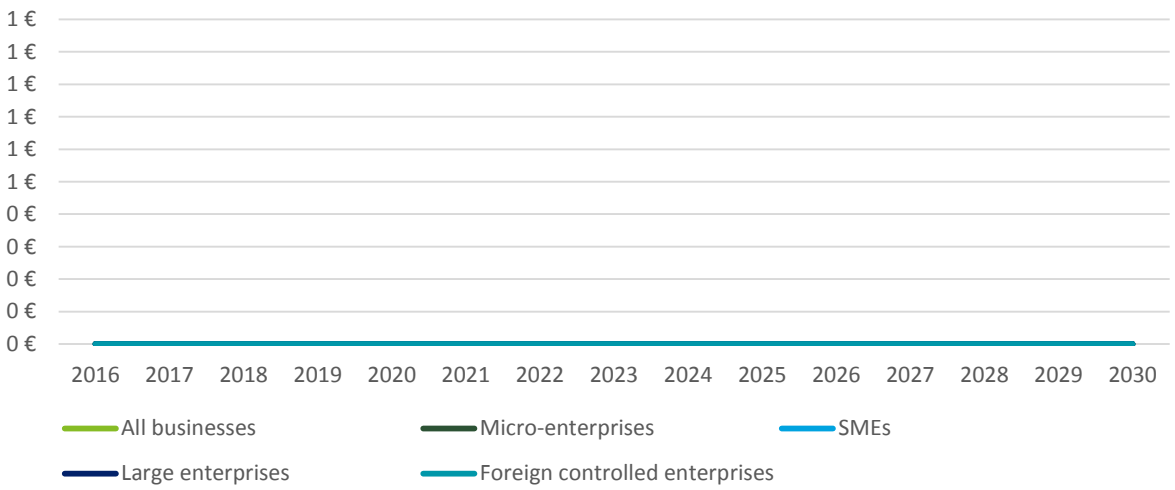
The graph clearly shows that the average compliance costs for businesses is expected to decrease between 2016 and 2030, as at the same time the number of businesses affected by the ePD increases.

Annual costs from administrative burden under policy option 3 ("Browser solution")

The following two graphs present the development of the annual costs from administrative of businesses affected by the ePD under policy option 3 ("Browser solution"). While the first graph

displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

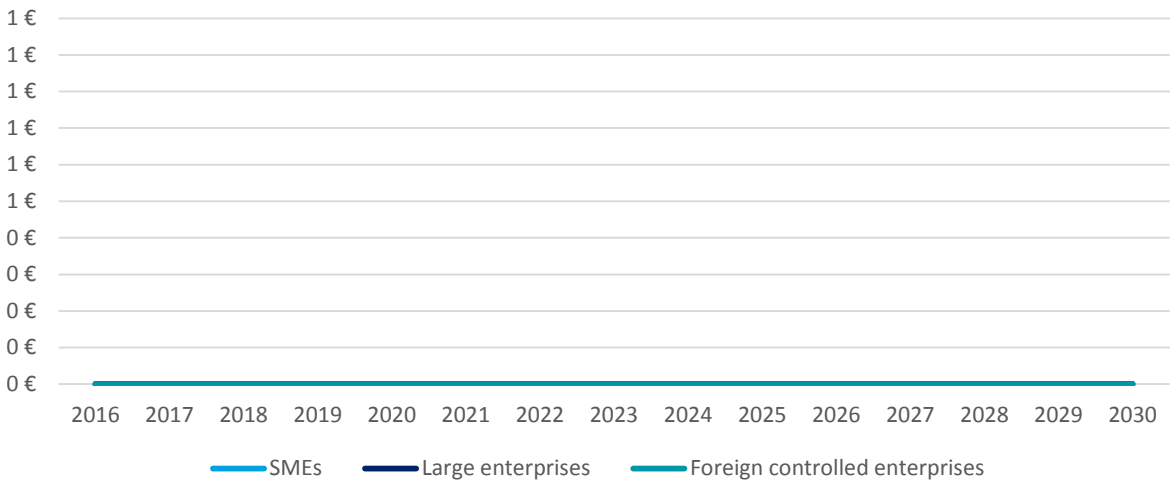
Figure 82 – Costs from administrative burden of businesses affected by the ePD per year (policy option 3, "Browser solution" 2016-2030)



Source: Deloitte

Similarly to the compliance costs, costs from overall annual administrative burden are expected to also increase slightly between 2016 and 2030.

Figure 83 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Browser solution" 2016-2030)

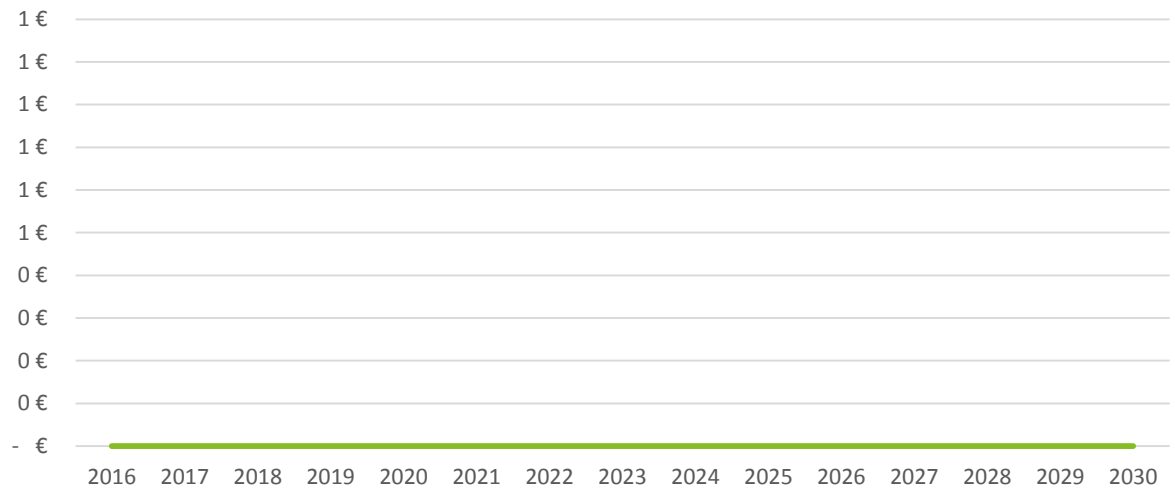


Source: Deloitte

As regards the costs from administrative burden for SMEs, large enterprises, and foreign controlled enterprises, an increasing trend can be observed from 2016-2030. Especially for SMEs, costs from administrative burden are expected to grow significantly until 2030.

The following graph visualises the development of the average costs from administrative burden for businesses from 2016 to 2030 under policy option 3 ("Browser solution"). No difference has been made between average costs for different size classes of businesses.

Figure 84 – Average costs from administrative burden per business affected by the ePD per year (policy option 3, "Browser solution" 2016-2030)



Source: Deloitte

Overall, the above graph shows that there will be a clear reduction of costs from administrative burden for across all types of businesses affected by the ePD until 2030, as at the same time the number of businesses affected by the ePD increases.

Policy option 3 ("browser solution"): Overall values 2016-2030

While the above section has presented average annual values, this section provides the key quantitative estimates for the overall time period of 2016-2030 (i.e. the sums of each individual annual value of the time period) under policy option 3 ("browser solution"). This estimate is relevant to assess the overall costs of compliance and administrative burden stemming from the ePD for different types of businesses.

The following table contains information on:

- Compliance costs (in million Euro); and
- Administrative burden (in million Euro).

The number of businesses affected is not presented as this number is – over the entire time period – subject to double counting.[545] Compared to the above section, average compliance cost per business, as well as average costs from administrations burden per business are not relevant to present in this section as they are *average* values and not *overall* values.

The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Overall value (2016-2030):* Denotes the overall annual value of the quantitative indicator for which data has been estimated. This means, for instance, that all SMEs in the EU together have will incur compliance costs of 463. EURm over the entire time period of 2016-2030 (see the light green cell);

[545] This is due to the fact that businesses are affected by the ePD over longer time frames than just one year. An alternative way of phrasing this is that the ePD does not affect an entirely different set of businesses each and every year.

- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the overall value between 2016 and 2030 under policy option 3 ("browser solution") compared to the overall value under the baseline scenario; and
- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the overall value between 2016 and 2030 under policy option 3 ("browser solution") compared to the overall value under the baseline scenario.

Table 88 – Key quantitative data estimated in relation to policy option 3 ("browser solution", overall 2016-2030)

Quantitative indicator	Overall value (2016-2030)	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Compliance costs (in million Euro)	6,099.2 €	-14,231.5 €	-70.0%
Micro-enterprises	5,458.4 €	-12,736.2 €	-70.0%
SMEs	436.6 €	-1,018.7 €	-70.0%
Large enterprises	15.0 €	-35.0 €	-70.0%
Foreign controlled enterprises	189.3 €	-441.6 €	-70.0%
Administrative burden (in million Euro)	3.12 €	-0.3 €	-10.0%
Micro-enterprises	2.4 €	-0.3 €	-10.0%
SMEs	0.5 €	-0.1 €	-10.0%
Large enterprises	0.0 €	0.0 €	-8.8%
Foreign controlled enterprises	0.2 €	0.0 €	-10.0%

Source: Deloitte

Under policy option 3 ("browser solution"), as can be seen from the table above, businesses are expected to incur less compliance costs and costs from administrative burden between 2016 and 2030 than they would in the baseline scenario.

In absolute terms, compliance costs are expected to decrease by 14,231 EURm to 6,099 EURm compared to the overall amount incurred in the baseline scenario. This equals a reduction of roughly 70%.

As argued in the REFIT section 6.2.2, the magnitude of the compliance costs should be seen in relation to the overall value of EU GDP. This way, the magnitude of compliance costs is marginal compared to the overall value of the economy.

As regards the costs from administrative burden, reductions are expected to be less pronounced. Overall, it is expected that 300,000 Euro can be saved under policy option 3 ("browser solution") between 2016 and 2030 at EU level. This is expected to result in an overall amount of 3.1 EURm of costs from administrative burden. The reduction is expected to be 10% compared to the overall amount incurred in the baseline scenario.

Part B2: "Tracking companies solution" – Key quantitative findings from the economic analysis

Policy option 3 ("Tracking companies solution"): Average annual values and changes compared to the current situation

Similarly to the information provided for the baseline scenario, the overall quantitative results of the analysis concerning policy option 3 ("tracking companies solution") are presented in Table 73:

- Number of businesses affected (in million);
- Compliance costs (in million Euro);
- Average compliance cost per business (in Euro);
- Administrative burden (in million Euro); and
- Average costs from administrative burden per business (in Euro).

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Annex A: Economic Analysis

Further information in this regard, as well as an explanation of the approach used for the estimation of the quantitative results data is provided in the section on the basic assumptions used for the assessment of the impacts of the policy options in Annex A concerning the Economic Analysis.

The following table presents the quantitative findings for policy option 3 ("tracking companies solution"). The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Average annual value:* Denotes the average annual value of the quantitative indicator for which data has been estimated. This means, for instance, that 52,000 SMEs are affected by issues relating to the ePD per year (see the light blue cell), facing a total amount of 38.8 EURm per year (see the light green cell) at an average cost of compliance per business of 747 Euro (see the dark blue cell);
- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the average annual value compared to the baseline scenario (2016-2030); and
- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the average annual value compared to the baseline scenario (i.e. 2016-2030).

Visualisations of the year-over-year development of the quantitative indicators are presented afterwards, as well as overall values for the timeframe 2016-2030.

Table 89 – Key quantitative data estimated in relation to policy option 3 ("tracking companies solution", 2016-2030)

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Number of businesses affected (in million)	0.741	-2.96	-80.0%
Micro-enterprises	0.663	-2.65	-80.0%
SMEs	0.052	-0.21	-80.1%

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Large enterprises	0.002	-0.01	-77.8%
Foreign controlled enterprises	0.024	-0.10	-80.2%
Compliance costs (in million Euro)	542.2 €	-813.2 €	-60.0%
Micro-enterprises	485.2 €	-727.8 €	-60.0%
SMEs	38.8 €	-58.2 €	-60.0%
Large enterprises	1.3 €	-2.0 €	-60.0%
Foreign controlled enterprises	16.8 €	-25.2 €	-60.0%
Average compliance cost per business (in Euro)	747.0 €	373.5 €	100.0%[546]
Administrative burden (in million Euro)	0.226 €	-0.005 €	-2.2%
Micro-enterprises	0.178 €	-0.003 €	-1.7%
SMEs	0.033 €	-0.001 €	-2.9%
Large enterprises	0.002 €	0.000 €	0.0%
Foreign controlled enterprises	0.014 €	0.000 €	0.0%
Average costs from admin. burden per business (in Euro)	136.0 €	108.2 €	390.0%

Source: Deloitte

Under policy option 3 ("tracking companies solution"), the analysis shows that – per year between 2016 and 2030 – around 741,000 businesses will be affected by the ePD in the EU. The majority of these businesses will be micro-enterprises with less than 10 employees (663,000). Around 52,000 SMEs that have between 10 and 250 employees are estimated to be affected per year until 2030 while the number of large enterprises is negligible with around 2,000 per year. Approx. 24,000 foreign controlled enterprises that operate in the EU will be affected.[547]

The businesses affected by the ePD are estimated to incur an annual value of 542 EURm to comply with Art. 5(3) and Art. 13. In addition, these businesses are expected to incur an unspecifiable amount of additional costs with regard to other provisions such as the consumer provisions. Again, micro-enterprises are expected to incur the lion share of these costs (around 485 EURm).

On *average*, an EU business is expected to incur 747 Euro per year with regard to the ePD until 2030. This does, however, not mean that e.g. large enterprises may not incur significantly more costs while the costs may be significantly lower for micro-enterprises.

In addition to the compliance costs related to the direct implementation of the ePD, businesses will also incur significant opportunity costs for lost business opportunities.

[546] This increase of the average compliance cost per business (in Euro) by 100% is explained by the following reasoning: While it is expected that the policy option reduces the number of affected businesses by 80%, the overall costs are only expected to decrease by 60%. This means that the financial burden would have to be shouldered by less businesses (in relative terms) compared to the baseline scenario. This means that each business is expected to incur, on average, more costs under this policy option than in the baseline scenario. Overall, however, the compliance costs are still expected to be lower under this policy option than in the baseline scenario.

[547] The estimated numbers of affected businesses should be understood as annual values. However, the overall number of businesses affected by the ePD between 2016 and 2030 is not the sum of each annual value. The reason for this is that the majority of businesses will be affected not only once but on several occasions across this time frame while some businesses will be replaced by others due to the general life cycle of businesses (company birth, insolvency). This means that, in relation to the former argument, the projected value is likely underestimating the actual number of businesses affected, while the latter argument, the projection is likely to overestimate the number of affected businesses.

In relation to administrative burden, mostly stemming from the notification obligations for telecommunication service providers under Article 4, it has been estimated that an annual amount of 226,000 Euro is incurred, i.e. around 136 Euro per affected business per year.

Policy option 3 ("Tracking companies solution"): Visualisation of the development 2016-2030

In this section, we present visualisations of the development of the following quantitative indicators between 2016 and 2030 under policy option 3 ("Tracking companies solution"):

- The number of businesses affected;
- The compliance costs; and
- The costs from administrative burden.

It has been decided to use such a form of visualisation instead of providing the data by means of tables in order to make the sheer amount of data more accessible to the reader and to clearly be able to show the *development of the quantitative indicators over time* – which is not always easy to spot when looking at raw figures.

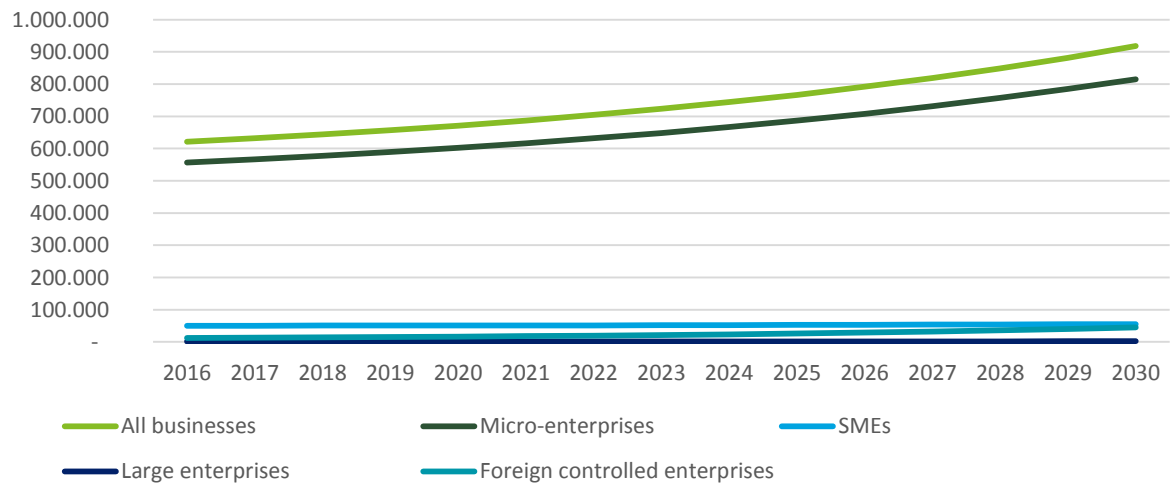
The graphs visualise the data per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Graphical comparisons of the quantitative indicators under each policy option with the baseline scenario are provided in section 9.8.1.

Number of businesses affected under policy option 3 ("Tracking companies solution")

The following two graphs present the development of the number of businesses affected by the ePD under policy option 3 ("Tracking companies solution"). While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

Figure 85 – Number of businesses affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030)



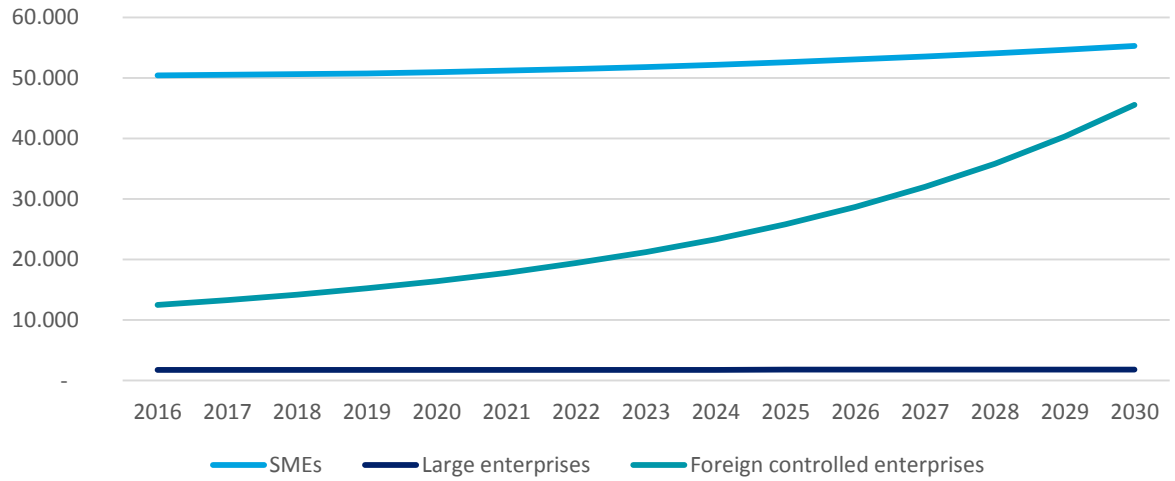
Source: Deloitte

The trends that can be seen from the graphs above and below in relation to the growth of the number of businesses affected by the ePD are similar to those in the baseline scenario:

- The overall number of businesses affected by the ePD is expected to grow from 2016 to 2030

- SMEs, large enterprises, and foreign controlled enterprises are of less importance for the overall growth of the number of businesses affected by the ePD;
- The number of SMEs affected is expected to increase slightly
- The number of large enterprises is expected to remain stable
- The number of foreign controlled enterprises affected by the ePD is expected to increase significantly until 2030.

Figure 86 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030)

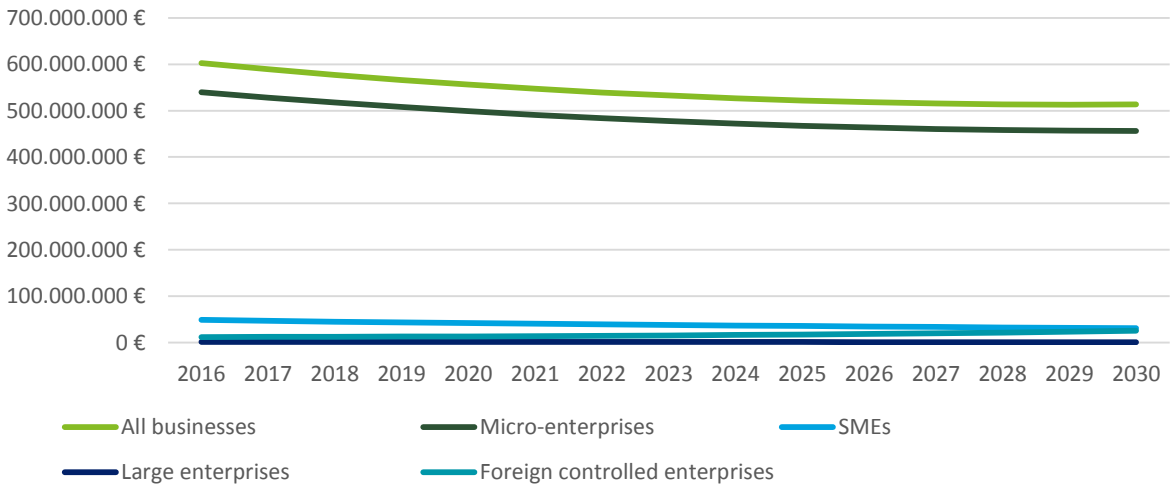


Source: Deloitte

Annual compliance costs under policy option 3 ("Tracking companies solution")

The following two graphs present the development of the annual compliance costs of businesses affected by the ePD under policy option 3 ("Tracking companies solution"). While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

Figure 87 – Compliance costs of businesses affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030)

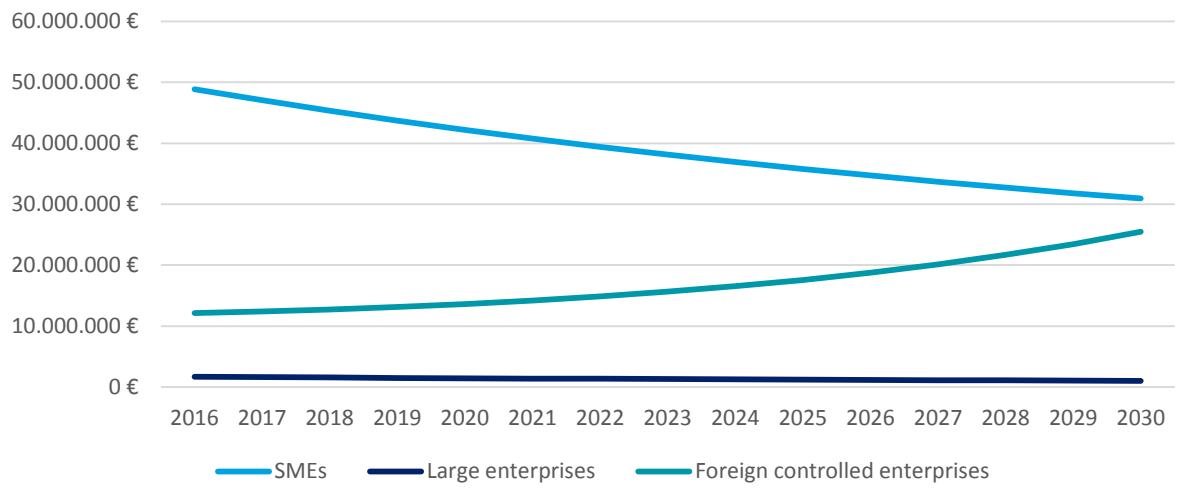


Source: Deloitte

The graph above shows the annual overall compliance costs for businesses will decrease from 2016 to 2030. Looking in more detail at annual overall compliance costs for SMEs, large enterprises, and

foreign controlled enterprises (see figure below), it can be seen that – while compliance costs for SMEs will decrease noticeable – they are expected to increase distinctly for foreign controlled enterprises and remain relatively stable for large enterprises.

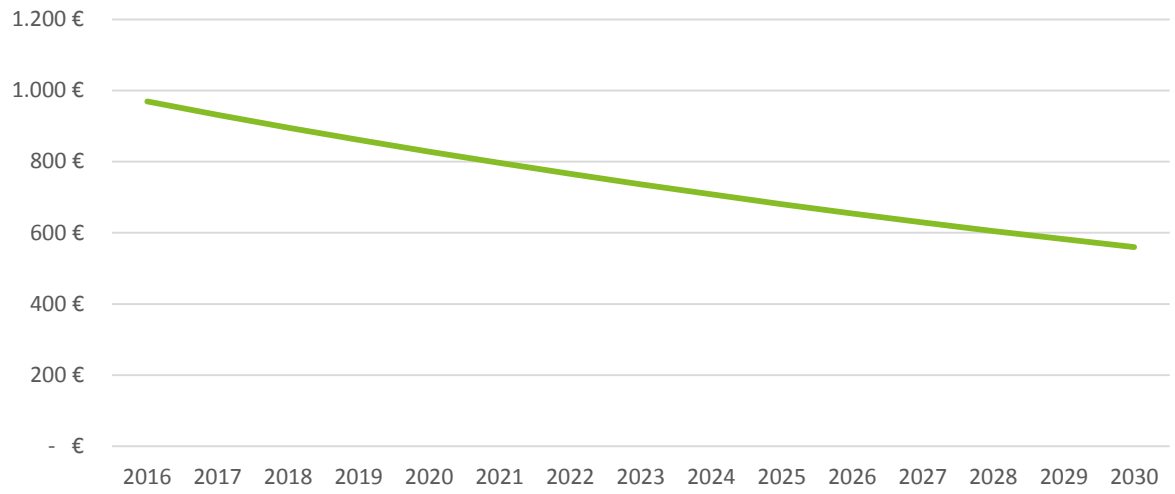
Figure 88 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030)



Source: Deloitte

The following graph visualises the development of the average compliance costs for businesses from 2016 to 2030 under policy option 3 ("Tracking companies solution"). No difference has been made between average costs for different size classes of businesses.

Figure 89 – Average compliance costs of per business affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030)



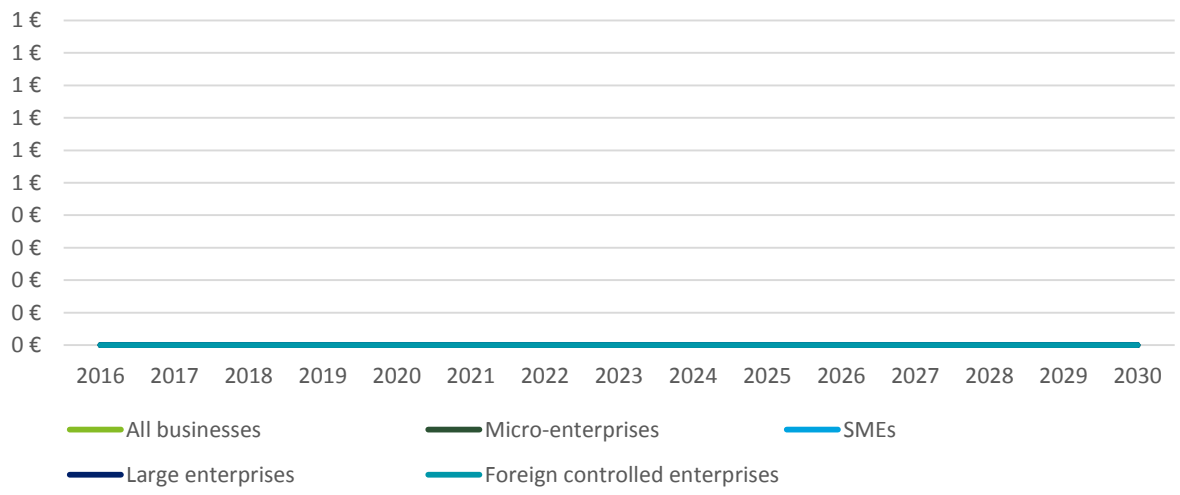
Source: Deloitte

The graph clearly shows that the average compliance costs for businesses are expected to decrease drastically between 2016 and 2030, as at the same time the number of businesses affected by the ePD increases.

Annual costs from administrative burden under policy option 3 ("Tracking companies solution")

The following two graphs present the development of the annual costs from administrative burden of businesses affected by the ePD under policy option 3 ("Tracking companies solution"). While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

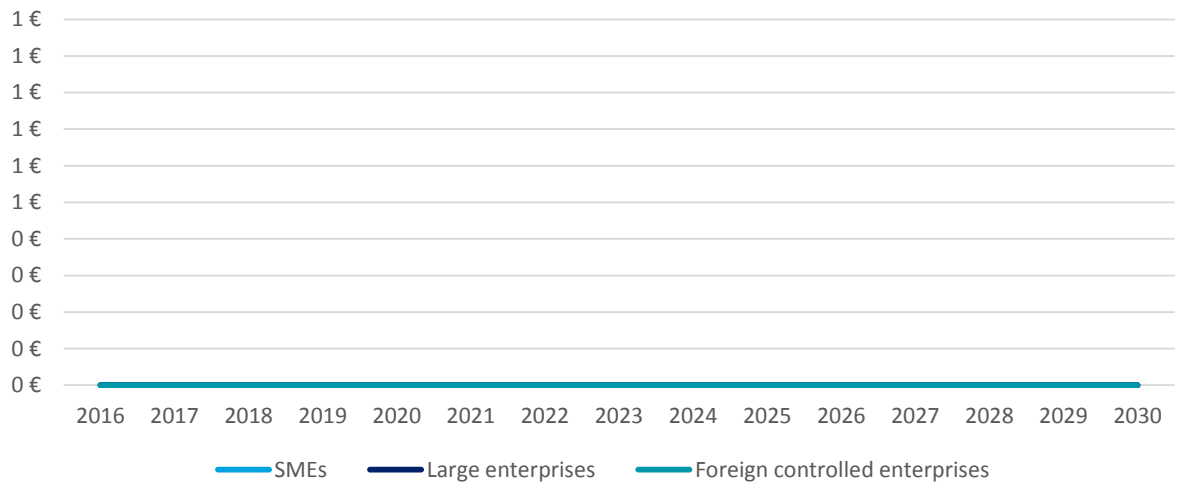
Figure 90 – Costs from administrative burden of businesses affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030)



Source: Deloitte

Unlike the compliance costs, costs from overall annual administrative burden are expected to slightly increase between 2016 and 2030.

Figure 91 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030)

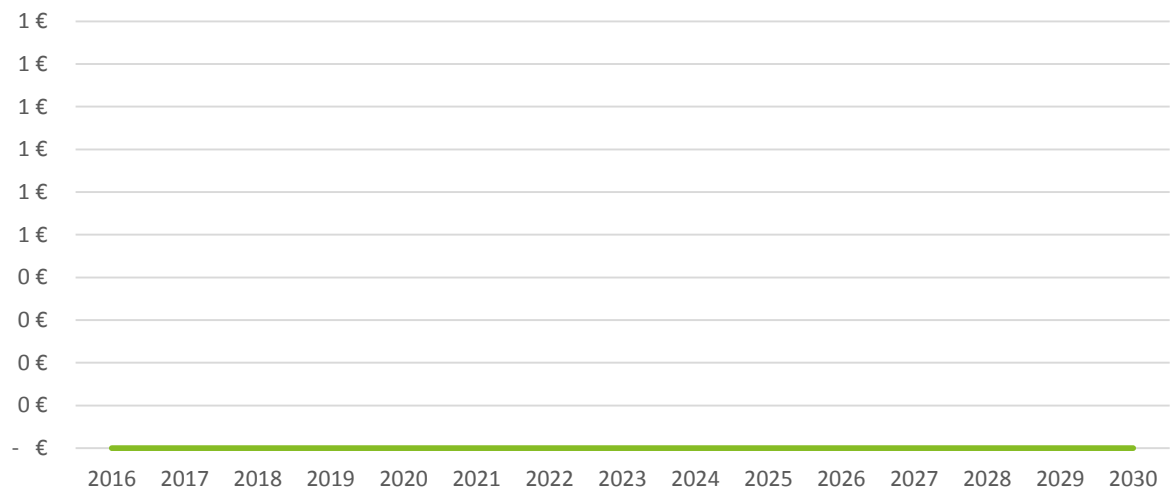


Source: Deloitte

As regards the costs from administrative burden for SMEs, large enterprises, and foreign controlled enterprises, an increase is expected from 2016 to 2030. Especially for SMEs, costs from administrative burden will continue to grow significantly until 2030.

The following graph visualises the development of the average costs from administrative burden for businesses from 2016 to 2030 under policy option 3 ("Tracking companies solution"). No difference has been made between average costs for different size classes of businesses.

Figure 92 – Average costs from administrative burden per business affected by the ePD per year (policy option 3, "Tracking companies solution" 2016-2030)



Source: Deloitte

Overall, the above graph shows that a clear reduction of costs from administrative burden is expected across all types of businesses affected by the ePD from 2016 to 2030, as at the same time the number of businesses affected by the ePD increases.

Policy option 3 ("tracking companies solution"): Overall values 2016-2030

While the above section has presented average annual values, this section provides the key quantitative estimates for the overall time period of 2016-2030 (i.e. the sums of each individual annual value of the time period) under policy option 3 ("tracking companies solution"). This estimate is relevant to assess the overall costs of compliance and administrative burden stemming from the ePD for different types of businesses.

The following table contains information on:

- Compliance costs (in million Euro); and
- Administrative burden (in million Euro).

The number of businesses affected is not presented as this number is – over the entire time period – subject to double counting.[548] Compared to the above section, average compliance costs per business, as well as average costs from administrative burden per business are not relevant to present in this section as they are *average* values and not *overall* values.

The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Overall value (2016-2030):* Denotes the overall annual value of the quantitative indicator for which data has been estimated. This means, for instance, that all SMEs in the EU together

[548] This is due to the fact that businesses are affected by the ePD over longer time frames than just one year. An alternative way of phrasing this is that the ePD does not affect an entirely different set of businesses each and every year.

have will incur compliance costs of 582.1 EURm over the entire time period of 2016-2030 (see the light green cell);

- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the overall value between 2016 and 2030 under policy option 3 ("tracking companies solution") compared to the overall value under the baseline scenario; and
- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the overall value between 2016 and 2030 under policy option 3 ("tracking companies solution") compared to the overall value under the baseline scenario.

Table 90 – Key quantitative data estimated in relation to policy option 3 ("tracking companies solution"), overall 2016-2030)

Quantitative indicator	Overall value (2016-2030)	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Compliance costs (in million Euro)	8,132.3 €	-12,198.4 €	-60.0%
Micro-enterprises	7,277.8 €	-10,916.7 €	-60.0%
SMEs	582.1 €	-873.2 €	-60.0%
Large enterprises	20.0 €	-30.0 €	-60.0%
Foreign controlled enterprises	252.4 €	- 378.5 €	-60.0%
Administrative burden (in million Euro)	3.4 €	-0.07 €	-2.0%
Micro-enterprises	2.7 €	-0.05 €	-2.0%
SMEs	0.5 €	-0.01 €	-2.0%
Large enterprises	0.0 €	0.00 €	-2.9%
Foreign controlled enterprises	0.2 €	0.00 €	-1.9%

Source: Deloitte

Under policy option 3 ("tracking companies solution"), as can be seen from the table above, businesses are expected to incur less compliance costs and costs from administrative burden between 2016 and 2030 than they would in the baseline scenario.

In absolute terms, compliance costs are expected to decrease by 12,198 EURm to 8,132 EURm compared to the overall amount incurred in the baseline scenario. This equals a reduction of roughly 60%.

As argued in the REFIT section 6.2.2, the magnitude of the compliance costs should be seen in relation to the overall value of EU GDP. This way, the magnitude of compliance costs is marginal compared to the overall value of the economy.

As regards the costs from administrative burden, reductions are expected to be less pronounced. Overall, it is expected that 700,000 Euro can be saved under policy option 3 ("tracking companies solution") between 2016 and 2030 at EU level. This is expected to result in an overall amount of 3.4 EURm of costs from administrative burden. The reduction is expected to be 2% compared to the overall amount incurred in the baseline scenario.

Part B3: "Publishers solution" – Key quantitative findings from the economic analysis

Policy option 3 ("Publishers solution"): Average annual values and changes compared to the current situation

Similarly to the information provided for the baseline scenario, the overall quantitative results of the analysis concerning policy option 3 ("publishers solution") are presented in Table 73:

- Number of businesses affected (in million);
- Compliance costs (in million Euro);
- Average compliance cost per business (in Euro);
- Administrative burden (in million Euro); and
- Average costs from administrative burden per business (in Euro).

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Annex A: Economic Analysis

Further information in this regard, as well as an explanation of the approach used for the estimation of the quantitative results data is provided in the section on the basic assumptions used for the assessment of the impacts of the policy options in Annex A concerning the Economic Analysis.

The following table presents the quantitative findings for policy option 3 ("publishers solution"). The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Average annual value:* Denotes the average annual value of the quantitative indicator for which data has been estimated. This means, for instance, that 160,000 SMEs are affected by issues relating to the ePD per year (see the light blue cell), facing a total amount of 92.2 EURm per year (see the light green cell) at an average cost of compliance per business of 591 Euro (see the dark blue cell);
- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the average annual value compared to the baseline scenario (2016-2030); and
- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the average annual value compared to the baseline scenario (i.e. 2016-2030).

Visualisations of the year-over-year development of the quantitative indicators are presented afterwards, as well as overall values for the timeframe 2016-2030.

Table 91 – Key quantitative data estimated in relation to policy option 3 ("publishers solution"), 2016-2030)

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Number of businesses affected (in million)	2.22	-1.48 €	-40.0%
Micro-enterprises	1.99	-1.33 €	-40.0%
SMEs	0.16	-0.10 €	-39.8%

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Large enterprises	0.01	-0.004 €	-44.4%
Foreign controlled enterprises	0.07	-0.05 €	-40.5%
Compliance costs (in million Euro)	1,287.6 €	-67.8 €	-5.0%
Micro-enterprises	1,152.3 €	-60.6 €	-5.0%
SMEs	92.2 €	-4.9 €	-5.0%
Large enterprises	3.2 €	-0.2 €	-5.0%
Foreign controlled enterprises	40.0 €	-2.1 €	-5.0%
Average compliance cost per business (in Euro)	591.4 €	217.9 €	58.3%
Administrative burden (in million Euro)	0.23 €	-0.005 €	-2.2%
Micro-enterprises	0.18 €	-0.004 €	-2.2%
SMEs	0.03 €	-0.001 €	-2.9%
Large enterprises	0.00 €	0.000 €	0.0%
Foreign controlled enterprises	0.01 €	0.000 €	0.0%
Average costs from admin. burden per business (in Euro)	45.33 €	17.6 €	63.3%

Source: Deloitte

Under policy option 3 ("publishers solution"), the analysis shows that – per year between 2016 and 2030 – around 2.2 million businesses will be affected by the ePD in the EU. The majority of these businesses will be micro-enterprises with less than 10 employees (2.0 million). Around 160,000 SMEs that have between 10 and 250 employees are estimated to be affected per year until 2030 while the number of large enterprises is negligible with around 10,000 per year. Approx. 70,000 foreign controlled enterprises that operate in the EU will be affected.[549]

The businesses affected by the ePD are estimated to incur an annual value of 1.29 EURb to comply with Art. 5(3) and Art. 13. In addition, these businesses are expected to incur an unspecifiable amount of additional costs with regard to other provisions such as the consumer provisions. Again, micro-enterprises are expected to incur the lion share of these costs (around 1.15 EURb).

On *average*, an EU business is expected to incur 591 Euro per year with regard to the ePD until 2030. This does, however, not mean that e.g. large enterprises may not incur significantly more costs while the costs may be significantly lower for micro-enterprises.

In addition to the compliance costs related to the direct implementation of the ePD, businesses will also incur significant opportunity costs for lost business opportunities.

In relation to administrative burden, mostly stemming from the notification obligations for telecommunication service providers under Article 4, it has been estimated that an annual amount of 230,000 Euro is incurred, i.e. around 45 Euro per affected business per year.

[549] The estimated numbers of affected businesses should be understood as annual values. However, the overall number of businesses affected by the ePD between 2016 and 2030 is not the sum of each annual value. The reason for this is that the majority of businesses will be affected not only once but on several occasions across this time frame while some businesses will be replaced by others due to the general life cycle of businesses (company birth, insolvency). This means that, in relation to the former argument, the projected value is likely underestimating the actual number of businesses affected, while the latter argument, the projection is likely to overestimate the number of affected businesses.

Policy option 3 ("Publishers solution"): Visualisation of the development 2016-2030

In this section, we present visualisations of the development of the following quantitative indicators between 2016 and 2030 under policy option 3:

- The number of businesses affected;
- The compliance costs; and
- The costs from administrative burden.

It has been decided to use such a form of visualisation instead of providing the data by means of tables in order to make the sheer amount of data more accessible to the reader and to clearly be able to show the *development of the quantitative indicators over time* – which is not always easy to spot when looking at raw figures.

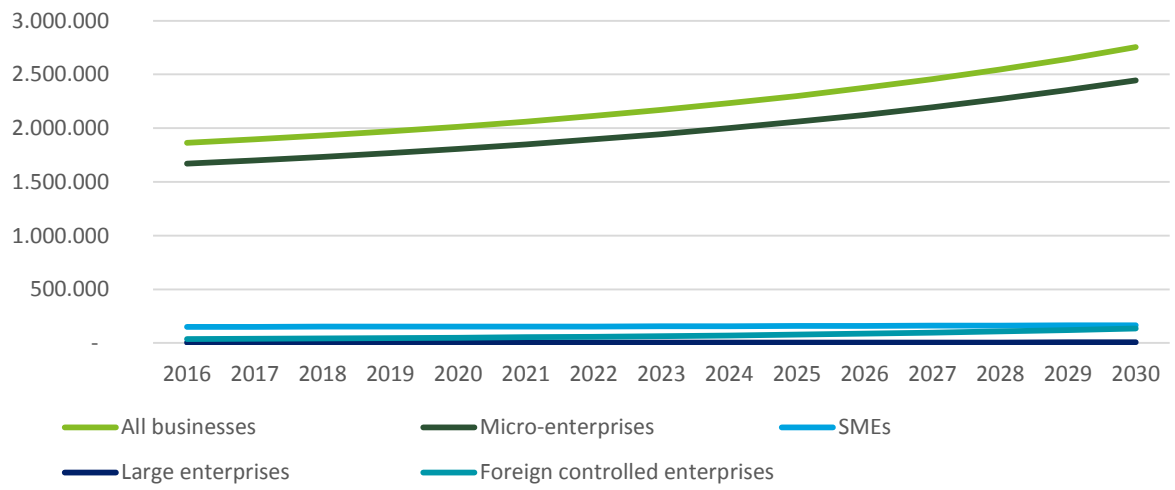
The graphs visualise the data per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Graphical comparisons of the quantitative indicators under each policy option with the baseline scenario are provided in section 9.8.1.

Number of businesses affected under policy option 3 ("Publishers solution")

The following two graphs present the development of the number of businesses affected by the ePD under policy option 3 ("Publishers solution"). While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

Figure 93 – Number of businesses affected by the ePD per year (policy option 3, "Publishers solution" 2016-2030)



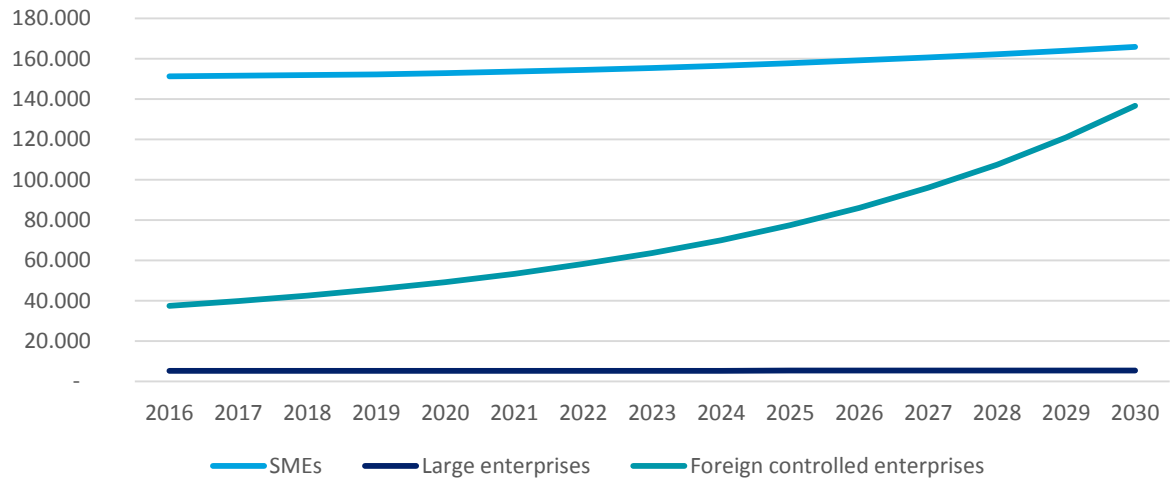
Source: Deloitte

The trends that can be seen from the graphs above and below in relation to the growth of the number of businesses affected by the ePD are similar to those in the baseline scenario:

- The overall number of businesses affected by the ePD is expected to grow from 2016 to 2030
- SMEs, large enterprises, and foreign controlled enterprises are of less importance for the overall growth of the number of businesses affected by the ePD;
- The number of SMEs affected is expected to increase slightly
- The number of large enterprises is expected to remain stable

- The number of foreign controlled enterprises affected by the ePD is expected to increase significantly until 2030

Figure 94 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Publishers solution" 2016-2030)

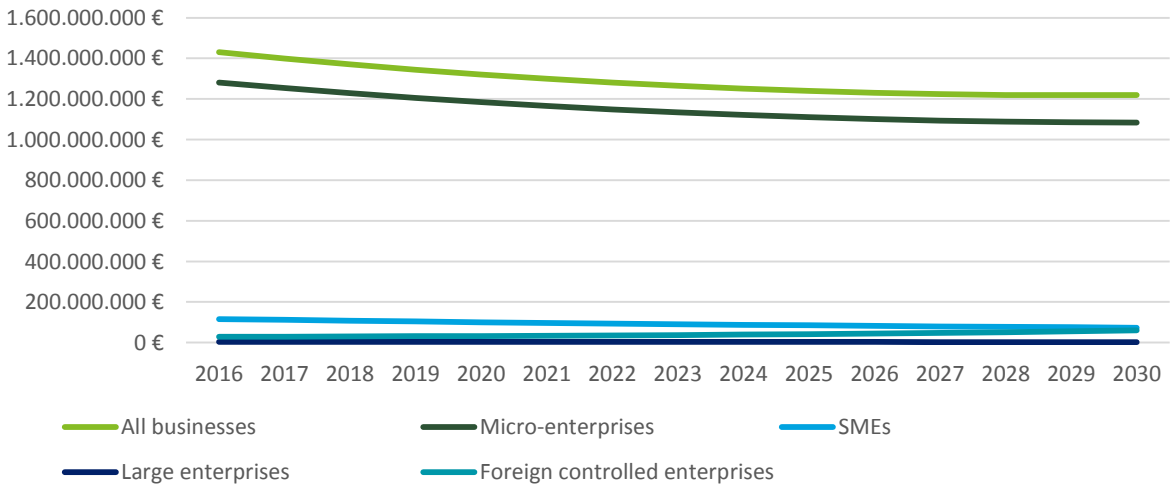


Source: Deloitte

Annual compliance costs under policy option 3 ("Publishers solution")

The following two graphs present the development of the annual compliance costs of businesses affected by the ePD under policy option 3 ("Publishers solution"). While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

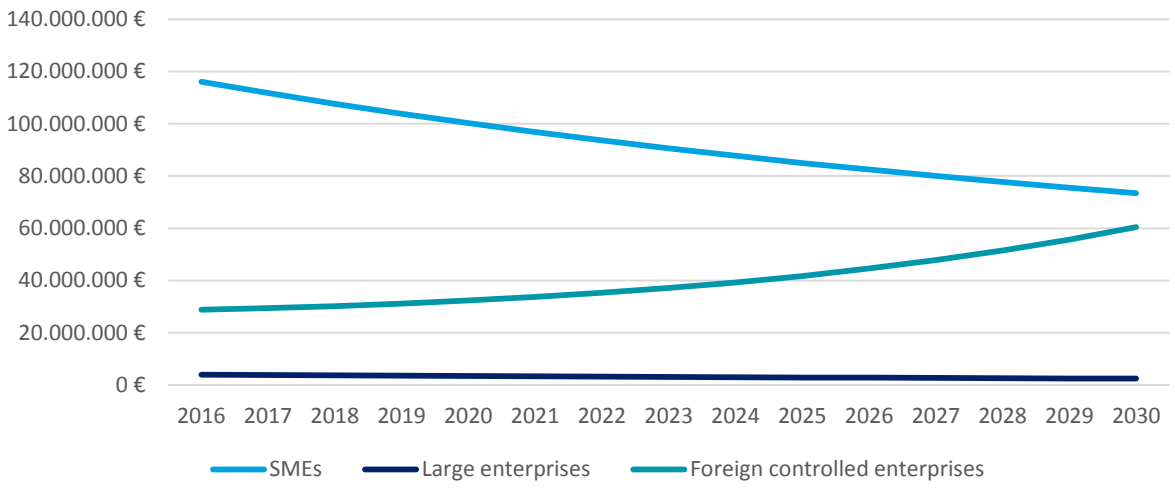
Figure 95 – Compliance costs of businesses affected by the ePD per year (policy option 3, "Publishers solution" 2016-2030)



Source: Deloitte

The graph above shows the annual overall compliance costs for businesses is expected to decrease from 2016 to 2030. Looking in more detail at annual overall compliance costs for SMEs, large enterprises, and foreign controlled enterprises (see figure below), it can be seen that – while compliance costs for SMEs will decrease – they are expected to increase for foreign controlled enterprises and remain relatively stable for large enterprises.

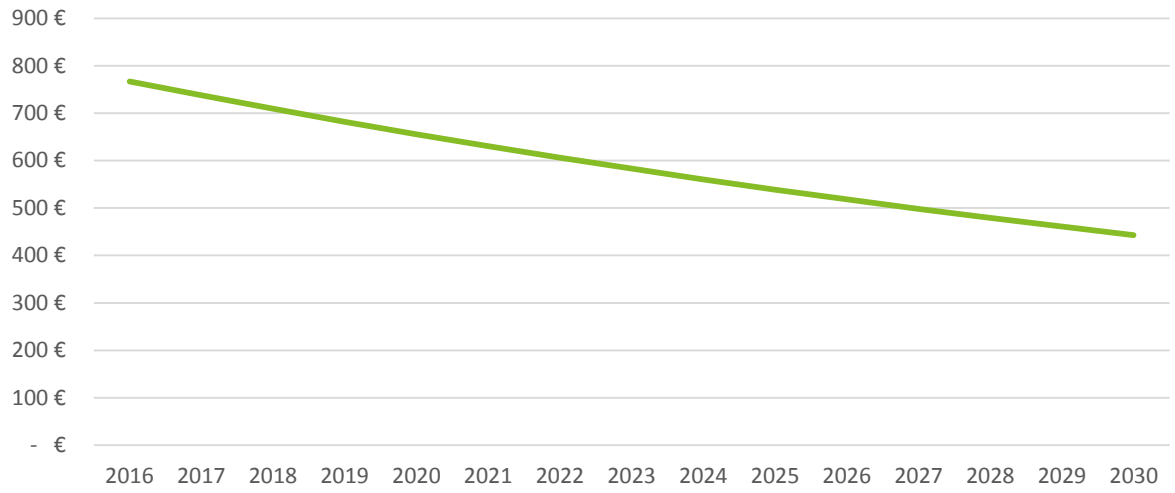
Figure 96 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Publishers solution" 2016-2030)



Source: Deloitte

The following graph visualises the development of the average compliance costs for businesses from 2016 to 2030 under policy option 3 ("Publishers solution"). No difference has been made between average costs for different size classes of businesses.

Figure 97 – Average compliance costs of per business affected by the ePD per year (policy option 3, "Publishers solution" 2016-2030)



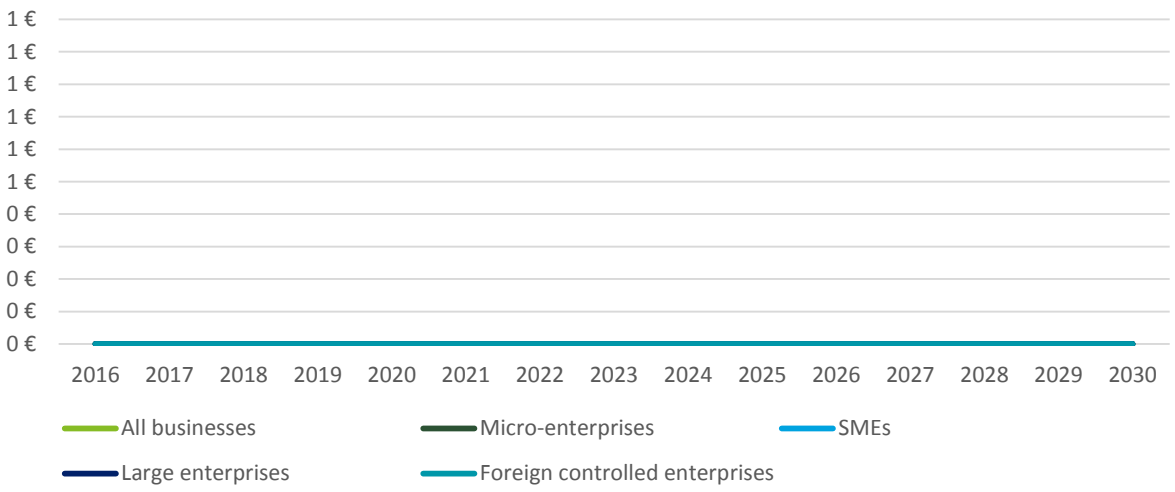
Source: Deloitte

The graph clearly shows that the average compliance costs for businesses is expected to decrease between 2016 and 2030, as at the same time the number of businesses affected by the ePD increases.

Annual costs from administrative burden under policy option 3 ("Publishers solution")

The following two graphs present the development of the annual costs from administrative of businesses affected by the ePD under policy option 3 ("Publishers solution"). While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

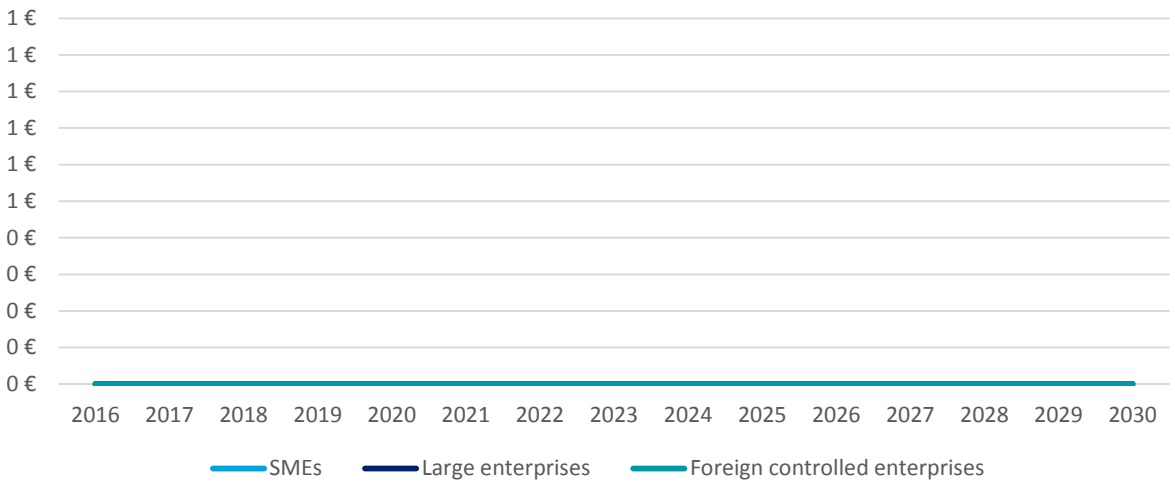
Figure 98 – Costs from administrative burden of businesses affected by the ePD per year (policy option 3, "Publishers solution" 2016-2030)



Source: Deloitte

Unlike the compliance costs, costs from overall annual administrative burden is expected to slightly increase between 2016 and 2030.

Figure 99 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 3, "Publishers solution" 2016-2030)

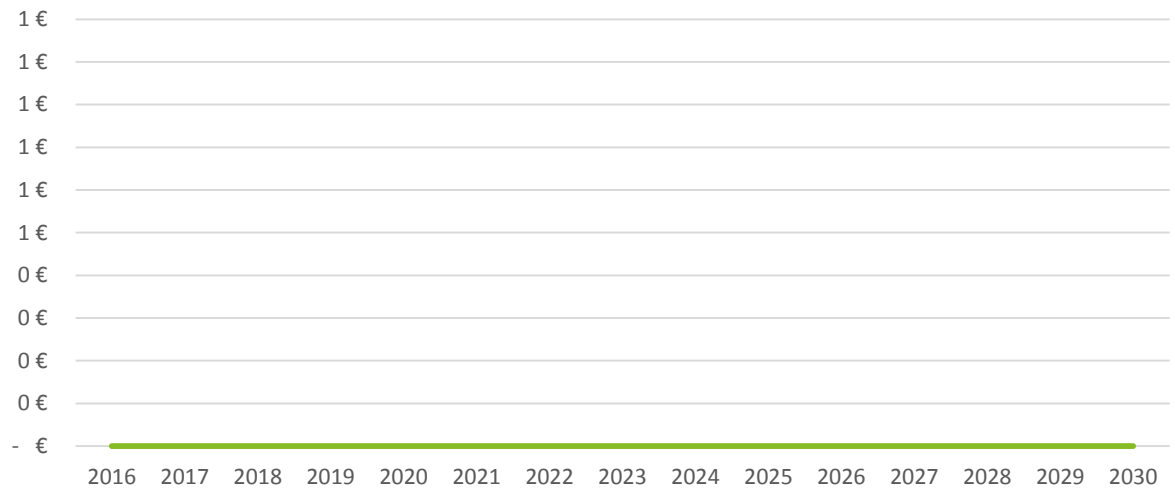


Source: Deloitte

As regards the costs from administrative burden for SMEs, large enterprises, and foreign controlled enterprises, an increase is expected from 2016 to 2030. Especially for SMEs, costs from administrative burden will continue to grow significantly until 2030.

The following graph visualises the development of the average costs from administrative burden for businesses from 2016 to 2030 under policy option 3 ("Publishers solution"). No difference has been made between average costs for different size classes of businesses.

Figure 100 – Average costs from administrative burden per business affected by the ePD per year (policy option 3, "Publishers solution" 2016-2030)



Source: Deloitte

Overall, the above graph shows that there a reduction of costs from administrative burden is expected across all types of businesses affected by the ePD from 2016 to 2030, as at the same time the number of businesses affected by the ePD increases.

Policy option 3 ("publisher's solution"): Overall values 2016-2030

While the above section has presented average annual values, this section provides the key quantitative estimates for the overall time period of 2016-2030 (i.e. the sums of each individual annual value of the time period) under policy option 3 ("publisher's solution"). This estimate is relevant to assess the overall costs of compliance and administrative burden stemming from the ePD for different types of businesses.

The following table contains information on:

- Compliance costs (in million Euro); and
- Administrative burden (in million Euro).

The number of businesses affected is not presented as this number is – over the entire time period – subject to double counting.[550] Compared to the above section, average compliance cost per business, as well as average costs from administrative burden per business are not relevant to present in this section as they are *average* values and not *overall* values.

The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Overall value (2016-2030):* Denotes the overall annual value of the quantitative indicator for which data has been estimated. This means, for instance, that all SMEs in the EU together have will incur compliance costs of 1,383 EURm over the entire time period of 2016-2030 (see the light green cell);

[550] This is due to the fact that businesses are affected by the ePD over longer time frames than just one year. An alternative way of phrasing this is that the ePD does not affect an entirely different set of businesses each and every year.

- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the overall value between 2016 and 2030 under policy option 3 ("publishers solution") compared to the overall value under the baseline scenario; and
- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the overall value between 2016 and 2030 under policy option 3 ("publisher's solution") compared to the overall value under the baseline scenario.

Table 92 – Key quantitative data estimated in relation to policy option 3 ("publisher's solution"), overall 2016-2030)

Quantitative indicator	Overall value (2016-2030)	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Compliance costs (in million Euro)	19,314.2 €	-1,016.5 €	-5.0%
Micro-enterprises	17,284.8 €	-909.7 €	-5.0%
SMEs	1,382.5 €	-72.8 €	-5.0%
Large enterprises	47.5 €	-2.5 €	-5.0%
Foreign controlled enterprises	599.3 €	-31.5 €	-5.0%
Administrative burden (in million Euro)	3.4 €	-0.069 €	-2.0%
Micro-enterprises	2.7 €	-0.054 €	-2.0%
SMEs	0.5 €	-0.010 €	-2.0%
Large enterprises	0.0 €	-0.001 €	-2.9%
Foreign controlled enterprises	0.2 €	-0.004 €	-1.9%

Source: Deloitte

Under policy option 3 ("publishers solution"), as can be seen from the table above, businesses are expected to incur less compliance costs and costs from administrative burden between 2016 and 2030 than they would in the baseline scenario.

In absolute terms, compliance costs are expected to decrease by 1,017 EURm to 19,314 EURm compared to the overall amount incurred in the baseline scenario. This equals a reduction of roughly 5%.

As argued in the REFIT section 6.2.2, the magnitude of the compliance costs should be seen in relation to the overall value of EU GDP. This way, the magnitude of compliance costs is marginal compared to the overall value of the economy.

As regards the costs from administrative burden, reductions are expected to be less pronounced. Overall, it is expected that 34,000 Euro can be saved under policy option 3 ("publishers solution") between 2016 and 2030 at EU level. This is expected to result in an overall amount of 3.4 EURm of costs from administrative burden. The reduction is expected to be 2% compared to the overall amount incurred in the baseline scenario.

Impacts on costs for public authorities

In the table below, we provide an assessment of the impacts of policy option 3 on public administrations. The table contains:

- Qualitative reasoning used for the quantitative assessments of the impacts of the policy options on businesses (in particular on compliance costs and costs related to administrative burden) complemented where possible with exact cost estimates;
- A rating of the magnitude of these costs, according to the scheme portrayed below, serving to make the impacts of the options comparable; and

- The frequency of costs (as far as information is available).

The general approach used for these qualitative ratings is outlined in Annex A on the Analysis of the impacts of the policy options on the costs for public administrations.

No difference has been made between the three different sub-options foreseen by policy option 3 as each of them is expected to have the same impact on public authorities.

Table 93 – Qualitative classification of the impacts of policy option 3 on costs for public administrations

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
Objective 1: Ensuring effective confidentiality and security of communications				
1. The new instrument would propose a technology neutral definition of electronic communications, encompassing all the additional elements under **Option 2** (1, 2 and 3). It would specify a general principle of confidentiality of communications (i.e. nobody can process data relating electronic communications), except with the consent of the parties to a communication.	See the table on policy option 2 for the detailed assessment.	MS	-1	One-off and recurring
2. Clarify that **consent can be given by means of the appropriate settings** of a browser or other application. Consent under this option will be in line with the concept of consent under the GDPR[551]. Require browsers and/or other similar platforms to provide their products and services with **privacy friendly settings to reinforce user's control** over the flow of data from and into their terminal equipment. This may also entail addressing the interactions between web sites, advertisers and users regarding whether they accept to be tracked, for example there may be a situation where a user may have set a default privacy setting rejecting third party cookies and thus disallowing the tracking but the user is ready to accept third party cookies/tracking from a particular tracking. This option does not provide for a **prohibition of the practice of denying access to a website** or an	The Commission would need to bear costs related to the drafting of such standards/delegated acts. It can be assumed that it would need to devote slightly more resources to this in the beginning. Updates or additional guidance may then become necessary at a later stage as well. It may be assisted by ENISA or the JRC on these matters. We note that no budget change is foreseen for this.	EU	1	One-off and recurring

[551] See Recital 32 of the GDPR: "*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website,* ***choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data****. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided*."

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
online service in case users do not provide consent to third party cookies/tracking. Under the new instrument, the Commission would be empowered to issue delegated acts or to mandate industry standards under EU rules (e.g. Radio Equipment Directive) to impose these requirements.[552]				
3. Impose enhanced transparency requirements on entities processing communications data (e.g., websites, mobile apps and Wi-Fi), by obliging them to display a concise privacy warning message (e.g. informing users accessing free online services that "the service is financed by OBA and the users' browsing data will be used for this purpose"). The Commission would have implementing powers to specify the exact form and content of the message to be displayed.	No specific impact on public administrations is expected.	EU/MS	0	
4. Reinforce and streamline enforcement powers: The new instrument would lay down effective investigation and enforcement powers of national competent authorities. This would address the problems of ineffective and inconsistent enforcement.	Additional resources could be needed to implement the powers to impose **sanctions for breaches** of ePrivacy rules.	MS	1	One-off and recurring
Objective 2: Ensuring effective protection against unsolicited communications				
5. All the measures from 4 to 5 under **Option 2**.	See the table on policy option 2 for the detailed assessment.	MS	0	Recurring
6. Require opt-in consent for all types of unsolicited communications, while keeping the existing business relationships exception for email.[553]	Some Member States already follow this approach. For the others, it is expected that the costs relating to overseeing these provisions would not change significantly after introducing an opt-in regime.	MS	0	Recurring
7. Clarify the provision on presentation of calling line	No significant impacts are expected.	EU/MS	0	

[552] Regulation 1025/2012/EU, OJ L 316, 14.11.2012, p. 12–33.

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
identification to include the right of users to reject calls from specific numbers (or categories of numbers).				
Objective 3: Simplifying the legal framework and adapting it to the new market and technological reality				
8. Propose changes aimed at **clarifying and minimising the margin of manoeuvre of certain provisions** identified by stakeholders as a source of confusion and legal uncertainty.[554]	The Commission would need to assign staff to drafting the new piece of legislation and to follow the legislative process.	EU	1	One-off
	As the measures under this policy option would be adopted in form of a Regulation, there would be no costs from transposing the piece of legislation. The old rules only would need to be repealed.	MS	1	One-off
9. Consider introducing consistency mechanisms for the ePrivacy rules.	The option does not specify clearly, what the consistency mechanism would entail. We assume that it would be similar to that of the GDPR. Such a consistency mechanism would entail additional costs for the authorities. In particular, they would need to spend additional time, including to cooperate and exchange information with other authorities. The main costs for competent authorities would relate to the additional need for resources as the consistency mechanism would be broadened to aspects relating to the ePD. In relation to GDPR matters, it was estimated in the related Impact Assessment that authorities would need at least 2 or 3 persons working on matters in relation to the consistency mechanism.[555] The efforts related to an ePrivacy consistency mechanism would be less compared to the efforts required for the GDPR-related aspects. It could e.g. be assumed that each authority would need to assign 0.25 FTE for such tasks. At the same time, the implementation of the consistency mechanism would slightly decrease the case load of national authorities in relation to cross-border cases. More specifically, the authorities would no longer be directly involved in cases where the data controller has its main establishment in another Member State. On this basis, the overall impact is assessed to entail moderate costs. As the option only aims at considering a consistency mechanism, these	MS	1	

[554] This would cover in particular more detailed rules on the scope of the ePrivacy instrument, the exceptions to the consent requirements and the scope of the unsolicited communications provisions.
[555] Commission Staff Working Paper on Impact Assessment on the General Data Protection Regulation proposal, 25.01.2012, SEC 2012(72), p 103. We note that it was not indicated whether these persons would be FTEs.

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
	costs would of course only be incurred if a decision is actually taken.			
	Again, we assume that it would be similar to that of the GDPR. EU bodies would be involved to handle notifications of cases with a European impact. The consistency mechanism under the GDPR requires resources particularly from the EDPS, provides the secretariat of the European Data Protection Board and operates the IT system to be used for the communication between national authorities and the European Data Protection Board. For GDPR related aspects, it was estimated that the tasks require 10 FTE posts and that the EDPS budget would have to be increased by approximately 3 million Euros annually on average for the first six years of operation.[556] It can be assumed that the creation of a consistency mechanism would be considerably less compared to the consistency mechanism for the GDPR. For example, it is possible that about one fifth of the resources would be needed, equalling 1-2 additional FTEs at the EDPS to account for the increased work load and an increase in the budget of 600000 for the first six years. This is, however, only an estimate based on the content of the two instruments. As the option only aims at considering a consistency mechanism, these costs would of course only be incurred if a decision is actually taken.	EU	1	
10. Repeal provisions on security, automatic call forwarding and the provisions on itemised billing.	The data breach provisions explicitly require the involvement of authorities. Authorities need to deal with the data breach notifications of businesses, which includes correspondence as well as potentially checking that the service providers implemented appropriate technological protection measures. The actual number of data breaches dealt with varies significantly per Member State.[557] In the Online survey carried out by Deloitte with competent authorities, tasks related to Article 4 were considered among the most time-consuming tasks. Yet, again the actual time spent depends very much on the Member State. For example, as concerns the time to deal with one personal data breach, three authorities indicated that this takes less than one working day, 4 indicated that it takes between 1 day and less than a week and three	MS	-2	Recurring

[556] Commission Staff Working Paper on Impact Assessment on the General Data Protection Regulation proposal, 25.01.2012, SEC 2012(72), p 103.
[557] For example, in 2015, the highest number of complaints was reported for Ireland (2317), followed by the UK (550). Sweden (24), Greece (15), Estonia (5), Romania (3) and Belgium (1) followed with significantly less. Cyprus and Croatia reported that no breaches occurred. No information is available for the other Member States.

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
	authorities indicated that it takes 1 week or more. None of the authorities consulted indicated that the provisions on itemised billing require significant resources. Thus, the impact of repealing these provisions is assumed to be negligible. On this basis, the overall impact is assumed to be medium.			
11. Repeal the provisions on traffic data and location data to reflect the fact that the traffic and location data are more and more a homogeneous category, both in terms of privacy intrusiveness and technological availability. The processing of traffic and location data will be regulated under the general provision of confidentiality of communications.	As the content of the provisions is not changed significantly, the impact of this change are expected to be negligible.	MS	0	
12. Specify that service providers can only process communications data with the consent of the users, although they are allowed to refuse access to the services in the absence of consent. Providing for additional/broadened exceptions to the consent and enhanced transparency rules (points 1, 2 and 3 above) for specific purposes which give rise to little or no privacy risks: a. Transmission or service: the processing of communications data is necessary for the purpose of the transmission of the communication or for providing a service requested by the user. b. Security: the processing of traffic data is necessary to protect, maintain and manage the technical security of a network or service, with appropriate privacy safeguards. c. Billing: in line with the current provision on traffic data, communications data may be retained insofar as necessary for billing or	No significant impacts are expected. As concerns the exceptions on cookies, the situation may be more complex compared to the current situation. Under the current regime, every website using cookies in principle needed a banner. Under this policy option, authorities would need to differentiate between websites using cookies that are not privacy invasive and covered by the exceptions, and those using privacy invasive techniques. Yet, we note that such analyses have been carried out in the past using statistical automated tools. For example, in the Cookie Sweep Action organised by the WP29 in 2015, a distinction between first party and third party cookies was already made.[558] Thus, we do not expect that the exceptions would lead to higher costs for authorities.	MS	0	Recurring

[558] See: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp229_en.pdf

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
network management purposes. d. For a lawful business practice provided that there are no significant risks for the privacy of individuals. In particular, the data collection is performed solely by the entity concerned or third-parties on behalf of the ECS for the purpose of web analytics and web measurement.				
Overall implications (EU)			**3**	
Overall implications (MS)		**0**		

Source: Deloitte

Other economic impacts

Based on the **extension of the scope to OTTs**, this option would impacts on the **competitive relationship between ECS and OTT providers**. At the same time, **OTTs would face stricter standards compared to the current situation**. These points, including their effects on **SMEs**, are discussed in detail under policy option 2. However, the negative effects on these players would be smaller compared to option 2 based on the **repeal of the provisions on traffic and location data.** On this basis, the restrictions faced by the new players would not be as severe. In addition, this would have positive impacts on telecom providers, as the regime on communications data would be less strict and complex, placing them on an equal footing with OTT.

Based on the **enhanced transparency requirements on the entities processing communications data**, the businesses that need to implement these requirements may face **opportunity costs**. Based on the warning message, it is possible that some consumers may refrain from using the website/service concerned. At the same time, the behaviour of most consumers is not based solely on privacy risks but to a great extent also on benefits associated with a current service. On this basis, the likelihood that they use another service may depend on the existence of valid alternatives.[559]

The **introduction of a "do not track by default"-solution** (Point 2) would also lead to **opportunity costs**, because OBA may not be an as effective tool anymore as it is today. However, the exact effects depend on consumers' behaviour. In principle, there are different possibilities for consumers:

- It may be expected that many consumers do not change the privacy by default setting once it is set on do-not-track by default. They would in this scenario not be tracked, unless they provide for exceptions to this rule, i.e. allow specific websites to track them. In this context it is important to note that the option does not prohibit the practice of denying access to a website/service in case the user does not give his/her consent. Thus, many consumers will (as in the current situation) still give their consent if needed. It is likely that many consumers may do this for those websites they regularly use, trust and/or are dependent on. Their choice will also depend on the extent to which cookies or other technologies are needed for the services they use.
- Some consumers may change the settings so that they allow all websites to track them by default. They could then still prohibit tracking for individual websites. It is possible that consumers, who feel that they do not track setting hinders their web-browsing experience and/or who do not value privacy, choose this option. Here, the situation would be comparable to the current situation.

On this basis, it is possible that cookies or other technologies would be accepted for a smaller number of websites compared to the baseline scenario. This hinders businesses to "get to know" their customers online and, thus, provide them with targeted advertisements for more efficient sales. In addition, this could also have an impact on consumer prices because it is the efficiency of OBA that enables businesses to lower prices for specific target customers (which in turn increases the number of customers and thus the overall sales revenue). Yet, based on the likely behaviour of consumers in light of current experiences with the cookie banner, many consumers will still consent to being tracked by websites they need. On this basis, these impacts would likely not be very high.

[559] On the privacy paradox, see for example: https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Liu_Privacy-paradox_v10.pdf

Moreover, the do-not-track by default could have **negative impacts on competition** with larger, established market players who may have an advantage over smaller companies (especially those entering a market, e.g. from across borders) due to their sheer size and existing customer base, as well as the inability of SMEs to catch-up by providing efficient, innovative solutions based on OBA.

It is also possible that **software developers** (i.e. those supporting businesses with the implementation of the consent mechanism) would incur losses, because under the do-not-track by default solution, privacy is built-in by design. The magnitude of this negative impact is, however, not clear because: (1) The magnitude depends on whether the browser solution, tracking company solution or publishers solution would be chosen. It is expected that the losses would be bigger under the browser solution, as only a very limited number of companies (mainly browser providers) would need to implement the relevant privacy solutions. Under the other solutions, a larger number of players may still need services to implement consent mechanisms (tracking companies or publishers); (2) No software developer only works on privacy solutions. This means that albeit their sales could take a small decrease, they would simply focus their operation on another service; (3) Software developers would find another product / service they can sell in another market (e.g. also outside the EU) as a replacement of online privacy solutions; and (4) The overall market for software developers is growing. This means that although online privacy solutions as a service would decline in terms of economic importance, the overall revenues are still expected to grow in the future due to the general market trend and new types of software to be developed in the future.

Based on the **clarification of the scope of Article 13 on unsolicited communications**, additional businesses may incur opportunity costs. This is discussed in detail under policy option 2.

The change to a pure opt-in scheme on unsolicited communications will lead to opportunity costs for advertising businesses in the Member States that currently employ an opt-out scheme. The relevant businesses would have to review their business models and limit marketing by only sending out unsolicited communications to subscribers for which they have received consent. This is expected to raise the costs of marketing campaigns.

The table below further illustrates the wide diversity of regimes on unsolicited communications calls (with human intervention) and the fragmentation of the rules in the EU. The table shows that in relation to fixed-line phones, 9% of EU businesses currently are governed by an opt-in regime while the share is 36% in relation to mobile phones. By contrast, 91% of EU businesses are currently governed by an opt-out regime in relation fixed-line phones while 64% are governed by an opt-out regime in relation to mobile phones.

Table 94 – Opt-in and opt-out regimes per Member State

Member States	Number of businesses	Fixed-line phones		Mobile phones	
		Opt-in	Opt-out	Opt-in	Opt-out
Austria	321,661	X		X	
Belgium	593,421		X	X	
Bulgaria	319,856	X		X	
Croatia	147,337		X		X
Cyprus	46,938	X		X	
Czech Republic	995,754		X		X
Denmark	212,740	X[1]	X[2]	X[1]	X[2]
Estonia	64,040		X		X

Member States	Number of businesses	Fixed-line phones		Mobile phones	
		Opt-in	Opt-out	Opt-in	Opt-out
Finland	229,248		X		X
France	3,188,138		X	X	
Germany	2,193,135	X[1]	X[3]	X[1]	X[3]
Greece	700,166		X		X
Hungary	514,537	X		X	
Ireland	146,741		X	X	
Italy	3,715,164		X		X
Latvia	100,491	X		X	
Lithuania	174,611	X		X	
Luxembourg	31,385	X		X	
Malta	26,193		X		X
Netherlands	1,054,562		X		X
Poland	1,549,326		X		X
Portugal	781,823		X		X
Romania	455,852	X		X	
Slovakia	400,683	X[1]	X[3]	X[1]	X[3]
Slovenia	130,088		X		X
Spain	2,377,191		X	X	
Sweden	673,218		X		X
United Kingdom	1,841,715		X		X
		11	20	15	16
Number / share of businesses affected	22,986,014	1,965,331	21,020,683	11,077,380	14,715,192
	100%	9%	91%	36%	64%

Source: European Commission, tabulation by Deloitte. [1]For 'consumers'; [2] For 'businesses'; [3] For 'other market players'. Statistical data from taken from Eurostat (most recent data from 2014).

The fact that the new e-privacy instrument would be a **Regulation** together with **clarification of certain rules** would address the issue of fragmentation. In addition, the consideration to introduce the **consistency mechanism** for e-privacy may positively contribute to consistent implementation. These measures would have a **positive impact on the internal market and potentially on revenues of businesses**. Businesses considering cross-border activities would no longer face 28 different legal frameworks, but would be able to rely on harmonised rules across the EU. On this basis, cross-border activities would be less complicated and less costly compared to the baseline scenario.

On this basis, the picture is mixed: this policy option would have some negative impacts in particular for businesses that need to implement Article 5(3) and Article 13 (notably on opportunity costs and competition, as explained above). At the same time, there would be positive impacts based on the reduction of fragmentation and the repeal of the provisions on traffic and location data.

9.5.3 Effectiveness in reaching the policy objectives

In this section, the effectiveness of policy option 3 in reaching the policy objectives is assessed. It is shown in the following sub-sections that the effectiveness of this option is high to all specific objectives.

Specific Objective 1: To ensure effective confidentiality and security of communications

In addition to the positive impacts described under policy option 2, this option would further support the effective confidentiality and security of communications by **specifying a general principle of confidentiality of communications.** On this basis, the rules would be more transparent and would encompass more situations/services, thus supporting the achievement of this objective.

In addition, the **new rules introduced in relation to Article 5(3)** (Points 2 and 3) would further reinforce the transparency of the use of cookies and other tracking technologies.

The clarification that consent may be given via browsers and requiring the providers to implement privacy friendly settings by default, would increase protection and transparency. For example, users would in fewer instances be tracked unknowingly, if tracking is rejected by default and only allowed in case the users make exceptions for specific services. In addition, this measure would simplify the management of consent for users. Yet, the exact effects would depend on the solution chosen. Under the browser solution, users would be able to manage their preferences in a centralised way for all online services, which is expected to be the least complicated option. We also note in this context that disabling tracking via the *Firefox* in-browser protection decreased median load time for webpages by 44% and data usage by 39% (for a sample of top 200 *Alexa* news sites).[560]

The introduction of increased transparency requirements would further support this objective, as consumers would receive clearer information on what websites do with their data. On this basis, they may take informed decisions about which services to use.

Finally, by **streamlining and reinforcing the enforcement**, this option would contribute to a more effective and consistent enforcement of the rules.

On this basis, policy option 3 would significantly contribute to achieving this objective.

Specific Objective 2: To ensure that citizens are effectively protected against unsolicited marketing communications

In addition to the positive impacts described under policy option 2, this option would further support the achievement of this objective.

The **imposition of the opt-in consent** would increase the protection of users, as an opt-in regime increases the hurdle for businesses use unsolicited marketing communications. In particular, this would reduce the possibility of error by direct marketers, i.e. reaching persons that do not want to be reached, and shift the burden of proof from citizens to callers to demonstrate that they have the person's consent. This would mean that citizens may receive less marketing communications they do not want. In addition, it would be easier for citizens to seek legal redress and enforcement of the rules.

[560] Kontaxis, Georgios and Chew, Monica (2015): Tracking Protection in Firefox For Privacy and Performance, http://ieee-security.org/TC/SPW2015/W2SP/papers/W2SP_2015_submission_32.pdf.

In addition, the **clarification of the rule on calling line control** would make it easier for citizens to avoid unwanted marketing calls, as they would be able to block certain (categories of) numbers.

Thus, this option would significantly contribute to achieving this objective.

Specific Objective 3: To simplify the legal framework and adapt it to the new legal, market and technological reality

In addition to the positive elements of Option 2, this option would further contribute to achieving this objective.

In general terms, the fact the e-privacy instrument would be adopted in the **form of a regulation** and the **clarification of certain rules** would contribute to simplification and harmonisation. As noted in the section on economic impacts, this would improve the situation for businesses. It would also increase transparency for citizens.

The **changes to Article 5(3)** would also contribute to the simplification. In particular, under the browser solution enforcement of the rules would be easier as fewer players would be covered.

The potential **introduction of a consistency mechanism** would contribute to a more consistent and effective enforcement, as competent authorities would cooperate and exchange information on an organised basis.

The **repeal of outdated or unnecessary provisions** and **the introduction of exceptions for consent** would further simplify the regulatory framework and ensure consistency with other pieces of legislation, such as the GDPR. For example, the deletion of Article 4 would prevent a duplication of notification schemes. In addition, this option would ensure that the new instrument would be in line with the market and technological reality. For example, the introduction of exceptions for Article 5(3) means that non-privacy invasive techniques are no longer covered by this provision. On this basis, fewer websites would be covered by Article 5(3).[561]

Thus, this option would achieve this objective.

9.5.4 Social impacts

No significant social impacts are expected.

9.6 Policy Option 4: Far reaching reinforcement of privacy/confidentiality and simplification

Under this option, the Commission would propose a new ePrivacy Regulation with more far reaching measures reinforcing the protection of privacy/confidentiality and guaranteeing greater simplification/harmonisation.

The specific elements of the policy option can be found in chapter 8.2.

[561] Based on the 2014 Cookie Sweep, 74 out of 474 websites only used first party cookies. In addition, 15 out of 474 only used session cookies (first and third party). Article 29 Data Protection Working Party (2015), Cookie Sweep Combined Analysis – Report, WP 229.

9.6.1 Overview of assessments

In the following table we present an overview of our assessment of policy option 4. The detailed assessment according to the individual assessment criteria can be found in the following sub-sections.

Table 95 – Qualitative rating of the impacts of Policy Option 4

Assessment criteria	Rating			Brief explanation of the rating
	"Browser solution"	"Tracking company solution"	"Publisher solution"	
Economic impacts				
Impacts on costs for businesses	-4	-2	-1	While some new cost elements would apply, businesses would overall incur less compliance costs and administrative burden compared to the baseline scenario. Significant savings would in particular be incurred due to the changes to Article 5(3) and the introduction of additional exceptions. Cost savings would be largest in the browser solution.
Impacts on costs for public authorities	4	4	4	This option would entail some additional costs for the EU, e.g. related to the drafting of standards (rated at 3) and some additional costs for the Member States, e.g. related to additional enforcement efforts needed (rated at 1).
Other economic impacts	3	3	3	This policy option would have the same impacts option 3. In addition, further opportunity costs and effects on competition and the digital economy can be expected based on further restrictions of the advertisement business.
Effectiveness in reaching the policy objectives				
Objective 1: To ensure effective confidentiality and security of communications	-3	-3	-3	This option brings important improvements, e.g. based on the extension of the scope and the proposed changes to Article 5(3). While protection for citizens will be particular high when browsing the web, the repeal of some additional provisions such as those on calling line identification and directories of subscribers would have negative effects.
Objective 2: To ensure that citizens are effectively protected against unsolicited marketing communications	-3	-3	-3	The clarification of the provision and introduction of a special prefix would bring would bring important improvements. In addition, the imposition of the opt-in consent would increase the protection of users who would benefit from more transparent and effective rules across the EU. This option would further increase citizens' protection by repealing the provision allowing marketers to target previous customers. On this basis, citizens would receive a smaller number of marketing communications without consent.
Objective 3: To simplify the legal framework and adapt it to the new legal, market and technological reality	-3	-2	-2	This option would have a positive impact on this objective, notably by clarifying certain provisions, reinforcing the cooperation between competent authorities and repealing the security rules. It provides for additional consistency by giving the Commission implementing powers for deciding on the application of the ePD and by repealing additional consumer provisions.
Social impacts	1	1	1	There may be some negative effects on

Assessment criteria	Rating			Brief explanation of the rating
	"Browser solution"	"Tracking company solution"	"Publisher solution"	
				employment.
Total	-5	-2	-1	

Source: Deloitte

9.6.2 Economic impacts

Within this section on the assessment of the economic impacts of policy option 4, we are focusing on three key aspects: (1) The impacts on compliance costs and administrative burden for businesses (incl. SMEs and micro-enterprises), and (2) on costs for public authorities; as well as (3) other economic impacts such as on competiveness and competition in the Digital Single Market.

For illustrative purposes, we focus on the "browser solution" only as cost savings would be largest here.

Impacts on compliance costs and administrative burden for businesses

In this section, we provide the following:

- ***Part A:*** A detailed qualitative assessment table regarding the impact of each element of the policy option 4; and
- ***Part B:*** The key quantitative findings from the economic analysis in relation to the impact of policy option 4.

The former will feed into the latter with regard to the assessment of the economic impact of the policy option.

Part A: Detailed qualitative assessment tables

A more **detailed qualitative assessment table** regarding the impact of each element of policy option 4 is provided below. The table contains:

- Qualitative reasoning used for the quantitative assessments of the impacts of the policy options on businesses (in particular on compliance costs and costs related to administrative burden);
- An indication of the types of businesses affected by each element;
- Qualitative rating / colour coding of the expected impacts of each element of the options;
- An indication whether or not businesses would incur compliance costs or costs related to administrative burden from each specific element;
- The frequency of costs (as far as information is available); and
- The existence / emergence of opportunity costs in relation to each of the elements of the policy options.

As described in Annex A on the *general approach used to translate qualitative reasoning into quantitative assumptions*, the ratings contained in the below table of this Part B have been used as a qualitative basis for the quantitative assessment of the impacts of the policy options in Part A above.

Table 96 – Qualitative classification of the impacts of policy option 4 on costs for businesses

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
Objective 1: Ensuring effective confidentiality and security of communications						
1. All the measures under No 1, 2, 3 and 4 of Option 3.	See below.					
i. Extension of the scope of the ePD to OTTs providing communications functions, such as webmail, Internet messaging, VoIP.	OTT providers would need to implement the entire ePD. This would entail a review and adaptation of their current data processing practices, which would be based on thorough legal review of the new rules, potentially with external support. Ongoing compliance would also increase.[562] While the costs associated with Art. 5.3 and 13 should already apply to these players now, additional costs would ensue based on the implementation of other provisions (e.g. confidentiality of communications).	OTT	1	x		One-off and recurring
	Administrative burden would not increase significantly, as the main cause of administrative burden (Article 4) will be removed. Some costs may ensue in relation to audits. We note in this context that these businesses will already face some costs in relation to audits based on the new requirements of the General Data Protection Regulation. Thus, while the costs based on the ePD would increase, the actual costs that these business will incur at the end may not change significantly.	OTT	1		x	Recurring

[562] Although they may follow some of the requirements, e.g. relating to confidentiality of communications, already now voluntarily, these would then be because of the ePD.

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
ii. Clarify that the ePD applies to publicly available communications networks, such as in particular commercial Wi-Fi networks in stores, hospitals, airports, etc. Only services which occur in an official or employment situation solely for work-related or official purposes, as well as use of services for exclusively domestic purposes, may be exempted.	Business may need to spend less time on interpreting the provisions. Potentially, this also decreases the need for legal advice. At the same time, there may be more businesses applying the ePD (e.g. those that previously did not consider their Wi-Fi network or IoT devices to be covered).	All businesses	0	x		Recurring
iii. On the protection of terminal equipment devices: Specify that the protection applies to any machine that is connected to the network (including M2M communications, such as for example, a refrigerator connected to a grocery store web site).	Business may need to spend less time on interpreting the provisions. Potentially, this also decreases the need for legal advice. At the same time, there may be more businesses applying the ePD (e.g. those that previously did not consider their Wi-Fi network or IoT devices to be covered).	All businesses	0	x		Recurring
iv. Clarify that consent can be given by means of the appropriate settings of a browser or other application. Consent under this option will be in line with the concept of consent under the GDPR[563]. Require browsers and/or other similar platforms to provide their products and	The businesses concerned need to implement privacy-friendly settings. We note that at least some browsers already offer such functions. The extent to which these would have to be updated depends on the exact specifications mandated by the Commission and the solution taken with respect to settings for individual websites. Slightly higher costs for providers of browsers would emerge if solution 1 is adopted,	Providers of browsers	1	x		Mainly one-off

[563] See Recital 32 of the GDPR: "*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website,* ***choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data****. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided*."

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
services with privacy friendly settings to reinforce user's control over the flow of data from and into their terminal equipment. This may also entail addressing the interactions between web sites, advertisers and users regarding whether they accept to be tracked, for example there may be a situation where a user may have set a default privacy setting rejecting third party cookies and thus disallowing the tracking but the user is ready to accept third party cookies/tracking from a particular tracking. This option does not provide for a **prohibition of the practice of denying access to a website** or an **online service** in case users do not provide consent to third party cookies/tracking. Under the new instrument, the Commission would be empowered to issue delegated acts or to mandate industry standards under EU rules (e.g. Radio Equipment Directive) to impose these requirements.[564] *NB: There are different potential technical solutions to facilitate users to diverge from their default setting for individual websites, all with different implications on costs. The following scenarios exist: (1) All*	i.e. if all communication would run via the browsers. Browsers would then need to implement functions that enable the users to diverge from their default settings for individual websites. However, such solutions already exist, which is why it can be expected that they would be relatively easy to implement. In general, this element only concerns a small fraction of all businesses applying the ePD. The browser market itself is highly concentrated in Europe: Users of *Google*'s *Chrome* browser account for a half of all website visitors, while close to a third of all users relies on Safari and Firefox. Four major companies dominate the market of browsers used by consumers: 94% of all website visitors in Europe rely on software from *Google* (*Chrome*, *Android browser*), *Apple* (*Safari*), *Microsoft* (*IE*, *Edge*, *IEMobile*) and *Mozilla* (*Firefox*). There are some additional browser operators with smaller market shares, including e.g. *Opera* and *Yandex*.[565] On this basis, an overall moderate increase for browsers may be expected for all three solutions.					
	Additional impacts for solution 1 (All communication runs centralised via the browsers)					
	Assuming that the communication would exclusively run via the browsers, all the costs would lie with the browser providers (as reflected above). Websites on the other hand, would have no specific costs. Thus, in comparison to the current situation, websites would save the costs they incur now to implement the cookie banner. As this is considered the main cost associated for	Website operators	-3	x		

[564] Regulation 1025/2012/EU, OJ L 316, 14.11.2012, p. 12–33.
[565] Data for geographic Europe only, based on visitors of a sample of 3 million websites globally accessible on http://gs.statcounter.com/

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
communication runs centralised via the browsers; (2) The party placing the cookie is responsible for asking the consent; (3) Individual websites are responsible for asking the consent. In agreement with the Commission, we provide alternative assessments for these three points.	businesses with the ePD, this would be a significant decrease.					
	Additional impacts for solution 2 (The party placing the cookie is responsible for asking the consent)					
	Websites would have no specific costs. Thus, in comparison to the current situation, websites would save the costs they incur now to implement the cookie banner. As this is considered the main cost associated for businesses with the ePD, this would be a significant decrease.	Website operators	-3	x		
	In this scenario, the costs would lie with the companies placing the data. It is expected that this would be slightly more expensive compared to solution 1, as a higher number of businesses would be concerned. Although most tracking cookies are placed by few main players, other smaller players will be affected as well. Furthermore, this solution would require the development of new practical and technical solutions to implement the option.	The parties placing the cookie	2	x		
	Additional impacts for solution 3 (Individual websites are responsible for asking the consent)					
	In this case, there would be no significant changes for website operators, as they would in principle still employ cookie banners (or a similar technical solution).	Website operators	0			
v. Impose enhanced transparency requirements on entities processing communications data (e.g., websites, mobile apps and Wi-Fi), by obliging them to display a concise privacy warning message (e.g. informing users accessing free online services that "the service is financed by OBA and the users' browsing data will be used for this	All businesses would need to check whether this provision applies to them. Those businesses processing or monitoring the usage of terminal equipment would need to update their website to implement the new message. As it is just a notification and not a consent mechanism, this should be relatively easy to implement. In addition, it is assumed that a relatively small number of businesses would be concerned by this change.	All businesses processing or monitoring the usage of terminal equipment	1	x		Mainly one-off

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
purpose"). The Commission would have implementing powers to specify the exact form and content of the message to be displayed.						
vi. Reinforce and streamline enforcement powers: The new instrument would lay down effective investigation and enforcement powers of national competent authorities. This would address the problems of ineffective and inconsistent enforcement.	There are no direct costs stemming from this element. There may be small savings based on the increased clarity as to the competent authority. The costs associated with penalties cannot be estimated as these would occur only in case of breaches. We also note that some penalties already exist in Member States.	All businesses	0	x	x	One-off & recurring
2. Explicitly prohibit the practice of denying access to a website or an online service in case users do not provide consent to tracking (so-called cookie-wall).	The prohibition of denying access to a website/service in case users do not consent to tracking will lead to an increase of IT costs for businesses. Businesses will need to amend their websites/services so that they are also available to the extent possible without the use of cookies. For example, this could mean that in effect two versions of website need to be offered. There may also be a loss of revenue, e.g. because advertisements would be worth less if they cannot be targeted based on users' behaviour.	Website operators	3	x		
Objective 2: Ensuring effective protection against unsolicited commercial communications						
3. All the measures under No 5, 6, and 7 of Option 3.	See below.					
i. Clarify the scope of the provision and make it technologically neutral: clarify that it applies to any form of unsolicited electronic communication, irrespective of the technological means used. The provision would apply, for	Business may need to spend less time on interpreting the provisions. Potentially, this also decreases the need for legal advice. At the same time, there may be more businesses applying the ePD.	All businesses	0	x		Mainly one-off

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
example, also to advertisings messages sent on OTT platforms.						
ii. Mandate the use of a special prefix distinguishing direct marketing calls from other calls.	Some costs may ensue from the obligation to use a specific prefix in order to distinguish direct marketing calls from other calls. These costs relate to (1) the subscription to having such a number; (2) paying the calls issued to customers; and (3) registering such a number with the national telecommunication authority. For one business, this may cause costs of around 500 Euro yearly. We provide further details on this cost estimate in the text box below Table 81.	All businesses	1	x		One-off & recurring
iii. Require opt-in consent for all types of unsolicited communications, while keeping the existing business relationships exception for email.[566]	The businesses in Member States that currently apply the opt-out regime would need to revise their practices and update the mechanisms they use to obtain consent. This would entail e.g. the technical implementation of consent boxes on their websites. However, the practices would only change in some of the Member States. In Member States that already apply the opt-in regime, no additional costs would ensue. As concerns the ongoing costs, it is expected that they are similar under both regimes. Furthermore, some cost savings may be expected as the situation will be simplified due to harmonisation. Therefore, businesses operating in different Member States would no longer need to implement different regimes. On this basis, an overall moderate increase is expected.	All businesses	1	x		One-off & recurring

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
iv. Clarify the provision on presentation of calling line identification to include the right of users to reject calls from specific numbers (or categories of numbers).	No costs for businesses are expected to be associated with this element as it does not entail changing the current technical systems in place with regard to calling line identification and there is no need to introduce a new system.		0			
4. Under this option, the Commission would also repeal the provision allowing direct marketers to send communications to subscribers and users when they have received their contact details in the context of a previous business relationship[567].	Revision of practices, possibly legal advice, possibly additional efforts to retrieve consent	All businesses	3	x		One-off & recurring
Objective 3: Simplifying the legal framework and adapting it to the new market and technological reality						
5. Measures 8 - 12 of Option 3	See below.					
i. Propose changes aimed at **clarifying and minimising the margin of manoeuvre of certain provisions** identified by stakeholders as a source of confusion and legal uncertainty.[568]	There would be cost savings in relation to legal advice for businesses operating cross-border, as they would no longer need to deal with different legal framework. There would also be savings, as businesses would no longer need to implement different rules.	All businesses	-3	x		Recurring
ii. Consider introducing consistency mechanisms for the ePrivacy rules.	There may be some small cost savings as it may be clearer for businesses which authority they need to contact and as interchanges with authorities may be simplified.	All businesses	-1		x	
iii. Repeal provisions on security, automatic call forwarding and the provisions on itemised billing.	Business would no longer need to deal with personal data breach notifications under the ePD (only under the GDPR).	ECS	-3		x	

[567] Article 13(2).
[568] This would cover in particular more detailed rules on the scope of the ePrivacy instrument, the exceptions to the consent requirements and the scope of the unsolicited communications provisions.

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
	Small savings for businesses already applying Article 4. These savings would e.g. relate to the maintenance of systems. However, we note that similar costs may be incurred based on the GDPR. There would be no significant cost savings relating to the provision on itemised billing, as recurring costs are negligible based on feedback received from businesses.	Mainly ECS	-1	x		Recurring
iv. Repeal the provisions on traffic data and location data to reflect the fact that the traffic and location data are more and more a homogeneous category, both in terms of privacy intrusiveness and technological availability. The processing of traffic and location data will be regulated under the general provision of confidentiality of communications.	Possibly, there would be some small time savings / savings of legal advice due to simplifications. At the same time, the practices would need to be checked.	All businesses	0	x		
v. Specify that service providers can only process communications data with the consent of the users, although they are allowed to refuse access to the services in the absence of consent. Providing for additional/broadened exceptions to the consent and enhanced transparency rules (points 1, 2 and 3 above) for specific purposes which give rise to little or no privacy risks:	See below.					
a. Transmission or service: the processing of communications data is necessary for the purpose of	No significant costs would occur, as this is similar to the current exceptions.		0	x		One-off & recurring

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
the transmission of the communication or for providing a service requested by the user.						
b. Security: the processing of traffic data is necessary to protect, maintain and manage the technical security of a network or service, with appropriate privacy safeguards.	This would lead a simplification, resulting in fewer businesses that need to apply the provisions mentioned.	All businesses	-1	x		One-off & recurring
c. Billing: in line with the current provision on traffic data, communications data may be retained insofar as necessary for billing or network management purposes.	No cost-related impact is expected.	All businesses	0	x		
d. For a lawful business practice provided For a lawful business practice provided that there are no significant risks for the privacy of individuals. In particular, the data collection is performed solely by the entity concerned or third-parties on behalf of the ECS for the purpose of web analytics and web measurement..	On this basis, the number of businesses that need to obtain consent for using cookies would decrease significantly. On average, the businesses falling under this exception may thus be assumed to save 300 Euro per year.		-3	x		
e. Specify that service providers can only process communications data with the consent of the users, although they are allowed to refuse access to the services	The impact of this option depends on the types of safeguards specified (under discussion and review) and on the willingness of businesses to apply these safeguards. In theory, there could be additional costs for businesses to understand and implement the safeguards. At	The parties placing the cookies	0	x		

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
in the absence of consent. Providing for additional/broadened exceptions to the consent and enhanced transparency rules (points 1, 2 and 3 above) for specific purposes which give rise to little or no privacy risks:	the same time, there could be savings if the safeguards are applies, not too costly and businesses would not need to implement any mechanism for consent.[569]On this basis, it is not yet possible to indicate a robust rating.					
6. Commission's implementing powers for deciding on the correct application of the ePD instrument where there is an issue of consistency or coherence with EU law.	No significant impacts on businesses are expected.	All businesses	0		x	Recurring
7. Repeal the provisions on calling line identification and directories of subscribers.	It was indicated to Deloitte by businesses that these provisions do not entail any significant recurring costs. Only one respondent to the public consultation mentioned that there could be significant costs in relation to the provision on directories of subscribers. However, this would only apply to specific businesses. On this basis, no significant cost savings can be expected.	ECS	-1	x		Recurring
Overall implications (Compliance)	**Scenario 1 (Browsers)**		**-1**			
	Scenario 2 (Parties placing the cookies)		**1**			
	Scenario 3 (Websites)		**2**			
Overall implications (Admin burden)			**-3**			
Overall implications on the number of businesses affected	Based on the new exceptions, the website that use non-privacy invasive cookies would no longer be affected by the consent rule. Based on current statistics, this would lead to a 30% decrease. Depending on the development in relation to the use of cookies, the actual number could be slightly lower		**-8**			

[569] This also depends on the solution taken for point 2 of this option.

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency
	as well. An additional decrease is possible based on the possibility to introduce adequate safeguards. The magnitude of this impact is unknown, as it depends on the types of safeguards employed and the willingness of businesses to implement these. At the same time, Point 5(i) may lead to a moderate increase of businesses applying the ePD, as it is clarified that the scope of the provision is technologically neutral and e.g. also applies to advertisings on OTT platforms.					

Source: Deloitte

Part B: Key quantitative findings from the economic analysis

Policy option 4: Average annual values and changes compared to the current situation

Similarly to the information provided for the baseline scenario, the overall quantitative results of the analysis concerning policy option 4 are presented in Table 73:

- Number of businesses affected (in million);
- Compliance costs (in million Euro);
- Average compliance cost per business (in Euro);
- Administrative burden (in million Euro); and
- Average costs from administrative burden per business (in Euro).

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Annex A: Economic Analysis

Further information in this regard, as well as an explanation of the approach used for the estimation of the quantitative results data is provided in the section on the basic assumptions used for the assessment of the impacts of the policy options in Annex A concerning the Economic Analysis.

The following table presents the quantitative findings for policy option 4. The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Average annual value:* Denotes the average annual value of the quantitative indicator for which data has been estimated. This means, for instance, that 30,000 SMEs are affected by issues relating to the ePD per year (see the light blue cell), facing a total amount of 92.2 EURm per year (see the light green cell) at an average cost of compliance per business of 3,548 Euro (see the dark blue cell);
- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the average annual value compared to the baseline scenario (2016-2030); and
- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the average annual value compared to the baseline scenario (i.e. 2016-2030).

Visualisations of the year-over-year development of the quantitative indicators are presented afterwards, as well as overall values for the timeframe 2016-2030.

Table 97 – Key quantitative data estimated in relation to policy option 4 (2016-2030)

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Number of businesses affected (in million)	0.37	-3.33	-90.0%
Micro-enterprises	0.33	-2.98	-90.0%
SMEs	0.03	-0.24	-90.0%
Large enterprises	0.001	-0.008	-88.9%
Foreign controlled enterprises	0.01	-0.11	-90.1%

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Compliance costs (in million Euro)	1,287.6 €	-67.8 €	-5.0%
Micro-enterprises	1,152.3 €	-60.6 €	-5.0%
SMEs	92.2 €	-4.9 €	-5.0%
Large enterprises	3.2 €	-0.2 €	-5.0%
Foreign controlled enterprises	40.0 €	-2.1 €	-5.0%
Average compliance cost per business (in Euro)	3,548.1 €	3.174.7 €	850.0%[570]
Administrative burden (in million Euro)	0.22 €	-0.007 €	-3.0%
Micro-enterprises	0.18 €	-0.006 €	-3.3%
SMEs	0.03 €	-0.001 €	-2.9%
Large enterprises	0.00 €	0.000 €	0.0%
Foreign controlled enterprises	0.01 €	0.000 €	0.0%
Average costs from admin. burden per business (in Euro)	269.2 €	241.4 €	870.0%

Source: Deloitte

Under policy option 4, the analysis shows that – per year between 2016 and 2030 – around 370,000 businesses will be affected by the ePD in the EU. The majority of these businesses will be micro-enterprises with less than 10 employees (330,000). Around 30,000 SMEs that have between 10 and 250 employees are estimated to be affected per year until 2030 while the number of large enterprises is negligible. Approx. 10,000 foreign controlled enterprises that operate in the EU will be affected.[571]

The businesses affected by the ePD are estimated to incur an annual value of 1.3 EURb to comply with Art. 5(3) and Art. 13. In addition, these businesses are expected to incur an unspecifiable amount of additional costs with regard to other provisions such as the consumer provisions. Again, micro-enterprises are expected to incur the lion share of these costs (around 1.15 EURb).

On *average*, an EU business is expected to incur 3,548 Euro per year with regard to the ePD until 2030. This does, however, not mean that e.g. large enterprises may not incur significantly more costs while the costs may be significantly lower for micro-enterprises.

In addition to the compliance costs related to the direct implementation of the ePD, businesses will also incur significant opportunity costs for lost business opportunities.

In relation to administrative burden, mostly stemming from the notification obligations for telecommunication service providers under Article 4, it has been estimated that an annual amount of 220,000 Euro is incurred, i.e. around 269 Euro per affected business per year.

[570] This increase of the average compliance cost per business (in Euro) by 850% is explained by the following reasoning: While it is expected that the policy option reduces the number of affected businesses by 90%, the overall costs are only expected to decrease by 5%. This means that the financial burden would have to be shouldered by less businesses (in relative terms) compared to the baseline scenario. This means that each business is expected to incur, on average, more costs under this policy option than in the baseline scenario. Overall, however, the compliance costs are still expected to be lower under this policy option than in the baseline scenario.

[571] The estimated numbers of affected businesses should be understood as annual values. However, the overall number of businesses affected by the ePD between 2016 and 2030 is not the sum of each annual value. The reason for this is that the majority of businesses will be affected not only once but on several occasions across this time frame while some businesses will be replaced by others due to the general life cycle of businesses (company birth, insolvency). This means that, in relation to the former argument, the projected value is likely underestimating the actual number of businesses affected, while the latter argument, the projection is likely to overestimate the number of affected businesses.

Policy option 4: Visualisation of the development 2016-2030

In this section, we present visualisations of the development of the following quantitative indicators between 2016 and 2030 under policy option 4:

- The number of businesses affected;
- The compliance costs; and
- The costs from administrative burden.

It has been decided to use such a form of visualisation instead of providing the data by means of tables in order to make the sheer amount of data more accessible to the reader and to clearly be able to show the *development of the quantitative indicators over time* – which is not always easy to spot when looking at raw figures.

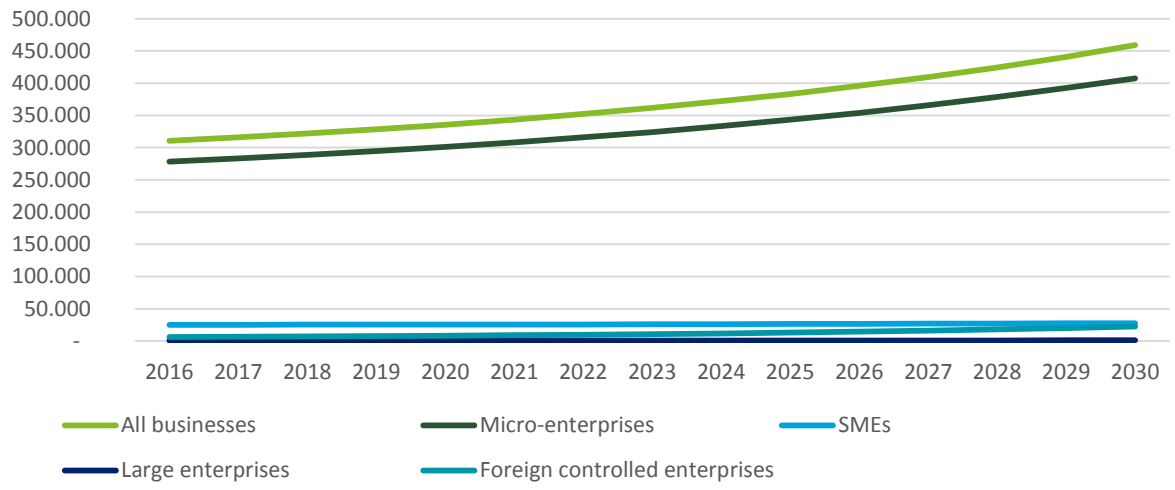
The graphs visualise the data per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Graphical comparisons of the quantitative indicators under each policy option with the baseline scenario are provided in section 9.8.1.

Number of businesses affected under policy option 4

The following two graphs present the development of the number of businesses affected by the ePD under policy option 4. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

Figure 101 – Number of businesses affected by the ePD per year (policy option 4, 2016-2030)

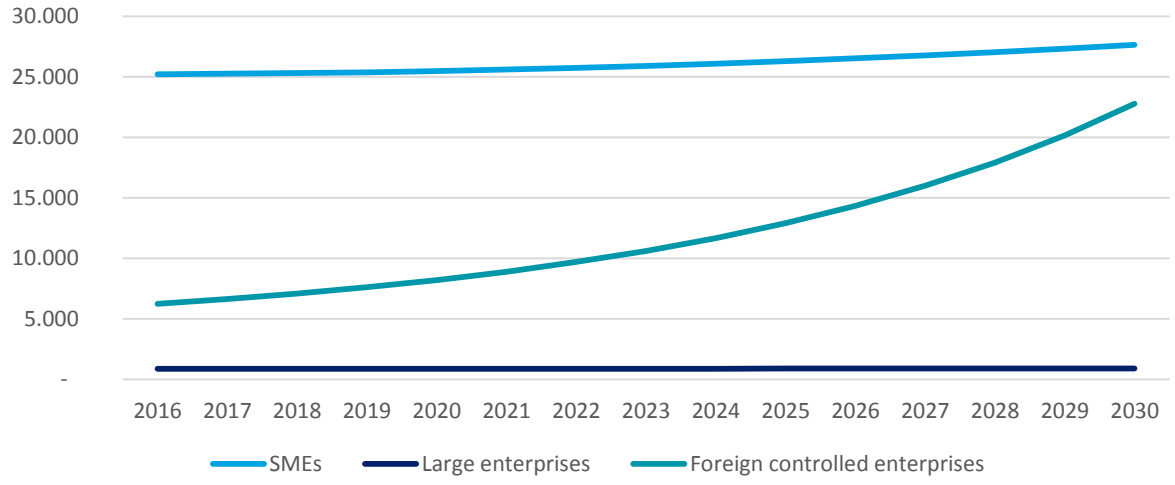


Source: Deloitte

The trends that can be seen from the graphs above and below in relation to the growth of the number of businesses affected by the ePD are similar to those in the baseline scenario:

- The overall number of businesses affected by the ePD is expected to grow from 2016 to 2030
- SMEs, large enterprises, and foreign controlled enterprises are of less importance for the overall growth of the number of businesses affected by the ePD;
- The number of SMEs affected is expected to increase slightly
- The number of large enterprises is expected to remain stable
- The number of foreign controlled enterprises affected by the ePD is expected to increase significantly until 2030

Figure 102 – Number of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 4, 2016-2030)

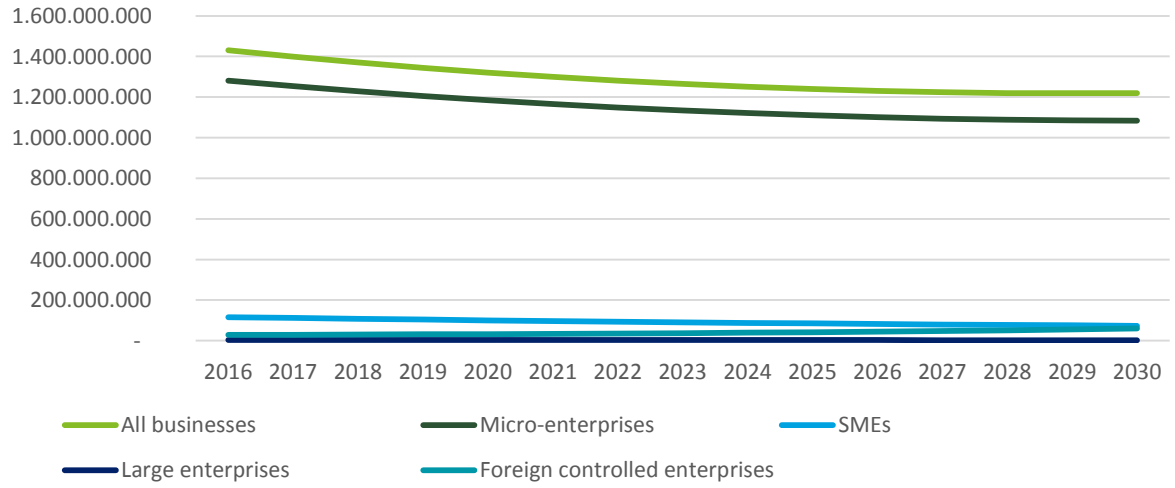


Source: Deloitte

Annual compliance costs under policy option 4

The following two graphs present the development of the annual compliance costs of businesses affected by the ePD under policy option 4. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

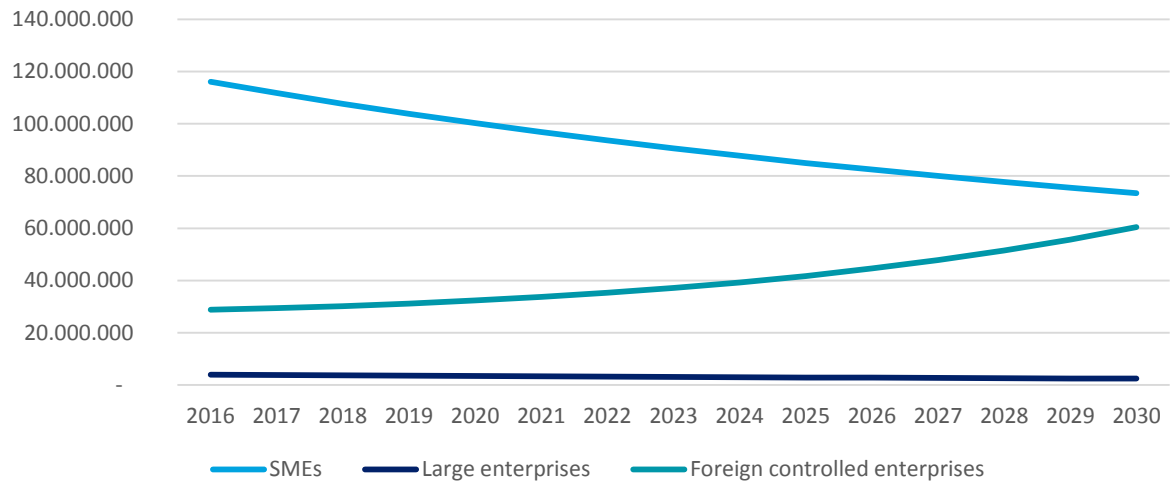
Figure 103 – Compliance costs of businesses affected by the ePD per year (policy option 4, 2016-2030)



Source: Deloitte

The graph above shows the annual overall compliance costs for businesses are expected to decrease from 2016 to 2030. Looking in more detail at annual overall compliance costs for SMEs, large enterprises, and foreign controlled enterprises (see figure below), it can be seen that – while compliance costs for SMEs are expected decrease – they will increase for foreign controlled enterprises and remain relatively stable for large enterprises.

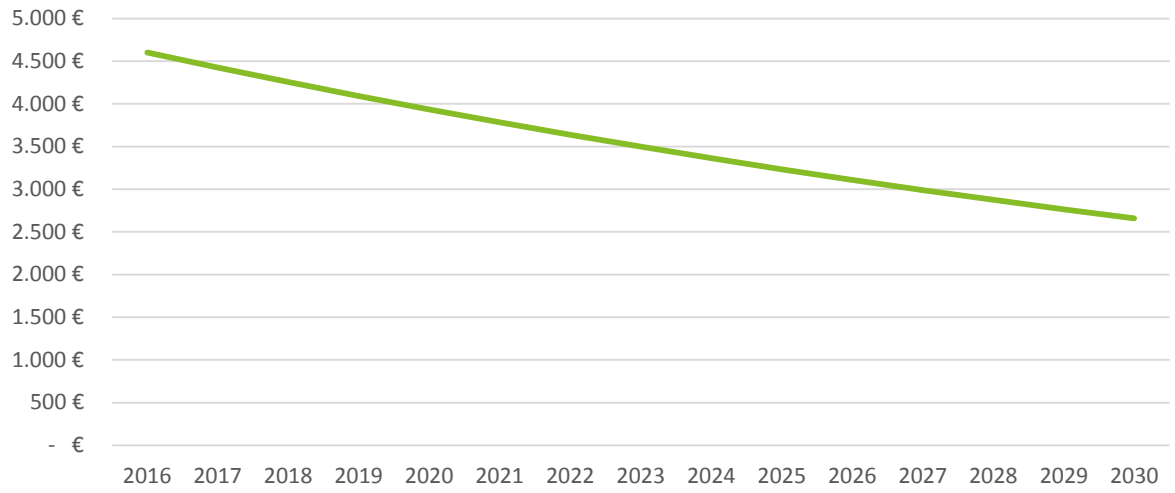
Figure 104 – Compliance costs of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 4, 2016-2030)



Source: Deloitte

The following graph visualises the development of the average compliance costs for businesses from 2016 to 2030 under policy option 4. No difference has been made between average costs for different size classes of businesses.

Figure 105 – Average compliance costs of per business affected by the ePD per year (policy option 4, 2016-2030)



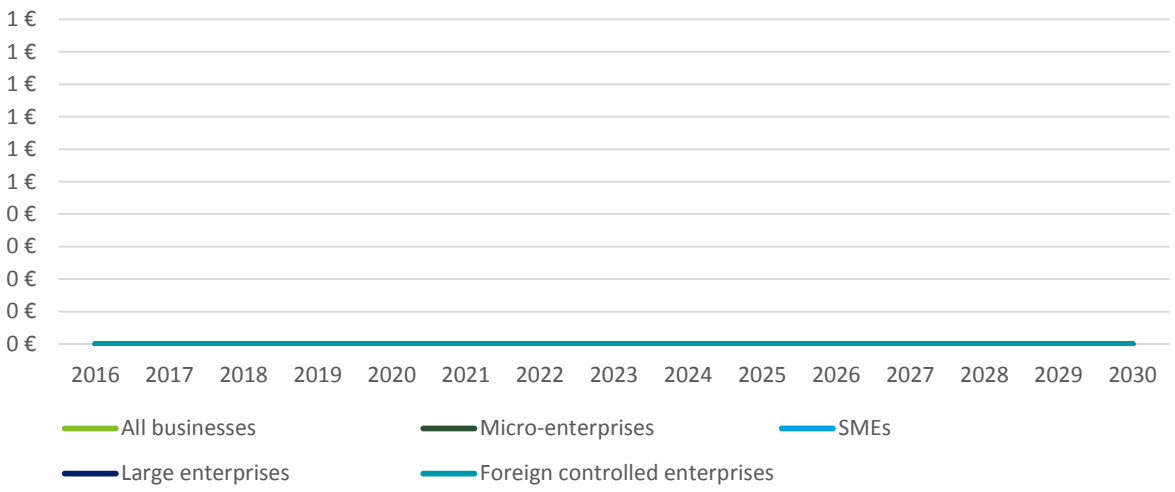
Source: Deloitte

The graph clearly shows that the average compliance costs for businesses are expected to decrease between 2016 and 2030, as at the same time the number of businesses affected by the ePD increases.

Annual costs from administrative burden under policy option 4

The following two graphs present the development of the annual costs from administrative of businesses affected by the ePD under policy option 4. While the first graph displays the overall situation, the second graph focuses only on SMEs, large enterprises, and foreign controlled enterprises affected by the ePD.

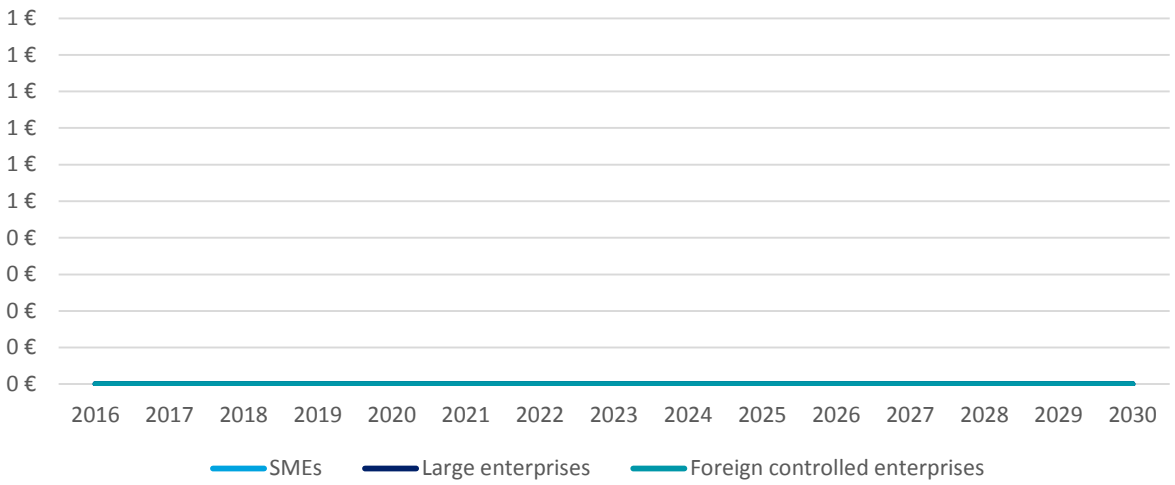
Figure 106 – Costs from administrative burden of businesses affected by the ePD per year (policy option 4, 2016-2030)



Source: Deloitte

Unlike the compliance costs, costs from overall annual administrative burden is expected to slightly increase between 2016 and 2030.

Figure 107 – Costs from administrative burden of SMEs, large enterprises, and foreign controlled enterprises affected by the ePD per year (policy option 4, 2016-2030)

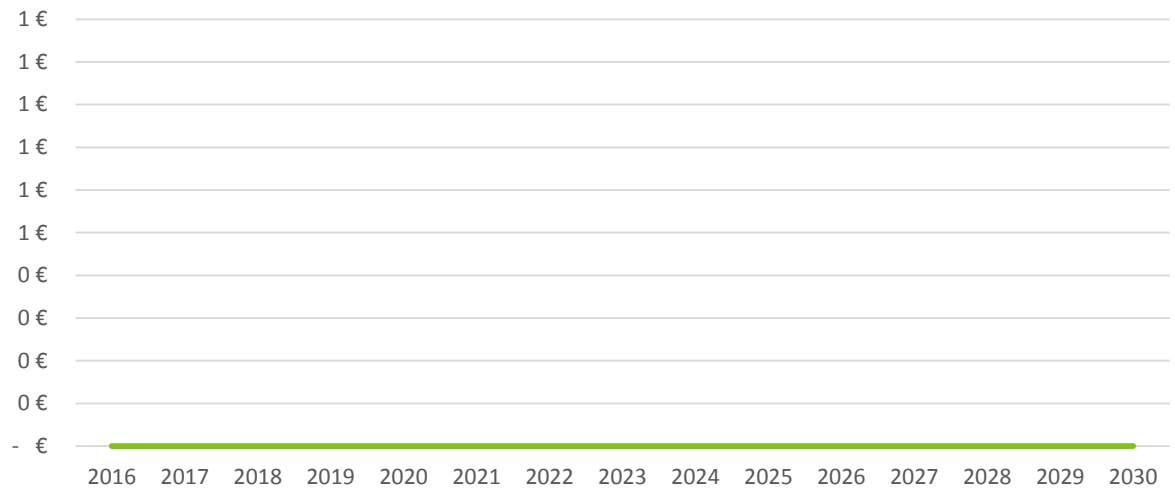


Source: Deloitte

As regards the costs from administrative burden for SMEs, large enterprises, and foreign controlled enterprises, an increase is expected from 2016 to 2030. Especially for SMEs, costs from administrative burden will continue to grow significantly until 2030.

The following graph visualises the development of the average costs from administrative burden for businesses from 2016 to 2030 under policy option 4. No difference has been made between average costs for different size classes of businesses.

Figure 108 – Average costs from administrative burden per business affected by the ePD per year (policy option 4, 2016-2030)



Source: Deloitte

Overall, the above graph shows that there will be a clear reduction of costs from administrative burden for across all types of businesses affected by the ePD from 2016 to 2030, as at the same time the number of businesses affected by the ePD increases.

Policy option 4: Overall values 2016-2030

While the above section has presented average annual values, this section provides the key quantitative estimates for the overall time period of 2016-2030 (i.e. the sums of each individual annual value of the time period) under policy option 4. This estimate is relevant to assess the overall costs of compliance and administrative burden stemming from the ePD for different types of businesses.

The following table contains information on:

- Compliance costs (in million Euro); and
- Administrative burden (in million Euro).

The number of businesses affected is not presented as this number is – over the entire time period – subject to double counting.[572] Compared to the above section, average compliance cost per business, as well as average costs from administrative burden per business are not relevant to present in this section as they are *average* values and not *overall* values.

The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Overall value (2016-2030):* Denotes the overall annual value of the quantitative indicator for which data has been estimated. This means, for instance, that all SMEs in the EU together have will incur compliance costs of 1,382.5 EURm over the entire time period of 2016-2030 (see the light green cell);
- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the overall value between 2016 and 2030 under policy option 4 compared to the overall value under the baseline scenario; and

[572] This is due to the fact that businesses are affected by the ePD over longer time frames than just one year. An alternative way of phrasing this is that the ePD does not affect an entirely different set of businesses each and every year.

- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the overall value between 2016 and 2030 under policy option 4 compared to the overall value under the baseline scenario.

Table 98 – Key quantitative data estimated in relation to policy option 4 (overall 2016-2030)

Quantitative indicator	Overall value (2016-2030)	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Compliance costs (in million Euro)	19,314.2 €	-1,016.5 €	-5.0%
Micro-enterprises	17,284.8 €	-909.7 €	-5.0%
SMEs	1,382.5 €	-72.8 €	-5.0%
Large enterprises	47.5 €	-2.5 €	-5.0%
Foreign controlled enterprises	599.3 €	-31.5 €	-5.0%
Administrative burden (in million Euro)	3.36 €	-0.104 €	-3.0%
Micro-enterprises	2.63 €	-0.082 €	-3.0%
SMEs	0.49 €	-0.015 €	-2.9%
Large enterprises	0.03 €	-0.001 €	-2.9%
Foreign controlled enterprises	0.20 €	-0.007 €	-3.3%

Source: Deloitte

Under policy option 4, as can be seen from the table above, businesses are expected to incur less compliance costs and costs from administrative burden between 2016 and 2030 than they would in the baseline scenario.

In absolute terms, compliance costs are expected to decrease by 1,016 EURm to 19,314 EURm compared to the overall amount incurred in the baseline scenario.

As argued in the REFIT section 6.2.2, the magnitude of the compliance costs should be seen in relation to the overall value of EU GDP. This way, the magnitude of compliance costs is marginal compared to the overall value of the economy.

As regards the costs from administrative burden, reductions are expected to be less pronounced. Overall, it is expected that 104,000 Euro can be saved under policy option 4 between 2016 and 2030 at EU level. This is expected to result in an overall amount of 3.4 EURm of costs from administrative burden. The reduction is expected to be 3% compared to the overall amount incurred in the baseline scenario.

Impacts on costs for public authorities

In the tables below, we provide an assessment of the impacts of policy option 4 on public administrations. The table contains:

- Qualitative reasoning used for the quantitative assessments of the impacts of the policy options on businesses (in particular on compliance costs and costs related to administrative burden) complemented where possible with exact cost estimates;
- A rating of the magnitude of these costs, according to the scheme portrayed below, serving to make the impacts of the options comparable; and
- The frequency of costs (as far as information is available).

The general approach used for these qualitative ratings is outlined in Annex A on the Analysis of the impacts of the policy options on the costs for public administrations.

Table 99 – Qualitative classification of the impacts of policy option 4 on costs for public administrations

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
Objective 1: Ensuring effective confidentiality and security of communications				
1. All the measures under No 1, 2, 3 and 4 of Option 3.	See the table on policy option 2 for the detailed assessment.	EU	-1	
		MS	1	
2. Explicitly prohibit the practice of denying access to a website or an online service in case users do not provide consent to tracking (so-called cookie-wall).	There may be a slight increase of costs for Member States based on that the checking of compliance may be more time consuming and it is possible that the number of complaints by citizens could increase.	MS	1	x
Objective 2: Ensuring effective protection against unsolicited commercial communications				
3. All the measures under No 5, 6, and 7 of Option 3.	See the table on policy option 2 for the detailed assessment.	MS	0	Recurring
4. Under this option, the Commission would also repeal the provision allowing direct marketers to send communications to subscribers and users when they have received their contact details in the context of a previous business relationship[573].	No specific impact on public administrations is expected.	EU/MS	0	
Objective 3: Simplifying the legal framework and adapting it to the new market and technological reality				
5. Measures 8 -12 of Option 3	See detailed assessment above.	EU	1	
		MS	1	
6. Commission's implementing powers for deciding on the correct application of the ePD instrument where there is an issue of consistency or coherence with EU law.	The Commission would need to dedicate resources to dealing with these issues. The number of resources needed would depend on the extent to which there are disputes. However, it is difficult to estimate, as the impact would also depend on the number of cases in which the Commission might decide to adopt such acts. It is expected that the impact would be moderate, including because the consistency mechanism is introduced at the same time and also gives a forum for handling cases with a European impact.	EU	1	

[573] Article 13(2).

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
7. Repeal the provisions on calling line identification and directories of subscribers.	None of the authorities consulted indicated that the provisions on itemised billing require significant resources. Thus, the impact of repealing these provisions is assumed to be negligible.	MS	0	
Overall implications (EU)		**1**		
Overall implications (MS)		**3**		

Source: Deloitte

Other economic impacts

This policy option would have the same impacts option 3. In addition, further opportunity costs and effects on competition and the digital economy can be expected based on further restrictions of the advertisement business.

The **prohibition of the practice of denying access to a website/service for users who do not consent** would to a great extent restrict OBA. On this basis, consumers would be less likely to give consent while still using the relevant services. This hinders businesses to "get to know" their customers online and, thus, provide them with targeted advertisements for more efficient sales. There may also be a loss of revenue, e.g. because advertisements would be worth less if they cannot be targeted based on users' behaviour. This is likely to render business models that are largely financed by means of advertising unviable.

The **repeal of the provision allowing marketers to target previous customers** may result in a loss of revenue for traders, as marketing to previous clients is restricted.

These effects are likely to be even harder on **SMEs**.

9.6.3 Effectiveness in reaching the policy objectives

In this section, the effectiveness of policy option 4 in reaching the policy objectives is assessed. It is shown in the following sub-sections that the effectiveness of this option is high in relation to all specific objectives.

Specific Objective 1: To ensure effective confidentiality and security of communications

This option would entail the same impacts as described under option 3.

In addition, the **prohibition of the practice of denying access to a website/service for users who do not consent** would further increase the protection for citizens, as it would not be possible any longer base the access to a site or service on consent. On this basis, citizens would have a more meaningful choice.

However, the **repeal of some additional provisions such as those on calling line identification and directories of subscribers** would slightly decrease the achievement of this objective. Indeed, some of the consumer rights that are still considered for a part of the affected population would be removed.

Specific Objective 2: To ensure that citizens are effectively protected against unsolicited marketing communications

This option would have the same positive effects as option 3. In addition, it would further increase citizens' protection by **repealing the provision allowing marketers to target previous customers**. On this basis, citizens would receive a smaller number of marketing communications without consent.

Specific Objective 3: To simplify the legal framework and adapt it to the new legal, market and technological reality

This option would have largely the same impacts as option 3.

At the same time, it provides for additional consistency by **giving the Commission implementing powers for deciding on the application of the ePD.** This way, a very high level of harmonisation could be achieved in relation to the enforcement of the new instrument.

Additional simplification could be achieved by **repealing additional consumer provisions.**

9.6.4 Social impacts

The **prohibition of the practice of denying access to a website/service for users who do not consent** may affect employment in those sectors that rely on OBA (e.g. advertisement sector), as OBA-based business models may become less viable. It is likely that such effects would be challenging rather in the short or medium term until these sectors have adjusted to the new situation.

In addition, the **repeal of the provision allowing marketers to target previous customers** may have small negative impacts on employment, as marketing campaigns cannot be as targeted. This could potentially affect businesses in all sectors as all businesses as well as the advertisement sector rely on effective marketing campaigns. It is likely that such impacts would be felt rather short-medium term, as resources would it is highly likely that resources would be shifted to other forms of marketing. At the same time, there would also be a positive impact on society as the disturbance of citizens by unwanted marketing communications would decrease.

9.7 Policy Option 5: Repeal of the ePD

Under this option, the Commission would propose the repeal of the ePD. With the repeal of the ePD, the confidentiality of electronic communications would fall under the general data protection regime as laid down in the DPD and as of 2018 the GDPR.

The specific elements of the policy option can be found in chapter 8.2.

9.7.1 Overview of assessments

In the following table we present an overview of our assessment of policy option 5. The detailed assessment according to the individual assessment criteria can be found in the following sub-sections.

Table 100 – Qualitative rating of the impacts of Policy Option 5

Assessment criteria	Rating	Brief explanation of the rating
Economic impacts		
Impacts on costs for businesses	-20[574]	As the ePD would be repealed under this Policy Option, all costs relating to compliance with and administrative burden stemming from the ePD would be abolished.

[574] Under policy option 5, business would incur no costs under the ePD anymore as the ePD would be repealed (i.e. cost reduction of 100% or simpler -100%). Based on the translation factor generally used for the assessments, this -100% can be transformed into a rating of -20 for consistency reasons. In fact, however, the qualitative rating for policy option 5 is of less relevance than the assumption that costs will be reduced by 100% (i.e. an assumption that cannot be made without a qualitative rating for the other policy options).

Assessment criteria		Rating	Brief explanation of the rating
	Impacts on costs for public authorities	2	There would very low costs for EU and national administrations for repealing existing legislation.
	Other economic impacts	-2	There would be positive impacts on competition and the internal market, as this policy option would ensure that the same rules apply to all players and across the EU.
Effectiveness in reaching the policy objectives			
	Objective 1: To ensure effective confidentiality and security of communications	3	While confidentiality and security would to an extent be covered by the GDPR, there would be a decrease in protection in particular in relation to the confidentiality of communications and consumer rights.
	Objective 2: To ensure that citizens are effectively protected against unsolicited marketing communications	2	The GDPR gives consumers the right to object to data processing for direct marketing purposes. This basic opt-out regime effectively prescribes a uniform rule with regard to unsolicited communications across all EU Member States. Nevertheless, this new rule is not able to address other present challenges, e.g. that updating of opt-out directories is perceived as burdensome by stakeholders.
	Objective 3: To simplify the legal framework and adapt it to the new legal, market and technological reality	-3	The objective is expected to be fully achieved by policy option 5, as this policy option would ensure that the same rules apply to all players and across the EU..
Social impacts		0	This option may to produce positive effects for the employment, in the ECS sector and advertisement market, as the more liberal regimes may boost competitiveness in these sectors. However, there would be negative impacts on society based on the lower degree of protection of confidentiality and security as well as against unsolicited marketing communications.
Total		-18	

Source: Deloitte

9.7.2 Economic impacts

Within this section on the assessment of the economic impacts of policy option 5, we are focusing on three key aspects: (1) The impacts on compliance costs and administrative burden for businesses (incl. SMEs and micro-enterprises), and (2) on costs for public authorities; as well as (3) other economic impacts such as on competiveness and competition in the Digital Single Market.

Impacts on compliance costs and administrative burden for businesses

In this section, we provide the following:

- ***Part A:*** A detailed qualitative assessment table regarding the impact of each element of the policy option 5; and
- ***Part B:*** The key quantitative findings from the economic analysis in relation to the impact of policy option 5.

The former will feed into the latter with regard to the assessment of the economic impact of the policy option.

Part A: Detailed qualitative assessment tables

A more **detailed qualitative assessment table** regarding the impact of each element of policy option 5 is provided below. The table contains:

- Qualitative reasoning used for the quantitative assessments of the impacts of the policy options on businesses (in particular on compliance costs and costs related to administrative burden);
- An indication of the types of businesses affected by each element;
- Qualitative rating / colour coding of the expected impacts of each element of the options;
- An indication whether or not businesses would incur compliance costs or costs related to administrative burden from each specific element;
- The frequency of costs (as far as information is available); and
- The existence / emergence of opportunity costs in relation to each of the elements of the policy options.

As described in Annex A on the *general approach used to translate qualitative reasoning into quantitative assumptions*, the ratings contained in the below table of this Part B have been used as a qualitative basis for the quantitative assessment of the impacts of the policy options in Part A above.

Table 101 – Qualitative classification of the impacts of policy option 5 on costs for businesses

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency	Opportunity costs
Objective 1: Ensuring effective confidentiality and security of communications							
1. The GDPR provides for reinforced rights of individuals and the obligations of data controllers, which are in keeping with the challenges of the digital age. The consent rule under the GDPR has been in particular substantially strengthened with a view to ensure that it is freely-given. The GDPR addressed the issue of unbalance of economic power between the controller and the processor, requesting that this aspect be taken into account in the assessment of the validity of consent.	As the ePD would be repealed under this Policy Option, all costs relating to compliance with and administrative burden stemming from the ePD would be abolished. We have not prepared at qualitative rating for this but expect that a reduction of costs directly / indirectly linked to the ePD of 100% would be realised. The same is true for the number of businesses affected. This does of course not mean that businesses would not incur any costs at all with regard to the privacy and confidentiality of electronic communications but these would be incurred under the GDPR and are thus outside the scope of this study.	All businesses	n/a	X	X		
2. The GDPR would guarantee more effective enforcement in view of the reinforced powers conferred on data protection authorities.		All businesses	n/a	X	X		
Objective 2: Ensuring effective protection against unsolicited commercial communications							
3. Unsolicited communications would be essentially regulated under a general a opt-out regime across 28 MS.	See above.	All businesses	n/a	X	X		
Objective 3: Simplifying the legal framework and adapting it to the new market and technological reality							
4. All providers of electronic communications will be subject to the same rules without discrimination based on the technology used	See above.	All businesses	n/a	X	X		

Implications for businesses	Obligations relating to compliance costs/admin burden	Type of business	Change compared to status quo	Compliance	Admin burden	Frequency	Opportunity costs
5. There would be no duplication of rules in the security area and all the ePD provisions related to specific issues in the electronic communications sector (e.g. directories of subscribers) would be dealt with on the basis of the general data protection rules.	See above.	All businesses	n/a	X	X		
Overall implications (Compliance)			-100% (this equals a rating of -20 based on the factor used to calculate percentages for the other policy options[575])				
Overall implications (Admin burden)			-100%				
Overall implications on the number of businesses affected			-100%				

Source: Deloitte

[575] Further details are contained in Annex A.

Part B: Key quantitative findings from the economic analysis

Policy option 5: Average annual values and changes compared to the current situation

Similarly to the information provided for the baseline scenario, the overall quantitative results of the analysis concerning policy option 5 are presented in Table 73:

- Number of businesses affected (in million);
- Compliance costs (in million Euro);
- Average compliance cost per business (in Euro);
- Administrative burden (in million Euro); and
- Average costs from administrative burden per business (in Euro).

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

Annex A: Economic Analysis

Further information in this regard, as well as an explanation of the approach used for the estimation of the quantitative results data is provided in the section on the basic assumptions used for the assessment of the impacts of the policy options in Annex A concerning the Economic Analysis.

The following table presents the quantitative findings for policy option 5. The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Average annual value:* Denotes the average annual value of the quantitative indicator for which data has been estimated. This means, for instance, that 0 SMEs are affected by issues relating to the ePD per year (see the light blue cell), facing a total amount of 0 EURm per year (see the light green cell) at an average cost of compliance per business of 0 Euro (see the dark blue cell);
- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the average annual value compared to the baseline scenario (2016-2030); and
- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the average annual value compared to the baseline scenario (i.e. 2016-2030).

Visualisations of the year-over-year development of the quantitative indicators are presented afterwards, as well as overall values for the timeframe 2016-2030.

Table 102 – Key quantitative data estimated in relation to policy option 5 (2016-2030)

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Number of businesses affected (in million)	0.00	- 3.70	-100.0%
Micro-enterprises	0.00	- 3.313	-100.0%
SMEs	0.00	- 0.261	-100.0%

Quantitative indicator	Average annual value 2016-2030	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Large enterprises	0.00	- 0.009	-100.0%
Foreign controlled enterprises	0.00	- 0.121	-100.0%
Compliance costs (in million Euro)	0.00 €	-1,355.4 €	-100.0%
Micro-enterprises	0.00 €	-1,213.0 €	-100.0%
SMEs	0.00 €	-97.0 €	-100.0%
Large enterprises	0.00 €	-3.3 €	-100.0%
Foreign controlled enterprises	0.00 €	-42.1 €	-100.0%
Average compliance cost per business (in Euro)	0.00 €	n/a	n/a
Administrative burden (in million Euro)	0.00 €	-0.23 €	-100.0%
Micro-enterprises	0.00 €	-0.18 €	-100.0%
SMEs	0.00 €	-0.03 €	-100.0%
Large enterprises	0.00 €	0.00 €	-100.0%
Foreign controlled enterprises	0.00 €	-0.01 €	-100.0%
Average costs from admin. burden per business (in Euro)	0.00 €	n/a	n/a

Source: Deloitte

Policy option 5: Overall values 2016-2030

While the above section has presented average annual values, this section provides the key quantitative estimates for the overall time period of 2016-2030 (i.e. the sums of each individual annual value of the time period) under policy option 5. This estimate is relevant to assess the overall costs of compliance and administrative burden stemming from the ePD for different types of businesses.

The following table contains information on:

- Compliance costs (in million Euro); and
- Administrative burden (in million Euro).

The number of businesses affected is not presented in terms of overall values relating to the whole period 2016-2020, as it would not be possible to simply add up the businesses affected each year. This would lead to double-counting, due to the fact that businesses are affected by the ePD over longer time frames than just one year.[576] On this basis, it is more appropriate to examine the number of businesses affected on an annual basis. Compared to the above section, average compliance cost per business, as well as average costs from administrative burden per business are not relevant to present in this section as they are *average* values and not *overall* values.

The table contains four columns:

- *Quantitative indicator:* Denotes the type of quantitative indicator for which data has been estimated, as well as the respective type of business;
- *Overall value (2016-2030):* Denotes the overall annual value of the quantitative indicator for which data has been estimated. This means, for instance, that all SMEs in the EU together have will incur compliance costs of 0 EURm over the entire time period of 2016-2030 (see the light green cell);

[576] An alternative way of phrasing this is that the ePD does not affect an entirely different set of businesses each and every year.

- *Absolute Δ to baseline scenario:* Denotes the absolute change (i.e. increase or decrease in terms of numbers) of the overall value between 2016 and 2030 under policy option 5 compared to the overall value under the baseline scenario; and
- *Relative Δ to baseline scenario:* Denotes the relative change (i.e. increase or decrease in terms of percent) of the overall value between 2016 and 2030 under policy option 5 compared to the overall value under the baseline scenario.

Table 103 – Key quantitative data estimated in relation to policy option 5 (overall 2016-2030)

Quantitative indicator	Overall value (2016-2030)	Absolute Δ to baseline scenario	Relative Δ to baseline scenario
Compliance costs (in million Euro)	0.0 €	-20,330.7 €	-100.0%
Micro-enterprises	0.0 €	-18,194.6 €	-100.0%
SMEs	0.0 €	-1,455.3 €	-100.0%
Large enterprises	0.0 €	-50.0 €	-100.0%
Foreign controlled enterprises	0.0 €	-630.9 €	-100.0%
Administrative burden (in million Euro)	0.0 €	-3.5 €	-100.0%
Micro-enterprises	0.0 €	-2.7 €	-100.0%
SMEs	0.0 €	-0.5 €	-100.0%
Large enterprises	0.0 €	0.0 €	-100.0%
Foreign controlled enterprises	0.0 €	-0.2 €	-100.0%

Source: Deloitte

Impacts on costs for public authorities

In the tables below, we provide an assessment of the impacts of policy option 5 on public administrations. The table contains:

- Qualitative reasoning used for the quantitative assessments of the impacts of the policy options on businesses (in particular on compliance costs and costs related to administrative burden) complemented where possible with exact cost estimates;
- A rating of the magnitude of these costs, according to the scheme portrayed below, serving to make the impacts of the options comparable; and
- The frequency of costs (as far as information is available).

The general approach used for these qualitative ratings is outlined in Annex A on the Analysis of the impacts of the policy options on the costs for public administrations.

Table 104 – Qualitative classification of the impacts of policy option 5 on costs for public administrations

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
Objective 1: Ensuring effective confidentiality and security of communications				
1. The GDPR provides for reinforced rights of individuals and the obligations of data controllers, which are in keeping with the challenges of the digital age. The consent rule under the GDPR has been in particular substantially strengthened with a view to ensure that it is freely-given. The GDPR addressed the issue of unbalance of economic power between the controller and the processor, requesting that this aspect be taken into account in the assessment of the validity of consent.	As the ePD would be repealed under this Policy Option, all costs stemming from the ePD would be abolished. We have not prepared at qualitative rating for this but expect that a reduction of costs directly / indirectly linked to the ePD of 100% would be realised. This does of course not mean that public authorities would not incur any costs at all with regard to the privacy and confidentiality of electronic communications but these would be incurred under the GDPR and are thus outside the scope of this study.	EU	n/a	
		MS	n/a	
2. The GDPR would guarantee more effective enforcement in view of the reinforced powers conferred on data protection authorities.		MS	n/a	x
Objective 2: Ensuring effective protection against unsolicited commercial communications				
3. Unsolicited communications would be essentially regulated under a general an opt-out regime across 28 MS.	See above.	MS	n/a	Recurring
Objective 3: Simplifying the legal framework and adapting it to the new market and technological reality				
4. All providers of electronic communications will be subject to the same rules without discrimination based on the technology used	See above.	EU	n/a	
		MS	n/a	
5. There would be no duplication of rules in the security area and all the ePD provisions related to specific issues in the electronic communications sector (e.g. directories of subscribers) would be dealt with on the basis of the general data protection rules.	See above.	EU	n/a	
Horizontal aspect				
Repeal of legislation	There would be low costs for both EU and national administrations associated with the repeal of existing legislation.	EU/MS	1	
Overall implications (EU)		1		

Elements of the option	Obligations	Type of authority	Change compared to status quo	Frequency
Overall implications (MS)		1		

Source: Deloitte

Other economic impacts

The repeal of the ePD would generally have positive impacts.

ECS providers would face a less restrictive legal framework including on the processing of communications data, which would be based on the GDPR. This would allow them to develop new business models and would place them on equal footing with OTTs. Thus, ECS may face an **increase in revenues** and **competitiveness would be increased**.

We note in this context that it is possible that there would be **shift in revenue between ECS and OTTs**. Some consumers currently refrain from using alternative internet-based communication tools partially due to privacy concerns. For example, a Commission's external study found that 37% of consumers consider concerns about privacy an important reason against using the internet for phone calls.[577] This reason would lose its relevance if all communication services would be subject to the same rules.

However, it is possible that such potential losses for ECS providers could be outweighed by the increase of flexibility for ECS and the possibility for them to develop new business models mentioned above. Furthermore, businesses would be free to implement their own privacy policies (in line with the GDPR) and privacy may be used as a selling argument by businesses. Thus, the actual effects on the market would largely depend on the way businesses sell their services and consumers' preferences.

As the **GDPR would contain a general opt-out requirement for unsolicited marketing communications**, further positive impacts would be expected for businesses. This would significantly reduce the legal requirements for direct marketing campaigns and would thus boost competitiveness.

Finally, the option would have positive impacts on the **internal market,** as this option would ensure that all providers across the EU face the same legal standards in relation to privacy. Thus, cross-border activities would be easier as businesses would not have to deal with differing legal standards.

9.7.3 Effectiveness in reaching the policy objectives

In this section, the effectiveness of policy option 5 in reaching the policy objectives is assessed. It is shown in the following sub-sections that the effectiveness of this option is limited in relation to the first two specific objectives. The third specific objective could be achieved by this option.

Specific Objective 1: To ensure effective confidentiality and security of communications

In absence of the ePD, the newly adopted GDPR fully accounts for the **protection of personal data** processed in the context of any electronic communication – regardless of the underlying format or technology. Several stakeholders, especially in the ECS and OTT sector, have argued that ePD rules are no longer needed and that the objectives of the ePD would be achieved by the GDPR alone.

[577] Ecorys-TNO, *Study on future trends and business models in communication services* (SMART 2016/0019).

The GDPR puts strong emphasis on the role of free consent (opt-in) to services by users and a default privacy by design for all services processing personal data and lays down security obligations and notification schemes for breaches.[578]

On this basis, the security of personal data is expected to be ensured to a similar extent compared to the current situation. However, in several ways the standard of protection for citizens would be weaker compared to the current situation, limiting the achievement of this objective. First, **processing of personal data would be possible for additional legal grounds other than consent** (Article 6 of the GDPR). In addition, in the context of the ePD, **confidentiality of communications** is not limited to the processing of personal data. The ePD aims at protecting communications irrespective of their content and the type of terminal equipment used. In absence of the ePD:

- Operators would be able to process communications data without user consent;
- No general prohibition to intercept communications would exist at EU level[579]; and
- There would be no rules on the security and confidentiality of communications of legal persons, we the GDPR only covers natural persons.

In addition, **the GDPR does not contain any of the specific user rights** laid down in the ePD, including e.g. on itemised billing and directories of subscribers. We note that at least some parts of the users considered these as an added value based on the stakeholder consultations carried out as part of this study and by the Commission. Thus, the achievement of this objective would further decrease.

Given these differences between the GDPR and the ePD, the security of personal data is expected to remain equal regardless of policy option 5. Nevertheless, the policy option is not expected to achieve the objective of ensuring effective confidentiality and security of communications.

Specific Objective 2: To ensure that citizens are effectively protected against unsolicited marketing communications

The GDPR gives consumers the right to **object to data processing for direct marketing purposes**. This basic opt-out regime effectively prescribes a uniform rule with regard to unsolicited communications across all EU Member States. Nevertheless, this new rule is not able to address other present challenges, namely that:

- Updating of opt-out directories is perceived as burdensome by stakeholders;
- Responsibility to ensure protection from unsolicited communication is placed at the sole responsibility of citizens; and
- Enforcement of compliance would be more challenging to competent authorities.

We note in this context that some Member States already apply an opt-out regime. In this Member States, there would be no changes to the current situation.

In addition, in absence of the ePD users' would only be able to block certain callers based on their phone numbers if they use modern terminal equipment that offers this functionality.

[578] See: Article 5 (1) demanding the secure processing of personal data (Article 32 specifying security obligations), Article 7 and 8 specifying the nature of consent and the possibility for withdrawal, Article 25 outlining the data protection by design and default requirements, whereas Article 33 and 34 prescribe reactions to data breaches and the notification of data subjects.
[579] Even though some Member States protect users in this regard through national law.

Therefore, policy option 5 is not expected to effectively ensure citizen protection from unsolicited marketing communications.

Specific Objective 3: To simplify the legal framework and adapt it to the new legal, market and technological reality

A repeal of the ePD would logically entail a removal requirements reported as outdated or unnecessary. The option of suppressing users' calling line identification (Article 8) are nowadays ensured in modern terminal equipment. Thus, the legal framework for ECS would be simplified and adapted to developments in technology.[580]

In absence of the ePD, the GDPR will still apply to all forms of electronic communication alike, regardless of the underlying technology. This is expected to **increase harmonisation** since:

- Possible conflicts through national interpretations of the ePD with the uniform GDPR removed,
- Competent authorities, services and users only need to know about one set of rules, and

Thus, the objective is expected to be fully achieved by policy option 5.

9.7.4 Social impacts

This option may to produce positive effects for the employment, in the ECS sector and advertisement market, as the more liberal regimes may boost competitiveness in these sectors.

However, there would be negative impacts on society based on the lower degree of protection of confidentiality and security as well as against unsolicited marketing communications.

9.8 Comparison of policy options

9.8.1 Comparison of qualitative rating of the impacts of the options

The following table presents an overview of the qualitative rating attributed to all policy options.

On this basis, **Policy Option 3 with the Browser solution is the best performing policy option**. It achieves cost savings for businesses and entails very low costs for public administration. This option would have positive impacts on competition, notably based on the extension of the scope to OTTs. At the same time, some stakeholders would incur opportunity costs (OTTs and other businesses based on the change to Article 13). The impact on SMEs would be mixed. In addition, policy option achieves the best rating when it comes to the achievement of the objectives. It does not have any significant social impacts.

We note that policy option 5 also scores well, especially because it would entail the highest cost savings for businesses. However, it does not reach 2 of the three policy objectives studied and is thus not considered to be effective:

[580] It is important to note, that not all citizens have decided to adopt new technologies offering these option - thus not being able to gain the same benefit from simplification than for example smartphone users.

Table 105 – Qualitative rating of the impacts of the policy options

Assessment criteria	Baseline scenario	Policy Option 1	Policy Option 2	Policy Option 3			Policy Option 4			Policy Option 5
				"Browser solution"	"Tracking companies solution"	"Publisher solution"	"Browser solution"	"Tracking companies solution"	"Publisher solution"	
Economic impacts										
Impacts on costs for businesses	0	1	1	-8	-6	-5	-4	-2	-1	-20
Impacts on costs for public authorities	0	14	0	3	3	3	4	4	4	2
Other economic impacts	0	0	1	1	1	1	3	3	3	-2
Effectiveness in reaching the policy objectives										
Objective 1: Ensuring effective confidentiality of communications	0	-1	-2	-3	-3	-3	-3	-3	-3	3
Objective 2: Ensuring effective protection against unsolicited commercial comm.	0	-1	-2	-3	-3	-3	-3	-3	-3	2
Objective 3: Simplifying the legal framework and adapting it to the new legal, market and technological reality	0	-1	-2	-3	-2	-2	-3	-2	-2	-3
Social impacts	0	0	0	0	0	0	1	1	1	0
Total	0	12	-4	-13	-10	-9	-5	-2	-1	-18

Source: *Deloitte*

9.8.2 Comparison of economic impacts of policy options

In this section, the policy options are compared against the baseline scenario.

As a first step, the main quantitative outcomes of the economic analysis are presented in the form of tables. This section will contain separate tables concerning:

- Average annual values;
- Absolute changes of the average annual value compared to the REFIT / baseline scenario; and
- Relative changes of the average annual value compared to the REFIT / baseline scenario.

This section contains the average values for the quantitative indicators:

- The number of businesses affected;
- Compliance costs, incl. average compliance costs per business; and
- Administrative burden, incl. average costs from administrative burden per business.

The figures are presented per size class of business, i.e. in relation to micro-enterprises, SMEs, large enterprises, as well as for foreign controlled enterprises.

As a second step, the results are compared against the baseline scenario in the form of charts in order to be able to spot clearly the different impacts of the policy options compared to the baseline scenario.

A sub-section is devoted to each of the above quantitative indicators. Within each sub-section, different figures are provided in relation to: Micro-enterprises; SMEs; large enterprises; foreign controlled enterprises; and all businesses (i.e. the sum of the aforementioned).

In relation to policy option 3, only the “browser solution” has been visualised.

The number of citizens affected by the ePD under each policy option is not compared with the baseline scenario. The reason for this is that the policy options have no impact on the number of citizens affected – both are independent from each other. This means that, under each policy option, the number of citizens affected is equal to the baseline scenario.

Key findings of the quantitative analysis: Average values over time

Table 106 – Key figures of the quantitative assessments concerning businesses (absolute values)

Average annual value	REFIT	Today	Baseline scenario	Policy Option 1	Policy Option 2	Policy Option 3[581]			Policy Option 4	Policy Option 5
	(2002-2015)	(2016 snap shot)	(2016-2030)	(2016-2030)	(2016-2030)	(2016-2030)			(2016-2030)	(2016-2030)
						"Browser"	"Tracking companies"	"Publishers"		
Number of businesses affected (in million)	2.84	3.11	3.70	3.70	3.89	0.19	0.74	2.22	0.37	0.00
Micro-enterprises	2.53	2.78	3.31	3.31	3.48	0.17	0.663	1.99	0.33	0.00
SMEs	0.26	0.25	0.26	0.26	0.27	0.01	0.052	0.16	0.03	0.00
Large enterprises	0.01	0.01	0.01	0.01	0.01	0.00	0.002	0.01	0.001	0.00
Foreign controlled enterprises	0.05	0.06	0.12	0.12	0.13	0.01	0.024	0.07	0.01	0.00
Compliance costs (in million Euro)	1,861.7 €	1,505.7 €	1,355.4 €	1,423.15	1,558.7 €	406.6 €	542.152	1,287.6 €	1,287.6 €	0.0 €
Micro-enterprises	1,655.8 €	1,349.0 €	1,213.0 €	1,273.6 €	1,394.9 €	363.9 €	485.188	1,152.3 €	1,152.3 €	0.0 €
SMEs	169.8 €	122.2 €	97.0 €	101.9 €	111.6 €	29.1 €	38.808	92.2 €	92.2 €	0.0 €
Large enterprises	5.6 €	4.2 €	3.3 €	3.5 €	3.8 €	1.0 €	1.332	3.2 €	3.2 €	0.0 €
Foreign controlled enterprises	30.5 €	30.3 €	42.1 €	44.2 €	48.4 €	12.6 €	16.823	40.0 €	40.0 €	0.0 €
Average compliance cost per business (in Euro)	658.4 €	484.5 €	373.5 €	392.2 €	409.1 €	2,240.9 €	746.978	591.4 €	3,548.1 €	0.0 €
Administrative burden (in million Euro)	0.28 €	0.23 €	0.23 €	0.23 €	0.21 €	0.208 €	0.226 €	0.23 €	0.22 €	0.00 €
Micro-enterprises	0.23 €	0.19 €	0.18 €	0.18 €	0.16 €	0.163 €	0.178 €	0.18 €	0.18 €	0.00 €
SMEs	0.03 €	0.03 €	0.03 €	0.03 €	0.03 €	0.031 €	0.033 €	0.03 €	0.03 €	0.00 €
Large enterprises	0.00 €	0.00 €	0.00 €	0.00 €	0.00 €	0.002 €	0.002 €	0.00 €	0.00 €	0.00 €
Foreign controlled enterprises	0.02 €	0.01 €	0.01 €	0.01 €	0.01 €	0.013 €	0.014 €	0.01 €	0.01 €	0.00 €
Average costs from admin. burden per business (in Euro)	48.9 €	36.0 €	27.8 €	28.0 €	23.8 €	499.5 €	135.982 €	45.33 €	269.2 €	0.0 €

[581] As part of this model, it was not possible to estimate reasonable average compliance costs and costs from administrative burden for businesses for the "browser" and the "tracking companies solution" of policy option 3. The reason for this is that the average costs are calculated on the basis of all businesses affected, i.e. also those that would incur higher costs than others and vice versa. As part of these two solutions, however, a very small share of businesses would have to bear the largest share of costs (i.e. browser operators and tracking companies) while the costs would be significantly lower for others. Therefore, it is not appropriate to indicate an "average amount per business" as this would return misleading estimates.

Source: Deloitte

Table 107 – Key figures of the quantitative assessments concerning businesses (absolute changes)

Absolute changes of the average annual value compared to the REFIT / baseline scenario	REFIT	Today	Baseline scenario	Policy Option 1	Policy Option 2	Policy Option 3			Policy Option 4	Policy Option 5
						(2016-2030)				
	(2002-2015)	(2016 snap shot)	(2016-2030)	(2016-2030)	(2016-2030)	"Browser"	"Tracking companies"	"Publishers"	(2016-2030)	(2016-2030)
Number of businesses affected (in million)	n/a	n/a	0.86	0.00	0.19	-3.52	-2.96	-1.48	-3.33	-3.70
Micro-enterprises	n/a	n/a	0.78	0.00	0.17	-3.15	-2.65	-1.33	-2.98	-3.31
SMEs	n/a	n/a	0.00	0.00	0.01	-0.25	-0.21	-0.10	-0.24	-0.26
Large enterprises	n/a	n/a	0.00	0.00	0.00	-0.01	-0.01	0.00	-0.01	-0.01
Foreign controlled enterprises	n/a	n/a	0.07	0.00	0.01	-0.12	-0.10	-0.05	-0.11	-0.12
Compliance costs (in million Euro)	n/a	n/a	-506.3 €	67.8 €	203.3 €	-948.8 €	-813.2 €	-67.8 €	-67.8 €	-1,355.4 €
Micro-enterprises	n/a	n/a	-442.8 €	60.6 €	181.9 €	-849.1 €	-727.8 €	-60.6 €	-60.6 €	-1,213.0 €
SMEs	n/a	n/a	-72.8 €	4.9 €	14.6 €	-67.9 €	-58.2 €	-4.9 €	-4.9 €	-97.0 €
Large enterprises	n/a	n/a	-2.3 €	0.2 €	0.5 €	-2.3 €	-2.0 €	-0.2 €	-0.2 €	-3.3 €
Foreign controlled enterprises	n/a	n/a	11.6 €	2.1 €	6.3 €	-29.4 €	-25.2 €	-2.1 €	-2.1 €	-42.1 €
Average compliance cost per business (in Euro)	n/a	n/a	-284.9 €	18.7 €	35.6 €	1,867.4 €	373.5 €	217.9 €	3,174.7 €	-373.5 €
Administrative burden (in million Euro)	n/a	n/a	-0.04 €	0.002 €	-0.02 €	-0.023 €	-0.005 €	-0.005 €	-0.007 €	-0.23 €
Micro-enterprises	n/a	n/a	-0.05 €	0.002 €	-0.02 €	-0.018 €	-0.003 €	-0.004 €	-0.006 €	-0.18 €
SMEs	n/	n/	0.01 €	0.000 €	0.00 €	-0.003 €	-0.001 €	-0.001 €	-0.001 €	-0.03 €
Large enterprises	n/a	n/a	0.00 €	0.000 €	0.00 €	0.000 €	0.000 €	0.000 €	0.000 €	0.00 €
Foreign controlled enterprises	n/a	n/a	0.00 €	0.000 €	0.00 €	-0.001 €	0.000 €	0.000 €	0.000 €	-0.01 €
Average costs from admin. burden per business (in Euro)	n/a	n/a	-21.2 €	0.278 €	-4.0 €	471.8 €	108.2 €	17.6 €	241.4 €	-27.8 €

Source: Deloitte

Table 108 – Key figures of the quantitative assessments concerning businesses (relative changes)

Relative changes of the average annual value compared to the REFIT / baseline scenario	REFIT	Today	Baseline scenario	Policy Option 1	Policy Option 2	Policy Option 3	Policy Option 4	Policy Option 5
	(2002-2015)	(2016 snap	(2016-2030)	(2016-2030)	(2016-2030)	(2016-2030)	(2016-2030)	(2016-2030)

		shot)				“Browser”	“Tracking companies”	“Publishers”		
Number of businesses affected (in million)	n/a	n/a	30.2%	0.0%	5.0%	-95.0%	-80.0%	-40.0%	-90.0%	-100.0%
Micro-enterprises	n/a	n/a	30.9%	0.0%	5.0%	-95.0%	-80.0%	-40.0%	-90.0%	-100.0%
SMEs	n/a	n/a	1.6%	0.0%	5.0%	-95.0%	-80.1%	-39.8%	-90.0%	-100.0%
Large enterprises	n/a	n/a	0.0%	0.0%	0.0%	-100.0%	-77.8%	-44.4%	-88.9%	-100.0%
Foreign controlled enterprises	n/a	n/a	157.4%	0.0%	5.0%	-95.0%	-80.2%	-40.5%	-90.1%	-100.0%
Compliance costs (in million Euro)	n/a	n/a	-27.2%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
Micro-enterprises	n/a	n/a	-26.7%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
SMEs	n/a	n/a	-42.9%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
Large enterprises	n/a	n/a	-40.9%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
Foreign controlled enterprises	n/a	n/a	38.0%	5.0%	15.0%	-70.0%	-60.0%	-5.0%	-5.0%	-100.0%
Average compliance cost per business (in Euro)	n/a	n/a	-43.3%	5.0%	9.5%	500.0%	100.0%	58.3%	850.0%	-100.0%
Administrative burden (in million Euro)	n/a	n/a	-16.0%	0.9%	-10.0%	-10.0%	-2.2%	-2.2%	-3.0%	-100.0%
Micro-enterprises	n/a	n/a	-21.3%	1.1%	-9.9%	-9.9%	-1.7%	-2.2%	-3.3%	-100.0%
SMEs	n/	n/	25.9%	0.0%	-8.8%	-8.8%	-2.9%	-2.9%	-2.9%	-100.0%
Large enterprises	n/a	n/a	-33.3%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	-100.0%
Foreign controlled enterprises	n/a	n/a	-6.7%	0.0%	-7.1%	-7.1%	0.0%	0.0%	0.0%	-100.0%
Average costs from admin. burden per business (in Euro)	n/a	n/a	-43.3%	1.0%	-14.3%	1700.0%	390.0%	63.3%	870.0%	-100.0%

Source: Deloitte

Expected development of the number of businesses affected over time

This section presents the impacts of the policy options on the number of businesses affected by the ePD compared to the baseline scenario.

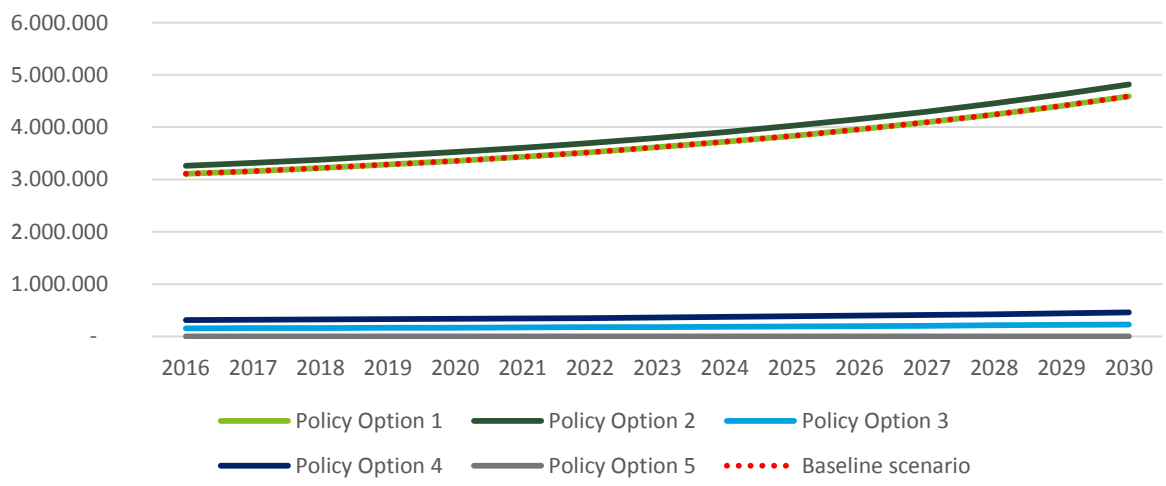
In the baseline scenario, roughly 3 million businesses in the EU are affected by the ePD today. It is expected that this number will grow to approx. 4.5 million in 2030.

The following graph shows that, while under policy option 1 the same number of businesses is expected to be affected as under the baseline scenario, less businesses would be affected under the other policy options. This said, while no businesses would be affected under policy option 5 due to the repeal of the ePD, the number of affected micro-enterprises is expected to be stable over time at around 200,000 per year under the "browser solution" of policy option 3.

Under both policy options 2 and 4, slightly less businesses would be affected by the ePD compared to the baseline scenario.

The same logic concerning the impact of the policy options on the number of affected businesses applies to all size classes.

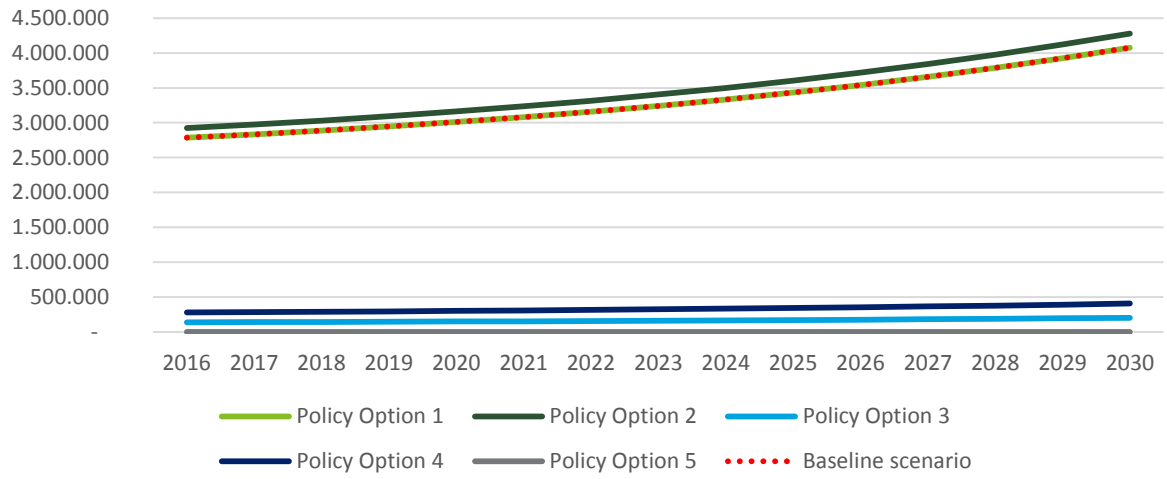
Figure 109 – Overall number of businesses affected by the ePD per year under each policy option and the baseline scenario (2016-2030)



Source: Deloitte

In the baseline scenario, roughly 2.75 million micro-enterprises in the EU are affected by the ePD today. It is expected that this number will grow to approx. 4.0 million in 2030. Similar to the logic outlined in relation to all businesses, the policy options are expected to reduce the number of affected micro-enterprises (see figure below).

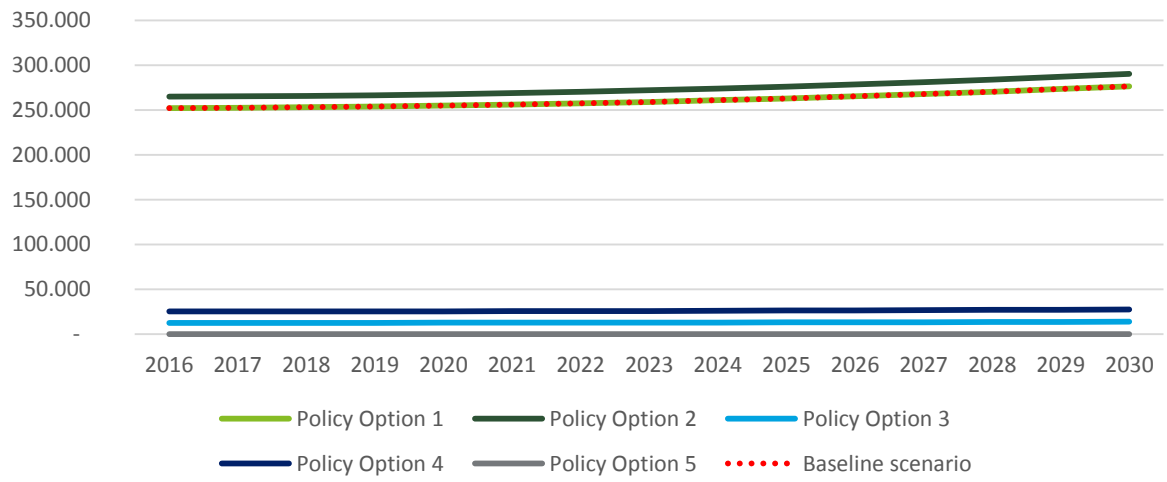
Figure 110 –Number of micro-enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030)



Source: Deloitte

In the baseline scenario, roughly 250,000 SMEs in the EU are affected by the ePD today. It is expected that this number will grow to approx. 275,000 in 2030. Similar to the logic outlined in relation to all businesses, the policy options are expected to reduce the number of affected SMEs (see figure below).

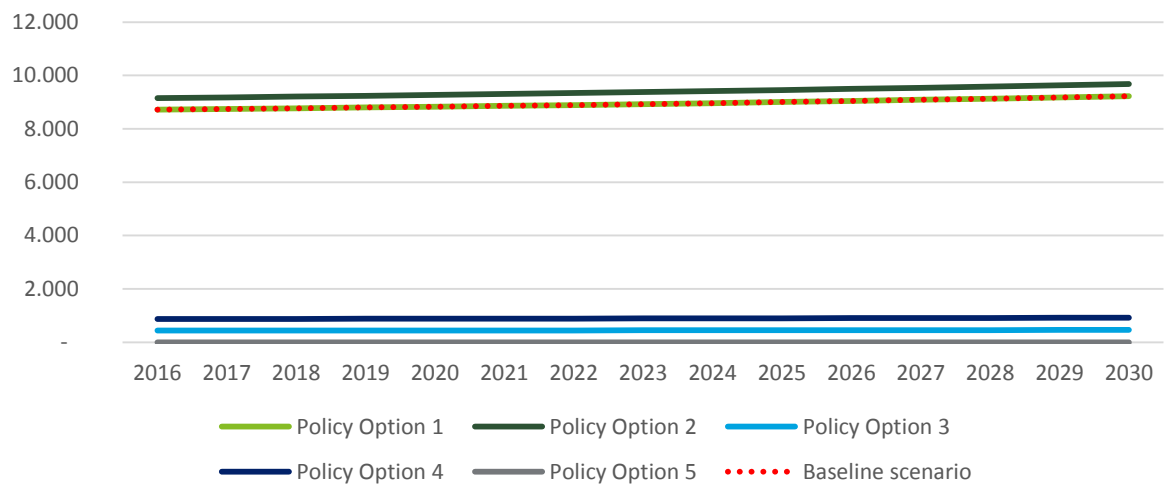
Figure 111 –Number of SMEs affected by the ePD per year under each policy option and the baseline scenario (2016-2030)



Source: Deloitte

In the baseline scenario, slightly less than 9,000 large enterprises in the EU are affected by the ePD today. It is expected that this number will grow to slightly more than 9,000 in 2030. Similar to the logic outlined in relation to all businesses, the policy options are expected to reduce the number of affected SMEs (see figure below).

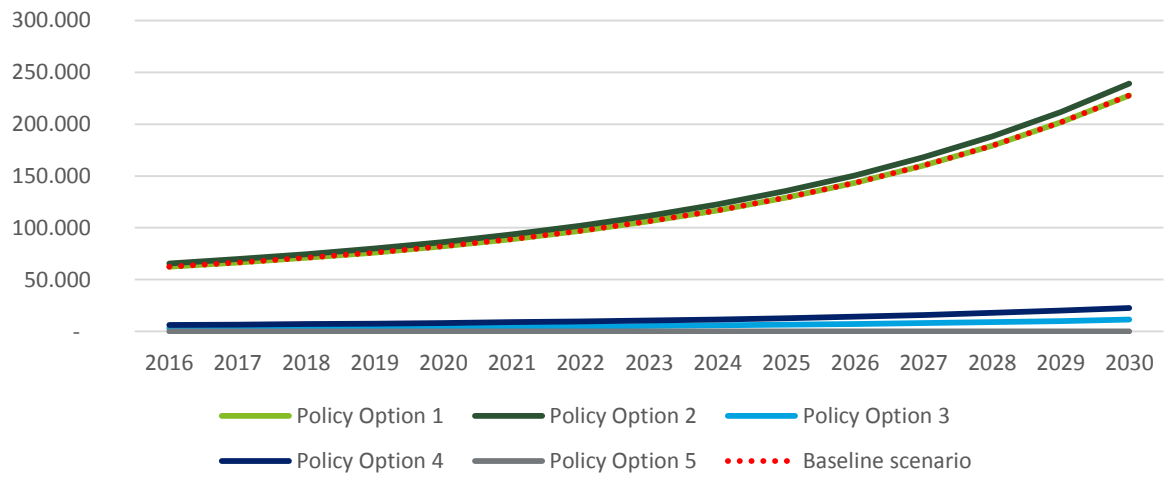
Figure 112 –Number of large enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030)



Source: Deloitte

In the baseline scenario, roughly 60,000 foreign controlled enterprises in the EU are affected by the ePD today. It is expected that this number will grow to approx. 220,000 in 2030. Similar to the logic outlined in relation to all businesses above, the policy options are expected to reduce the number of affected SMEs (see figure below).

Figure 113 –Number of foreign controlled enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030)



Source: Deloitte

The next section presents the comparison between the policy options and the baseline scenario in relation to the compliance costs.

Expected development of the compliance costs over time

This section presents the impacts of the policy options on the compliance costs incurred by businesses compared to the baseline scenario.

In the baseline scenario, annual compliance costs for all businesses affected by the ePD are expected to decrease from 1.5 EURb in 2016 to roughly 1.25 EURb in 2030.

As can be seen in the figure below, differences exist between the policy options not only in relation to the magnitude of the impacts but also in relation to its direction.

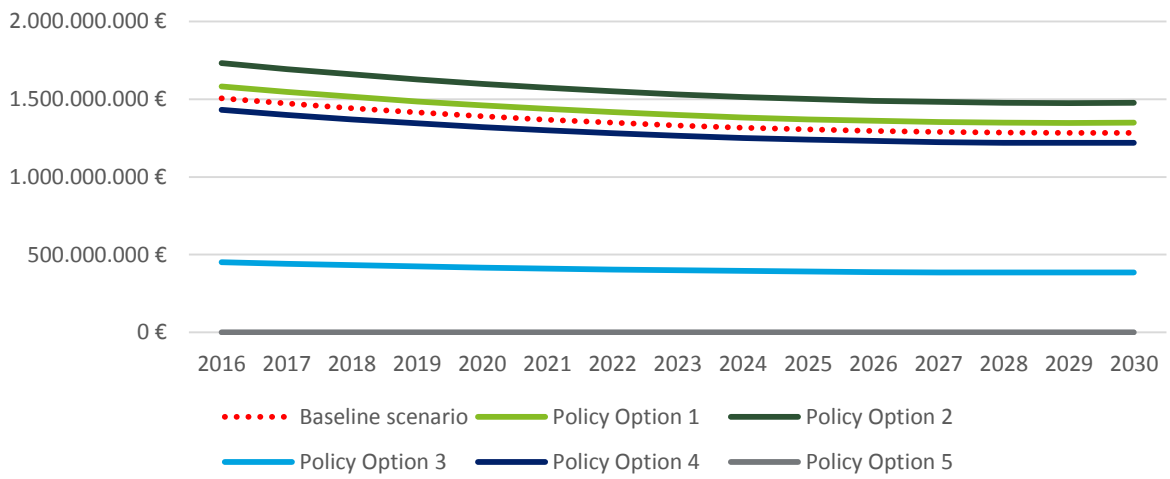
While policy options 1, 2, and 4 are expected to increase the compliance costs compared to the baseline scenario, policy option 3 and in particular policy option 5 are expected to reduce the compliance costs.

Under policy option 3, annual compliance costs for all businesses affected by the ePD are expected to decrease to roughly 400 EURm.

Under policy option 5, no costs to comply with the ePD will be incurred anymore as this policy option would repeal the ePD.

The same logic concerning the impact of the policy options on the compliance costs for affected applies to all size classes.

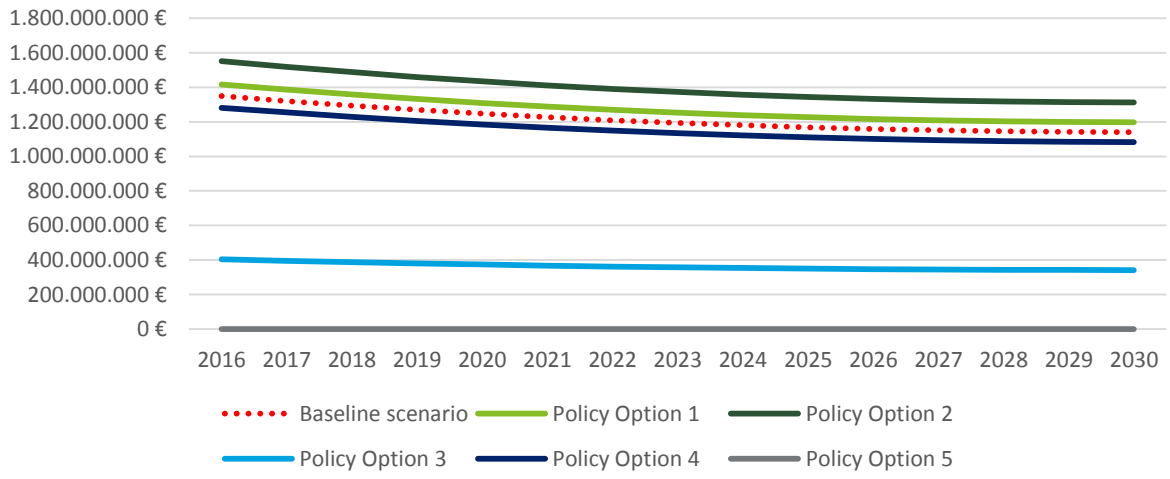
Figure 114 – Compliance costs for all businesses affected by the ePD per year under each policy option and the baseline scenario (2016-2030)



Source: Deloitte

In the baseline scenario, annual compliance costs for micro-enterprises affected by the ePD amount to slightly less than 1.4 EURb today. This amount is expected to decrease until 2030 to roughly 1.2 EURb. Similar to the logic outlined in relation to all businesses above, the policy options are expected to increase (policy options 1, 2, and 4) or decrease (policy options 3 and 5) the compliance costs for micro-enterprises.

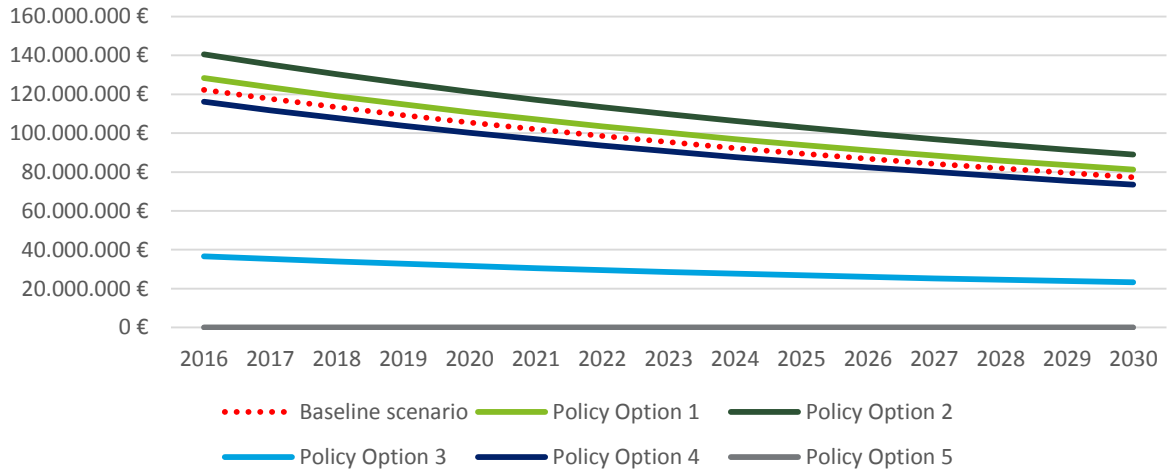
Figure 115 – Compliance costs for micro-enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030)



Source: Deloitte

In the baseline scenario, annual compliance costs for SMEs affected by the ePD amount to 120 EURm today. This amount is expected to decrease until 2030 to roughly 80 EURm. Similar to the logic outlined in relation to all businesses above, the policy options are expected to increase (policy options 1, 2, and 4) or decrease (policy options 3 and 5) the compliance costs for SMEs.

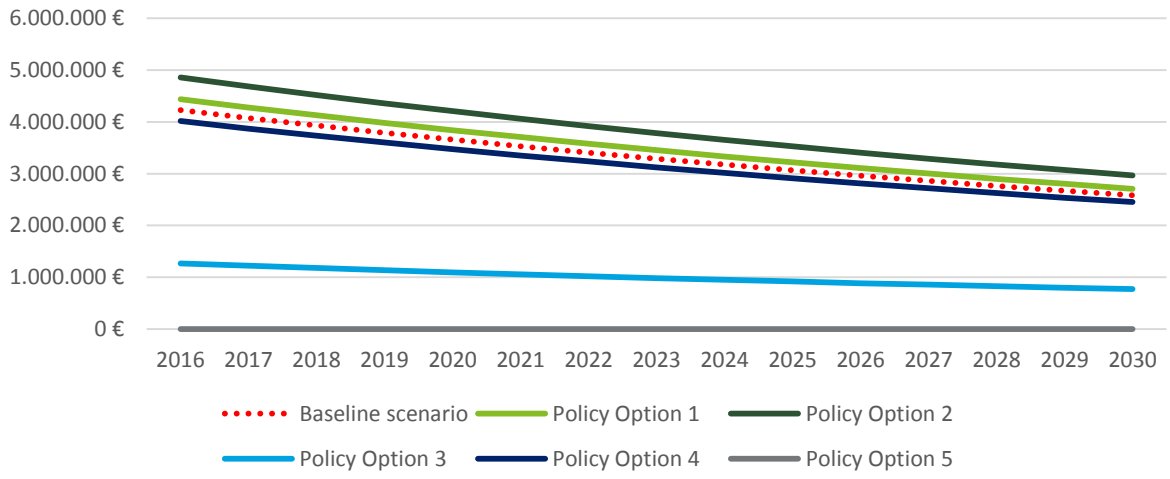
Figure 116 – Compliance costs for SMEs affected by the ePD per year under each policy option and the baseline scenario (2016-2030)



Source: Deloitte

In the baseline scenario, annual compliance costs for large enterprises affected by the ePD roughly amount to 4 EURm today. This amount is expected to decrease until 2030 to around 2.5 EURm. Similar to the logic outlined in relation to all businesses above, the policy options are expected to increase (policy options 1, 2, and 4) or decrease (policy options 3 and 5) the compliance costs for large enterprises.

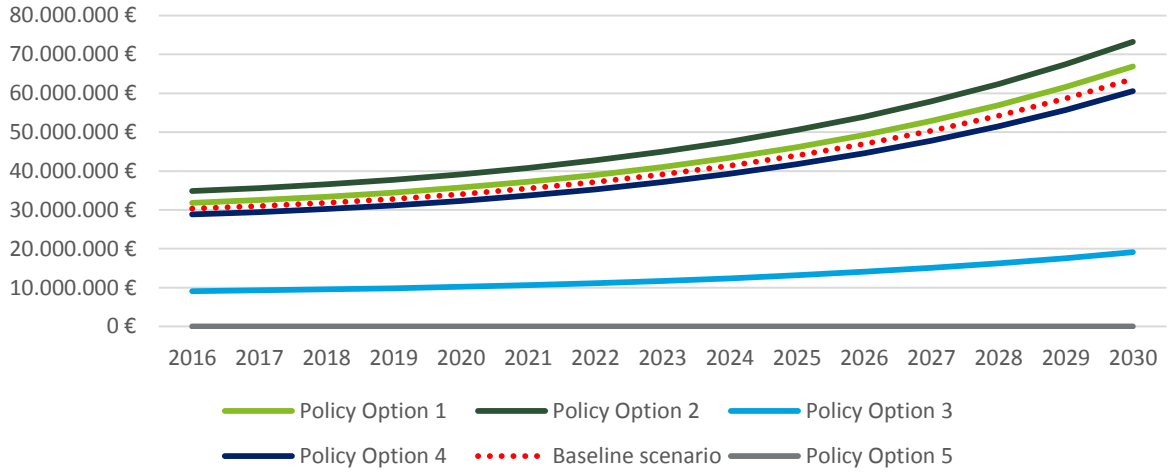
Figure 117 – Compliance costs for large enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030)



Source: Deloitte

In the baseline scenario, annual compliance costs for foreign controlled enterprises affected by the ePD amount to 30 EURm today. This amount is expected to increase until 2030 to roughly 60 EURm. Conversely to the logic outlined in relation to all businesses above, policy options 1, 3 and 5 are expected to decrease the compliance costs for foreign controlled enterprises while the other policy options are expected to increase the costs compared to the baseline scenario.

Figure 118 – Compliance costs for foreign controlled enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030)



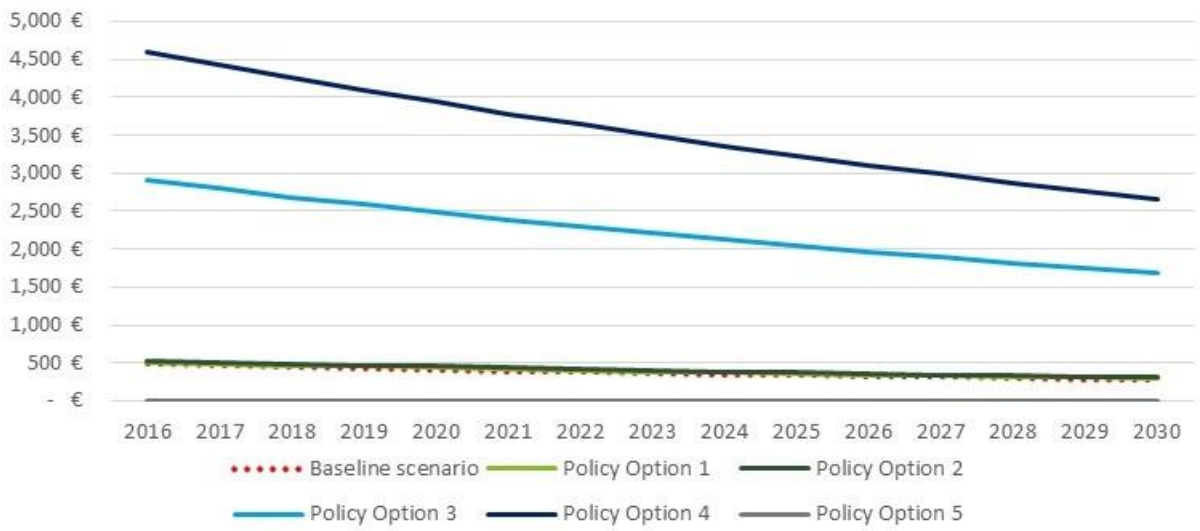
Source: Deloitte

The following graph presents the average compliance costs for all businesses affected by the ePD per year under each policy option and the baseline scenario. While, an average business today pays close to 500 Euro per year to comply with the ePD, this amount is expected to decrease to under 300 Euro in 2030. This means that the annual compliance costs for an average business across the entire time period of 2016-2030 is roughly 375 Euro.

All policy options are expected to (slightly) increase the annual compliance cost for an average business.

The “browser solution” of Policy option 3 is expected to increase the amount to close to 3,000 Euro today and to roughly 1.750 Euro in 2030. This is due to the limited number of businesses that would be affected by the ePD under this options and, thus, would individually have to bear extra costs.

Figure 119 –Average compliance costs for all businesses affected by the ePD per year under each policy option and the baseline scenario (2016-2030)



Source: Deloitte

The next section presents the comparison between the policy options and the baseline scenario in relation to the costs from administrative burden.

Expected development of the costs from administrative burden over time

This section presents the impacts of the policy options on the costs from administrative burden incurred by businesses compared to the baseline scenario.

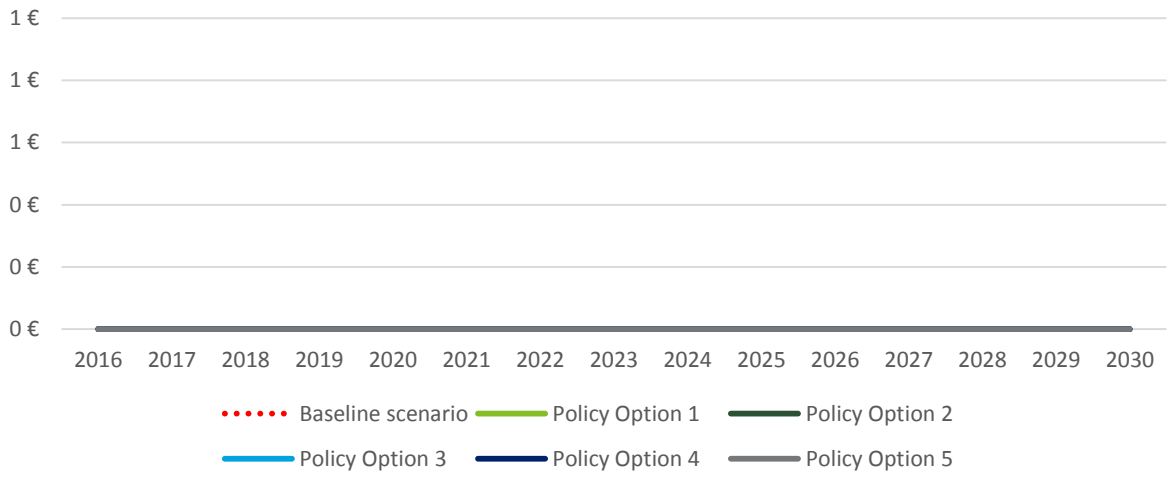
In the baseline scenario, annual costs from administrative burden for all businesses affected by the ePD are expected to increase slightly from.

As can be seen in the figure below, differences exist between the policy options not only in relation to the magnitude of the impacts but also in relation to its direction.

While policy options 1, 2, and 4 are expected to slightly increase the costs from administrative burden compared to the baseline scenario, policy option 3 and in particular policy option 5 are expected to reduce the compliance costs.

The same logic concerning the impact of the policy options on the annual costs from administrative burden for affected applies to all size classes.

Figure 120 – Costs from administrative burden for all businesses affected by the ePD per year under each policy option and the baseline scenario (2016-2030)

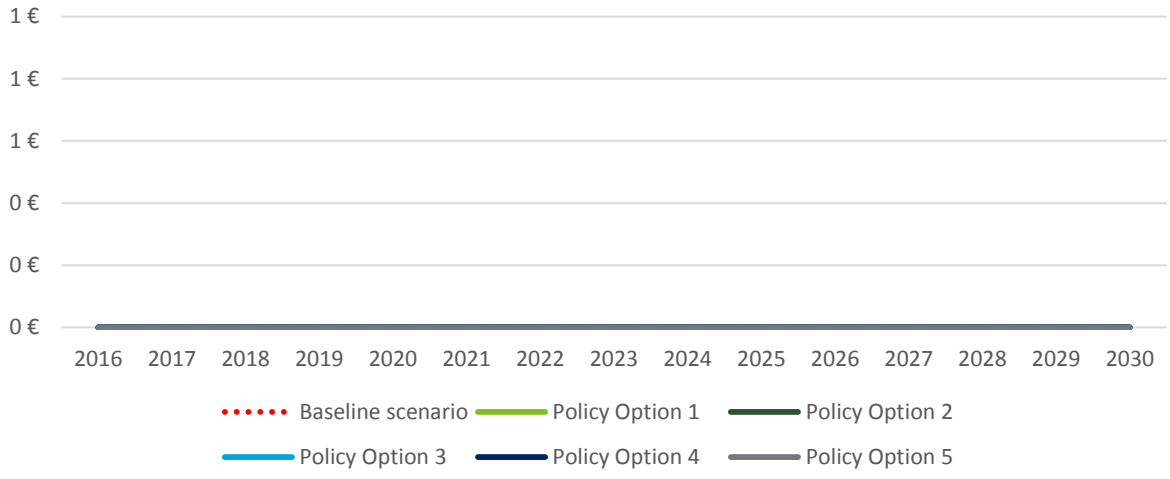


Source: Deloitte

The next graph visualises the annual costs from administrative burden for micro-enterprises. As can be seen, the costs are expected to decrease slightly until 2030.

The same logic as for all businesses (see above) concerning the impact of the policy options on the costs from administrative burden applies to this size class.

Figure 121 – Costs from administrative burden for micro-enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030)

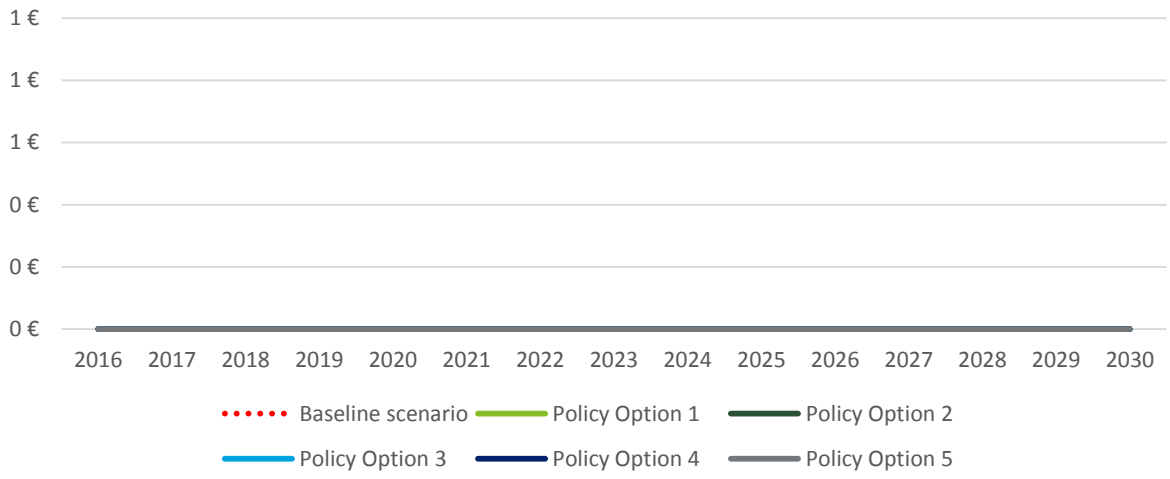


Source: Deloitte

The next graph visualises the annual costs from administrative burden for SMEs. As can be seen, the costs are expected to increase strongly until 2030.

The same logic as for all businesses (see above) concerning the impact of the policy options on the costs from administrative burden applies to this size class.

Figure 122 – Costs from administrative burden for SMEs affected by the ePD per year under each policy option and the baseline scenario (2016-2030)

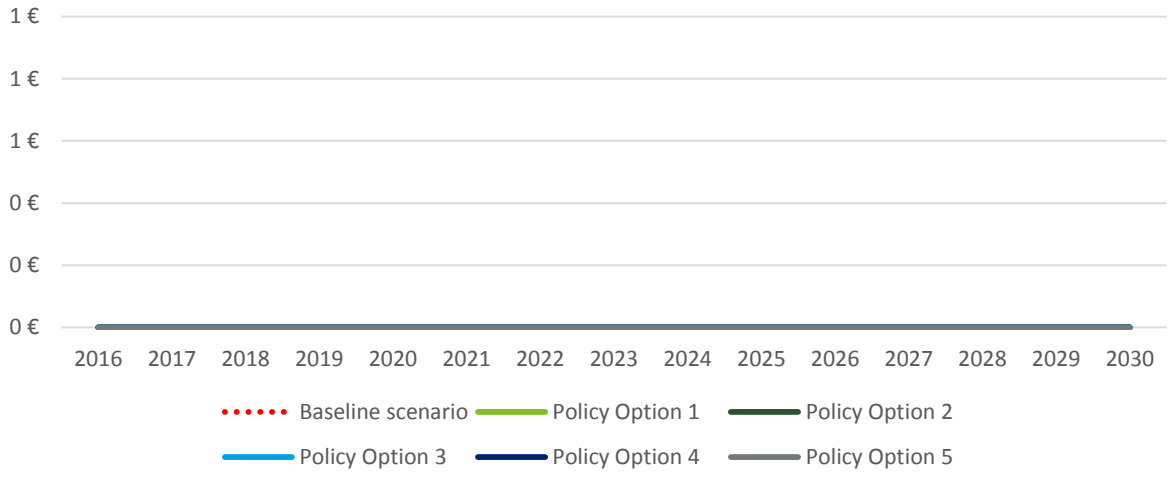


Source: Deloitte

The following graph visualises the annual costs from administrative burden for large enterprises. As can be seen, the costs are expected to increase slightly until 2030.

The same logic as for all businesses (see above) concerning the impact of the policy options on the costs from administrative burden applies to this size class.

Figure 123 – Costs from administrative burden for large enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030)

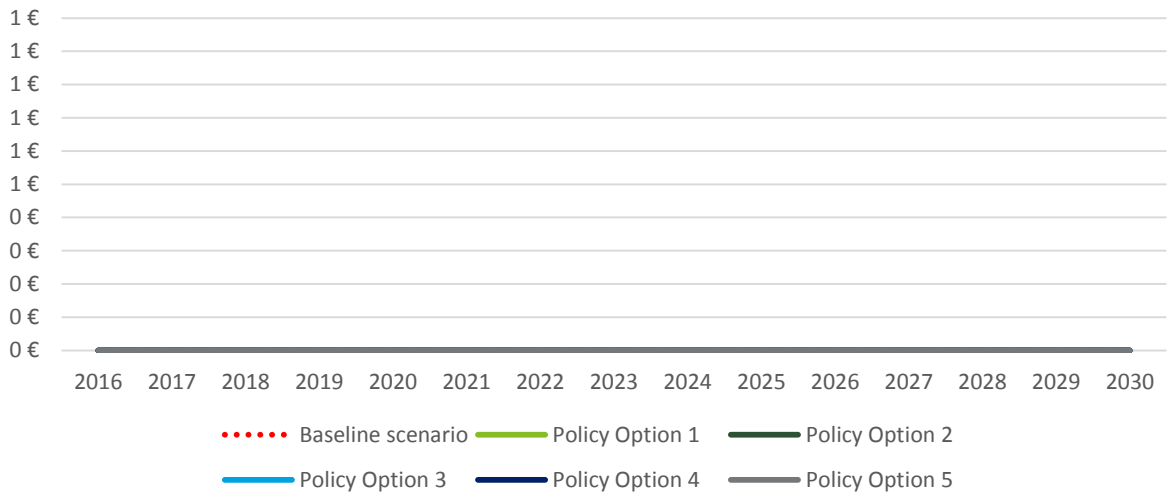


Source: Deloitte

The next graph visualises the annual costs from administrative burden for SMEs. As can be seen, the costs are expected to increase slightly until 2030.

The same logic as for all businesses (see above) concerning the impact of the policy options on the costs from administrative burden applies to this size class.

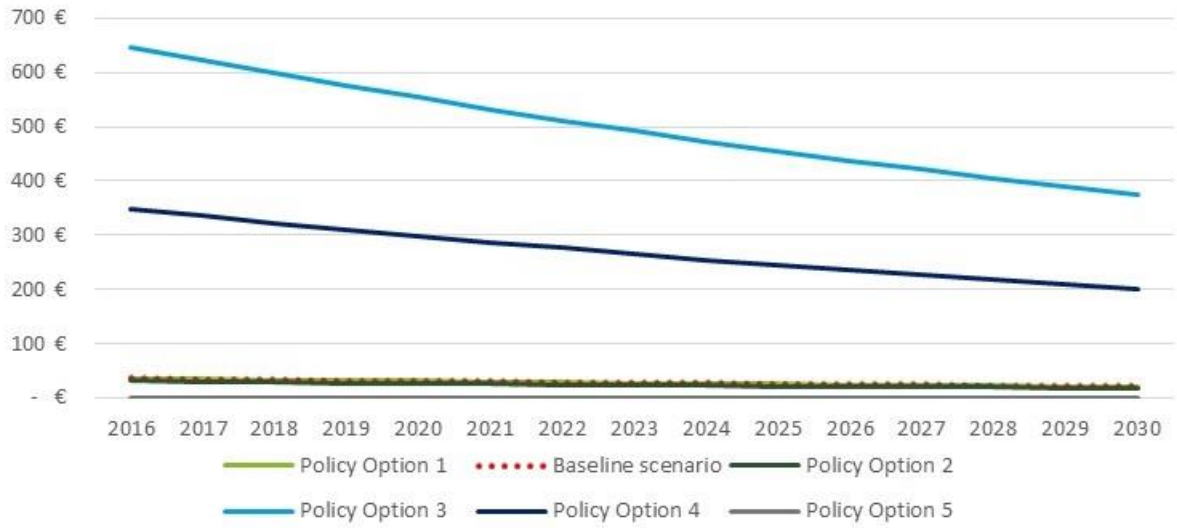
Figure 124 –Costs from administrative burden for foreign controlled enterprises affected by the ePD per year under each policy option and the baseline scenario (2016-2030)



Source: Deloitte

The following figure presents the average costs from administrative burden for all businesses affected by the ePD per year under each policy option and the baseline scenario. Apart from the situation under the "browser solution" of policy option 3, these costs are marginal.

Figure 125 –Average costs from administrative burden for all businesses affected by the ePD per year under each policy option and the baseline scenario (2016-2030)



Source: Deloitte

The next section presents the comparison between the policy options and the baseline scenario in relation to the qualitative ratings applied in the respective Parts B of each specific section on the assessment of the economic impact of the policy options.

Key findings concerning the number affected citizens

Table 109 – Key figures of the quantitative assessments concerning citizens (absolute values)

Average number of citizens affected per year (in million)	REFIT (2002-2015)	Today (2016 snap shot)	Baseline scenario (2016-2030)	Policy Option 1 (2016-2030)	Policy Option 2 (2016-2030)	Policy Option 3 (2016-2030)	Policy Option 4 (2016-2030)	Policy Option 5 (2016-2030)
Internet to browse online	304.8	397.7	487.0	487.0	487.0	487.0	487.0	487.0
Online social networks	214.9	280.4	365.1	365.1	365.1	365.1	365.1	365.1
E-Mail	280.2	382.4	483.0	483.0	483.0	483.0	483.0	483.0
Instant messaging (e.g. WhatsAppWhatsApp)	156.9	280.4	446.1	446.1	446.1	446.1	446.1	446.1
VoIP	58.5	209.0	398.2	398.2	398.2	398.2	398.2	398.2
Mobile phone to make calls or send texts	369.1	469.1	514.9	514.9	514.9	514.9	514.9	514.9
Fixed phone line	477.2	397.7	309.0	309.0	309.0	309.0	309.0	309.0

Source: Deloitte

Table 110 – Key figures of the quantitative assessments concerning citizens (absolute changes)

Absolute changes compared to the initial problem / baseline scenario (in million)	REFIT (2002-2015)	Today (2016 snap shot)	Baseline scenario (2016-2030)	Policy Option 1 (2016-2030)	Policy Option 2 (2016-2030)	Policy Option 3 (2016-2030)	Policy Option 4 (2016-2030)	Policy Option 5 (2016-2030)
Internet to browse online	-	-	182.1	-	-	-	-	-
Online social networks	-	-	150.2	-	-	-	-	-
E-Mail	-	-	202.8	-	-	-	-	-
Instant messaging (e.g. WhatsApp)	-	-	289.2	-	-	-	-	-
VoIP	-	-	339.7	-	-	-	-	-
Mobile phone to make calls or send texts	-	-	145.9	-	-	-	-	-
Fixed phone line	-	-	- 168.2	-	-	-	-	-

Source: Deloitte

Table 111 – Key figures of the quantitative assessments concerning citizens (relative changes)

Relative changes compared to the initial problem / baseline scenario (in %)	REFIT (2002-2015)	Today (2016 snap shot)	Baseline scenario (2016-2030)	Policy Option 1 (2016-2030)	Policy Option 2 (2016-2030)	Policy Option 3 (2016-2030)	Policy Option 4 (2016-2030)	Policy Option 5 (2016-2030)
Internet to browse online	-	-	60%	0%	0%	0%	0%	0%
Online social networks	-	-	70%	0%	0%	0%	0%	0%
E-Mail	-	-	72%	0%	0%	0%	0%	0%
Instant messaging (e.g. WhatsAppWhatsApp)	-	-	184%	0%	0%	0%	0%	0%
VoIP	-	-	581%	0%	0%	0%	0%	0%
Mobile phone to make calls or send texts	-	-	40%	0%	0%	0%	0%	0%
Fixed phone line	-	-	-35%	0%	0%	0%	0%	0%

Source: Deloitte