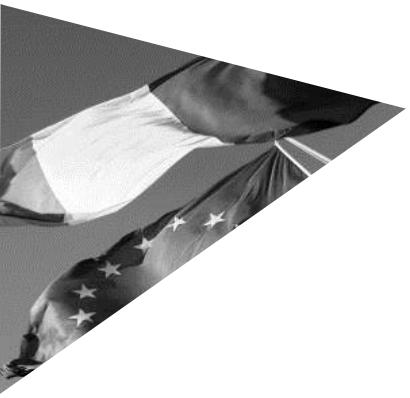
© 2015 Property of Ernst & Young Associés et Ernst & Young Société d'Avocats – Confidential. This report is reserved for your internal use and is indissociable from the contextual elements used as a basis for its elaboration.

European Commission – DG Justice

Evaluation study on Regulation (EC) No 45/2001

Final report

May 2015



Building a better working world

This study was requested by the European Commission, DG Justice in view of the amendment of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1–22).

Authors: EY France

- for EY Société d'avocats: Fabrice Naftalski, Christina Samaras
- for EY Advisory: Marie Brunagel, Véronique Ménez

The information and views set out in this study are those of the authors 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.

Table of contents

1 Objectives and approach 9

1.1 Objectives and scope of the evaluation 9

1.2 Data gathering methods and tools 12

2 Evaluation framework 16

3 Effectiveness 18

3.1 Methodology used to answer the evaluation questions on effectiveness 18

3.2 Contribution of the Regulation to ensuring the protection of fundamental rights and freedoms (Objective 1) 21

3.3 Contribution of the Regulation to ensuring the free flow of personal data (Objective 2) .. 58

3.4 . Contribution of the Regulation to establishing a relevant and effective governance system (Objective 3) 64

4 Efficiency 103

4.1 Methodology for answering the evaluation question 103

4.2 Implementation of the Regulation (EC) No. 45/2001 reached a total cost of 28 million euros in 2014, corresponding to 210 FTEs performed by 1455 staff 105

4.3 Breakdown of costs per activity 109

5 Relevance 121

5.1 Methodology to assess the evaluation question 121

5.2 Items identified whose relevance is questioned 121

6 Coherence 123

6.1 Access to documents versus data protection 123

6.2 Coherence between Regulation (EC) No. 45/2001 and the ePrivacy Directive 123

6.3 Miscellaneous: coherence with further identified legislation 123

7 Impact 127

7.1 Clarification of the principle of data minimization 127

7.2 Introduction of the transparency principle and increased information obligation 128

7.3 Introduction of the right to be forgotten and data portability 129

7.4 Enhancing accountability of data controllers and reinforcing security 129

8 Key findings and recommendations 134

8.1 An effective governance system, structured around two pillars: the DPO and the EDPS 134

8.2 The system for the enforcement of the Regulation could be enhanced, notably through greater use of sanctions 135

8.3 Some of the Regulation's key requirements (e.g. on data retention or data security) need to be better implemented to achieve "real and operational" compliance 136

8.4 Effective communication channels between the EDPS and EU institutions and bodies, even if there is still room for improvement 137

8.5 The rules enshrined in chapter IV relating to the telecommunications sector are outdated 138

8.6 The principles and rules enshrined in the Regulation are to a large extent relevant to meet the objectives of the Regulation, although some core definitions lack clarity 138

8.7 Data protection matters in EU institutions and bodies represent an overall estimated cost of 28 million euros, although the allocation of resources could be questioned 139

8.8 The notification and prior checking system is excessively burdensome 140

8.9 The articulation of access to documents and data protection has raised operational difficulties 141

8.10 The transfer rules and mechanisms need to be clarified and simplified 142

8.11 Shortcomings have been identified in the EDPS consultation process 143

9 Annexes 145

9.1 List of DPOs and DPCs 145

9.2 List of consulted documentation 146

Content of the report

The present report is the first volume of the evaluation study on Regulation (EC) No 45/2001 covering the presentation of the objectives of the study, the answers to the evaluation questions and the conclusions and recommendations.

Chapter 1 presents the objectives and background of the study and the approach proposed.

Chapter 2 presents the evaluation framework developed by the evaluators to address the evaluation questions.

Chapters 3 to 7 present the answers to the evaluation questions relating to effectiveness, efficiency, relevance, coherence and impacts.

Chapter 8 provides a synthesis of the key findings and proposed recommendations based on the analyses of the evaluator.

A second volume contains the five case studies.

Glossary

- BYOD: Bring Your Own Device
- CCTV: Closed-Circuit Television
- CIS: Custom Information System
- CJEU: Court of Justice of the European Union
- CNIL: Commission Nationale de l'Informatique et des Libertés
- DC : Data Controller
- DG BUDGET: Directorate-General for the Budget
- DG CONNECT: Directorate-General for Communications Networks, Content and Technology
- DG DIGIT: Directorate-General for Informatics
- DG Interpretation or SCIC: Directorate-General for Interpretation
- DG HR: Directorate-General of Human Resources and Security
- DG JUST / DG JUSTICE: Directorate-General of Justice
- DPC: Data Protection Coordinator
- DPO: Data Protection Officer
- EC: European Commission
- ECB: European Central Bank
- ECDC: European Centre for Disease Prevention and Control
- EDPS: European Data Protection Supervisor
- EEAS: European External Action Service
- EIB: European Investment Bank
- EMA: European Medicines Agency
- EPSO: European Personal Selection Office
- ESA: European School of Administration
- EU: European Union
- EU LISA: EU Agency for Large-scale IT Systems
- EUROFOUND: European Foundation for the Improvement of Living and Working Conditions
- EUROPOL: European Police Office
- FTE: Full-Time Equivalent
- GDPR: General Data Protection Regulation
- HRBA: Human Resources and Business Administration
- IDOC: Commission's Investigation and Disciplinary Office
- IT: Information Technology
- JSB: Joint Supervisory Body
- LIBE Committee: Civil Liberties, Justice and Home Affairs Committee
- LISO: Local Information Security Officer
- MEP: Member of European Parliament
- OJ: Official Journal of the European Union
- OLAF: European Anti-Fraud Office
- P&C: Policy and Consultation
- PMO: PayMaster Office
- PO: Publication Office
- SCG: Supervision Coordination Group
- S&E: Supervision and Enforcement
- SIS: Schengen Information System
- SLA: Service Level Agreement
- TEC: Treaty Establishing the European Community
- TFEU: Treaty on the Functioning of the European Union
- VIS: Visa Information System

List of figures and tables

Figure 1 - Targets of the online survey 14
Figure 2 - Participation rate by data protection role 14
Figure 3 - How often do you update existing privacy/information notices to inform data subjects of their rights and the data processing operation as well as purposes? (Source: EY survey) 24
Figure 4 - Do you estimate that guidance (e.g. responses to questions, guidelines, opinions, etc.) provided by the EDPS is helpful? (Source: EY survey) 28
Figure 5 –In principle, personal data must only be collected and processed for specified, explicit and legitimate purposes. Nevertheless, internal rules adopted by an EU institution or body may change the initial purpose for which data were collected. Is this possibility used within your institution/body? (Source: EY survey) 29
Figure 6 - Is a risk assessment methodology defined and performed on the information systems supporting personal data? (source: EY survey) 34
Figure 7 - After having performed a risk assessment analysis on the information systems supporting personal data, IT security measures could be defined to mitigate the risks identified. Are there any processes in place to monitor the efficiency of these measures? (Source: EY survey) 35
Figure 8 – If another institution or body acts as data processor, is there a process in place ensuring that the services comply with the data protection legal requirements (ensuring that the service provider acts only on instructions from the controller)? (Source: EY survey) 36
Figure 9 - Are you aware of the existence of processes ensuring that service providers comply with the regulation? (Source: EY survey) 38
Figure 10 - Has your institution or body adopted standard security and confidentiality clauses, specific to the processing of personal data by controllers or processors? (Source: EY survey) 39
Figure 11 - If yes, are those standard clauses used in your institution or body when entering into an agreement with a data processor? (Source: EY survey) 39
Figure 12 - Do you have a background in data protection? (Source: EY survey) 66
Figure 13 - In your opinion, does your position in your institution or body allow you to exercise your functions in total independence? 67
Figure 14 - On average, how much time do you spend on data protection matters as a DPO per week? (Source: EY survey) 70
Figure 15 - Within your institution or body, are you confident that the register is up to date? (Source: EY survey) 72
Figure 16 – 2013 opinions per main prior check category (Source: EDPS 2013 annual report) 83
Figure 17 - Number of prior check opinions delivered by EDPS per year (source: 2013 EDPS annual report) 84
Figure 18 - Number of complaints per year (source: EDPS 2013 annual report) 87
Figure 19 - Number of inspections performed by EDPS from 2009 to 2013 (source: EDPS annual reports) 91
Figure 20 – Number of legislative opinions and comments (formal and informal) provided by the EDPS in the last 10 years (source: EDPS annual reports) 97
Figure 21 - Changes in total EDPS budget and number of official staff since 2004 (source: EDPS) 106
Figure 22 On average, how much time do you spend on data protection matters as a DPO per week? 107
Figure 23 - In your capacity as DPO, do you have a team working for you (other than the DPCs)? 107
Figure 24 On average, how much time do you spend on data protection matters as a DPC per week? 107
Figure 25 - In your quality as DPC, do you have a team working for you? (Source: EY survey) 107
Figure 26 - Approximately how many data controllers are in your institution or body? (Source: EY survey) 109

Figure 27 - On average, how much time do you spend on data protection activities? (Source: EY survey) 109
Figure 28 - Evolution of EDPS official staff by unit since 2008 (source: EDPS Annual report) 110
Figure 29 - Changes in S&E unit activities since 2004 (source: EDPS annual reports) 111
Figure 30 - Trend in legislative opinions and comments provided by the EDPS since 2004 (source: EDPS annual reports) 112
Figure 31 - On annual average, how much time do you spend as a DPO on each of the following data protection activities? (Source: EY survey) 114
Figure 32 - How would you consider the time you spend to performing each of these activities? (Source: EY survey) 115
Figure 33 - Words cloud based on DPOs proposition to improve the activities (wordle.net) 118
Figure 34 - What could be the impact of the implementation and application of such principle on your day-to-day work? (Source: EY survey) 128
Figure 35 - Which mechanisms would best improve accountability in the context of EU institutions and bodies? (Source: EY survey) 130
Figure 36 – What would be the impact of the introduction of the Privacy Impact Assessments prior to risky processing operations? (Source: EY survey) 131
Figure 37 – Do you think it would be worthwhile to create a code of conduct in terms of better protection of personal data and simplification of the work? (Source: EY survey) 131
Figure 38 –Have you ever experienced personal data breaches? (Source: EY survey) 132
Figure 39 - Do you think that this rule is useful and should be kept in future Regulation (EC) 45/2001? (Source: EY survey) 132
Figure 40 - Should you consider that the implementation and application of the obligation to notify data breaches would have an impact on your day to day work, do you know any mitigation measures that could be taken? (Source: EY survey) 132

Table 1: Evaluation questions 16
Table 2 - Intervention logic of Regulation (EC) No. 45/2001 20
Table 3 –DPOs and DPCs costs estimates 108
Table 4 – Time spent by DCs on several data protection activities (source: EY survey) 119

1 Objectives and approach

1.1 Objectives and scope of the evaluation

Within a general context of reform of the EU data protection legal framework, the European Commission intends to amend the current Regulation (EC) No 45/2001 in order to align this text with the principles and rules that will be applicable to Member States.

1.1.1 Objectives

The purpose of the assignment is two-fold: on the one hand, to conduct an **in-depth analysis of the current data protection legal framework** as it is applied by the EU institutions, bodies, offices and agencies; on the other hand, to **develop recommendations** on the basis of the findings in view of the possible amendments.

From a legal perspective, the study aims to assess the implementation, application and enforcement of the current Regulation (EC) No 45/2001[1] (hereinafter referred to as "the Regulation") by the EU institutions, bodies, offices, and agencies. The assignment also aims to identify further European legislation relating to data protection in order to assess the articulation of the Regulation with the existing EU legal framework.

From a more comprehensive perspective, the study evaluates the relevance, coherence, efficiency, effectiveness and impact of Regulation (EC) No 45/2001 taking into account its foreseen amendment. This is achieved through the definition of an evaluative framework, comprising a set of evaluation questions covering all aforementioned criteria. Detailed responses will be provided for each question, thus enabling the objectives of the study to be achieved.

Based on the final evaluation report and the related recommendations, the European Union will be able to implement appropriate actions to amend Regulation (EC) No 45/2001.

The main purpose of this study is the evaluation of the current EU *acquis* (i.e. Regulation 45/2001 as it is currently applied, implemented and enforced). The study does not include an economic analysis highlighting different policy options, as there is a consensus on the amendment of Regulation (EC) No 45/2001 in order to align it with the principles and rules of the GDPR (except when the rule is not relevant or suitable for the EU institutions, agencies and bodies).

In addition, as the amendment of Regulation (EC) No 45/2001 will not have an economic impact on Member States and as the impact on EU institutions and bodies is expected to be limited, an

[1] *OJ L 8, 12.1.2001, p. 1–22.*

assessment of the impact of the possible amendments (as brought about by the GDPR) on EU institutions, bodies and agencies would not be relevant. Nevertheless, the study should identify the key changes (e.g. introduction of privacy impact assessments, notification of personal data breaches, etc.) and identify some possible impacts for EU institutions, agencies and bodies.

1.1.2 Scope

The scope of the study concerns Regulation (EC) No 45/2001 as it is implemented, applied, and enforced by EU institutions, agencies and bodies and as it is articulated with other key legislations.

Thus, all EU institutions, agencies and bodies may be concerned by Regulation (EC) No 45/2001. In addition, during the inception work, over 1800 legal texts have been identified making reference to Regulation (EC) No 45/2001.

A specific approach and several data collection and analysis methods and tools (including legal analysis) have been developed (and described hereunder) to ensure the best coverage of the scope of Regulation (EC) No 45/2001.

The following approach has been implemented:

- Regarding the analyses of the implementation, application and enforcement of Regulation (EC) No 45/2001, **all EU institutions, bodies and agencies** are taken into account. Guidance and implementing rules adopted by EU bodies, enforcement actions and significant case law are covered by the documentary review. The analysis of the Regulation (EC) No 45/2001 is also fed by the consultation of all relevant EU institutions, agencies and bodies and stakeholders through an online survey (DPOs, DPCs, data controllers and IT staff members). Additional face to face or phone interviews have been conducted with a sample of stakeholders to go in more depth into the key issues raised by the responses to the survey. These tools contribute to identifying similar or diverging views on Regulation (EC) No 45/2001 interpretation/application.
- Regarding the analysis of the articulation of Regulation (EC) No 45/2001 with other legal texts, an exhaustive legal analysis is not realistic. As mentioned in the terms of reference and after an initial literature review, some legal texts appear to be of particular interest for the study. Thus, focus was placed on the analysis of the articulation of Regulation (EC) 45/2001 with the legal framework applicable to the police and criminal justice sector, ePrivacy Directive and Regulation (EC) No 1049/2001 regarding public access to documents. The case studies are dedicated to these analyses.
- Regarding the prospective part of the study, an in-depth legal analysis of GDPR has been conducted. The main principles and rules have been identified in order to assess their relevance with regard to Regulation (EC) No 45/2001.
- From an IT perspective, the study evaluates the maturity levels of the EU institutions, bodies, offices and agencies regarding information security and the protection of personal data. The evaluative framework includes questions on the implementation of specific IT controls.

1.1.3 Approach proposed

The methodology focuses on ways to demonstrate relevance, coherence, efficiency, effectiveness and impact of Regulation (EC) No. 45/2001. Throughout the evaluation process, we follow a mixed-method approach: legal analysis and evaluative analysis developed on the basis of data collected in the field (survey and interviews with stakeholders).

The approach comprises **three main phases**:

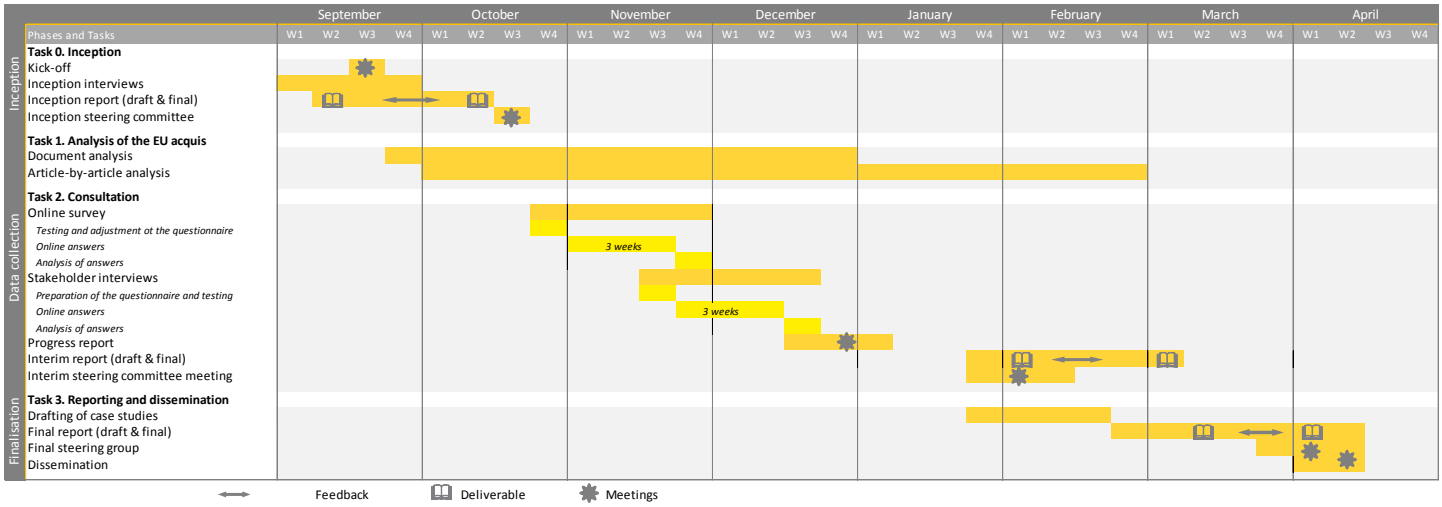
(1) **Inception phase**: to set up the scope and evaluation framework (relevant legal framework, relevant ECJ case law, evaluation questions, evaluation criteria and indicators), identifying documents relevant for the analysis, drafting data collection tools (i.e. written consultation and target groups) and providing an updated work plan for implementation;

(2) **Data collection and legal analysis phase**: to compile evidence from relevant documents and thorough legal analysis, collect information on the application and enforcement of the Regulation through a written consultation and interviews with key stakeholders, to provide input for case studies thereof, and to formulate preliminary answers/hypotheses for each of the evaluation questions;

(3) **Reporting phase:** to compile the results of the legal analysis, data collection and desktop analysis phase and develop the case studies. The team provides answers to the evaluation questions, an article-by-article analysis, and translates the findings into conclusions and recommendations, which can be considered by the Commission and subsequently translated into more specific actions to amend Regulation (EC) No. 45/2001.

1.1.4 Timeline

The figure below presents the work programme implemented for the contract period. It is detailed week by week.



The key phases in the Gantt chart are listed below:

Milestone	Timing
Draft inception report	10.09.2014
Kick-off meeting	15.09.2014
Steering committee meeting 1	14.10.2014
Inception Report	10.2014
Feedback	Max 20 days after receipt of the Inception Report 15 days after receipt of EC feedback
Online survey	Approx. 3 weeks, 11.2014
Stakeholder interviews	Approx. 3 weeks, 11-12.2014
Progress Report	December 2014
Steering committee group meeting and first Draft Interim Report	20 January 2015
Final Interim Report	12.03.2015
Steering group meeting 2	19.03.2015
Final workshop	26.3.2015
Final Report	27.4.2015
Feedback	Max 45 days after receipt of the Draft Final Report 15 days after receipt of EC feedback
Steering group meeting 3	30.04.2015 Within 2 weeks after submission of the Final Report
Final Report *(full and draft of the public version)*	05.2015 20 days after receipt of last EC feedback
Public Version of the Final report	20 days after approval of the Final Report

1.2 Data gathering methods and tools

The evaluation framework developed in the inception report identifies the sources of information that have been considered as relevant in order to carry out the required analysis and consequently answer the key questions of the study.

This section sets out in more detail the existing data and sources of information that were used (secondary data) to conduct our analysis and the tools implemented to gather additional data (primary data).

1.2.1 Data collection methods

Secondary data

Secondary data, i.e. existing data or sources of information were mainly based on a thorough literature review including:

- **Legal framework**: (i) analysis of EU *acquis* related to Regulation (EC) No 45/2001 (including case law) and (ii) analysis of the coherence of Regulation (EC) No 45/2001 with Regulation (EC) No 49/2001 and other relevant legislation;
- **Legal doctrine**: position papers, selection of opinions and relevant working documents;
- **Monitoring and implementation data**: mainly EDPS annual reports and surveys on compliance of EDPS with Regulation (EC) No 45/2001.

A list of key documents was identified, collected and analysed to address the evaluation questions. The list of key documents reviewed is available in the annex.

The documentary review was carried out prior to the interviews in order to focus on the collection of primary data (i.e. non existing data) when performing interviews. Interviews can result in the identification of further relevant documents for the evaluation.

Primary data

In addition to the existing data that provides input for the evaluation, additional data has been gathered to complete the existing source of information mainly based on three tools:

- **Written stakeholder consultation**: an online survey targeted DPO, DPC, data controllers and IT staff to gather quantitative and qualitative data on their perception of the implementation, application and enforcement of the Regulation.
- **Several interviews** with key stakeholders were performed in order to obtain the opinion of various stakeholders on the Regulation, and focus on specific issues relating to the case studies.
- **The direct observation of the DPO meeting** in Thessaloniki in November 2014 allowed the evaluators to better identify the main issues relating to the Regulation reform and clarify their understanding of the DPOs' expectations.
- **A workshop with the steering group** will allow initial discussion on the results collected in order to highlight the major results and discuss the final conclusions and recommendations.

Based on these various sources, a **draft article-by-article analysis** will provide an overview of the evaluation.

1.2.2 Data collection tools

Online survey

The online questionnaire was developed in line with the evaluation framework, and in close cooperation with DG Justice. Structured around five themes, it covers each of the evaluation indicators for which existing data was not sufficient:

(i) identification of the respondent

(ii) description of the respondent's activity,

(iii) perception of the implementation of the Regulation

(iv) specific questions adapted to the respondent's data protection role in his/her institution (data protection officer, data protection coordinator, data controller, IT staff).

(v) prospective questions

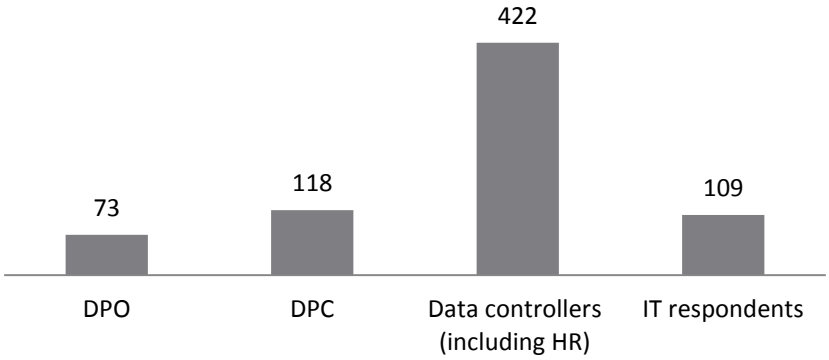
The detailed questionnaire is available in the annex to this document.

A wide survey covering all institutions, bodies and agencies of the EU and targeting all kinds of profiles related to data protection activities

- The survey was made up of 194 questions divided into identification questions and specific questions addressed to DPOs, DPCs, DC and IT staff. Each respondent was invited to provide answers relating to his or her role(s) regarding data protection.

- 722 people were targeted by the survey including DPOs (and assistants to DPOs), DPCs, data controllers and IT staff from EU institutions, bodies and agencies. Targets were identified by DG Justice via the network of DPOs.

Figure 1 - Targets of the online survey

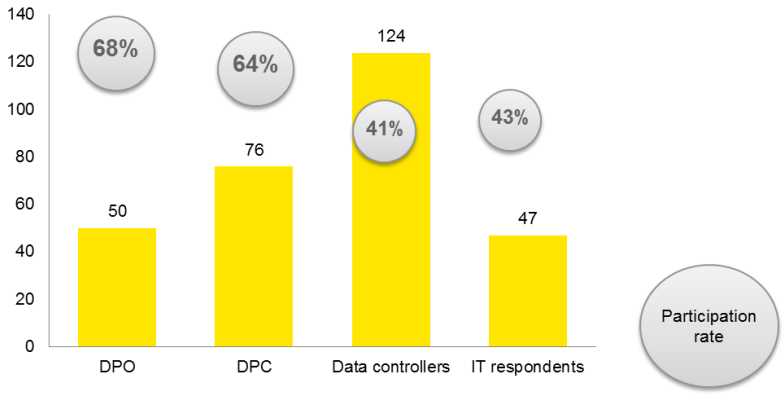


- 64 institutions, agencies and bodies were invited to take part in the survey, 52 of which participated.

A satisfactory participation rate of 40% of the targets and 81% of EU institutions, bodies and agencies, with a variety of profiles

The overall participation rate is quite satisfactory with an overall participation of 289 usable answers (excluding duplicates and empty answers), i.e. 40% rate. The participation rate differed from one profile to another. Higher participation was observed among DPOs (including his or her team) and DPC profiles than among IT and data controllers.

Figure 2 - Participation rate by data protection role



52 institutions, bodies and agencies contributed to the survey, leading to a participation rate of 81% of the surveyed entities, 75% of them providing between one and five answers. In line with their high representativeness in the initial contact list, the European Commission, the Council and EEAS represent 38% of respondents.

In spite of the length of the questionnaire, the quality of results is very satisfactory as even open questions received a relatively high number of answers.

The questionnaire was tested with several respondents over the phone before the online survey was launched.

Case studies

Case studies provide an in-depth examination of key issues related to the regulation, notably on external coherence aspects. Five case studies were performed in order to provide input for the evaluation:

- Application of the Regulation to agencies and bodies in the area of judicial cooperation in criminal matters and police cooperation;
- Articulation with the e-privacy Directive;
- Articulation with access to document rules of Regulation (EC) No 1049/2001;
- Data retention with respect to EU institutions staff data;
- Evaluation of articulation of Supervisory and Advisory roles of EDPS.

Interviews

The evaluation team has conducted interviews with the EDPS and a selection of stakeholders (DPOs, data controllers and IT officers).

Interview guides were developed based on evaluation themes that are relevant to the interviewees. The interview guide for EDPS interviews is provided as an example in the annex hereto.

2 Evaluation framework

The terms of reference of this study request a thorough evaluation of the relevance, coherence, efficiency, effectiveness and impact of Regulation (EC) No 45/2001. Whilst a specific list of evaluation questions to address was not provided, we have formulated the following key questions based on the issues raised by the terms of reference and our understanding of the European Commission expectations and validated during the inception phase.

As mentioned, these questions provide a strong indication of the focus areas of the evaluation study and will serve as the foundation of our work. The final report will give detailed answers to each individual question.

Table 1: Evaluation questions

Theme	Focus	Evaluation question(s)
Effectiveness	Implementation, application and enforcement of the Regulation	– How has Regulation (EC) 45/2001 been implemented, applied and enforced across Union institutions/bodies/offices/agencies? – In particular, emphasis should be put on the following aspects: o What are the mechanisms in place to ensure data subject rights? o How has Regulation (EC) 45/2001 been applied in the context of IT systems at EU level processing data of all individuals? o How has Regulation (EC) 45/2001 been applied in the context of Police and Judicial Cooperation? *Case study*
	Benefits for individuals and EU institutions	– How and to what extent Regulation (EC) 45/2001 has fulfilled its general and specific objectives? – How appropriate are the governance aspects of the application of Regulation (EC) 45/2001, including the role of the European Data Protection Supervisor (EDPS) and Data Protection Officers (DPOs) (including also the role of the Joint Supervisory Bodies of EUROPOL and EUROJUST)? *Case study*
Coherence	Articulation with other legislation/ directives/ regulations	– How Regulation (EC) 45/2001 is articulated with the ePrivacy Directive 2002/58/EC (as amended) and issues related to communications by Union institutions/bodies/offices/agencies? *Case study* – How is Regulation (EC) 45/2001 articulated with EU transparency and access to documents requirements, legislation and policies for Union institutions/bodies/ offices/agencies in force, in particular Regulation (EC) No

Theme	Focus	Evaluation question(s)
		1049/2001? *Case study – Where appropriate, how is Regulation (EC) 45/2001 articulated with further relevant identified Union legislation during the study?
Efficiency	Administrative costs associated with application of the Regulation	– What has been the impact of Regulation (EC) 45/2001 in terms of costs and administrative burden for Union institutions, bodies, offices and agencies, since it was put into application?
Relevance	Relevance of provisions of Regulation (EC) 45/2001	– How relevant and appropriate are the provisions of Regulation (EC) 45/2001 especially in the light of the recent technological developments?
		PROSPECTIVE QUESTIONS[2]
Relevance	Data protection reforms at EU level	– How relevant are the key elements of the EU data protection reform for EU institutions, bodies, offices and agencies, taking into account their specificities?
Impact	Potential impacts of the amendments	– What is the potential impact of the amendment of Regulation (EC) 45/2001 on existing personal data systems and processes and compliance procedures? – What could be done to minimise potential adverse impacts identified?

The last questions are prospective questions. They lead directly to the drafting of our recommendations.

[2] Please note that the evaluation study is not an impact assessment of potential amendments made to Regulation (EC) 45/2001. Therefore, the study shall only highlight in general terms (i) whether the main changes brought about by the GDPR are relevant (ii) whether these relevant changes result in adverse impacts, and identify potential mitigation measures.

3 Effectiveness

How has Regulation (EC) No 45/2001 been implemented, applied and enforced across Union institutions/bodies/offices/agencies and how and to what extent Regulation (EC) No 45/2001 has fulfilled its general and specific objectives?

3.1 Methodology used to answer the evaluation questions on effectiveness

Understanding of the question

In order to assess the effectiveness of Regulation (EC) No. 45/2001, it is necessary to:

- identify, according to the recitals and the provisions of Regulation (EC) No. 45/2001, the general and more specific objectives of this text
- link these objectives to the relevant provisions
- for each provision, assess its implementation, application and enforcement

Our analysis of the effectiveness questions will cover all provisions of Regulation (EC) No. 45/2001.

The evaluation of the implementation of Regulation (EC) No. 45/2001 refers to the process of putting the Regulation into execution, notably by adopting Rules of Procedure[3] and documented processes. Thus, the evaluation of the implementation focuses on the existence of implementing rules and other related procedures and internal rules.

The analysis of the application of Regulation (EC) No. 45/2001 requires assessing whether, how and to what extent EU staff members make use of the existing implementing rules and existing procedures. Detailed indicators and descriptors (qualitative indicators) have been developed to evaluate the provisions.

The enforcement of Regulation (EC) No. 45/2001 refers to the means implemented in order to ensure compliance with the data protection requirements enshrined in Regulation (EC) No. 45/2001.

Identification of objectives of Regulation (EC) No. 45/2001

The evaluation study analyses the benefits that Regulation (EC) No. 45/2001 has brought to both individuals and institutions. For this purpose, the study will assess whether Regulation (EC) No. 45/2001 fulfils its **three main objectives**:

- ensure effective compliance with the rules governing the protection of individuals' fundamental rights and freedoms (recital 13),

[3] Decision of the European Data Protection Supervisor of 17 December 2012 on the adoption of Rules of Procedure.

- ensure the free flow of personal data between Member States and the Community institutions and bodies, and between and within the Community institutions and bodies for purposes connected with the exercise of their respective competences (recital 13),
- establish a relevant and effective governance system to supervise and monitor the application of Regulation (EC) No. 45/2001, notably by establishing an independent supervisory body.

The figure below presents these main objectives, develops more specific, related objectives, and identifies the underlying provisions and recitals of Regulation (EC) No. 45/2001.

Table 2 - Intervention logic of Regulation (EC) No. 45/2001

GENERAL OBJECTIVES	SPECIFIC OBJECTIVES	RELATED RECITALS AND PROVISIONS
Ensure protection of fundamental rights and freedoms - "ensure effective compliance with the rules governing the protection of individuals' fundamental rights and freedoms" (Recital 13)	Establish rights for data subjects	Recitals 2 & 5, Art. 11 to 19, Art. 32 & 33
	Establish appropriate sanctions for offenders and remedies for data subjects	Recitals 2 & 5, Art. 32, 33, 47 and 49
	Establish obligations for those who process personal data (data protection principles)	Recitals 2 & 5, Art. 4 to 6, Art. 10, Art. 25.1, Art . 29 to 31
	Ensure security and confidentiality	Art. 21 to 23
	Ensure that the EU legislator and other institutions/bodies are aware of data protection requirements and integrates data protection in the law making and implementation process	Art. 28.1 and 28.2.
	Ensure a consistent and homogeneous application of the rules for the protection of individuals fundamental rights and freedoms with regard to the processing of personal data throughout the European Union	Recital 12 Art. 24, 25 and Art. 46
	Achieve the right balance between the protection of personal data and other legitimate public interests or other freedoms or rights	Recital 2 and 20
	Ensure protection of personal data and privacy in the context of internal telecommunication network	Chapter IV
Ensure the free flow of personal data between MS and the Community institutions and bodies and between and within the Community institutions and bodies **Recital 24, Art. 7 to 9**	Ensure free flow of personal data within or between Community institutions or bodies	Art. 7
	Ensure free flow of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46/EC	Art. 8
	Ensure free flow of personal data to recipients, other than Community institutions and bodies, which are not subject to Directive 95/46/EC	Art. 9
Establish a relevant and effective governance system, notably an independent supervisory system **Recitals 5 &32** **Section 8 and Chapter V**	Establish a DPO in each Community institution and body (who ensures that the provisions of the Regulation are applied and who advises controllers to comply with their obligations)	Recital 32, Section 8
	Establish an independent supervisory body responsible for monitoring the application of Regulation (EC) 45/2001 and related implementing rules	Recital 5, Chapter V

Source: Analysis EY on the basis of Regulation (EC) No. 45/2001.

Proposed approach and limits

As mentioned above, for each provision, we assessed its implementation, application and enforcement, on the basis of detailed indicators and descriptors.

The information gathered through the documentary review, the online questionnaires and the interviews provided data relating to the indicators and allowed the evaluator to conclude on the achievement of the specific objectives and the contribution of Regulation (EC) No. 45/2001 to the general objectives.

Regulation (EC) No 45/2001 has been evaluated through the combined analysis of documentary review, and quantitative and qualitative data gained through the online survey and interviews.

As regards the implementation of Regulation (EC) No 45/2001, the evaluator was informed of the existence of internal procedures adopted by the EDPS (i.e. a manual for handling complaints or conducting inspections), but these documents were not always disclosed to the evaluator.

The analysis of the effectiveness of Regulation (EC) No 45/2001 requires understanding (i) how Regulation (EC) No 45/2001 has been implemented, applied and enforced throughout EU institutions and bodies and (ii) how and to what extent it has fulfilled its main general and specific objectives.

As indicated in the effectiveness framework, Regulation (EC) No 45/2001 has three main objectives, namely, the protection of a fundamental right to personal data protection (i), the free-flow of personal data (ii) and the establishment of a data protection governance system which includes an independent supervisory authority (iii).[4]

3.2 Contribution of the Regulation to ensuring the protection of fundamental rights and freedoms (Objective 1)

This section aims to assess how and to what extent Regulation (EC) No 45/2001 has contributed to the protection of fundamental rights and freedoms of data subjects.

As explicitly specified in Recital 2, a "fully-fledged system of protection of personal data" requires (i) the **establishment of rights** for data subjects and (ii) **obligations** for those who process personal data, but also (iii) **appropriate sanctions** for offenders and monitoring by an independent supervisory body. Moreover, the Regulation should ensure consistent and homogeneous application of the rules for the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data (Recital 12) (iv).Regulation (EC) No 45/2001 also provides for specific rules applicable to the telecommunications sector (v).

[4] See Recital (5) of Regulation (EC) No 45/2001, *"A Regulation is necessary to provide the individual with legally enforceable rights, to specify the data processing obligations of the controllers within the Community institutions and bodies, and to create an independent supervisory authority responsible for monitoring the processing of personal data by the Community institutions and bodies"*.

3.2.1 Rights for data subjects and means to exercise them

The Regulation establishes rights for data subjects and means to exercise them

Regulatory framework

Pursuant to Recital 2 of the Regulation, a system of protection of personal data requires *inter alia* the establishment of rights for data subjects. Recital 5 adds that the Regulation provides the individual with legally enforceable rights.

Regulation (EC) No 45/2001 creates rights for data subjects in order to protect their personal data (Article 13 to 19): right of access, right of rectification, blocking, erasure, notification to third parties, right to object and right not to be subject to automated individual decisions). Moreover, Regulation (EC) No 45/2001 sets out the right for the data subject to be informed and lays down the information to be supplied to data subjects, where the data has been obtained from the data subject (Article 11) and where they have not (Article 12).

Right of access

Pursuant to Article 13 of Regulation (EC) No 45/2001, the data subject has the right to obtain from the controller within three months and free of charge: (a) if data relating to him or her is being processed; (b) information on the purposes of the processing, the categories of data concerned and the recipients to whom data is being disclosed; (c) **communication in an intelligible form** of the data being processed and any information regarding their source; (d) knowledge involved in any automated decision process concerning him or her.

It stems from Article 13 of the Regulation that the right of access enshrined in the Regulation includes the right to data portability in an intelligible form (Article 13 (c)) which is very close to the right enshrined in Article 18 of the GDPR. Our understanding is that the "electronic means" provided by the GDPR could be considered as covered by the "intelligible form" as laid down by Article 13.

Right of rectification

Pursuant to Article 14 of the Regulation (EC) No 45/2001, data subjects have the right to have their data rectified without delay in case of inaccurate or incomplete personal data.

Right of blocking

Pursuant to Article 15 of Regulation (EC) No 45/2001, data subjects have the right to obtain from the data controller the blocking of their data where:

- their accuracy is contested by the data subject;
- the controller has to maintain the data for purposes of proof, or;
- the processing is unlawful and the data subject opposes their erasure and demands their blocking instead.

Blocked data may only be used for purposes of proof, or with the consent of the data subject, or for the protection of the rights of a third party. Technical means must be implemented to indicate that the data cannot be used.

This article should be read in the light of the right to be forgotten and to erasure as provided by Article 17.4 of the proposed GDPR.

Right of erasure, right to object and notification to third parties (Articles 16 and 18)

Data subjects have the right to obtain the erasure of their data if the processing is unlawful and to object to the processing for legitimate reasons. Data subjects also have the right to be notified that their data is being disclosed to third parties. The data controller must notify third parties to whom data have been disclosed of any erasure, rectification or blocking (unless this proves impossible or involves disproportionate efforts).

Automated Individual decisions

Pursuant to Article 19 of Regulation (EC) No 45/2001, data subjects have the right not to be subject to automated individual decisions which produce legal effects, in certain circumstances.

Regarding the right to lodge a complaint, please see below.

Implementation and Application

Data subjects' rights are properly implemented in processes and procedures

The obligation to create rights for data subjects and the means to exercise them have effectively been implemented and applied throughout EU institutions and bodies. However, further improvements should be made to increase the application of the rights.

EU institutions and bodies have developed specific procedures and means to implement data subjects' rights; a large majority of EU institutions[5] have drafted forms available on their intranets or websites in order to enable data subjects to exercise their rights. The mechanisms in place are rarely built into the IT systems (i.e. the data subjects may rarely automatically access and rectify the data processed themselves).

Moreover, the survey shows that 66% of the EU institutions and bodies consulted have adopted procedures/mechanisms relating to the drafting of information notices.

Data subjects' rights for data subjects are applied, although some drawbacks remain

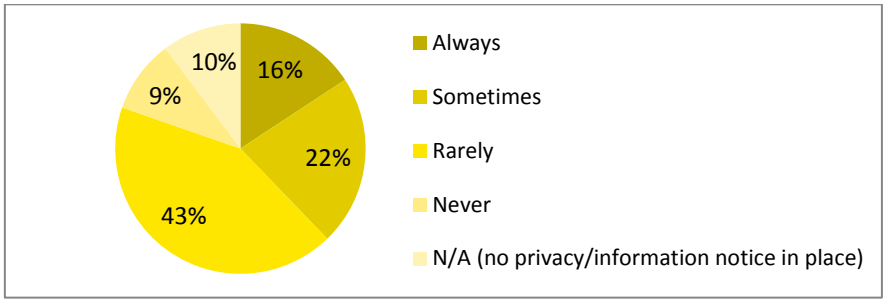
Generally speaking, the number of requests to exercise rights and related complaints received by EU institutions and bodies is low (most of the EU institutions and bodies consulted received fewer than 10 requests per year, if any). This could be linked either to a high level of protection and trust relating to the processing of personal data or to poor knowledge of data protection matters and in particular of the rights provided by Regulation (EC) No 45/2001.

It appears from the esurvey and the interviews performed with DPOs and data controllers that EU institutions and bodies usually respond without delay to requests from data subjects. Some criticism relating to the responses received have been raised by few data subjects interviewed.

Moreover, privacy statements are drawn up in order to inform data subjects on their rights and obligations. In this respect, information notices are usually drafted in the case of a new data processing operation. It should be underlined that these notices are rarely updated as only 16% of the data controllers consulted systematically update their privacy notices.

[5] 77% of the EU institutions and bodies consulted have developed specific procedures/mechanisms/processes or internal rules relating to data subjects' rights.

Figure 3 - How often do you update existing privacy/information notices to inform data subjects of their rights and the data processing operation as well as purposes? (Source: EY survey)



Concerns regarding practices arise from the difficulty in exercising rights in IT systems that existed prior to Regulation (EC) No 45/2001. For example, it may appear to be difficult to erase data from systems such as SYSPER.

When EU institutions and bodies are faced with requests from data subjects to exercise their rights, the following concerns arise, as expressed by the DPOs and IT officers surveyed and interviewed:

- At EU institutions and bodies, a majority of currently used IT systems have not been designed to automatically process data subjects' requests. Hence, manual operations are required to comply with data subject requests. For instance, when personal data are stored in a database, a database administrator needs to access the data and read, change or erase it.

  As for every manual operation on IT systems, this process could be costly while introducing risks of errors in data processing;
- IT systems' architectures are heterogeneous and several ways of managing data exist. For example, personal data can be used by several IT systems but stored in a single location or used by one system but stored in several locations. Therefore, if data erasure is necessary to comply with a data subject's request, this could have a significant impact on overall data consistency. Moreover, depending on the context, it may be difficult to identify all the locations where the data are stored.

The perception of stakeholders (notably the DPO network and the data controllers) is that the time spent on the drafting of privacy statements is excessive and that the new Regulation should rather focus on "real" compliance, meaning accountability and effective information.

In this respect, user-friendly information notices could enhance the effectiveness of rights. This is also in line with the principle of transparent information and communication enshrined in Article 11 of the proposed GDPR.

As regards the right of blocking, this right is effectively implemented and applied by EU institutions and bodies, although the DPO network has underlined that the provision should specify that blocking is a temporary measure or a measure undertaken when erasure is not possible. Moreover, it was underlined by stakeholders that this right is unpractical.

The right not to be subject to individual automated decisions is in practice rarely applied by EU institutions and bodies. This provision is nevertheless of particular importance in the context of the development of big data and profiling trends and has been reinforced by Article 20 of the proposed GDPR.
Article 19 of Regulation (EC) No 45/2001 addresses risky data processing operations and is fully

relevant for EU institutions and bodies. This provision should be supported by guidance to ensure that data controllers are aware of their obligations in this regard.

Conclusion and recommendations

The Regulation establishes appropriate rights for data subjects, although the right of blocking could be further specified in order to fully achieve the objective.

Raising awareness on data protection (notably the rights of data subjects) and better information could be foreseen in order to facilitate the implementation and application of data subjects' rights.

Even though means to enable data subjects to exercise their rights have been implemented, it appears that the number of requests and complaints remains low. Increasing awareness on data protection issues and better information on the rights enshrined in Regulation (EC) No 45/2001 could enhance the effectiveness of the rights.

- A user-friendly privacy statement, as well as further training on data protection issues, could be implemented in order to raise data subjects' awareness of their rights. Specific guidance on the provision related to the automated individual decision (Article 19) should be foreseen.
- The dissemination of a data protection culture within EU institutions and bodies through high-level management would significantly increase the enforcement of rights. The attachment of DPOs and DPCs to senior management could be a factor in promoting this goal.
- Old IT systems may hamper the capacity of the mechanisms in place to exercise rights as the exercise of rights may in certain circumstances require complex manual intervention. The architecture of such systems was designed before Regulation (EC) No 45/2001 existed and changes to that architecture would require significant budgetary efforts. On the other hand, new IT systems are usually designed to take data protection obligations into account in the light of the data protection by design principle.

3.2.2 The Regulation establishes obligations for data controllers

Regulation (EC) No 45/2001 effectively establishes obligations for the data controller relating to (1) the lawfulness of the processing of personal data and (2) to the security and confidentiality of the personal data processed.

Regulation (EC) No 45/2001 establishes obligations for data controllers pertaining to the lawfulness of the processing (including the processing of specific categories of personal data)

Regulatory Framework

Pursuant to Articles 4 and 5 of Regulation (EC) No 45/2001, the data controller must process personal data in accordance with the principles relating to the lawfulness of the processing. The lawfulness of the processing requires that the data controller verifies that the processing complies with the main data protection principles.

Obligation to ensure data quality

The data controller must:

- *"Process personal data fairly and lawfully;*
- *Collect personal data for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of personal data for historical, statistical or scientific purposes shall not be considered incompatible provided that the controller provides appropriate safeguards, in particular to ensure that the data are not processed for any other purposes or used in support of measures or decisions regarding any particular individual;*
- *Ensure that data are adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed and accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;*
- *Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."*

"Regarding the processing of personal data for historical, statistical or scientific use for longer periods, the data should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes."

Obligation to ensure the lawfulness of the processing

Article 5 of the Regulation lays down the grounds for the lawful processing of personal data.

Personal data shall be processed only pursuant to the following purposes in order to be legitimate:

- *if the processing is necessary for the performance of a task carried out in the public interest. This includes the processing "necessary for the performance of the management and functioning" of the institutions (Recital 27) (Article 5 (a)), or*
- *if the processing is necessary for compliance with a legal obligation(Article 5 (b)), or*

- *if the processing is necessary for the performance of a contract (to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract) (Article 5 (c)), or*
- *if the data subject has given his or her consent (Article 5 (d)), or*
- *if the processing is necessary in order to protect the vital interests of the data subject (Article 5 (e)).*

Implementation and Application
This obligation has been effectively implemented and applied within EU institutions and bodies.

Data quality and lawful processing

The data protection obligations relating to data quality and lawfulness of the processing provided for by the Regulation are largely implemented.

Implementation

Although procedures and internal rules pertaining to data protection principles are established in more than 69% of the EU institutions and bodies, these implementing processes could be further improved. Specific procedures and guidelines relating to data retention are also provided to data controllers within several EU institutions and bodies (77% of the data controllers consulted).

Stakeholders underlined that the procedures relating to data protection principles are not always suitable to meet operational needs and are deemed to be theoretical (rather than practical) (see figure 4). Therefore, there is a need to adopt simplified procedures targeting data controllers' concrete needs rather than publishing theoretical procedures relating to data protection procedures.

Application

Articles 4 and 5 of Regulation (EC) No 45/2001 are broadly applied by EU institutions and bodies although difficulties of interpretation and application should be underlined.

The main data protection principles enshrined in Article 4 of the Regulation are globally well understood by DPOs, although the principle relating to the "fair" processing of personal data needs further clarification or guidance as to its meaning.

Regarding the establishment of data protection retention periods, data controllers lack concrete guidance on what should be considered as reasonable periods. When a specific document relating to file retention periods has not been published, it appears that the data controller must refer to the periods laid down by specific legislation and to the opinions and guidelines of the EDPS. In this respect, data controllers emphasise that EDPS guidance is often general and does not reflect their operational challenges.

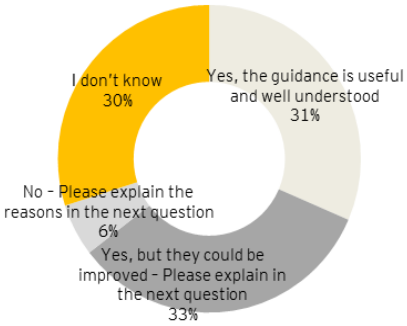
Difficulties relating to data retention periods are further addressed in the case study "Data retention in the HR context".

EU institutions and bodies may face difficulties in interpreting the provisions of Article 5, notably with regard to the assessment of the legal basis of the processing operations (Article 5 (b)).

In addition, the criteria pertaining to the lawfulness of the processing may appear unclear to DPOs and *a fortiori* to data controllers. The assessment of the lawfulness of the processing may be challenging in practice. The most commonly used criteria are those stated in 5a), 5b) and 5d). 5c) is of limited use for the EU institutions and bodies and 5e) is rarely used. Sometimes, two criteria are

used (e.g. consent and performance of tasks in the public interest). Only 31% of data controllers consider that the EDPS guidance is useful and well understood.

Figure 4 - Do you estimate that guidance (e.g. responses to questions, guidelines, opinions, etc.) provided by the EDPS is helpful? (Source: EY survey)



Consent is, in certain circumstances, used in cases where the EU institutions and bodies wish to use the photographs of officials, for example for communication purposes.

Data controllers are often not sufficiently aware of data protection requirements and obligations. They rely extensively on the DPOs in order to assess the legal feasibility of the data processing operation.

However, data controllers bear the responsibility of verifying that the contemplated data processing operations are compliant with the data protection principles related to the quality of data and the legitimacy of the processing. The analysis of the legal feasibility of the processing is often performed during the notification of the operations. Notification of processing operations obliges the data controllers to carry out an evaluation of the legal feasibility of the operation (or at least to inform the DPO). At the same time, notifications appear to be burdensome and bureaucratic and do not necessarily result in the correct application of data protection principles *(see below and efficiency analysis).* Please note that the obligation of the data controller to notify data processing operations is developed below (see evaluation of the effectiveness of the obligation to keep a DPO register).

The application of the rules relating to the processing of personal data for historical, statistical or scientific use have led to difficulties with respect to (i) the rules enshrined in the Archive Regulation (see evaluation question on coherence); (ii) to the need to anonymise or encrypt the personal data included in the document kept for historical purposes.

Change of purpose

The Regulation provides for derogation from the fundamental principle of purpose limitation.

Regulatory framework

Article 6 of Regulation (EC) No 45/2001 sets out an exception to the purpose limitation principle, as it provides that personal data may be processed for purposes other than those for which they have been collected **if the change of purpose is expressly permitted by the internal rules of the EU institution or body.**

In addition, this provision specifies that "**personal data collected exclusively for ensuring the security or the control of the processing systems or operations shall not be used for any other**

purpose, with the exception of the prevention, investigation, detection and prosecution of serious criminal offences" (Article 6.2.).

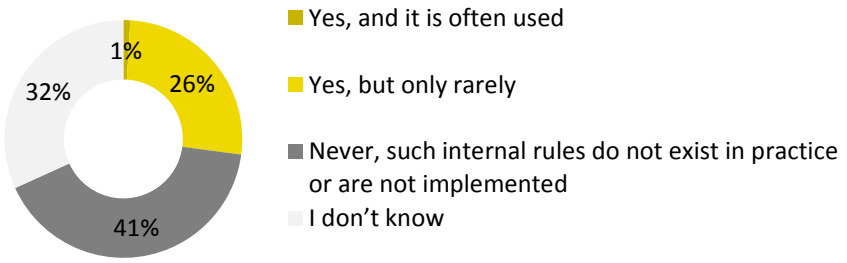
Implementation and Application

The rules relating to the change of purpose of the data collected are not effectively implemented and applied, as the wording is unclear and deter EU institutions and bodies from applying the provision.

It seems that the provision relating to change of purpose is implemented in certain EU institutions and bodies but is rarely used. In the event of change of purpose, the register and the privacy notices are updated.

However, several stakeholders find it difficult to interpret this provision, notably because the provision does not specify what can be considered as an "internal rule" within the meaning of the Regulation. In this regard, the Civil Service Tribunal seems to consider that these rules should be written and that a mere practice adopted by an institution is not sufficient.[6]This considerable room for *manoeuvre* by EU institutions and bodies could be problematic and raises interpretation concerns among EU institutions and bodies as to what is meant by internal rules.

Figure 5 –In principle, personal data must only be collected and processed for specified, explicit and legitimate purposes. Nevertheless, internal rules adopted by an EU institution or body may change the initial purpose for which data were collected. Is this possibility used within your institution/body? (Source: EY survey)



The EDPS is sometimes consulted with regard to the use of the change of purpose provision. For example, according to the EDPS 2013 Annual Report, an EU body consulted the EDPS on the legality of using personal data collected from an access security or time management system in order to instruct a disciplinary procedure in an investigation.[7]

The EDPS underlines the necessity of interpreting the change of purpose provision strictly and respecting the proportionality and necessity principles when applying it. Thus, the EDPS' interpretation is to consider that the change of purpose provision solely applies to secondary purposes and that the adoption of internal rules is an additional safeguard in order to ensure compliance with the purpose limitation principle.

According to the evaluator, the relevance of this provision could be challenged as it questions one of the core principles of data protection (purpose limitation). In the absence of appropriate guidance pertaining to these internal rules, the application of the provision is merely arbitrary.

[6]J UDGMENT OF THE EUROPEAN UNION CIVIL SERVICE TRIBUNAL (First Chamber), 5 July 2011 Paragraph 119.
[7] See 2013 Annual Report, page 39.

Prohibition to process sensitive data unless in predefined cases

Regulatory framework

According to Article 10 of Regulation (EC) No 45/2001, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life is prohibited except in certain specific circumstances.

These predefined situations are the following:

- processing for which the data subject has given his or her consent (Article 10. 2 a);
- processing for the purpose of complying with employment law (Article 10. 2 b);
- processing in order to protect vital interests (Article 10.2 c)
- processing of data manifestly made public by the data subject or necessary for the establishment, exercise or defense of legal claims (Article 10.2 d)
- processing by a non-profit-seeking body (in specific circumstances detailed by Article 10.2 e)
- processing for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services by medical professionals (Article 10.3).

Additional exemptions for substantial public interest may be laid down by the Treaties and the EDPS, subject to additional safeguards (Article 10.4).

In addition, processing of data relating to offences, criminal convictions or security measures may only be carried out if authorised by the Treaties or the EDPS (Article 10.5).

The EDPS must determine the conditions under which a personal number or other identifier of general application may be processed by EU institutions and bodies (Article 10.6).

Article 10 should be read in the light of Article 27 that lays down the processing operations likely to present significant risk with respect to the rights and freedoms of data subjects that are submitted to prior checking by the EDPS.

Implementation and Application

Implementation

Processes/procedures/internal rules relating to the processing of special categories of data have been implemented in half of the EU institutions and bodies consulted.

It appears that the processes/procedures/internal rules relating to the processing of sensitive data are usually linked to the rules governing the processing operations subject to prior checking. In this regard, it is worth mentioning that 74% of the EU institutions and bodies consulted have implemented prior check processes/procedures/internal rules. Nevertheless, the conditions governing the processing of sensitive data cannot be reduced to the performance of prior checking by the EDPS as (i) the scope of prior checking does not encompass all processing operations relating to sensitive data, (ii) the processing of sensitive data includes other requirements in addition to prior checking.

This provision needs to be implemented according to dedicated rules to cover all types of processing of special categories of data which cannot be comprehensively covered by prior checking rules.

Article 10.6 states that the EDPS *"shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body."* It appears that the EDPS has not issued guidelines on these conditions and generally approves the use of these personal data in its prior checking opinions.[8] In this regard, the EDPS considers that the use of an identification number in a selection/recruitment procedure is reasonable "insofar as it facilitates the identification of the applicant during the recruitment procedure."

We are not aware of any specific guideline provided by the EDPS "determining the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body."

Application

Stakeholders consulted have not raised any major difficulties pertaining to the application of the rules enshrined in Article 10. Some interpretation issues have nonetheless been identified.
Article 10.2.e) raises interpretation issues relating to the meaning of *"a non-profit-seeking body which constitutes an entity integrated in a Community institution or body, not subject to national data protection law by virtue of Article 4 of Directive 95/46/EC, and with a political, philosophical, religious or trade-union aim"* and whether this provision applies to trade unions within theEU institutional framework.

The Court of Justice has ruled that the derogation provided by Article 10.3 relating to the processing of personal data for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services by medical professionals cannot serve as the legal basis for the transfer of health data between EU institutions in the context of recruitment.[9]

Conclusion and proposed recommendations

- **The Regulation establishes adequate obligations for data controllers and safeguards relating to the processing of special categories of personal data.**
- **The fact that stakeholders have not raised concerns about the application of Article 10 could be an indicator that this provision is not fully or really understood/known by DPOs and data controllers. It is necessary to ensure that DPOs and data controllers are aware of the conditions pertaining to the processing of special data.**
- **The data protection obligations are reasonably implemented across EU institutions and bodies. In any case, making use of concrete and simplified procedures pertaining to these principles would significantly increase the effectiveness of the processing obligations.** Stakeholders have emphasised the need for simplified data protection procedures that fit the day-to-day needs. EDPS guidance should also follow this path (in particular regarding the conservation of personal data). Guidance relating to the processing of specific categories of personal data should be drawn up. Moreover, EU institutions that have issued guidelines on the data protection obligations should make them available to other EU bodies. This is particularly relevant for agencies or institutions with part-time DPOs that lack resources dedicated to data protection.

[8] *"Evaluation of Regulation 45/2001: Contribution of the DPO"*.
[9] Civil Service Tribunal, 5 July 2011, F-46/09.

- **The change of purpose provision should be clarified or deleted from Regulation (EC) No 45/2001 (see *relevance)* because (i) deviation from the purpose limitation principle is not supported by any legitimate grounds, (ii) the provision generates legal uncertainty.**

Obligations pertaining to the implementation of security and confidentiality measures

The Regulation provides for the obligation of the controller to implement the appropriate technical and organizational measures in order to ensure the security of the personal data processed.

Regulatory framework

Article 22 of the Regulation provides for the obligation of data controllers to properly manage security risks related to personal data processing. The data controller is responsible for designing, implementing and maintaining the appropriate technical and organisational measures to ensure the security of personal data processing activities. These measures aim in particular to prevent "any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing."

Furthermore, the article enumerates a non-exhaustive list of control objectives that must be implemented, as appropriate, whenever personal data are processed by automated means in order to ensure an appropriate level of security (Article 22.2). This list is consistent and covers the main control objectives the implementation of which contributes to the cover of most security risks related to the processing of personal data. Nonetheless, this list should not be considered sufficient. The specific features of each data processing operation and the systems used must be taken into account to define the appropriate controls necessary to ensure the cover of all security risks.

Implementation

Article 22 of the Regulation is implemented across EU institutions and bodies. Nonetheless, the level of implementation of this article remains heterogeneous and not all EU bodies have implemented it effectively.

The implementation of Article 22 requires EU institutions and bodies to design, implement and maintain appropriate policies, procedures and systems to manage risks for all processes involving personal data in order to ensure that the requirements are met.

Based on the interviews conducted with data protection officers and the IT officers' answers to the survey, a large majority of EU institutions and bodies implements Article 22 of the Regulation. The internal processes and procedures of such entities incorporate the requirements laid down by Article 22. Procedures and methodologies detailing how risk assessment, mitigation and monitoring should be performed are available for the staff of these entities.

However, a thorough analysis of the survey's results brings to light two main observations:

- Levels of implementation of Article 22 vary among EU bodies. Half of IT officers surveyed have described the implementation of this article as insufficient within their entity. The security requirements are partially incorporated into internal processes. Risk assessment procedures and frameworks are loosely defined and formalised. Few methodologies and guidelines are available to support such entities' staff in conducting effective risk assessments and implementing appropriate security measures.

The other half of IT officers surveyed have described the implementation of Article 22 as good to very good. Formalised internal procedures, frameworks and methodologies incorporating risk assessment principals are available to support IT officers in appropriately assessing and mitigating risks related to personal data processing.

No specific pattern, explaining the observed distribution of EU entities, can be highlighted. Nonetheless, certain factors can explain the effectiveness of the implementation of Article 22 in some entities. Indeed, EU institutions and bodies acting as regulation authorities or those operating in a highly regulated context have effectively implemented the Regulation. For example, the EDPS, which works directly on data protection issues, the European Central Bank, which is in charge of banking ecosystem regulations, and EU LISA, which operates large-scale and security-sensitive IT systems, appear to have correctly implemented the Regulation.

- The perceived level of implementation of Article 22 can vary across the units and divisions and among the personnel within an EU institution or body. Data protection officers, management staff and IT officers of the same EU entities have answered the survey in contradictory ways. In addition, in some cases personnel sharing the same role within the same institution perceive the level of implementation of Article 22 differently.

Application

Article 22 of the Regulation is insufficiently applied across EU institution and bodies.

The application of Article 22 requires EU institutions and bodies to actually include risk assessment, mitigation and monitoring principles in all processes involving personal data. Therefore, all IT processes and projects should include risk assessment. The security measures mitigating the identified risks must also be implemented and the identified risks continuously monitored.

Information security has four main aspects which are availability, confidentiality, integrity and accountability. When processing personal data, EU entities are exposed to risks that could affect one or more aspects of personal data security. Therefore, all four aspects should be considered when identifying and analysing security risks.

The interviews conducted with the EDPS, data protection officers and IT security officers have emphasised the low level of maturity of EU institutions and bodies in terms of the application of Article 22. In the majority of EU entities, risk management is rarely performed and few measures mitigating identified security and data privacy risks are actually implemented. This finding is borne out by the answers given by the staff of EU entities in response to the survey.

Two major trends arise regarding the application of Article 22. Based on the interviews conducted with data protection officers and the answers to the survey, only a third of EU institutions and bodies conduct risk assessments and privacy assessments on most of personal data processing.

In such entities, several risk assessments have been carried out. The scope of these risk assessments covers most of the personal data processing activities and underlying information systems. For each personal data processing operation, these entities identify and analyse the associated security risks before implementing mitigation measures, both technical and organisational, in order to reduce the risk exposure and ensure the security of personal data processing. Continuous monitoring and reporting is also in place in order to ensure the appropriate continuous management of these risks.

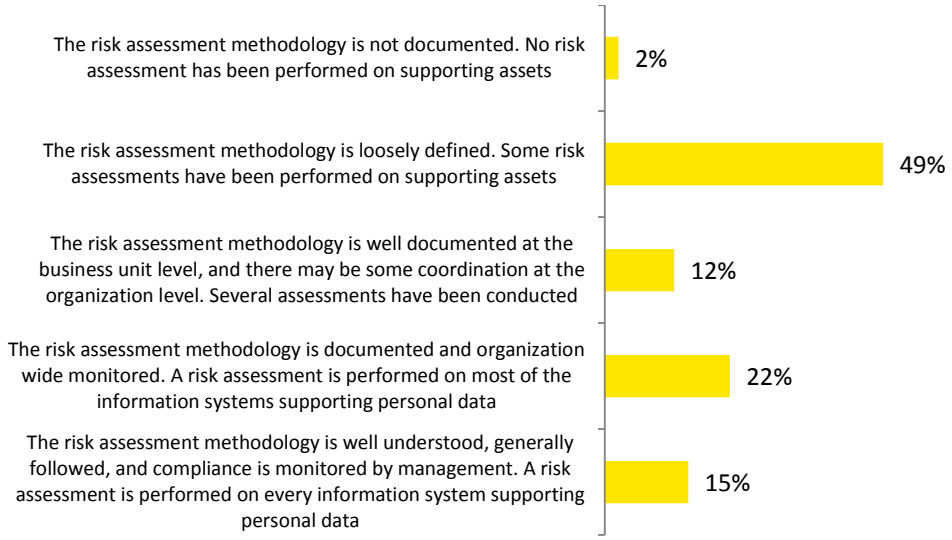
Logical access controls and network restrictions are among security measures that have been implemented according to data protection officers interviewed.

It should also be noted that where personal data processing operations are likely to raise significant risks, certain EU institutions and bodies may use anonymisation or pseudonymisation mechanisms to mitigate the identified risks.

The survey conducted highlighted that among respondent EU entities, few have formally defined a process for data anonymisation and/or pseudonymisation. Nonetheless, ad hoc processes are largely used for data anonymisation or limited data anonymisation is performed.

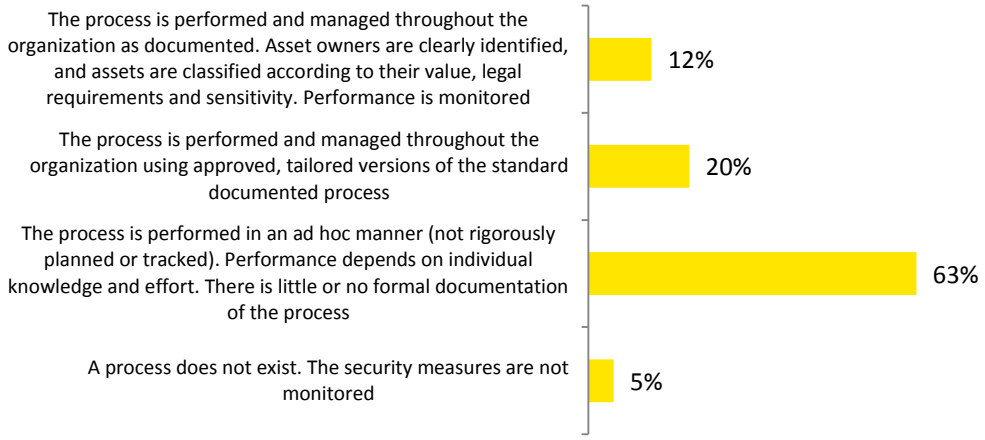
Furthermore, some of these entities carry out regular risk assessments in order to accommodate new potential threats and monitor the efficiency of the measures implemented.

Figure 6 - Is a risk assessment methodology defined and performed on the information systems supporting personal data? (source: EY survey)



On the other hand, two thirds of 20 EU institutions and bodies consulted (on IT aspects) are insufficiently applying Article 22 of the Regulation. Few risk assessments have been performed and not all data processing activities and assets have been addressed. In addition, when risk assessments are carried out, they seem to be performed in an ad hoc manner. They are not rigorously planned or tracked. The performance of these risk assessments is therefore not homogeneous and mostly depends on the individual knowledge and effort of the personnel involved.

Figure 7 - After having performed a risk assessment analysis on the information systems supporting personal data, IT security measures could be defined to mitigate the risks identified. Are there any processes in place to monitor the efficiency of these measures? (Source: EY survey)



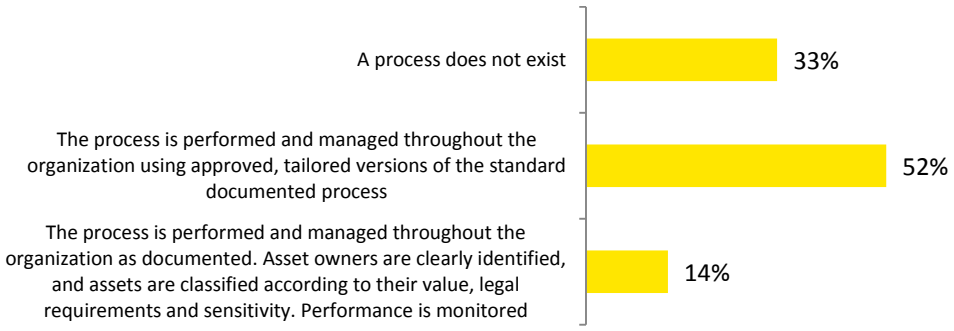
The interviews conducted have highlighted a lack of awareness and willingness from project managers who consider data privacy and security as a constraint bringing few gains to projects while costing more. Therefore, the latter are reluctant to conduct risk and privacy impact assessments.

The lack of formalised procedures and methodologies and coordination at the organisational level in some entities can also explain the insufficient application of Article 22 of the Regulation.

As a supervisory body, the EDPS plays a key role in enforcing the implementation of this article.

The EDPS is in charge of enforcing the implementation and application of Regulation (EC) No 45/2001 and therefore of Article 22. In this regard, the EDPS IT policy unit regularly conducts technical security inspections (see below on the assessment of inspections conducted by the EDPS).The IT policy unit may intervene when appropriate. These inspections are led by the IT policy unit's staff and aim to identify gaps between what is implemented and applied and the current Regulation. According to DPOs and IT officers interviewed, several IT security incidents have been registered across EU institutions and bodies in recent years. Nonetheless, very few cases of data breach incidents, putting at personal data significant risk, have been recorded. According to IT officers surveyed, a process for the notification of data breach incidents to the DPO is available to IT staff, although it is insufficiently formalised and not systematically followed.

Figure 8 – If another institution or body acts as data processor, is there a process in place ensuring that the services comply with the data protection legal requirements (ensuring that the service provider acts only on instructions from the controller)? (Source: EY survey)



Nevertheless, it appears that the wording of Article 22 is often misunderstood by EU institutions and bodies. This provision encompasses a check list of control objectives and an obligation to design, implement and maintain risk management policies, procedures and systems on the basis of the state of art (Article 22.1). This Article states the need to properly manage IT risks and implement a comprehensive information security management system.

Many EU institutions and bodies have not fully grasped the meaning of the first paragraph of Article 22. The "risk-based approach" is often left out of the risk analysis conducted by EU institutions and bodies. Only confidentiality, integrity and availability are generally covered by currently implemented risk management processes.

In addition, the second paragraph of the Article is sometimes interpreted by EU institutions and bodies as being an exhaustive list of measures to comply with, which it is not.

Conclusion and proposed recommendations

Article 22 of Regulation (EC) 45/2001 is largely implemented but insufficiently applied by EU institutions and bodies.

Only a third of the 20 EU bodies consulted (IT officers) have effectively implemented and applied the security management set out by Article 22. The remaining entities have insufficiently and partially implemented and applied the Regulation.

- **Awareness raising is essential in order to increase the level of implementation of Article 22 within EU institutions and bodies.**

In order to effectively raise the level of implementation and application of Article 22, the DPOs of EU institutions and bodies, Local Information Security Officers and the EDPS should collaborate and organise regular workshops on data privacy and security issues to raise the level of awareness of staff involved in the processing of personal data.

Previous similar initiatives by DPOs have not fully reached the expected objectives, according to the feedback received. Attendance at these workshops was not mandatory and very few people attended. Therefore, we would recommend organising small-sized workshops and training sessions, but with mandatory presence.

- **Furthermore, regular inspections by the EDPS should be carried out in order to raise awareness on compliance.**
- Although the main principles of Article 22 are well understood, some misinterpretations still remain and prevent EU institutions and bodies from effectively assessing risks associated with personal data processing. Guidance from the EDPS or the EU institutions

and bodies could be helpful in order to highlight the necessity of implementing a risk management approach in accordance with Article 22.

The Regulation establishes an obligation to implement confidentiality and security measures as regards relationships with data processors.

Regulatory framework

Pursuant to Article 21 of Regulation (EC) No 45/2001, *"a person employed with a Community institution or body and any Community institution or body itself acting as processor"* must only process personal data under the instructions of the data controller (unless required to do so by national or community law).

Article 23 relates to the requirements pertaining to the data processing operations carried out by data processors. This provision states that in the event of personal data processing on behalf of the controller, EU institutions and bodies must ensure:

- that the data processor selected provides sufficient guarantees in respect of the technical and organisational security measures required by Article 22 and ensure compliance with those measures.
- the establishment of a contract or legal act binding the processor to the controller that must expressly stipulate in particular that:
  - The processor shall act only on instructions from the controller;
  - The obligations set out in Articles 21 and 22 shall also be incumbent on the processor unless the processor is already subject to obligations with regard to confidentiality and security laid down in the national law of one of the Member States.

Implementation and application

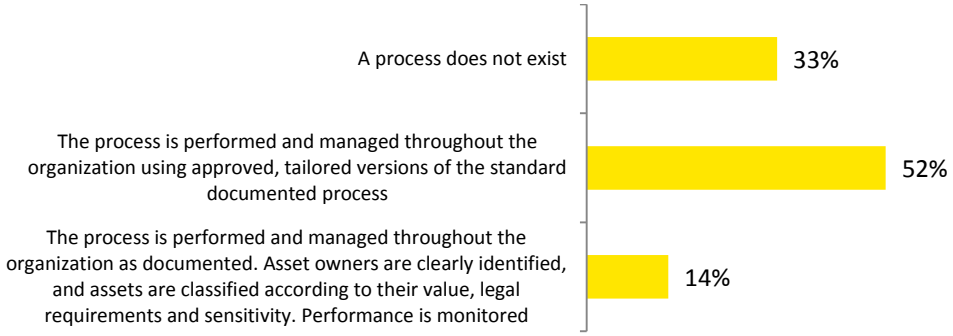
Articles 21 and Article 23 are effectively implemented and applied by EU institutions and bodies.

Based on the interviews conducted and the DPOs' answers to the survey, the requirements laid down by Articles 21 and 23 are effectively implemented by the majority of EU institutions and bodies.[10] The Regulation has been effectively translated into processes and procedures. These processes and procedures serve as guidance for entities' staff whenever personal data has to be processed on behalf of the controller.

The results of the consultation of the IT officers are in line with the above, insofar as they highlight the fact that a third of EU institutions and bodies seem not to have implemented the requirements laid down by Article 23 regarding specific procedures/processes.

[10] 69% of the EU institutions and bodies consulted have implemented processes/procedures/internal rules on security and confidentiality measures.

Figure 9 - Are you aware of the existence of processes ensuring that service providers comply with the regulation? (Source: EY survey)



Furthermore, it should be underlined that in the last bi-annual survey[11] conducted by the EDPS, the supervisor assessed the standard contractual clauses used by EU institutions that outsource to external processors. The General Report indicates that "a number of EU institutions are using the template clause elaborated by the Directorate-General for the Budget (DG Budget) of the Commission", which follows the prescriptions of Articles 22 and 23 of Regulation (EC) No 45/2001. The report contains additional guidance for data controllers outsourcing to external service providers (notably with regard to the necessity to avoid confusion between the contractor's obligations and the controller's obligations when processing the contractor's data and to avoid sub processing).

Some EU bodies have also adopted specific data protection clauses that are used in complex areas "where the standard clause was not deemed sufficient in relation to the activity envisaged."[12]

Application

The wording of Article 21 raises interpretation issues and is not adequate to address confidentiality matters.

- The wording of Article 21 targets only internal data processors who act under the instructions of data controllers, and not external data processors. The scope of this article should be broadened to include data processing operations carried out by external service providers.
- Moreover, this provision could be interpreted as stating that any person employed within an EU institution or body who processes personal data under the instruction of a data controller could be considered to be a data processor. This would mean that an official acting under the instruction of his head of unit would be considered to be a data processor. Should an official acting on the instruction of the data controller be considered to be data processor, the provisions of Article 23 would be applicable to that official and the provisions of Article 22 would have to be included in a written binding document. Moreover, this could also be considered as a transfer of personal data pursuant to Article 7.
- This provision also highlights consistency issues within the provisions of Regulation (EC) N° 45/2001. Indeed, the definition of a controller is unclear and inconsistent throughout the Regulation. In Article 2. (d), it seems that a controller is the institution /body or the unit/service/directorate within the EU institution or body. However, in Article 25, the name and address of the controller effectively indicated in the register are the details of the natural person responsible for the processing operation.

[11] EDPS, Measuring compliance with Regulation (EC) 45/2001in EU institutions ("Survey 2013"), General Report, page 14.
[12] *ibidem*

Article 23 is effectively applied by a large majority of EU institutions and bodies that use standard contractual clauses to enter into agreements with data processors.

The relationships between data controllers and data processors are governed by contracts and service level agreements (SLAs) ensuring that security and confidentiality requirements are met.

- Service level agreements and contracts binding service providers and controllers ensure the proper application of the Regulation.
- Most EU entities and bodies use standard EU confidentiality and security clauses when entering into agreements with external data processors. This is a strong indicator that Article 23 is effectively applied. Standard clauses relating to SLAs should also be encouraged.

Figure 10 - Has your institution or body adopted standard security and confidentiality clauses, specific to the processing of personal data by controllers or processors? (Source: EY survey)

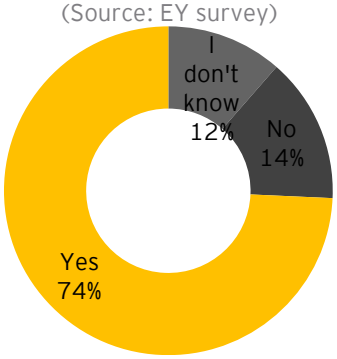
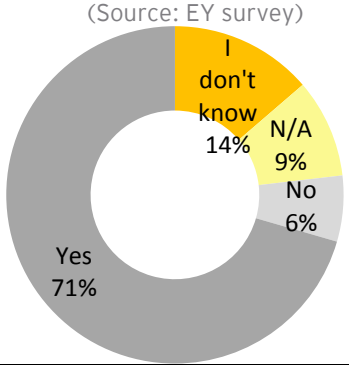


Figure 11 - If yes, are those standard clauses used in your institution or body when entering into an agreement with a data processor? (Source: EY survey)



Conclusion and proposed recommendations

The wording of Article 21 lacks of clarity as this provision could be interpreted as stating that any person employed within an EU institution or body who processes personal data under the instruction of the data controller could be considered to be a data processor. Moreover, the scope of the provision only targets internal data processors and should therefore be extended to external data processors.

The current level of implementation appears satisfactory, as in a majority of EU institutions and bodies standard confidentiality and security clauses are used.

<u>The following improvements should therefore be made:</u>

- **Clarify the wording of Article 21 in order to avoid any inconsistencies; it is recommended to broaden its scope of application[13];**
- **Ensure the broad circulation of the template clause of the DG Budget (European Commission) and other template clauses to be incorporated within SLAs.**

[13] Further clarification of the definitions of the controller and processor within the meaning of Article 2 of the Regulation is necessary (see Article-by-Article Analysis).

Obligations to collaborate with the EDPS

Regulatory Framework

Articles 29, 30 and 31 of Regulation (EC) No 45/2001 provide for the obligations of the controller (i) to provide information to the EDPS in the cases provided by Article 46(h) (e.g. in the context of authorizations and exemptions) and (ii) to cooperate and to react to allegations by the EDPS in the course of investigations.

Implementation and Applications

The evaluator is not aware of specific procedures/processes/internal rules pertaining to these specific obligations.

These obligations are applied by a large majority of EU institutions and bodies consulted.

EU institutions and bodies are cooperative and reactive in the course of investigations by the EDPS (see below). In this regard, the DPOs play a key role in the preparation of the investigations.

It appears that in some EU institutions and bodies (in particular, in the case of recently created agencies), DPOs are likely to carry out these obligations instead of the data controller.

Moreover, in the interviews with the EDPS, it was pointed out that in certain EU institutions and bodies there were delays in responding to the EDPS. Furthermore, it was underlined that the DPO is not systematically informed of the exchange of information between the EDPS and the data controller.

Conclusion and proposed recommendations

These obligations are applied by a majority of EU institutions and bodies. Current practices show that these obligations are not systematically carried out by data controllers who rely significantly on the DPOs. Some delays in responding to the EDPS have also been noted.

3.2.3 The Regulation establishes appropriate sanctions for offenders and remedies for data subjects

The Regulation establishes appropriate sanctions for offenders

Regulatory framework

In accordance with Recital 2, the protection of personal data requires that the Regulation establishes appropriate sanctions for offenders and a supervisor in order to monitor the application of the Regulation.

Pursuant to Article 49, an EU official or servant may be liable for disciplinary proceedings in accordance with the rules laid down by the Staff Regulation[14] or in the conditions of employment applicable to other servants in case of negligence or intentional failure to comply with the obligations laid down by the Regulation.

The Regulation does not empower DPOs to impose sanctions on data controllers.

Article 47 of the Regulation sets out the powers of supervision of the EDPS. The following sanctions/enforcement actions may be imposed by the EDPS: (i) warn or admonish the controller (Article 47 (d)), (ii) impose a temporary or definitive ban on processing (Article 47 (f)), (iii) refer the matter to the Community institution or body concerned and, if necessary, to the European Parliament, the Council and the Commission (Article 47 (g)), (iv) refer the matter to the Court of Justice of the European Union (Article 47 (h)), (v) intervene in actions brought before the Court of Justice of the European Union (Article 47 (i)).

Implementation and Application

The evaluator is not aware of any implementing rules on sanctions.

The sanctioning powers of the EDPS are not sufficiently applied.

Regarding the range of powers conferred by Regulation (EC) No 45/2001 upon the EDPS, the latter considers that its supervisory powers are extensive. On the basis of the interviews with the EDPS, the latter may advise data subjects in the exercise of their rights (Article 47 (a)). As a first step, the EDPS will refer the matter to the data controller (Article 47 (b)) and will check whether the request has first been submitted to the DPO. Article 47 (c) and (e) are the most commonly used powers. Moreover, the EDPS has intervened in several cases before the Court of Justice (see below).

However, the EDPS has rarely used its power to warn or admonish the data controller. The EDPS **has only banned processing operations in limited cases.**[15] The powers under Article 47 (g) and Article 47 (h) have never been used either.

In this regard, it is important to underline that the EDPS considers that the **data controller is the institution or the body and not the individual in charge of the processing.**

The EDPS highlighted that the mere existence of these powers is dissuasive without the need to actually use them. The powers are not used but are, according to the EDPS, very effective. The

[14] Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community (OJ 45 of the 14.6.1962, p. 1385) as lastly amended by Regulation (EU, Euratom) No. 1023/2013 of the European Parliament and of the Council of 22 October 2013 (OJ L 287 of the 29.10.2013, p. 15).

[15] The EDPS has, in the course of prior checking, prohibited processing operations.

perception of DPOs varies substantially insofar as several DPOs consider that the ineffectiveness of the sanctions results in a low level of enforcement of the Regulation provisions by the management.

The power to impose sanctions upon EU institutions and bodies is not effectively applied by the EDPS (see relevance for the appropriateness of the powers granted to the EDPS).

Moreover, stakeholders have the perception that the sanctions are not effectively applied and that they are not dissuasive. Data controllers within EU institutions and bodies are not sanctioned.

The appropriateness of the range of powers of the EDPS is further developed in the case study relating to the supervisory and advisory powers of the EDPS and the evaluation of the relevance of the sanctions.

Nevertheless, the Court of Justice of the European Union has effectively sanctioned an EU institution for a data protection violation.[16]

The argument pertaining to the infringement of the provisions of Regulation (EC) No 45/2001 has been brought in several cases before the Court of Justice.[17] For example, the unlawful disclosure of the name of an official subject to disciplinary proceedings by the European Commission is an infringement of the provisions of Regulation (EC) No 45/2001.[18]

Sanctions against offenders are rarely applied by EU institutions and bodies on the basis of the Staff Regulation or the conditions of employment applicable to other servants.

Disciplinary proceedings resulting from negligence or an intentional failure to comply with the obligations of Regulation (EC) No 45/2001 are almost never initiated. 94% of stakeholders indicated that they are not aware of any disciplinary actions undertaken for data protection breaches. The remaining 6% of stakeholders stated that they were aware of three sanctions within the European Commission in the last ten years.

Conclusions

- The EDPS does not apply its enforcement powers even though the appropriateness of the powers is not questioned by the stakeholders.
- Offenders are never (or extremely rarely) sanctioned for failure to comply with the rules enshrined in the Regulation. As a result, this reduces the incentive for controllers to comply with the provisions of the Regulation and substantially hinders its enforcement.
- The enforcement of the Regulation provisions relating to sanctions must be enhanced.

The Regulation provides for adequate remedies for data subjects

Regulatory framework

Pursuant to Article 32, any individual may lodge a complaint with the EDPS if the data subject considers that his or her right has been infringed as a result of the breach of personal data by an EU institution or body. This provision adds that "in the absence of a response by the EDPS within six months, the complaint shall be deemed to have been rejected."

[16] Judgment of the Civil Service Tribunal (First Chamber) of 5 July 2011.V v European Parliament. Public service. Case F-46/09; Judgment of the Civil Service Tribunal of 11 May 2010, Case F-30/08.
[17] See for example, Case F-130/07.
[18] Judgment of the Civil Service Tribunal of 11 May 2010, Case F-30/08 (paragraph 171).

The EDPS was entrusted with the following powers of remedy enshrined in Article 47:

- "(b) refer the matter to the controller in the event of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;
- (e) order the rectification, blocking, erasure or destruction of all data when they have been processed in breach of the provisions governing the processing of personal data and the notification of such actions to third parties to whom the data have been disclosed;
- (g) refer the matter to the Community institution or body concerned and, if necessary, to the European Parliament, the Council and the Commission;
- (h) refer the matter to the Court of Justice of the European Communities under the conditions provided for in the Treaty."

Individuals may also obtain judicial remedies, and actions against the decisions of the EDPS may be brought before the Court of Justice of the European Union.

The Court of Justice of the European Union has jurisdiction to hear claims for damages and may order an EU institution or body to pay damages. In this regard, arguments pertaining to the protection of personal data are often used by applicants to serve other interests.

Recital 31 specifies that "liability arising from any breach of this Regulation is governed by the second paragraph of Article 288 of the Treaty." Pursuant to the second paragraph of Article 340 of the TFUE (ex-Article 288 TEC), "in the case of non-contractual liability, the Union shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its institutions or by its servants in the performance of their duties." This principle is recalled in the fourth paragraph of Article 32.

Pursuant to Article 33, any EU staff member may lodge a complaint with the EDPS regarding an alleged breach of the provisions of this Regulation governing the processing of personal data, without acting through official channels. No prejudice may be suffered as a result of the complaint.

The EDPS makes the distinction between complaints lodged by individuals (Article 32) and complaints by EU staff (Article 33). While any individual may complain to the EDPS about an alleged violation of his or her rights to the protection of his or her personal data, it should be underlined that EU staff may complain about any alleged violation of data protection rules, whether he or she is directly affected or not.

Implementation and Application

Regulation (EC) No 45/2001 provides for remedies for individuals and staff members.

Pursuant to Article 46 of Regulation (EC) No 45/2001, the EDPS has the duty to hear and investigate complaints; this obligation is effectively implemented and applied *(see evaluation of supervisory power of the EDPS).*

Even if DPOs do not have the power to impose sanctions on data controllers (such as the power to ban a data processing operation), they are responsible for ensuring the internal application of the provisions of the Regulation. Therefore, DPOs may hear and investigate complaints. In practice, DPOs refer the matter to the controller who must remedy the breach.

The number of complaints made to DPOs and the EDPS is not significant and could indicate a lack of awareness on data protection. In 58% of the EU institutions and bodies, no personal data breach has

been reported and in 48% less than 10 data breaches have been identified. Only 2% of the EU institutions and bodies consulted have more than 10 reports of personal data incidents per year.

Feedback from data subjects indicates that the data controller does not always reply to their complaints.

Furthermore, the Court of Justice has effectively ordered an EU institution to pay damages to an individual whose medical data have been disclosed to the European Parliament (case V v Parliament (Case F-46/09) where the Parliament was ordered to pay to the applicant the sum of EUR 25,000, including any interest, for the material and non-material damage suffered.). The Civil Service Tribunal underlines that *"In accordance with settled case-law, the administration can be held liable in damages only if a number of conditions are satisfied: the illegality of the allegedly wrongful act committed by the institutions, actual harm suffered, and the existence of a causal link between the act and the damage alleged to have been suffered (judgments of 1 June 1994 in Case C-136/92 P Commission v Brazzelli Lualdi and Others, paragraph 42, and of 21 February 2008 in Case C-348/06 P Commission v Girardot, paragraph 52). Those three conditions are cumulative. The absence of any one of them is sufficient for the claim for damages to be dismissed."*

Conclusion and Recommendations

- Regulation (EC) No 45/2001 establishes adequate remedies for data subjects (including staff members). However, in practice the perception of data subjects on the one hand, and data controllers and DPOs on the other, on the processing of their complaints and the resulting remedies may vary. It should also be noted that the violation of data protection rules may be argued in order to serve interests other than the protection of personal data.
- There are several cases where an individual has obtained damages from an EU institution or body before the Court of Justice.

3.2.4 The Regulation ensures the consistent and homogeneous application of the data protection rules and principles

Regulatory framework

Pursuant to Recital 12, the Regulation ensures the "consistent and homogenous application" of the rules and principles with the regard to the protection of personal data throughout the EU institutions and bodies.

The coherence and the consistency of the data protection system are ensured by the appointment of the EDPS and the DPOs within each of the EU institutions and bodies.

In accordance with Recital 32 and Article 24. 1 (c), DPOs should ensure that the provisions of the Regulation are applied and advise controllers on fulfilling their obligations. In addition, DPOs must ensure that data subjects and controllers are informed of their rights and obligations.

Pursuant to Article 46 (c), the EDPS has the duty to ensure the application of Regulation (EC) No 45/2001 and any other community act relating to personal data.

Implementation and Application

Over time, coherence and consistency tools have been implemented by EU institutions and bodies. These are efficient tools ensuring the consistency and coherence of the application of the rules and principles.

The EDPS ensures the consistent application of the data protection rules, even though some improvements could be made.

Please also refer to the assessment of Articles 24 and 46 in the evaluation of the governance system of Regulation (EC) No 45/2001.

Through the development of guidance, the EDPS has ensured that all DPOs have access to the same level of information on data protection matters.

The EDPS has developed thematic guidelines in order to advise EU institutions and bodies and ensure the proper application of the data protection rules and principles.[19] For example, the EDPS has issued guidelines on "Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8)". This allows for considerable coherence in the way the DPOs perform their tasks. The guidelines are made available to the DPOs on the "DPO corner". Moreover, the EDPS provides guidance with regard to the application of the rules in its opinions (prior checking and consultation in the course of the legislative process) and advises EU institutions and bodies (notably thanks to the setting-up of the hotline).

The annual report published by the EDPS is also an important source of guidance for EU institutions and bodies.

Furthermore, the bi-annual surveys conducted by the EDPS enable the comparison of the level of implementation of the data protection rules throughout EU institutions and bodies. By comparing EU bodies, the EDPS provides guidance on the application of the rules. For example, in the last

[19] See for example Guidelines on Public Procurement, Grants and External Experts.

General Report[20], the EDPS compared the practices of EU institutions and bodies with regard to contractual clauses included in agreements entered into with data processors.

The EDPS has also organised training sessions and workshops for controllers, DPOs and data protection coordinators (DPCs), such as basic training for new DPOs on the prior checking procedure, special training for certain DPOs, and workshops for controllers.[21]

Nevertheless, stakeholders have highlighted two drawbacks:

- **Inadequacy of certain procedures:** the guidelines are not always suited to the performance of the day-to-day activities of EU institutions and bodies.
- **Timing:** the process of adopting guidelines is too lengthy and hinders the consistent application of the data protection rules and principles, especially with regard to the evolving technological environment (e.g. the need to be provided with guidelines in the context of cloud computing was underlined).

Finally, it should be stressed that the EDPS does not supervise EU bodies in the area of Police and Judicial Cooperation in Criminal Matters. Indeed, Regulation (EC) No 45/2001 used not to be applicable outside the scope of Community law. While the Community and its pillar structure have been replaced since the Treaty of Lisbon, this differentiation has persisted in the area of the protection of personal data and provides an explanation for the co-existence of unstandardised bodies of law. This is the case of EUROJUST and EUROPOL which apply their own body of rules and are supervised by Joint Supervisory Bodies.

Please refer to the case study dedicated to "Data protection in the area of police and judicial cooperation in criminal matters."

The DPOs ensure the consistent and coherent application of Regulation (EC) No 45/2001, primarily thanks to the development of the DPO network

Over time, the DPOs have fostered the development of the DPO network. A quartet composed of DPOs of EU institutions leads the network and organises bi-annual meetings. The DPO meetings last one and a half days; the EDPS is also present on the second day. The DPOs have emphasised the need to extend the length of the DPO meeting.

The DPOs have significantly increased their overall level of knowledge thanks to the better exchange of information within the network, which is composed of both legal officers and IT staff. Within the remit of the network, the DPOs have also adopted standards and guidelines that ensure coherence in the application of the provisions of the Regulation.[22]

The DPOs network has proven to be an efficient and flexible tool for fostering consistency and coherence in the application of the Regulation.

Improvements could be made:

- The meetings could be more frequent and/or last longer.

[20] EDPS, "Measuring compliance with Regulation (EC) 45/2001in EU institutions ("Survey 2013"), General Report, page 14.
[21] For example, a general workshop has been organised in the field of e-Communication, the use of mobile devices in the workplace and websites managed by EU institutions and bodies.
[22] *See* Professional Standards for Data Protection Officers of the EU institutions and bodies adopted by the Network of Data Protection Officers of the EU institutions and bodies.

- Awareness raising among high-level management as the DPOs may lack the appropriate authority in order to perform their tasks. This is particularly relevant when the DPO does not report to high-level management (such as the Executive Board).

The development of the DPCs network in large institutions has increased consistency and coherence in the application of data protection rules and principles.

Over the past few years, certain large institutions have formed networks of Data Protection Coordinators (DPC) in order to assist DPOs in the performance of their tasks. DPCs act as a intermediaries for DPOs in the institutions.[23] In some institutions DPCs are part of a core team (e.g. at the ECB), and in other institutions such as the European Commission, DPCs have been appointed in each Directorate General or Service. All DPCs fulfil similar tasks. Their function is usually provided for in the implementing rules adopted by EU institutions and bodies pursuant to Article 24.8 of the Regulation.[24] DPCs also attend network meetings.

It should be noted that the function of DPC is not provided for by Regulation (EC) No 45/2001.

Nevertheless, a certain amount of heterogeneity in the application of particular data protection rules and principles has been reported within the IT context.

Data protection rules and principles, such as the requirements to manage security risks related to personal data processing and to implement the appropriate security measures safeguarding the security of personal data processing, have been applied heterogeneously across EU institutions and bodies.

Please refer to the assessment of Article 22 in the evaluation of the effectiveness of Regulation (EC) No 45/2001.

Conclusions and suggestions

- **EU institutions and bodies have developed efficient tools to ensure the coherent and consistent application of the Regulation. These consistency tools could be further improved notably by publishing more practical and simplified guidelines and by increasing the collaboration of DPOs within the remit of the network. Moreover, the general level of the security of IT systems could be enhanced insofar as significant discrepancies among EU institutions and bodies have been underlined.**

- **Certain DPOs and DPCs would favour that the future Regulation defines the function of the DPCs in order to assert their authority within the institution. This option should be balanced against the inconvenience of adding an additional level of authority which will add complexity to data protection governance.**

[23] For further information, please refer to EDPS, Survey on the function of Data Protection Coordinators at the European Commission General Report.
[24] Article 14 of the implementing rules concerning the tasks, duties and powers of the Commission's Data Protection Officer (DPO) lays down provisions governing the function of the Data Protection Coordinator (DPC) in the various Directorates General (DG) and Services of the European Commission.

3.2.5 The Regulation achieves the right balance between the protection of personal data and other public interests

This section aims to assess the balance struck by Regulation (EC) No 45/2001 between the right to data protection and other legitimate interests in the light of Article 20 of Regulation (EC) No 45/2001.

The question pertaining to the articulation between Regulation (EC) No 45/2001 and access to public documents is analyzed in a specific case study.

Regulatory framework

Article 20 of the Regulation provides for derogation from the application of Article 4 (1) (Data protection principles on data quality), Article 11 (Information to be supplied where the data have been obtained from the data subject), Article 12 (1) (Information to be supplied where the data have <u>not</u> been obtained from the data subject, Articles 13 to 17 (Rights of data subjects), and Article 37(1) (erasure or anonymisation of traffic and billing data), where such restrictions constitute a necessary measure to safeguard:

"(a) the prevention, investigation, detection and prosecution of criminal offences;

(b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters;

(c) the protection of the data subject or of the rights and freedoms of others;

(d) the national security, public security or defence of the Member States;

(e) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (a) and (b)."

Furthermore, Article 20.2 specifies that Articles 13 to 16 do not apply when "*data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of compiling statistics, provided that there is clearly* ***no risk of breaching the privacy of the data subject and that the controller provides adequate legal safeguards****, in particular to ensure that the data are not used for taking measures or decisions regarding particular individuals."*

The data subject on whom a restriction is imposed must be informed of the principal reasons that have justified the restriction and of his or her right to have recourse to the EDPS (Article 20.3).

Where there is a restriction to the right of access of data subject on the basis of a derogation from Article 20.1, the EDPS "shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made. (Article 20.4)"

Article 20.5 adds that "provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect."

Implementation and Application

There are no procedures relating to these exceptions that we are aware of on the basis of the survey and the interviews.

Article 20 is applied by EU institutions but some drawbacks have been underlined relating to the scope of the Article and its coherence with other provisions.

The exceptions are applied by a limited number of EU institutions and bodies. Some interpretation issues have been raised.

According to current practices within EU institutions and bodies, Article 20.1 (a) is interpreted by the EDPS as including administrative inquiries and disciplinary proceedings in the light of Article 13 (1) (d) of Directive 95/46, which also refers to *"breaches of ethics for regulated professions."*

The exception relating to "important economic and public interest of a Member State or of the EU" seems too narrow to include all legitimate interests pursued by EU institutions or bodies such as *"security rules with regard to the protection of EU classified information which might justify the disclosure on the basis of a request for access to personal data pursuant to Article 13."*[25]

This reasoning could also be applied to the exception pertaining to "national security, public security or defense of the Member States", which could be broadened or clarified to cover the security interest of the EU institutions and bodies (notably in the case of security incidents).

Conclusion and suggestion

Article 20 is applied by certain EU institutions and bodies.

The scope of Article 20 could be extended, notably to cover the following situation:

- Article 20 (1) (a) relating to "the prevention, investigation, detection and prosecution of criminal offences" could be extended to administrative investigations and disciplinary measures;
- The exceptions under Article 20 (1) (b) and (d) could also be amended to address practical difficulties (such as the necessity to derogate from the data protection principles for specific security reasons);
- In the context of telecommunications, the exceptions provided by Article 20 could be extended to Articles 36, 37.2 and 38. In this regard, please refer to the *case study dedicated to the coherence between Regulation (EC) No 45/2001 and the ePrivacy Directive*.

[25] Letter from Sophie Louveaux and Hielke Hijmans to Marie-Hélène Boulanger dated 2 October 2013.

3.2.6 The Regulation ensures adequate protection in the context of internal telecommunications networks

The protection of personal data and privacy in the context of internal telecommunications networks is governed by Chapter IV of Regulation (EC) No 45/2001.

During the last decade, the use and management of telecommunications services in organisations have largely evolved to take into account technological developments and the convergence of telecommunications networks, and to meet users' needs. Today, IT and telecommunications are closely linked and even inseparable.

The evolution from analog to digital technology has facilitated the conversion of voice, data and video to the digital format. Increasingly, these are now being rendered through single networks bringing about a convergence in networks, services and also devices.

Vertical structures of independent networks (IT, fixed telecommunications, mobile telecommunications, etc.) have gradually been abandoned in favour of a horizontal structure based on the IP protocol to provide many types of content through a single network.

Hence, like most organisations, EU entities have been adopting voice and data networks convergence to simplify and optimise the management and operation of internal and external telecommunications networks while enhancing the productivity and responsiveness of employees.

Thus, legal frameworks governing the processing of personal data in IT systems also include in their scope the processing of personal data related to the use of telecommunications networks and equipment.

Given the stakeholders consulted, it is difficult to assess how Chapter IV of Regulation (EC) No 45/2001 was implemented and applied throughout EU Institutions and bodies. Nevertheless, it is important to underline that this chapter is now outdated in insofar as it was based on the first version of the ePrivacy Directive which was updated in 2002 and 2009. The Regulation was not amended accordingly.

Regulatory framework

Scope

Article 34 of the Regulation defines the scope of application of Articles 35 to 40. Pursuant to this Article, all processing of personal data relative to the use of telecommunications networks or terminal equipment operated under the control of an EU institution or body is governed by Chapter IV.

Security of Processing

Article 35 of the Regulation emphasises the need for EU institutions and bodies to assess security risks related to the use of telecommunications networks and terminals and implement, in conjunction with service providers, the appropriate technical and organisational measures to ensure their security.

The Article also requires EU institutions and bodies to properly implement the necessary alert mechanisms in order to ensure the notification of telecommunications users in case of risks pertaining to the breach of security.

Confidentiality of communications

Pursuant to Article 36, EU institutions and bodies must ensure the confidentiality of communications made using internal telecommunications networks and terminal equipment and comply with national and community prescriptions on the confidentiality of communications.

Traffic and billing data

Pursuant to Article 37, traffic data relating to users which are processed and stored during connections over telecommunications networks must be erased or made anonymous upon termination of the connection.

This Article also provides for an exception for budget and traffic management. These data must be erased or made anonymous when no longer needed and no later than six months after collection. Nevertheless, in cases of legal claims, a longer retention period is allowed.

Article 37 (3) regulates the processing of traffic and billing data for the purpose of budget and traffic management. The Article states that only employees of EU entities in charge of billing, traffic or budget are authorised to handle traffic and billing data processing.

Finally, Article 37 (4) provides for the right of users of EU entity telecommunications networks to receive non-itemised bills or other records of calls made.

Directories of users

Pursuant to Article 38, personal data contained in printed or electronic directories of users and access to such directories must be limited. Only access in line with the directory's purpose will be authorised.

The article also establishes that EU institutions and bodies must take all necessary measures to prevent personal data contained in those directories from being used for direct marketing purposes.

Presentation and restriction of calling and connected line identification

Pursuant to Article 39 of the Regulation (EC) 45/2001, the following possibilities must be made available via simple means for users of EU entity telecommunications networks:

- Calling users must have the possibility to prevent the presentation of the calling-line identification;
- Called users must have the possibility to prevent the presentation of the calling-line identification of incoming calls;
- Called users must have the possibility, when presentation of connected-line identification is offered, to prevent the presentation of the calling-line identification to the calling user.
- Called users must be informed when presentation of calling or connected-line identification is offered and of the three possibilities listed above.

Pursuant to Article 40, EU institutions and bodies may override the requirements of Article 39 under the following circumstances:

- On a temporary basis, upon application of a user requesting the tracing of malicious or nuisance calls;
- On a per-line basis for organisational entities dealing with emergency calls, for the purpose of answering such calls.

Implementation

The level of implementation of Chapter IV of the Regulation could be further improved.

Only 46% of the EU institutions and bodies consulted have adopted specific procedures/processes or internal rules specific to the telecommunications sector. Nevertheless, it should be noted that the security rules provided for in this chapter should be read in the light of Article 22 on the security of data processing. Therefore, these implementing rules on security can also be applied to rules applicable in the telecommunications sector. In this regard, several security officers have emphasised that there is no specific need to include a different body of rules relating to security within the context of telecommunications.

The EDPS is preparing guidelines on the processing of personal data relating to electronic communications by European Union institutions and bodies.

Moreover, the EDPS has indicated that the list mentioned in Article 37 (2) has never been established.

Although initially targeting telephone communications, the scope of Chapter IV is broadly applied to include all means of communications over telecommunications networks or terminal equipment (such as telephone, e-mail, Internet websites, etc.).

Levels of application of Article 35 appear to vary but the evaluator cannot be conclusive based on the information gathered. The following information was gathered during the consultation of stakeholders:

Regarding the security of processing, the provisions of Article 35 of Regulation (EC) N°45/2001 are similar to those of Article 22 as they provide for the implementation of appropriate technical and organisational measures. It follows from the foregoing that EU institutions and bodies must develop the appropriate procedures and frameworks for the assessment of security risks related to the use of telecommunications networks and terminals. In this regard, several security officers have emphasised that there is no specific need to include a different body of rules relating to security within the context of telecommunications.

Pursuant to Article 35, EU entities must also properly implement the necessary alert mechanisms in order to ensure the notification of telecommunications users in the event of any security breach risks. These notifications may include remediation and alternative solutions.

Through their internal policies, several EU institutions and bodies already implement an obligation to notify personal data breaches to their DPOs and the data subjects concerned. In most cases, the personal data breaches are systematically notified to the DPO of the institution or the body, but not systematically to the data subject concerned. Notification of data subjects is generally discussed with the DPO and depends on the gravity and timing of the data breach and the mitigation actions that might be taken.

In addition, EU institutions and bodies are currently facing a growing number of attacks targeting their telecommunications networks and equipment. EU entities that have insufficiently applied Articles 35 and 22 are struggling to maintain an appropriate level of security in the face of these attacks.

So far, EU institutions and bodies seem to have interpreted the rules enshrined in Chapter IV in the light of the provisions of the ePrivacy Directive (notably Article 5 relating to the confidentiality of communications).

The implementation and application of Article 36 requires that the EU institutions and bodies incorporate the proper technical and organisational mechanisms to safeguard the confidentiality of communications. EU institutions and bodies may need to intercept or oversee communications and related traffic data. They may need to record calls to certain helplines, security or emergency lines or switchboards aimed at a large number of users, in order, for example, to be able to verify the content of the communication afterwards and provide an accurate response, to retain evidence, to use as a training aid, etc.

The provision relating to traffic and billing data has raised some practical issues.

On principle, traffic data should be erased or made anonymous immediately after being processed and stored for the duration necessary to transmit communications (Article 37.1).

Article 37.2 provides for an exception relating to the processing of traffic data which is necessary for budget and traffic management. These data are indicated in a list subject to agreement by the EDPS. These data may be kept for a period of six months and should then be erased or made anonymous (Article 37.2). In practice, this traffic data may be relevant in the course of the investigation of criminal offences, administrative enquiries or disciplinary proceedings. Therefore, Article 20.1 is applicable to Article 37.1, meaning that, as an exception, after the establishment of calls and other connections, instead of being immediately erased or made anonymous, traffic data may be processed and stored in order to safeguard:

- (a) the prevention, investigation, detection and prosecution of criminal offences;
- (b) an important economic or financial interest of a Member State or the European Union;
- (c) the protection of the data subject or of the rights and freedoms of others;
- (d) the national security, public security or defense of the Member States;
- (e) a monitoring, inspection or regulatory task connected with the governance of criminal offences or economic or financial interests referred to in (a) and (b) .

Stakeholders have underlined that Article 20.1 should also cover Article 37.2. Indeed, should Article 20.1 only cover Article 37.1, it would be applicable to data which has already been erased or anonymised at the time of the investigation (insofar as Article 37.1 provides for immediate erasure or anonymisation).

The EDPS has indicated that the list mentioned in Article 37.2 has never been established.

Moreover, there is a practical difficulty of application relating to the technical feasibility of definitely erasing or anonymising traffic data in communication networks which were not all designed to offer this possibility.

Furthermore, regarding user directories, it was indicated that two kinds of directories exist. There are public directories with minimum information about staff members (name and function) and internal directories which contain additional information only accessible within EU institutions and bodies. The public directories of the European Commission are directly accessible on the internet.

In addition, it was indicated that the provisions relating to the presentation and restriction of calling- and connected-line identification are irrelevant and outdated, notably in the light of BYOD (Bring Your Own Device) and mobile telephones.

Conclusion and suggestion

As preliminary remark, it should be emphasised that the current rules enshrined in Chapter IV are **outdated in the light of the provisions of the ePrivacy Directive, as the ePrivacy Directive has**

been updated twice since the adoption of Regulation (EC) 45/2001, namely in 2002[26] and 2009[27]. In this regard, it should be noted that the European Commission has already implemented and applied the provisions relating to the use of cookies.

Moreover, given the principle of technological neutrality, the scope and the wording of the Regulation should remain sufficiently broad to encompass all current and future telecommunication technologies.

Raising awareness is essential in order to increase the level of implementation of Article 35 within EU institutions and bodies.

In order to effectively raise the level of implementation and application of Article 35, the EDPS and the data protection officers (DPOs) of EU institutions and bodies should collaborate and organise regular workshops on data privacy and security issues in order to raise the level of awareness of EU entities' staff on the general principles of data protection. Furthermore, regular inspections could be carried out in order to raise awareness on compliance.

Finally, several stakeholders pointed out that the prescriptions relating to calling- and connected-line identification are now outdated. Nowadays, EU entities' staff are accustomed to calling- and connected-line identification due to the widespread use of mobile phones where these features are enabled by default.

For further information, please refer to the case study dedicated to the telecommunications sector.

[26] Directive 2002/58/EC of the European Parliament and of the Council *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 of 31.7.2002, p.37).

[27] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, *amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws* (OJ L 337 of 18.12.2009, p.11).

3.2.7 The Regulation ensures that the EU legislator and other institutions/bodies are aware of data protection requirements and integrate data protection into the law making and implementation process

This section aims to assess how and to what extent this obligation has been implemented and applied in order to contribute to the protection of fundamental rights. Indeed, taking data protection issues into account at an early stage enables the proper achievement of this objective.

Regulatory framework

Regulation (EC) No 45/2001 provides for an advisory or consultative role for the EDPS towards (1) EU institutions and bodies when drawing up administrative measures relating to the processing of personal data (Article 28.1) and (2) the Commission when it adopts a legislative proposal relating to the protection of individuals' rights (Article 28.2). It should be noted that with regard to administrative measures, the EDPS supervises the consultative work performed by the DPOs.

Implementation and application

Nota bene: The analysis of the implementation and application of the Regulation is presented in the section dedicated to the EDPS (see below). The purpose here is to analyze the obligations set out by Article 28 in the light of the objective to protect fundamental rights.

Articles 46 and 28.2 of the Regulation assign to the EDPS a duty to **advise institutions and bodies on personal data protection matters**, and this duty is properly fulfilled by the EDPS.

Indeed, the Supervision and Enforcement unit of the EDPS is informed of the administrative measures relating to the processing of personal data that are adopted by EU institutions and bodies. The EDPS adopts opinions on administrative measures when it is consulted by DPOs, or at its own initiative. It has built a doctrine contributing to reducing the workload of DPOs and the EDPS.

As regards the **consultation of the EDPS by the European Commission in the course of the legislative process**, this role is not specifically described in the list of duties assigned to the EDPS in the legislation. To compensate for this lack of clarity, implementing rules[28] detail this role further in their Section 4 on legislative and policy consultation. They provide details on the scope of consultation in terms of documents, timing in the legislative process, types of opinions, etc. This role is performed by the Policy and Consultation unit of the EDPS.

The consultation can take several forms (formal legislative opinions, formal comments and informal comments at an early stage of the legislative process). The EDPS' activity advising the European Commission in the legislative process has significantly increased in recent years, notably in terms of informal comments provided. Informal comments allow for early integration of data protection measures into the process, resulting in a more effective final proposal. The poor definition of the duty assigned to the EDPS concerning this role has led to misunderstandings and sometimes even reluctance on the part of the European Commission to consult the EDPS. Thanks to awareness-raising efforts and constructive cooperation with the Commission, the involvement of the EDPS has increased over the years, based on a work programme and the drawing-up of a policy inventory.

[28] The EDPS Rules of procedure. It was also indicated that a note of the EC Secretary General reflecting the working arrangements between the Commission and the EDPS as to consultation work of 8 December 2008 was drawn up (paper not reviewed by the evaluator).

The consultation of the EDPS by other institutions (the European Parliament and the Council of the European Union) in the course of the legislative process is not explicitly provided for by the Regulation, although it has regular contacts with these institutions as further described in the section dedicated to the EDPS.

Conclusions and suggestion

The Regulation establishes the obligation to involve the EDPS in order to take data protection issues into consideration in the legislative and policy-making process.

Although the section dedicated to the contribution of the EDPS involving the provision of opinions on the legislative process impacting personal data is very limited in the Regulation, this role has reached a satisfactory level of maturity thanks to the implementing rules adopted by the EDPS and constructive cooperation with the European Commission. Several hurdles still need to be cleared, starting with the clarification of the process in the Regulation, to further the effectiveness of the support offered by the EDPS on the legislative process.

GENERAL CONCLUSION ON OBJECTIVE 1: PROTECTION OF FUNDAMENTAL RIGHTS AND FREEDOMS

Regulation (EC) No 45/2001 establishes appropriate rights for data subjects and obligations for data controllers. The Regulation also establishes safeguards relating to the processing of special categories of personal data. Some drawbacks have nevertheless been identified in the wording, interpretation or mere existence of certain provisions of the Regulation (e.g. change of purpose). The Regulation also provides for exemptions and restrictions in order to balance the protection of personal data against other legitimate interests. The scope of such a provision could be broadened to better address other public interests while maintaining a high level of protection of personal data. In addition, the governance system set out by the Regulation contributes to ensuring the protection of fundamental rights of individuals.

Data protection rights and obligations are reasonably implemented but simplified procedures would significantly increase the effectiveness of the application of the processing obligations.

Regulation (EC) NO 45/2001 establishes adequate remedies for data subjects (including staff members). However, in practice the perception of data subjects, data controllers and DPOs of the processing of complaints and the remedies provided may vary. It should also be noted that data protection breaches may be argued to serve interests other than the protection of personal data.

Nevertheless, the EDPS does not make sufficient use of its sanctioning powers even though the appropriateness of the range of powers is not questioned by the stakeholders. Offenders are never (or extremely rarely) sanctioned for failure to comply with the rules enshrined in the Regulation. As a result, this could reduce the incentive of controllers to comply with the provisions of the Regulation and hinder its enforcement. In this regard, the EDPS underlines that there is a high level of compliance when the EDPS takes action, even if this does not involve enforcement measures (e.g. compliance visits), and sanctions are only applied if necessary. Within the institutional framework, the work of the EDPS has focused on working towards compliance in cooperation with EU institutions and bodies (*e.g.* compliance visits).

EU institutions and bodies have developed efficient tools to ensure the coherent and consistent application of the Regulation (such as the creation of the DPC function and the DPO network) which could be further improved, notably by (1) publishing more practical and simplified guidelines and by increasing the collaboration of DPOs within the remit of the network and (2) enhancing the general level of the security of IT systems.

Finally, the Regulation establishes the obligation to involve the EDPS in order to take data protection issues into consideration in the legislative and policy-making process. The EDPS complies fully with this obligation, even though certain improvements could be made.

3.3 Contribution of the Regulation to ensuring the free flow of personal data (Objective 2)

According to Recital 9 of the Regulation, *"Directive 95/46/EC requires Member States to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data,* ***in order to ensure the free flow of personal data in the Community.****"*

Therefore, Regulation (EC) No 45/2001 sets out the rules governing the transfer of personal data within or between EU institutions and bodies (i), to recipients other than EU bodies subject to 95/46/EC (ii) and to recipients other than EU bodies in third countries (iii).

3.3.1 The Regulation ensures the free flow of personal data within or between EU institutions and bodies

Regulatory framework

Pursuant to Article 7 of the Regulation, the transfer of personal data within or between EU institutions or bodies is subject to certain specific conditions.

It stems from Article 7 that an EU institution or body may transfer personal data to another EU institution or body (or within the same EU institution or body) if the data are necessary for the legitimate performance of the public tasks covered by the competence of the recipient.[29] The controller and the recipient bear the responsibility for the legitimacy of this transfer. This provision applies without prejudice to Articles 4, 5, 6 and 10 of the Regulation.

Implementation and Application

Article 7 of the Regulation has been implemented and applied, but the wording of the provision has given rise to interpretation issues.

59% of the EU institutions and bodies consulted have implemented processes/procedures or internal rules on the transfer of personal data.

The application of this Article has given rise to several issues of interpretation regarding the necessity of the transfer in the performance of public tasks.[30] It appears that the Court of Justice of the European Union adopts a strict interpretation of the criteria of necessity.

The criterion of competence is not defined in the Regulation and this has raised interpretation issues.

In practice, DPOs and data controllers find it difficult to determine to what extent Article 7 is applicable **within EU institutions and bodies.** The threshold to apply in order to establish whether Article 7 is applicable to the disclosure of personal data within the same EU institution or body (e.g. between two officials of the same unit) is difficult to assess. This is partially due to the fact that neither the Regulation nor Directive 95/46/EC defines what should be considered as a "transfer of personal data". In the guidelines on transfer to third countries, the EDPS has specified that Article 7 applies to transfer from one Directorate General to another within the European Commission and

[29] Civil Service Tribunal, 5 July 2011, Case F46/09, paragraph 129.
[30] Ibidem.

from one institution to another located outside the EU (e.g. when the European External Action Service sends personal information to delegations around the world).

In this regard, it should be noted that the EDPS has called for a definition of this notion in the context of the data protection reform.[31] The Court of Justice has also provided some guidance relating to the definition of personal data to third countries in the *Bodil Lindqvist* case (see below)[32].

Moreover, the EDPS seems to apply Article 9 of the Regulation in the case of transfer to EUROJUST and EUROPOL, as the latter have a specific data protection regime and Directive 95/46/EC does not apply to them. Nevertheless, the EDPS considers that there is a presumption of adequacy because their data protection regime is broadly in line with the Directive and Regulation.[33]

Conclusion and Recommendations

The conditions governing the transmission of personal data within EU institutions and bodies should be clarified and specified in the Regulation. The lack of clarity of this provision may hinder the free flow of personal data.

3.3.2 The Regulation ensures the free flow of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46/EC

Regulatory framework

Article 8 of the Regulation lays down the conditions governing the transfer of personal data to recipients, other than EU institution or bodies, subject to national law implementing Directive 95/46/EC.[34] This is the case for transfers to private companies or national authorities.

Without prejudice to the application of Articles 4, 5, 6 and 10, these transfers require that the recipient establishes (i) **the necessity of the transfer for the performance of a task carried out in the public interest or subject to the exercise of public authority** or (ii) **the necessity of having the personal data transferred and that there is no potential prejudice of the data subject's legitimate interests.**

The wording of Article 8 only provides for the case where recipients request the transfer of personal data and does not provide for the rules applicable where an EU institution or body initiates the transfer. In those cases the EDPS has recommended that the controller conducts a necessity test.

Implementation and Application

59% of the EU institutions and bodies consulted have implemented processes/procedures or internal rules on the transfer of personal data.

Pursuant to Article 8 of Regulation (EC) No 45/2001, the burden of the proof of the necessity of the transfer rests on the recipient. The EDPS has adopted the position according to which the burden of

[31] EDPS, "Transfer of personal data to third countries and international organisations by EU institutions and bodies", position paper, 14 July 2014.
[32] Case C-101/01, Lindqvist [2003] ECR I-12971.
[33] EDPS "Transfer of personal data to third countries and international organisations by EU institutions and bodies", position paper, 14 July 2014, page 24.
[34] All EU Member States and the Member States of the EEA (Iceland, Norway and Liechtenstein) apply the provisions of Directive 95/46/EC.

the proof of the necessity rests on the sender when the latter initiates the transfer (e.g. the transfer of personal data from OLAF to national authorities).[35]

The criterion of necessity is interpreted strictly by the Court of Justice.[36]

This provision has also raised significant issues of articulation with the provisions laid down by Regulation (EC) No 1049/2001.

For an in-depth study of the case law relating to the application of Article 8 in the context of public access to documents, please refer to the dedicated case study. Indeed, requests for public access (to documents including personal data) must be considered as a transfer of personal data that must be compliant with Regulation 45/2001.

Finally, the question was raised whether Article 8 or Article 9 applies to the transfer of personal data to national authorities of the ex-third pillar. The EDPS has considered that the EU institution or body concerned should verify whether the Member State has implemented Directive 95/46/EC also with regard of national authorities. Should this be the case, Article 8 is applicable. On the contrary, Article 9 is applicable. The adequacy of the level of protection of personal data should nonetheless be presumed as all Member States have signed Convention 108.[37]

Conclusion and suggestions

Article 8 is implemented and applied. The major sources of concern relate to the application of Article 8 (b) in the context of public access to documents.

Please refer to the case study dedicated to access to documents.

3.3.3 The Regulation ensures the free flow of personal data to recipients, other than Community institutions and bodies, which are not subject to Directive 95/46/EC

Regulatory framework

Article 9 lays down the rules governing the transfer of personal data to recipients, other than EU institutions and bodies, in third countries (including to international organisations).

EU institutions and bodies must respect the **principle of adequate protection** (Article 9.1 and 9.2) which requires that the recipient assess the level of protection afforded by the third country or international organisation to the processing of personal data. In this regard, Article 9.2 outlines how the level of adequacy should be assessed. The data must be transferred solely to allow tasks covered by the competence of the controller to be carried out.

In the event that the European Commission has adopted an "Adequacy decision", there is no need for further assessment. The EU institution or body must take the necessary measures to comply with decisions taken by the Commission.

In the event that the EU institution or body considers that the third country or the international organization does not provide an adequate level of protection, it must inform the European

[35] Letter from Sophie Louveaux and Hielke Hijmans to Marie-Hélène Boulanger dated 2 October 2013.
[36] See case law on access to documents.
[37] Letter from Sophie Louveaux and Hielke Hijmans to Marie-Hélène Boulanger dated 2 October 2013.

Commission and the EDPS (Article 9.3). In this case, the European Commission must inform the Member States.

Paragraph 6 of Article 9 lays **down exceptions to the general principle of adequate protection** provided by Article 9.1 and 9.2 (such as if the data subject has given his or her consent, or if the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request).

Without prejudice to paragraph 6, the EDPS may **authorise** a transfer or a set of transfers of personal data to a third country or international organisation which does not ensure an adequate level of protection **"where the controller adduces adequate safeguards** with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; **such safeguards may in particular result from appropriate contractual clauses."**

The EU institution or body must inform the EDPS of categories of cases where they have applied Article 9.6 and Article 9.7.

Implementation and Application

The Rules governing the transfer of personal data outside the EU are implemented, but further simplification of the applicable rules should be considered.

59% of the EU institutions and bodies consulted have implemented processes/procedures or internal rules on the transfer of personal data.

The Court of Justice provided guidance relating to the definition of personal data to third countries in the Bodil Lindqvist case where the Court held that there is no transfer of personal data "where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country."

The EDPS interprets the notion of transfer of personal data as: "communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender subject to the Regulation that the recipients will have access to it."

It appears that the transfer of personal data is a major source of concern for numerous institutions which transfer personal data in the course of their activities, such as OLAF, the EEAS or the JRC.

Therefore, the EDPS issued a paper on the transfer of personal data to third countries and international organisations performed by EU institutions and bodies. This paper shed light on the complex body of rules governing the transfer of personal to third countries and international organisations. Annex 2 provides DPOs and data controllers with a checklist of the steps to be undertaken in case of transfer of data to third countries or third organisations. The EDPS also organises training sessions, such as the workshop organised in 2013 on transborder data flows for DPOs, to provide guidance on the legal regime established in Article 9 of Regulation 45/2001 and to exchange on mutual experience.

In the guidelines on transfer, the EDPS requires that the EU institutions and bodies assess the level of protection provided by the recipients. The adequacy must be documented. This could be deemed complex in practice. In cases where the European Commission has adopted an "Adequacy Decision", the decision is binding upon EU institutions and bodies and there is no need for such analysis.

Otherwise, EU institutions and bodies do not have the adequate resources and/or the competence to perform the assessment of the adequacy of a foreign country. Should the level of adequacy be inadequate or not feasible, the EU institution or body may rely on one of the derogations laid down in Article 9.6 "if the transfer is *not* repeated, massive, or structural".

If one of the derogations does not apply, the EU institution or body may adduce "adequate safeguards such as standard contractual clauses (SCC). Where SCC are used, there is no need for prior the consultation or authorization of the EDPS. When another specific legally binding instrument (other than SCC) is used, consultation of the EDPS is required. In the event of consultation, the EDPS may consider that an authorization is needed.

According to the EDPS guidelines, authorization by the EDPS is only required in specific situations (in comparison with the wording of Article 9.7). This is the case for transfers based "on specific safeguards which are **not incorporated in a legally binding instrument."** So far, there has only been one case of a request for authorization by OLAF.

Therefore, the DPOs emphasised that it would be useful to allow for the possibility of using standard clauses for transfers to third countries and international organisations instead of assessing the level of adequacy. These standard clauses could be submitted for validation to the EDPS. For example, it could be envisaged to use standard clauses when transferring personal data to a cloud computing service provider.

The transfer of personal data to international organisations may raise additional difficulties insofar as the use of standard contractual clauses may not be appropriate.

The EDPS requires that the DPOs keep a register of all transfers of personal data falling within the scope of Article 9.

Conclusion and suggestion

The available procedures relating to the transfer of data to third countries should be clarified. Moreover, the adequacy of protection is difficult for EU institutions and bodies to assess.

- Article 9 of Regulation (EC) No 45/2001 lacks clarity with regard to the rules applicable to the transfer of personal data to third countries. The guidelines of the EDPS provide useful information but appear insufficient to tackle all the practical issues arising under the application of Article 9. Moreover, these guidelines are very thorough and may be inappropriate for day-to-day use by data controllers. We note however that the check list in Annex 2 is a practical and very useful tool for interpreting Article 9. In particular, the fact that the criterion of necessity is only referred to in Articles 7 and 8, and not explicitly in Article 9, contributes to the lack of consistency of the transfer requirements.
- Furthermore, EU institutions and bodies do not have the resources or the competence to carry out adequacy assessments (including on the transfer documentation). This is particularly significant for small agencies.
- The use of standard contractual clauses (validated by the EDPS) could be a suitable means to facilitate the international transfer of data and ensure its free flow, while maintaining a high level of protection of personal data.

GENERAL CONCLUSION ON OBJECTIVE 2 : ENSURE FREE FLOW OF DATA

The Regulation establishes the conditions governing the transfer of personal data in order to ensure the free flow of personal data. The implementation and application of these provisions have

raised difficulties which are likely to hinder the effectiveness of the objective.

The amendment of Regulation (EC) No 45/2001 should clarify the rules applicable to transfer.

3.4. Contribution of the Regulation to establishing a relevant and effective governance system (Objective 3)

The evaluation of the effectiveness of the governance aspects of Regulation (EC) No 45/2001 requires assessing how the obligation to appoint a DPO and to appoint a supervisory authority has been implemented and applied.

- **The Regulation states that each European Union institution and body** must appoint a DPO, who ensures that the provisions of the Regulation are applied and who advises controllers to comply with their obligations.
- The Regulation establishes an independent supervisory body responsible for monitoring the application of Regulation (EC) No 45/2001.

3.4.1 Contribution of the Regulation to establishing a DPO in each EU institution and body

Regulation (EC) No 45/2001 provides for the mandatory appointment of a DPO within each of the EU institutions and bodies. The Regulation sets out the selection criteria as well as the main tasks and duties of the DPO. Moreover, Regulation (EC) No 45/2001 establishes a system of notification of processing operations (Article 25) which must be recorded in a register kept by the DPO (Article 26).

(1) Appointment of Data Protection Officers

Regulation (EC) No 45/2001 effectively establishes a DPO in each EU institution and body

Regulatory framework

Pursuant to Article 24.1 of Regulation (EC) No 45/2001, each institution or body must appoint a DPO. Recital 32 specifies that in each EU institution or body, a DPO *"should ensure that the provisions of this Regulation are applied and should advise controllers on fulfilling their obligations."*

The DPO must be appointed for a term of between two and five years, eligible to reappointment up to a maximum total term of ten years (Article 24.4).

He or she may be dismissed from the post of DPO by the institution or body which appointed him or her only with the consent of the EDPS, if he or she **no longer fulfils the conditions required for the performance of his or her duties (Article 24.4).**

After his or her appointment, the DPO must be registered with the EDPS (Article 24.5).

Implementation and Application

The obligation to appoint a DPO has been implemented in all EU institutions and bodies.

The obligation to appoint a DPO was implemented pursuant to the implementing rules adopted by each institution and body[38], as well the *Professional Standards for Data Protection Officers of the EU*

[38] See, for example, Commission Decision of 3 June 2008 adopting implementing rules concerning the Data Protection Officer pursuant to Article 24(8) of Regulation (EC) No 45/2001 on the protection of individuals with regard to the

institutions and bodies adopted by the Network of Data Protection Officers of the EU institutions and bodies. The position, tasks and duties of the DPO are described in these rules.

A DPO has been appointed in each of the EU institutions and bodies.

A DPO has been appointed in each of the institutions and bodies of the European Union.[39] Moreover, the DPO appointments have been notified to the EDPS.

DPOs are appointed for a term of between two and five years, eligible to reappointment up to a maximum total term of ten years. This term may raise practical difficulties, as it takes several years for DPOs to gain experience on data protection matters (notably in the case of part-time DPOs). By the time the DPOs reach an adequate level of knowledge, they have to leave their functions. In practice, there are some institutions and bodies where the previous DPO still acts as *de facto* DPO.

Conclusion and suggestion

- The obligation to appoint a DPO has been fully implemented and applied in all EU institutions and bodies consulted.
- DPOs are appointed for a specific term and for a maximum period of 10 years. This mandatory term has raised practical difficulties, notably for part time DPOs who need time to develop their skills on data protection matters. This term could therefore be made non-mandatory in order to give EU institutions and bodies (in particular agencies) the possibility of appointing DPOs for a longer term.

DPOs are not always selected on the basis of their knowledge in data protection, as training is often given after the appointment

Regulatory framework
DPOs are selected based on their personal and professional qualities, in particular expertise in data protection (Article 24.2).

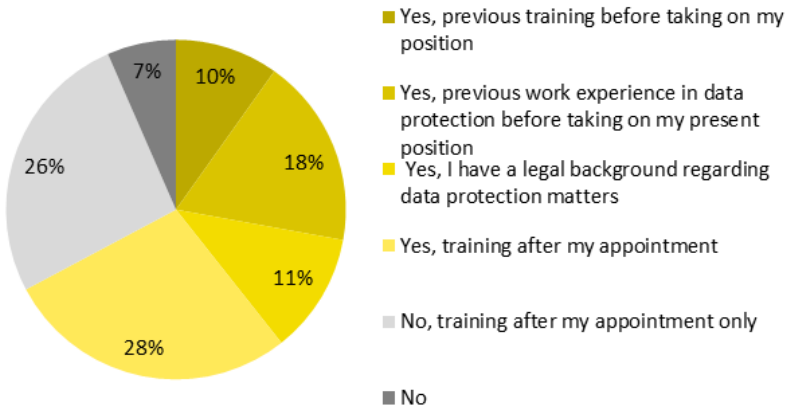
Implementation and Application
The selection procedure is effectively implemented and applied, all EU institutions and bodies having appointed DPOs. The DPOs gain experience and knowledge in data protection after their appointment.

33% of the DPO respondents surveyed declared that they did not have any background in data protection before taking up their position as a DPO.

processing of personal data by the Community institutions and bodies and on the free movement of such data (2008/597/EC), Official Journal of the European Union, 22.7.2008, L 193/7.

[39] Please note that the DPO of the European Commission is also the DPO for the Publications Office (PO), the European Personal Selection Office (EPSO) and the European School of Administration (ESA).

Figure 12 - Do you have a background in data protection? (Source: EY survey)



Considering the level of expertise required to perform DPO duties, this percentage calls for systematic training upon appointment, initiated by the EDPS. This difficulty can be resolved by the development of a "newcomers' training tool kit", available online, for newly appointed DPOs as suggested by several respondents, in addition to the existing tools (in particular: the *Professional Standards for DPOs of the EU institutions and bodies* working under Regulation (EC) 45/20011, training by EDPS or other providers, EU DPO network meetings). They should be given the opportunity to develop their skills (e.g. certification as a privacy professional). In this regard, training certification courses have been put in place within the DPO network.

DPOs may be subject to independence issues, especially in the case of part-time DPOs.

Regulatory framework

DPOs must be independent and their selection must not result in a conflict of interests between their function as DPO and other duties (Article 24.3).

Pursuant to Article 24.7, the DPO may not receive any instructions in the performance of his or her duties.

Implementation and Application

The independence of the DPO seems to be closely linked to his or her position within the hierarchy and the support provided by management for his or her function.

Only 24% of DPO respondents declared that their position allowed them to exercise their functions in **total independence**. Survey respondents provided several reasons for this:

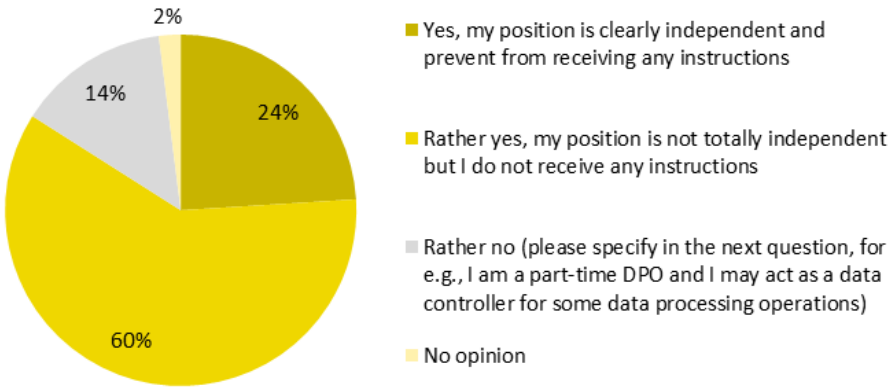
- When the DPO reports directly to the highest level of management (e.g. the Executive Director) who supports his or her actions, this fosters the independence and authority of the DPO with regard to his or her colleagues;
- Independence might be weakened where the DPO is a part-time DPO and acts as a data controller or performs other duties such as providing legal advice. In addition, this can place the DPO in situation where a conflict of interest arises.

The document on professional standards for DPOs issued by the DPO network gives a list of best practices to help ensure the independence of the DPO.[40]

[40] See Professional Standards for Data Protection Officers of the EU institutions and bodies adopted by the Network of Data Protection Officers of the EU institutions and bodies.

In order to foster DPO independence, it could be envisaged to allow smaller institutions to jointly appoint a DPO, similarly to the possibility of setting up common Joint Committees and common disciplinary boards (see Articles 9(1a) of the Staff Regulations and 5(1) of Annex IX to the Staff Regulations).

Figure 13 - In your opinion, does your position in your institution or body allow you to exercise your functions in total independence?



The Regulation also provides for an adequate range of powers and duties, although respondents mentioned insufficient resources to perform the duties

Regulatory framework

Article 24.1 enumerates the DPO's tasks, i.e.:

a) ensuring that controllers and data subjects are informed of their rights and obligations pursuant to this Regulation;

b) cooperating with the EDPS and responding to its requests;

c) ensuring in an independent manner the internal application of the provisions of this Regulation;

d) keeping a register of the processing operations carried out by the controller;

e) notifying the EDPS of the processing operations likely to present specific risks and falling under the scope of prior checking.

That DPO must thus ensure that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

In addition, the Annex to Regulation (EC) No 45/2001 stresses that:

- the DPO may make recommendations for the practical improvement of data protection within the institution or body and advise the controller with regard to the application of the Regulation
- the DPO may investigate on his or her own initiative or at the request of the institution/body, the controller of the Staff Committee concerned or any individual, matters directly relating to his or her tasks and which come to his or her notice, and report back to the person who commissioned the investigation or to the controller
- the DPO may be consulted by the institution or body, by the controller concerned, by the Staff Committee concerned and by any individual, without going through the official channels, on any matter concerning the interpretation or application of this Regulation

- no one shall suffer prejudice on account of a matter brought to the attention of the competent Data Protection Officer alleging that a breach of the provisions of this Regulation has taken place
- every controller concerned will be required to assist the DPO in performing his or her duties and to give information in reply to questions. In performing his or her duties, the DPO will have access at all times to the data forming the subject-matter of processing operations and to all offices, data-processing installations and data carriers.
- To the extent required, the Data Protection Officer must be relieved of other activities.
- The DPO and his or her staff are bound by a **duty of confidentiality** with respect to information or documents which they obtain in the course of their duties (in accordance with Article 339 of the Treaty on the functioning of the European Union, ex-Article 287 TCE).

Implementation and Application

The range of powers appears appropriate for the performance of the DPOs' tasks
Based on the interviews conducted, the range of powers set out by Regulation (EC) No 45/2001 is appropriate for the performance of the DPOs' tasks. The difficulties that DPOs may face when performing their tasks generally result from a lack of authority that can be linked in some cases to poor support from the management, or insufficient time to perform their duties.

Task 1: Ensuring that controllers and data subjects are informed of their rights and obligations pursuant to this Regulation

The survey reveals that informing data controllers is the top activity performed by DPOs, in terms of time spent. Moreover, 22% of them consider they should be increasing this activity, given the need to inform the data controllers. Several tips are given in the document issued by the DPO network on professional standards for DPOs concerning the informing of data controllers (training the controllers, developing guidelines, developing IT tools, attending management meetings on a regular basis, etc.). Data controllers are still significantly lacking in awareness on data protection matters: in some cases DPOs are obliged to draft notifications instead of the data controllers. DPOs, DPCs and data controllers all agree that the time dedicated to raising awareness within the institutions is insufficient compared to the needs, mainly because other tasks are too burdensome.

The informing of data subjects ranks third among the activities performed by DPOs in terms of time spent. Data subjects are mainly informed through information notices. This seems to be effective as most of the institutions have developed procedures for the exercise of data subjects' rights. The majority of data controllers have never received any requests from data subjects wishing to exercise their rights, but this is mainly because data subjects lack awareness on data protection matters. It is likely that the number of requests will increase over time.

Task 2: Cooperating with the EDPS and responding to its requests

According to the survey, liaising with the EDPS ranks second among the most time-consuming activities for DPOs. DPOs are bound by a duty of cooperation with the EDPS and at the same time they are bound by a duty of confidentiality towards the institution or body who has appointed them.

In practice, it may be hard to strike a balance between the duty to cooperate with the EDPS and the duty of confidentiality[41]. Indeed, DPOs are put in a difficult position, where they have to earn the trust of their management to effectively perform their duties, while at the same time they must collaborate with the EDPS. Some DPOs are thus afraid that if they report difficulties in the enforcement of the Regulation, their management will be subject to inspection by the EDPS.

Task 3: Ensuring in an independent manner the internal application of the provisions of this Regulation

The DPO is expected to provide the appointing institution/body with recommendations and advice on the application of data protection provisions. This task also enables the DPO to monitor the application of the Regulation. In the event of breach of the Regulation, the DPOs liaise with the data controller in order to remedy the breach. The annex to the Regulation states in this regard that "no one shall suffer prejudice on account of a matter brought to the attention of the competent Data Protection Officer alleging that a breach of the provisions of this Regulation has taken place." The evaluator is not aware of any prejudice resulting from the notification of breach.

DPOs are also expected to ensure compliance within their institutions although they do not have any enforcement power towards controllers. A number of best practices to ensure compliance are listed in the document on professional standards for DPOs. Furthermore, DPOs may also investigate certain data protection matters on their own initiative or at the request of the institution/body, the controller of the Staff Committee concerned or any individual, even though the survey showed that few inquiries are carried out by the DPOs.

The DPOs' powers allow for an appropriate level of implementation and application of this compliance check, as they have the power to investigate, they can ask a controller to assist them in performing their duties, and they have access to the data.

Tasks 4 (keeping a register of the processing operations carried out by the controller) and 5 (notifying the EDPS of the processing operations likely to present specific risks and falling under the scope of prior checking) are further detailed below.

Obligation to perform prior checking in the case of risky operations

Pursuant to Article 27 of Regulation (EC) No 45/2001, DPOs must submit "processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes" to the EDPS for prior checking.

The assessment of the supervisory powers of the EDPS is described below and includes an evaluation of the prior checking procedure.

It should be added that performing prior checking is excessively burdensome for DPOs. It could be envisaged to reduce the scope of prior checking and focus on the "risk-based approach" promoted by the GDPR.

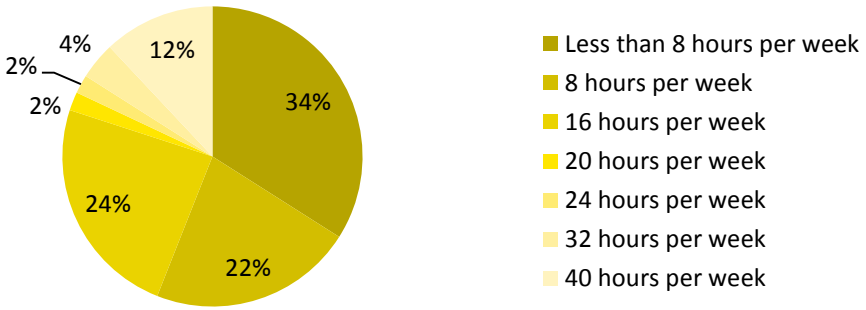
The DPO staff and resources are generally limited

According to Article 24.6, the institution or body which appointed the DPO must provide him or her with the staff and resources necessary to carry out his or her duties.

[41] The DPO and his or her staff are bound by a duty of confidentiality with respect to information or documents which they obtain in the course of their duties (in accordance with Article 339 of the Treaty on the functioning of the European Union, ex-Article 287 TCE).

Most DPOs work part time: only 12% of the DPO respondents work full time on data protection matters within their institution. They are assisted by 0.35 FTEs (on average) to carry out their duties (see evaluation question on efficiency).

Figure 14 - On average, how much time do you spend on data protection matters as a DPO per week? (Source: EY survey)



DPOs' activities require specific expertise and a certain amount of time to conduct the tasks properly, justifying the recommendation expressed in the annex to the Regulation (DPOs should be relieved of other activities). This is consistent with the improvements suggested by respondents (not only DPOs but also data controllers) to allocate more staff / resources to the DPOs so as to support them in their tasks and to avoid delays in the different procedures they are in charge of. The survey shows that the DPOs struggle to perform their tasks in a timely manner: notifications are performed prior to processing in only 50% of cases, the register is systematically updated in slightly less than 50% of cases, and a lack of staff awareness on data protection issues is frequently mentioned. Although not compulsory, the EDPS stresses the importance of appointing a full-time DPO both in the largest institutions and in smaller institutions in order to spread a data protection culture and establish relevant tools.

DPC networks have emerged in large-scale institutions (i.e. in the European Commission, the European Central Bank, the EEAS and the Council). The question arises as to whether to include an explicit reference to the role endorsed by DPCs, acting as intermediaries for DPOs in each division/DG or in a core team (for example, at the ECB).

The analysis of the appropriateness of the level of staff and resources is further detailed in the evaluation question relating to efficiency.

Each institution and body has adopted implementing rules laying down the status, tasks and duties of the DPOs.

Pursuant to Article 24.8, each institution or body must adopt implementing rules relating to the DPO in accordance with the provisions in the Annex. The implementing rules must in particular concern the tasks, duties and powers of the Data Protection Officer.

Implementation and application

Article 24.8 is implemented by the guidelines of the EDPS relating to the "implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8)".[42] In this paper, the EDPS recommends that rules relating to the role of the controllers and rules pursuant to which data subjects may exercise their rights should also be added. These guidelines give full details

[42] https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/10-07-29_Guidelines_DPO_tasks_EN.pdf.

of the information that should be enshrined in these implementing rules (e.g. the tasks, duties and powers of the DPO). The draft implementing rules are submitted to the EDPS for consultation.

The implementing rules are generally adopted or submitted to the EDPS for consultation in the year of, or the year after, the establishment of the EU body.[43]

Pursuant to the bi-annual survey conducted by the EDPS in 2013[44], almost all EU institutions have adopted implementing rules or are in the process of adopting these rules, except for the EUISS.

Conclusion

The obligation to adopt implementing rules has been implemented and applied by almost all EU institutions and bodies.

[43] See https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2014/14-01-24_survey_report_EN.pdf.
[44]

(2) Notification to the Data Protection Officer and Register

Regulatory framework

Pursuant to Article 25 of Regulation (EC) No 45/2001, data controllers must notify data processing operations to the DPOs. This notification covers all data processing operations.

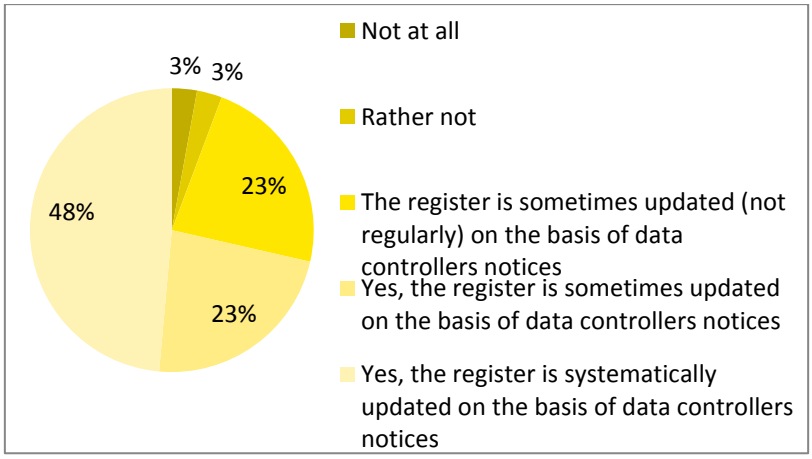
Pursuant to Article 26 of Regulation (EC) No 45/2001, DPOs must keep a register of data processing operations. Pursuant to Article 46 (i), the EDPS must "keep a register of processing operations notified to him or her by virtue of Article 27(2) and registered in accordance with Article 27(5), and provide means of access to the registers kept by the Data Protection Officers under Article 26"

Implementation and Application

The obligation to notify data processing operations is largely implemented and applied by a significant number of EU institutions and bodies, although 17% of the respondents to the survey declared that there were no notification procedures that they were aware of. **It is important to note that this obligation is upon the data controllers, even though they fully rely on the DPOs to complete the notification forms.**

The DPOs must keep a register of all notifications made in accordance with Article 25 (2). The register must be made available to the public via the EDPS. Slightly less than the majority of respondents declare that the register is systematically updated on the basis of data controllers' notifications.

Figure 15 - Within your institution or body, are you confident that the register is up to date? (Source: EY survey)



It appears that keeping a register of notifications has two **main benefits**: (i) raising data controllers' awareness of data protection rules and principles and (ii) keeping the DPO informed of the data processing operations carried out, especially within recently created agencies. Therefore, it seems that eliminating the notification system would significantly raise the risks relating to the protection of personal data and the privacy of individuals.

In terms of application, only half of the DPOs and DPCs are confident that the notifications are performed **prior** to the processing operations. However, DPOs keep a register of the processing operations notified to them. The problem often arises from the fact that data controllers do not perform notifications or notify the DPOs ex post.

Processing operations are recorded in an inventory or register by the DPO. A large majority of institutions keep both a register and an inventory.[45] Even if not directly provided for by the Regulation, inventories are essential compliance tools used by a large majority of EU institutions and bodies. EU institutions and bodies that have implemented such tools present a higher degree of data protection compliance.

Conclusions and suggestions

The DPOs and data controllers emphasised the need for "real compliance" rather than spending time on the drafting of notifications. The issue concerning notifications is twofold: on the one hand, the notifications have been and still are an essential tool for promoting compliance within the EU institutions and bodies, and on the other hand, performing notifications is a significant burden for institutions and bodies.

While the notification of data processing operations has in the past been an important compliance tool , it seems that a level of maturity towards data protection issues has been reached in a large majority of EU institutions and bodies. In order to reduce the administrative burden raised by the notification of data processing operations, **three changes might be undertaken in the light of the "risk-based approach" principle:**

- **Abolish the notification system**

The future Regulation (EC) No 45/2001 could abolish the notification procedure. This option would raise significant risks of decreasing the level of data protection compliance, notably in small EU bodies where the management's awareness on data protection is still low. As a mitigation measure, it might be possible to introduce an obligation for the DPO to keep an inventory of the processing operations.

- **Limit the scope of notifications to risky operations**

Notifications could be limited to data processing operations that present significant privacy-related-risks. This is in line with the "risk-based approach" as the data controllers would be required to perform an assessment of the risks related to the processing before notifying the operation. The main difficulty would be to set the threshold and raise data controllers' awareness on data protection issues.

- **Reduce the range of information required by Article 25.2**

Another possible option would be to reduce the scope of the information required for the notification. Notifications could thus be simplified. Nevertheless, this option would involve the risk of reducing the quality of the notification and reducing the level of compliance with the main data protection principles and rules, insofar as the completion of a notification is assimilated to a check list to verify the fulfilment of requirements.

Moreover, some improvements could be made to the current IT notification system:

- **Improving data privacy management tools for notification**

Finally, several DPOs have highlighted the fact that the available data protection management tools are not suitable and that user-friendly software would facilitate the notification processes.

[45] EDPS, 'Measuring compliance with Regulation (EC) 45/2001 in EU institutions ("Survey 2013")", General Report, Brussels, 24 January 2014.

It follows from the foregoing that the more effective option seems to be the reduction of the scope of the notification (i.e. establishing the responsibility and accountability of the data controllers who will be responsible for assessing the risks) while introducing an obligation for the DPOs to maintain a record of the data processing operations in an inventory, that could also flag those submitted for prior checking. It is crucial to underline the fact that this option would only be effective if an adequate level of maturity towards data protection issues is achieved in EU institutions and bodies.

3.4.2 Contribution of the Regulation to establishing an independent supervisory body

Pursuant to the Recital 5 of Regulation (EC) No 45/2001 and Article 41 of Regulation (EC) No 45/2001, an independent supervisory authority should be established, responsible for monitoring the processing of personal data by the Union institutions and bodies.

Article 41 of the Regulation also specifies the two roles assigned to EDPS including:

- **a supervisory role** : monitoring and ensuring the application of the provisions of this Regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body,
- **an advisory role**: i.e. advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data.

The evaluation team must assess the effectiveness of (1) the establishment of the EDPS, (2) the supervisory role of the EDPS and (3) the advisory role of the EDPS.

(1) Establishment of the EDPS

The creation of the EDPS and appointment of the supervisor and his assistant

Regulatory framework

Regulation (EC) No 45/2001 allows the effective establishment of an independent European Data Protection Authority

Article 8 of the Charter of Fundamental Rights[46] and Article 16 of the Treaty on the Functioning of the European Union[47] provide that compliance with the rules relating to the protection of individuals with regard to the processing of personal data concerning them by Union institutions, bodies, offices and agencies shall be subject to control by an independent authority.

Chapter V of the Regulation describes the general provisions for establishing an independent supervisory authority: the European Data Protection Supervisor. Article 41 of Regulation (EC) No. 45/2001 creates the European Data Protection Supervisor and defines its supervision and advisory role. Article 42 describes the appointment procedure for the Supervisor and the Assistant Supervisor. Article 43 provides that the European Data Protection Supervisor shall be assisted by a Secretariat and lays down a number of provisions concerning staff and budgetary matters. Article 44 relates to the independence of the EDPS and Article 45 to the duty of professional secrecy.

[46] OJ 2012 C 326.
[47] OJ 2012 C 326.

The provisions of Regulation (EC) No. 45/2001 are implemented by two specific texts: the Decision of the European Data Protection Supervisor of 17 December 2012 on the adoption of Rules of Procedure and Decision No. 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties.

Implementation and application

The obligation to establish the EDPS and appoint the Supervisor and Assistant Supervisor was implemented according to defined procedures…

On the basis of Regulation (EC) No 45/2001, notably Articles 41 and 42 as well as on the Decision of the European Parliament and the Council to appoint a European Data Protection Supervisor and an Assistant Supervisor[48], the EDPS was established on 17 January 2004. This Decision appointed Peter Hustinx and Joaquin Bayo Delgado as European Data Protection Supervisor and Assistant Supervisor. Each Supervisor and Assistant Supervisor have been appointed by a Decision of the European Parliament and the Council, following the procedure laid down in Article 42 of Regulation (EC) No. 45/2001. Giovanni Buttarelli (EDPS) and Wojciech Wiewiórowski (Assistant Supervisor) were appointed by a joint decision of the European Parliament and the Council. They were assigned a five year term, and they took office on 4 December 2014.The appointment procedure set out in Article 42 (1) of Regulation (EC) No 45/2001 is composed of two phases:

- First, the European Commission draws up a list of candidates, following a **public call for candidates**[49]. The public call for candidates specifies the job description, the selection and eligibility criteria, the recruitment policy, the appointment procedure and the link to the submission of applications. The European Commission selects the short-listed candidates and publishes the list. If the European Commission is not satisfied with the candidates; then the Commission will close the procedure and open a new call for candidates. Regarding the selection criteria, the European Commission must select candidates *"whose independence is beyond doubt and who are acknowledged as having the experience and skills required to perform the duties of European Data Protection Supervisor, for example because they belong or have belonged to the supervisory authorities referred to in Article 28 of Directive 95/46/EC"*. The specific selection criteria provided for in the calls for public candidates appear to be in compliance with Article 42 (2) and the requirements relating to the EDPS.
- Second, the European Parliament and the Council decide on the appointment on the basis of the Commission shortlist. The Supervisor and his/ her assistant are appointed [50] for a term of five years. The EDPS and his/ her Assistant are eligible for reappointment. Thus, Peter Hustinx was reappointed as EDPS in 2009.[51] This procedure has been applied for each appointment since the creation of the EDPS.

The appointment procedure is implemented and applied.

[48] Decision of the European Parliament and of the Council of 22 December 2003 appointing the independent supervisory body provided in Article 286 of the EC Treaty, 2004/55/EC, published on the Official Journal of the European Union on 17 Jan. 2004

[49] Cf.,
Administrative procedures of the European Commission "European Data Protection Supervisor- Publication of a vacancy notice for the positions of European Data Protection Supervisor and Assistant Supervisor, COM/2013/10338 (2013/C219A/01), published in the Official Journal of the European Union on 31 July 2013.

[50] Cf., Decision of the European Parliament and of the Council of 14 January 2009 appointing the European Data Protection Supervisor and the Assistant Supervisor (2009/30/EC).

[51] Decision of the European Parliament and of the Council of 14 January 2009 appointing the European Data Protection Supervisor and the Assistant Supervisor (2009/30/EC).

...although delays in the procedures should be avoided in order to limit potential criticism
However, Regulation (EC) No 45/2001 does not state any deadlines for the appointment of the EDPS and his/ her Assistant. It should be emphasized that during the last appointment procedure, the appointment of the current EDPS encountered substantial delays as the appointment took more than 16 months (July 2013-December 2014). Peter Hustinx sent several letters on this point to various EU officials and to the Greek Presidency of the Council expressing his concerns about the delays in the selection procedure as the mandate of the EDPS was expiring on 16 January 2014.[52] These concerns are in line with further criticisms expressed by privacy professionals as detailed below. Concerns were also raised by the DPOs as it appears that they faced delays in the processing of the questions they submitted for consultation.

In January 2014, the European Commission considered that none of the candidates were suitable *(see below)*. The European Commission published two new calls for candidates (one for the EDPS and one for the Assistant). In this regard, it is important to note that Article 42 does not explicitly prevent the European Commission from launching two different calls for candidates even though the wording of Article 42 refers to **"a public call for candidates".**

Further, the appointment procedure of the current European Data Protection Supervisor has been subject to criticism involving the level of transparency of the procedure related to the European Commission's discretion in the selection of the candidates. Indeed, according to the criticism raised by privacy professionals[53], the European Commission did not state the reasons why the candidates were not suitable for the EDPS position. The European Commission highlights on this point that there were no formal allegations that the appointment procedure did not comply with the Regulation.

This apparent lack of transparency is nevertheless mitigated by the fact that the public call for candidates further specifies objective selection criteria such as independence, knowledge and experience in data protection. The applicants must submit their Curriculum Vitae and a Motivation Letter.

Moreover, the hearings before the European Parliament are published. Declarations of absence of financial interest are submitted by the Supervisor and published on the website.

In light of Article 42 (2), it shall be assessed whether the appointment procedure guarantees the independence of the EDPS.

Article 42 on appointment states that the EDPS shall fulfil objective criteria such as independence and provides for requirements of experience and skills to perform the duties. As regards the EDPS, the Court stated that the rules set out in Article 42(4) and (5) of Regulation (EC) No. 45/2001 applicable to the circumstances in which the term served by the EDPS may be prematurely brought to an end are strictly limited. These rules allow "the EDPS to serve his/her full term of office, save where this is precluded for overriding and objectively verifiable reasons", and are therefore "an overarching requirement for its independence."[54]

However, it should be emphasized that the fact that the EDPS is proposed by the European Commission and appointed by the Council and the European Parliament may raise independence

[52] Letters from Peter Hustinx to Mr Maroš Šefčovič, Vice-President of the European Commission; Mr Juan Fernando López Aguilar, Chairman of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs and to Ambassador Théodoros N. Sotiropoulos, Permanent Representative of Greece regarding the appointment of the European Data Protection Supervisor and Assistant Supervisor, 7 January 2014.
[53] Cf. Christopher Kuner, "The baffling case of the headless EDPS", published on https://privacyassociation.org/news/a/the-edps-mess/.
[54] Case 288-12, paragraph 56.

issues insofar as these three EU institutions and bodies will be subject to the supervision of the EDPS. However, in the light of the case law of the Court of Justice (as described below), it is unlikely that the appointment procedure would result in "external influence which would be liable to have an effect on their decisions ". Furthermore, this appointment does not appear (in practice) to raise suspicions of partiality of the EDPS (see Commission v Germany[55], paragraph 36).

Article 41 and Article 42 of Regulation (EC) No. 45/2001 are thus implemented and applied. Based on the recent difficulties in appointing a new supervisor for the entity, the appointment procedures should introduce more transparency of the selection process and follow a strict schedule.

Staff and financial matters

Article 43 lists the regulations and general conditions governing the performance of the EDPS's duties, staff and financial resources.

The human and financial resources allow the EDPS to perform its tasks. The EDPS Rules of Procedure specify the rules governing the appointment and tasks of the EDPS Secretariat. This aspect will be further developed in the section relating to the questions evaluating efficiency.

The EDPS is an independent authority

Regulatory framework

Pursuant to Article 44.1 of Regulation (EC) No. 45/2001, the EDPS is an independent authority. Article 44.2 of the Regulation clarifies the concept by stating that the EDPS shall not seek or receive any instructions.[56]

Implementation and application

The establishment of independent supervisory authorities is an essential component of the protection of individuals with regard to the processing of personal data (see notably, Case 288-12, paragraph 48, Case C-518/07 Commission v Germany EU:C:2010:125, paragraph 23, and Case C-614/10 Commission v Austria EU:C:2012:631, paragraph 37).

In Commission v Germany (Case C-518/07, paragraph 30), the Court ruled on the meaning of the expression "with complete independence" by stating that a supervisory authority must be free from any direct or indirect external influence.

It follows from the foregoing that the Supervisory authority must carry out its activities in total independence. This independence includes the obligation to allow the Supervisor to exercise her/her duties without any external influence and to serve his/her full term of office (Case 288-12, paragraph 62). The operational independence to carry out the tasks is not sufficient to protect against any external influence (Case 288-12, paragraph 52). In addition to the criteria of independence required during the appointment procedure *(see above)*, the independence of the EDPS and his or her Assistant is ensured by the implementing acts (e.g. the EDPS has its own budget[57] and the Supervisors' salary, allowances and benefits are paid by the budget of the EDPS directly as per Decision 1247/2002/EC). The Rules of Procedure of the EDPS established in 2012 recall the principle of independence for the advisor (Article 3). Moreover, Article 15 of the EDPS

[55] Case C-518/07 Commission v Germany [2010] ECR I-1885.
[56] See in this regard, Judgment of the Court, 9 March 2010, Case C-518/07.
[57] Article 43(3) of Regulation (EC) No. 45/2001 sets a separate budget for the EDPS, which constitutes a guarantee of independence.

Rules of Procedure also stipulates that the EDPS is an independent expert in the field of data protection, bound by the principles of impartiality, integrity, transparency and pragmatism. Moreover, the EDPS is assisted by an autonomous secretariat.

It appears that the EDPS does not receive any instructions in the performance of its duties, which shows that functional independence is respected.

The EDPS and its staff are effectively subject to a duty of professional secrecy

Regulatory framework

Article 45 states the obligation for the EDPS and his/her staff *to be "subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties".*

Implementation and application

Article 45 is correctly implemented, as the EDPS has adopted an internal procedure for professional secrecy. The obligation is also recalled in several EDPS procedures and documents. For instance, from the Inspection Guidelines[58], *"due to the very nature of EDPS tasks, all members of staff are subject to strict confidentiality obligations, which are further enforced through internal rules and procedures."*

In this regard, the Staff Regulation[59] also states in Article 17 that any official must refrain from unauthorized disclosure of information received in the line of duty. External experts[60] and trainees[61] are also bound by the same confidentiality undertaking.

Staff members sign a **confidentiality declaration** when they join the EDPS. It follows from the foregoing that the EDPS staff is subject to strict confidentiality obligations. However, although the duty of professional secrecy is appropriately applied by the EDPS, the duty of professional secrecy has raised some issues in the course of inspections and legislative consultation:

- During the performance of inspections, some EU institutions and bodies require the inspectors to have security clearance. Security clearance is not mandatory to perform the EDPS tasks, except to access classified information. However, the EDPS remains flexible and tries to select staff members who have security clearances in order to perform these audits.
- Moreover, during the consultation process, it has been shown that institutions can be reluctant to submit to the EDPS legislative proposals impacting data protection or privacy that include highly confidential information.

Several tools and internal procedures allow for a satisfactory level of implementation and application of professional secrecy. However, increased communication on duty of secrecy of EDPS staff towards EU institutions and bodies could facilitate the performance of its duties.

[58] EDPS Inspections Guidelines adopted in November 2013.
[59] Regulation No. 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community (OJ 45 of 14 June 1962, p. 1385) as last amended by Regulation (EU, Euratom) No. 1023/2013 of the European Parliament and of the Council of 22 October 2013 (OJ L 287 of the 29 October 2013, p. 15).
[60] European Data Protection Supervisor decision of 28 April 2009 laying down rules on the secondment of national experts to the EDPS and replacing European Data Protection decisions on the subject.
[61] Decision of the European Data Protection Supervisor (EDPS) of 22 January 2013 concerning the provisions relating to the traineeships programme.

The EDPS publishes an annual report on its activities

Regulatory framework

In accordance with Article 48 (1) of Regulation (EC) No. 45/2001, the EDPS publishes an annual report on its activities and submits the report to the European Parliament, the Council and the European Commission. This rule is recalled in Article 14.1 of the EDPS Rules of Procedure. Pursuant to Article 14.2 of the EDPS Rules of Procedure, the Annual Report shall be submitted and published on the EDPS website no later than 1 July of the following year. Moreover, Article 14.3 states that the EDPS shall consider the comments submitted by EU institutions and bodies "with a view to subsequent possible examination of the report in the European Parliament". Recital 25 also states that the EDPS may publish additional reports on specific subjects.

Implementation and application

Article 48 (1) is effectively implemented and applied by the EDPS.

The first annual report was published on 18 March 2005 and took stock of the first year of existence of the EDPS (from 17 January 2004 to 31 December 2004). Each year, an annual report has been submitted to the European Parliament, the Commission and the Council and published, together with an executive summary and a press release (solely available from 2004-2007). Annual reports are available on the EDPS website in English and French at a minimum.[62] A paper version of the annual report is also available on the EU bookshop free of charge.

The annual reports are an important source of information and communication for the EDPS. The reports are thorough and cover all tasks of the EDPS. The reports outline the experience of the EDPS and tools implemented in order to carry out its mission. Article 48 (2) states that the Supervisor shall forward the report to the other Union institutions and bodies for comments with a view to possible examination of the report in the European Parliament.

In the performance of its activities, the EDPS encourages increased collaboration with institutions and bodies regarding the application and implementation of Regulation (EC) No. 45/2001. It appears that the report is not forwarded to EU institutions and bodies for comments. However, the EDPS is keen to receive feedback and comments from DPOs, DPCs and data controllers.

Annual reports are effectively published and provide a comprehensive overview of the activities of the EDPS. However, discussions on the report with other institutions and bodies have not been mentioned to the evaluator at this stage.

Moreover, the EDPS publishes reports on specific subjects such as strategy.

The EDPS has effectively drafted its Rules of Procedure

Regulatory framework

Regulation (EC) No. 45/2001 requires that the EDPS adopts its own Rules of Procedure.

[62] https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/Publications/AR.

Implementation and application

Under Article 46 (k) of the Regulation, the EDPS adopted its Rules of Procedure in December 2012.[63] These rules take stock of the substantive experience of the EDPS in the field of data protection. This document complements and interprets the rules and principles laid down in Regulation (EC) No. 45/2001. Some Procedures, such as the rules governing cooperation with Data Protection Officers were not foreseen by Regulation (EC) No. 45/2001.

The Rules of Procedure recall the core values and rules governing the general administration of the independent authority (Chapter I- Chapter IV). They also set forth detailed rules for the procedures and rules applied in the performance of the supervisory and consultation tasks (Chapter V, Specific Procedure).

Conclusions and recommendations on the general provisions related to the establishment of EDPS

Regulation (EC) No. 45/2001 achieved its objective to create an independent supervisory authority in order to monitor and ensure application of Regulation (EC) No. 45/2001. The implementation and application of the general provisions for the establishment of the EDPS are effective. At this stage, it is possible to make the following recommendations:

(1) Setting deadlines for the appointment procedure could reduce adverse effects caused by delays in the appointment;

(2) More transparency could be introduced in the supervisor selection procedure;

(3) Better communication on professional secrecy would enable the EDPS to perform its tasks more effectively.

[63] Decision of the European Data Protection Supervisor of 17 December 2012 on the adoption of the Rules of Procedure.

(2) Effectiveness of the Supervisory power

This section aims to assess how and to what extent the EDPS carries out its supervision and monitoring tasks.

Pursuant to Article 46 (c) of Regulation (EC) No. 45/2001, the EDPS monitors the processing of personal data carried out by EU institutions and bodies (except the Court of Justice of the European Union acting in its judicial capacity) and ensures compliance with Regulation (EC) No. 45/2001. The tasks of monitoring and supervising the implementation and application of Regulation (EC) No. 45/2001 cover more than 60 institutions and bodies. It has become clear from our interviews with the EDPS that the Court of Justice has a broader interpretation of its judicial capacity than the one the EDPS advocates, which has raised some issues relating to the publication of the names of applicants in decisions.

Over time, the EDPS has developed other monitoring and compliance tools, namely (i) the biannual monitoring survey, (ii) guidelines and (iii) compliance visits (Article 37 of the EDPS Rules of Procedure (visits) that allow effective application of the supervision powers. Compliance visits and surveys are tools developed by the EDPS which are not expressly provided for in Regulation (EC) No. 45/2001. Further, the EDPS also undertakes initiatives to raise awareness a by means of trainings and workshops.

The promotion of constructive dialogue with the DPOs is also a means to foster compliance (attendance at DPO network meetings, bilateral meetings, hotline for DPOs, written consultations). In addition, the EDPS monitors technological developments impacting data protection.

The EDPS performs prior checks of risky data protection processing

Regulatory framework

This section aims to assess how and to what extent the EDPS carries out prior checks (Article 46(j) and Article 27 of Regulation (EC) No 45/2001).

Pursuant to Article 27 of Regulation (EC) No. 45/2001, data processing operations likely to present specific risks to the rights and freedoms of data subjects given their nature, their scope or their purpose shall be subject to prior checking by the EDPS.

The following operations are likely to present such risks (Article 27.2):

"a) processing of data relating to health and to suspected offences, offences, criminal convictions or security measures;

(b) processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct;

(c) processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes;

(d) processing operations for the purpose of excluding individuals from a right, benefit or contract."

"The EDPS also considers that in certain cases, processing of biometric data and monitoring of electronic communications can pose specific risks and should therefore be prior checked."[64]

[64] https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/Supervision/priorchecking.

Implementation and application

Pursuant to Articles 27 and 46 of Regulation (EC) No. 45/2001, the EDPS carries out a prior check of notification received. These provisions of Regulation (EC) No. 45/2001 are effectively implemented by the EDPS Rules of Procedure, which supplement and interpret the prior check procedure laid down by Regulation (EC) No 45/2001 (Articles 19 to 23). The position paper on "Monitoring and Ensuring Compliance with Regulation (EC) 45/2001, 13 December 2010" also supplements the applicable rules and procedures. Moreover, 74% of EU institutions and bodies consulted state that procedures relating to the notification of processing operations subject to prior checking have been adopted.

Over time, the EDPS has set up and applied a prior check procedure.

The EDPS carries out prior checks on all notifications sent by the DPOs. The notifications are drafted by the DPOs on the basis of a form available on the DPO Corner. The DPOs also consult the EDPS in case there is a doubt as to the need for prior checking. These consultations allowed the EDPS to interpret the cases stipulated by Article 27 and gradually to set up the criteria for determining which processing operations are subject to prior checking.

In practical terms most processing submitted for prior checking falls under Article 27.2 of Regulation (EC) 45/2001. However, certain processing operations relating to cloud computing and RFID are also submitted for prior checking. Nonetheless, it should be emphasized that these operations are technologies/tools and not processing purposes. They may easily be linked to one of the operations set out in Article 27. A new technology is not a sufficient criterion in itself to be subject to prior checking. If significant security and/or data-protection risks were to be identified, the EDPS would conduct a prior check.

The EDPS pointed out that there is an issue of translation in Article 27.2, as "*mesures de suretés*" were translated by "security measures".

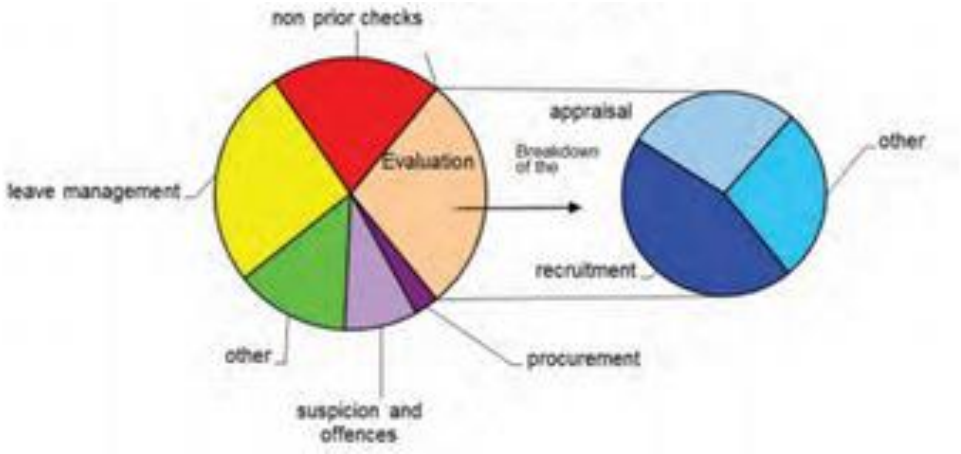
Article 27 2 (a), (b) and (d) are referred to on a regular basis. Article 27.2. (c) is rarely used (one prior check performed).

The EDPS has narrowed the scope of application of Article 27. 2 (a) relating *inter alia* to health data by stating that the processing of health data must play a key role.

The wording of Article 27 is unclear as to whether the list of Article 27.2 is exhaustive, notably with regard to the wording of Article 27.5.

The figure below illustrates the main prior check issues in 2013.

Figure 16 – 2013 opinions per main prior check category (Source: EDPS 2013 annual report)



The findings of the EDPS are enshrined in prior check opinions which are presented to the data controller and/or to the DPO of the institution or body concerned. The opinions usually indicate the set of recommendations that need to be adopted by the institution or body in order to comply with the legal requirements. The EDPS ensures follow-up on the recommendations and makes sure that the institution or body complies with the opinion.

Pursuant to Article 27, the opinion of the EDPS should be delivered prior to the start of the data processing operation ("*ex ante* prior check"). However, since some processing operations were carried out before the appointment of the EDPS, the Supervisor also carries out prior checking afterwards ("*ex post* prior check").

The EDPS shall deliver his/her opinion within two months. This period can be extended for a period of two months. If the EDPS has not delivered a reply by the end of the two-month period, it is deemed to be favourable.

Initially, the EDPS applied this deadline for both *ex ante* and *ex post* prior checks. This deadline put a strain on the EDPS. Since the end of 2013, the EDPS has changed its doctrine and considers that it is not bound by this deadline when the notification comes after the start of the processing operation. In this case, the institution or body has started the processing operation at its own risk. This practice has raised criticism from DPOs, who in practice need to wait for long periods before being provided with the opinion. According to the interviews performed, some prior check procedures are in progress for years. The perception of DPOs and data controllers on this point is that the practices of the EDPS are not in line with the decision-making processes.

In the event the notification identifies a violation of any provision of Regulation (EC) No. 45/2001, the EDPS make proposals to avoid such a breach. The data controller shall take the remarks of the EDPS into consideration.

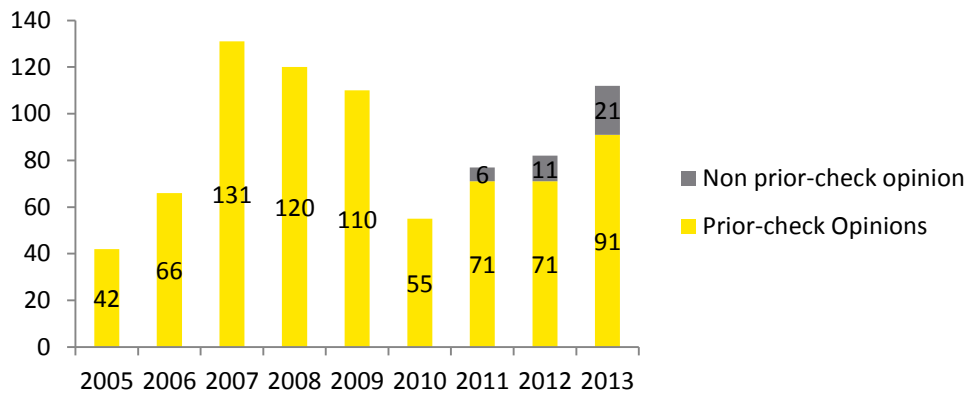
The EDPS follows up on the opinions although this is not expressly provided for by Regulation (EC) No. 45/2001. This appears to be an efficient means to enhance long-term compliance.

The EDPS keeps a register of all notifications of processing operations.

Prior checks previously represented 70% of the EDPS supervisory activity, and there was a need to increase the efficiency of prior check activities. The number of prior checks performed each year remains significant. The relatively high number for 2013 corresponds to the deadline of June 2013

to perform *ex post* prior checks, when the number of prior check notifications received by EDPS increased.

Figure 17 - Number of prior check opinions delivered by EDPS per year (source: 2013 EDPS annual report)



EDPS' effectiveness in performing prior checks has increased over time. This increased effectiveness had several causes:

- **The EDPS has gained maturity**. The EDPS has learned a lot about the application and implementation of Regulation (EC) No. 45/2001. A level of maturity has been achieved with regard to the processing of prior check notifications. The EDPS focuses on the accountability of institutions and bodies. Prior checking was an important tool to understand the constraints of EU institutions and bodies and to provide guidance to the EU institutions and bodies.
- **The EDPS has adopted thematic guidelines in order to facilitate the processing of prior check notifications starting in 2010.** These guidelines serve as a reference document against which agencies can measure their current practices. If a body has complied with the recommendations made by the EDPS in previous guidelines, in theory there is no need for prior checking (cf. the pilot case of EDPS Video-surveillance Guidelines of 17 March 2010). In the event the processing operation submitted does not fully comply with the previous recommendations, the EDPS provides an opinion limited to practices which are not in line with the guidelines. These issues include staff recruitment, health data at work, administrative inquiries and disciplinary proceedings, tasks, duties and powers of the DPO, video-surveillance, anti-harassment procedures and staff evaluations.[65]

- On the basis of Article 27.3, the EDPS has narrowed down the scope of application of prior checking and has simplified the opinion submitted after prior check, focusing on specific compliance issues. In this respect, Regulation (EC) No. 45/2001 does not provide any indication as to the form that the prior check should take. The wording of Regulation (EC) No. 45/2001 allows valuable flexibility for the EDPS to carry out prior checks. The general wording of Regulation (EC) No. 45/2001 also leaves room for interpretation of the operations subject to prior checking pursuant to Article 27 of Regulation (EC) No. 45/2001. For example, Article 27 b) regarding "operations intended to evaluate personal aspects relating to the data subject" was broadly interpreted at first and included tele-working. As for the form taken by opinions, the EDPS used to issue very thorough and comprehensive opinions which analyzed the data processing operations in light of every data protection

[65] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Factsheets/Factsheet_3_EN.pdf.

principle and rule. Over time, the EDPS allowed itself more flexibility. The EDPS aims to address only non-compliance issues and draft the related recommendations. In this regard, the EDPS was initially exhaustive in its recommendations; now it uses its best efforts to be selective and to prioritize the recommendations drawn up in the prior check opinions.

- **Follow-up on the recommendations made in opinions allows the EDPS to take stock of its previous experience and to build its guidelines.** Following up on the opinions is also an indicator of long term compliance.
- **Most of the vast backlog of ex-post prior checking** for processing operations has been notified to the EDPS.

Although EDPS has made substantial improvements over time, some drawbacks to the prior checks can still be observed.

- The wording of Article 27 is unclear as to whether the list that appears in paragraph 2 is exhaustive (in the light of Article 27.5).
- **The scope of application of Article 27 (1) and (2) appears to be unclear for some EU institutions and bodies.** DPOs (especially the newly appointed), when they take up their duties, tend to submit numerous notifications for prior checking even though the processing operations do not fall within the scope of Article 27 (2). Moreover, consultation of DPOs also relates to the interpretation of the general principle enshrined in Article 27(1). A significant number of prior checking notifications are not admissible but the EDPS needs to instruct the notification to reach this conclusion.
- **Furthermore, criticism has been raised concerning the opinion timeframes and their failure to reflect operational needs.** The DPOs and data controllers have highlighted significant delays in the processing of prior check notifications. In this regard, stakeholders sometimes have the perception that the EDPS occasionally asks questions solely for the purpose of postponing the deadline. Moreover, data controllers often provide *ex post* notification to the DPOs, notably in recently-created agencies. In these cases, the deadlines can be very long (up to two or three years). These delays are difficult to reconcile with operational needs and decision-making processes. Further, the opinions are sometimes perceived as too "legalistic" and remote from the operational activities of the institution or body concerned.

Conclusions and recommendations

Prior checks are implemented and performed effectively by the EDPS. In light of the amount of time spent on this activity by EDPS staff, the EDPS has developed several tools to facilitate and accelerate the performance of prior checks.

It follows from the foregoing that Article 27 and 46 (j) of Regulation (EC) No. 45/2001 are effectively implemented and applied. However, some further improvements could be considered (and/or are already planned by the EDPS).

- **Increased communication on prior checking is necessary.** DPOs and data controllers focus their efforts on prior checking in order to prove compliance with Regulation (EC) No. 45/2001. In light of this "risk-based approach", emphasis should be put on the implementation of the opinions and the recommendations and thus on compliance with the data protection principles and rights of data subject enshrined in Regulation (EC) 45/2001. Prior checking should only be considered as one aspect of compliance.
- **The performance of prior check is time consuming for the EDPS and for the DPOs in charge of drafting the notification. The preliminary analysis of eligibility for prior**

checking contributes to the heavy burden triggered by the prior check procedure. Further clarification of the scope of prior checking could help to reduce unfounded notifications. This burden prevents the EDPS from focusing on the performance of prior check itself. Further to the adoption of guidelines (see below), a dialogue should be engaged with EU institutions and bodies to reduce the administrative burden linked to prior checking. This will also allow the EDPS to respond to *ex ante* and *ex post* prior checks in a timely manner.

The implementation of Regulation (EC) No. 45/2001 should be further improved by the upcoming publication of prior check guidelines.

- In the draft guidelines relating to the EDPS, it is important to take stock of the prior check exercise (in particular, opinions delivered) and draw up the criteria for operations that fall under the scope of prior checking. This will reduce the number of prior check notifications submitted by the DPOs which fall outside the scope of Article 27 as interpreted by the EDPS.
- Opinions should be more operational and appropriate to data controller's needs.
- It will also be important to highlight vis-à-vis DPOs and data controllers that prior checking is an effective compliance tool but is only part of the requirements for compliance with the principles and rules enshrined in Regulation (EC) No. 45/2001. In this regard, focus should be put on accountability and pragmatism.
- The adoption of thematic guidelines to facilitate prior checking should be further developed as it allows increased efficiency.

The EDPS hears and investigates complaints

Regulatory framework

Article 32, 33, Article 46 (a) and (b)

Pursuant to Article 46 of Regulation (EC) No. 45/2001, the EDPS shall "hear and investigate complaints" as well as "conduct inquiries either on his or her own initiative or on the basis of complaints".

Implementation and application

Article 46 (a) and (b) of Regulation (EC) No. 45/2001 are effectively implemented.

The EDPS has established internal (internal manual for handling complaints and statistical tool to monitor complaint-related activity) and external procedures to handle complaints. The EDPS handles complaints according to the Rules of Procedure and following a complaints case manual. According to the 2013 Annual Report, a statistical tool designed notably to monitor specific cases has been developed. Moreover, information on the procedure to file a complaint is available on the website. The procedures are efficient and regularly updated and meet day to day operational needs.

The obligation to hear and investigate complaints has been implemented by Article 31 to 35 of the EDPS Rules of Procedure and has been interpreted by the position paper on "Monitoring and Ensuring Compliance with Regulation (EC) 45/2001, 13 December 2010". Moreover, the EDPS has adopted an internal manual for handling complaints[66] and an online form has been published on the EDPS website. 57% of the EU institutions and bodies consulted have a procedure relating to the handling of complaints.

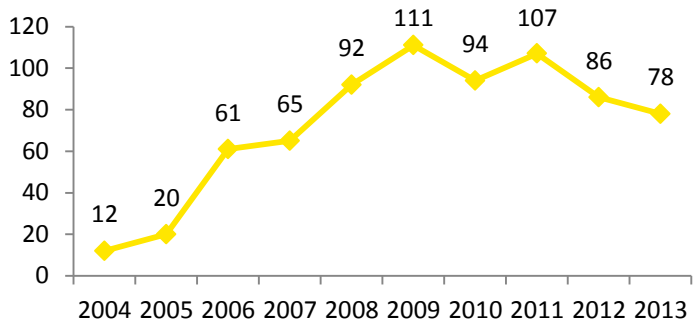
[66] This manual has not been disclosed to the evaluation team.

The EDPS effectively hears and investigates complaints.

The EDPS makes a distinction between complaints lodged by individuals (Article 32) and complaints by Union staff (Article 33). While any individual may make a complaint to the EDPS about an alleged violation of his/her rights to protect his/her personal data, it must be emphasized that EU staff may complain about any alleged violation of data protection rules, whether he or she is directly affected or not. The EDPS may also decide to launch inquiries on its own initiative even if a complaint is not relevant. **The EDPS may only investigate complaints submitted** by natural persons and which relate to the processing of personal information carried out by an EU institution or body. Complainants must identify themselves since anonymous complaints are not admissible.[67]If the complainant requests anonymity from the institution, the DPO or third party involved, he or she must explain the reasons therefor.

The number of complaints gradually increased until 2009.

Figure 18 - Number of complaints per year (source: EDPS 2013 annual report)



As a matter of principle, the EDPS guarantees the confidentiality of complaints, unless the EDPS is under a legal obligation to disclose information, for example within the scope of Regulation (EC) No. 1049/2001 (**Articles 33.3 and Articles 33.4 of the Rules of Procedure).**

The applicant may lodge a complaint with the EDPS by filling in a complaint submission form. Filing a complaint is free of charge. The EDPS examines all the complaints received. A preliminary examination is performed in order to analyze the admissibility of the complaint (i.e. whether a complaint meets the conditions for further inquiry).

If a complaint concerns a matter falling outside the EDPS' competence, it will be declared inadmissible. The complainant will be informed of this. If the case falls within the competence or jurisdiction of another body such as the ombudsman, the Court of Justice or a national data protection authority, the EDPS will inform the complainant. It has been stated that the EDPS does not directly refer the case to the competent body.

If a complaint is found to be admissible, the EDPS will carry out an inquiry to the extent which itfinds appropriate. The decision is disclosed to the complainant as well as to the data controller (who is responsible for processing the data).

Furthermore, in theory, the complaint will also be deemed inadmissible if the complainant has not first contacted the institution of body concerned in order to remedy the breach (unless the complainant has sufficient reasons for not doing so). The Rules of Procedure adopted by the EDPS also set a time limit for lodging complaint: in principle, a complaint must be lodged within two years of the date on which the complainant had knowledge of the facts on which it is based (Article 32.3).

[67] EDPS Annual report 2013.

Article 46 (a) of Regulation (EC) No. 45/2001 states that the EDPS shall *"hear and investigate complaints, and inform the data subject of the outcome within a reasonable period"*. The EDPS Rules of Procedure lay down the six-month deadline for the EDPS to respond to the complaint (Article 34(3) of the EDPS Rules of Procedure).

In the EDPS Rules of Procedure the EDPS sets out the criteria that need to be taken into account in the handling of a complaint (i.e. the nature and gravity of the alleged breach of data protection rules; the importance of the prejudice that one or more data subjects have or may have suffered as result of the violation; the potential overall importance of the case, also in relation to the other public and/or private interests involved; the likelihood of establishing that the infringement has occurred; the exact date when events happened, any conduct which is no longer yielding effects, the removal of these effects or an appropriate guarantee of such a removal.)

In some cases, the complaint results in an amicable solution without the need to adopt a formal decision. If an amicable settlement could not be reached, the EDPS adopts a formal decision. The EDPS has never sued an institution or body as a result of a complaint because according to the EDPS, the EU institution or body has always complied with the final decision adopted by the EDPS. Sometimes, the case may escalate to upper management and meetings may be organized.

Regarding the range of powers conferred upon the EDPS by Regulation (EC) No. 45/2001, the EDPS considers that the its supervisory powers are extensive; ranging from simply giving advice to data subjects to warning or admonishing the controller (Article 47 of Regulation (EC) No. 45/2001), to imposing a ban on the processing or referring the matter to the Court of Justice. Please also refer to the case study and the evaluation of the sanctions.

The EDPS' decision on complaints may be subject to review. It should be noted that any interested party can ask the EDPS for a review of itsdecision. The EDPS stated that of 32 review requests, only one had sufficient grounds. The review must be lodged within one month of the date of receipt of the decision. Concerned parties may also directly challenge the decision before the Court of Justice of the European Union in accordance with Article 263 of the TFEU.

The EDPS has established several filters to reduce the number of complaints that do not merit an inquiry or an in-depth examination by the EDPS, as shown herebelow.

- **Awareness. Better awareness and communication on the EDPS' competence, especially on the EDPS website. The EDPS website also explains the procedure and lists the documents and information that need to be provided in order to avoid delays in the handling of complaints.** The EDPS does not examine cases falling outside its competence and where applicable names the competent authority to handle the complaints. Complaints falling outside the competence of the EDPS but within the competence of another institution or body or national data protection authority may be referred directly to the competent authority unless it requires disproportionate administrative burden.
- **Relevance.** At the preliminary examination phase, the EDPS examines whether the complaint addresses facts "which are manifestly insignificant, or issues the investigation of which would require disproportionate efforts". In such cases, the complaint will not be investigated further.
- **Standardization. The complaint form has proven effectiveness.** The EDPS established a complaint submission form for individuals to lodge complaints. This form can be filled in electronically. This form aims to speed up the process and reduce the number of inadmissible complaints. It is the first filter layer, as the complainant must state the legal basis of the complaints. In addition, it provides the EDPS with the relevant information in order to process the complaints efficiently.

- **Subsidiarity. The complaint should first be submitted to the institution or body concerned before lodging the complaint with the EDPS.** The EDPS recommends that applicants first contact the institution or body concerned (the DPO or the data controller) before submitting the complaint to the EDPS. Nevertheless, complaints can be lodged directly with the EDPS should this be deemed necessary.

Conclusions

The obligation to hear and investigate complaints is effectively implemented and applied thanks to the adoption of procedures to reduce the burden for the EDPS. Some concerns have been raised in certain cases by data subjects who are not satisfied with the processing of the complaints by the DPOs and the EDPS. These concerns are more linked to the follow up by the controller than the processing by the EDPS or the DPO.

The EDPS effectively conducts inspections but the procedure and the number of inspections performed could be improved

Regulatory framework

Relevant provisions: Article 46 (b), 46 (c) and 47(2) of Regulation (EC) No. 45/2001, Articles 1, 17 and 6 of the EDPS Rules of Procedure

Pursuant to Article 46 (b) of Regulation (EC) No. 45/2001, the EDPS may decide to conduct inspections at its own initiative or following a complaint, within the powers conferred by Article 47 (2). The performance of inspections is a tool to ensure compliance with Regulation (EC) No. 45/2001, notably by identifying shortcomings and appropriate solutions.

Implementation and application

Articles 46 (b) and 47 (2) of Regulation (EC) No. 45/2001 have been implemented by the EDPS Rules of Procedures and the EDPS Policy Paper on Inspections[68] that specify the circumstances under which the EDPS may decide to launch inspections.

The EDPS Inspections Policy Paper should be read in the light of Article 36 of the EDPS Rules of Procedure that describes the circumstances under which inspections shall be carried out and the procedure to be followed.

The risk assessment tool used to perform inspections is described in the internal manual offering guidance to EDPS staff who handles inspections, which was compiled on the basis of experience in previous inspections.[69]

Articles 46 (b) and 47 (2) of Regulation (EC) No 45/2001 are applied.

According to the EDPS, the institutions/bodies to be investigated are chosen on the basis of objective criteria, for example: social factors, categories of the data processed (sensitive data, etc.) or existence of transfer of personal data to third countries that could trigger higher risks. The number of complaints may also be relevant information because it creates suspicion of lack of compliance.

[68] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04_EDPS_Inspection_guidelines_EN.pdf.
[69] This document has not been disclosed.

Inspections are part of Annual Inspection Planning (which starts in October the year preceding the inspection); it is based on the meeting dates and the schedules of team leaders and team members selected for the inspection. The team is built on a case-by-case basis and a team leader is appointed by the Head of the Supervision and Enforcement unit. More generally, inspections are part of the EDPS' overall strategy.. Inspections are carried out when on-the-spot verifications are considered to be necessary. Inspectors collect information and assess the evidence.

Three different types of inspections are performed by the EDPS: general inspections, targeted inspections and inspections of large-scale IT systems.

The inspections are always announced to the institutions and bodies, at least four weeks prior to the inspection date. Therefore, an appointment letter must be sent one month before the meeting. The EDPS does not carry out inspections without prior notice.

Prior to the inspection, the EDPS may ask for information and documents (preparatory paperwork and research is performed). The methods are specific to each case and the range of tasks performed by the EDPS during inspection is wide: having a look at documents, conducting interviews, organizing meetings, etc..

The inspection must be carried out after the adoption of a formal decision and a formal mandate. These documents are delivered to the institution or body. The inspection begins with a kick off meeting during which the EDPS explains the purpose and the scope of the inspection.

After the "on-the-spot" activities, the EDPS provides the inspected institution with a final report including feedback, based on all the information and documents collected. This inspection report is provided solely to the inspected institution or body. A summary of the inspection report is made public and there is a reference made in the annual report. It was underlined several times during the interview that the aim of the inspections is to promote compliance. Therefore, it is not a "naming and shaming" tool (in comparison with the general biannual survey published by the EDPS (presented below)).

Even though not explicitly provided for by Regulation (EC) No. 45/2001, the EDPS follows up on the inspections and monitors the implementation of the recommendations drawn up in the inspection report.

Although enforcement actions could be undertaken, the EDPS specified that most of the time the recommendations are an effective means of ensuring compliance. According to the EDPS, the application of sanctions is not necessary as the report is usually followed by implementation of the recommendations and the follow up period closes within a very reasonable time. The DPOs have highlighted that the use of the enforcement powers of the EDPS is not sufficiently deterrent to engage the management level of EU institutions and bodies towards compliance (Cf. above effectiveness of sanctions).

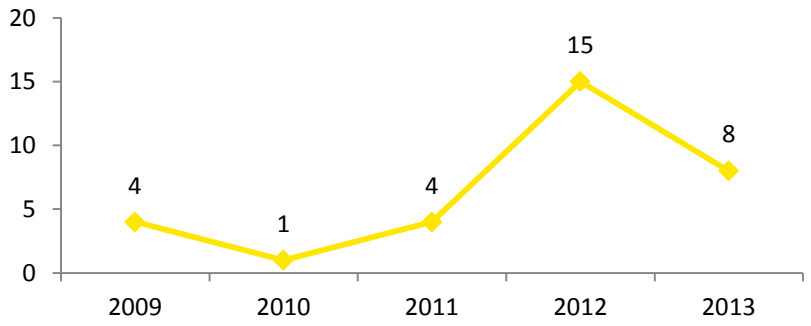
The duration of "on the spot" verification varies from one to four days. The duration of the whole procedure (preparation and follow up) is longer and varies according to the case.

In order to effectively raise awareness within institutions and increase collaboration with institutions and bodies, the time the EDPS dedicates to inspections increased. The EDPS has given priority to the performance of inspections in the light of available resources. Duration depends on inspections and what inspectors seek to investigate. It is difficult to give any kind of working estimate; duration depends on the body and the complexity of the issue as well as on the scope of the inspection. For example, as regards the inspection of CCTV devices, the scope was

limited to providing aspects to the general public and to Brussels-based institutions or bodies. Consequently, the amount of time spent was quite limited.

The figure below illustrates the emphasis placed on the performance of inspections in recent years.

Figure 19 - Number of inspections performed by EDPS from 2009 to 2013 (source: EDPS annual reports)



Efficiency has increased over time thanks to the adoption of revised workflows and procedures (in particular, the internal manual). The creation of the internal manual has proven to be an effective means to rationalize procedures. For instance, the internal manual provides for specific deadlines to meet. This motivates staff to stick to the deadlines. As with any audit tool, the existence of detailed workflow and processes is a cornerstone for the performance of inspections..

Relationships between the EDPS and DPOs during inspections are constructive and allow for increased effectiveness. The EDPS highlighted the extensive cooperation between the EDPS and the DPOs. The inspection can be a good time for training measures. The EDPS relies significantly on DPOs for practical arrangements (identifying people to meet, scheduling interviews, making information available, etc.). Therefore, cooperation is crucial at each stage of the inspection procedure (preliminary work, on-the-spot verification and follow-up).

Inspections generate a great deal of work for the DPOs. They are independent so their presence during the inspection is not mandatory, but they usually attend the meetings.

Nevertheless, major criticisms have been raised by DPOs who highlight that:

- the inspections are remote from the operational activities of the EU institution or body at issue (i.e. the EDPS does not have the appropriate work-field experience) ;
- the follow-up is not performed in a timely manner (sometimes two years after the inspections);
- the number of inspections is too limited;
- the inspections are closer to audits than to real inspections.

Conclusions and recommendations

Inspections are effectively implemented and applied, and the EDPS has decided to increase the time dedicated to inspections on the basis of the positive results observed.

The main challenges/drawbacks regarding inspections are the perception of EU institutions and bodies of this activity and EDPS resources dedicated to it.

- **Perception of EU institutions/bodies**

Inspections are perceived as retaliation measures by numerous EU institutions or bodies. It became clear during the consultation that some data controllers perceive the EDPS to be unaware of their operational constraints and environment. Some EU institutions and bodies consider EDPS' approach to be "bureaucratic", "legalistic" and a "source of unjustified stress". However, it should be underlined that for the EDPS inspection is an efficient compliance mechanism that should not be perceived as a punishment. The perception of inspections is a challenge for the EDPS.

Nonetheless, it must be emphasized that inspections are also powerful enforcement mechanisms that are increasingly being used to foster compliance across EU institutions and bodies.

- **Better communication and awareness raising**

More inspections could be carried out in order to raise awareness of data protection compliance, notably among management. It should be noted that the perception of inspections usually changes after the performance of an inspection, on the basis of the interviews with the EDPS. This is reflected by the fact that some feedback from EU institutions and bodies becomes positive after the inspection.

- **Communication will allow DPOs and data controllers to more easily accept the mandate of the EDPS, notably with regard to professional secrecy.** The EDPS staff is subject to strict confidentiality obligations. Staff members sign a confidentiality declaration when they join the EDPS. Some EU institutions and bodies require the inspectors to have a security clearance in order to access classified information. Security clearance is not mandatory to perform the EDPS tasks. However, the EDPS remains flexible and tries to select staff members who have security clearances to perform these audits.

As the number of inspections is increasing over time, the limited EDPS resources dedicated to inspections impede the applicability of the Regulation. It should be highlighted that in light of the future amendment of the Regulation, increased accountability should be linked to an increase of the number of inspections.

The EDPS is informed of and oversees the consultation for administrative measures

Regulatory framework

Relevant provisions: Article 28.1 and 46 (d) of Regulation (EC) No. 45/2001 and Articles 24 and 25 of the EDPS Rules of Procedure

Pursuant to Article 28.1 of Regulation (EC) No. 45/2001, *"the Community institutions and bodies shall inform the European Data Protection Supervisor when drawing up administrative measures relating to the processing of personal data involving a Community institution or body alone or jointly with others."* Pursuant to Article 46 d), the EDPS *"advise(s) all Community institutions and bodies, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of personal data, in particular before they draw up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of personal data "*.

Implementation and application

Article 28 (1) is effectively implemented by the EDPS Rules of Procedure (section 3) and the Policy on Consultations in the field of supervision and enforcement.

Although part of the EDPS' consultation powers are set forth in Regulation (EC) No. 45/2001, Article 24.3 of the EDPS Rules of Procedure states that the EDPS advises on the consultations first performed by the DPOs. Therefore, this task is part of the supervisory powers of the EDPS.

Article 28 (1) is effectively applied by the EDPS

Institutions and bodies must inform the EDPS when they take administrative measures such as implementing rules concerning the DPOs (Article 24.8 of Regulation (EC) No. 45/2001)and internal administrative rules relating to the processing of personal data (e.g. use of e-mail, e-monitoring, archiving, etc.) to allow the EDPS to provide any advice that might be deemed necessary. In this regard, the EDPS may adopt opinions on administrative measures related to data protection adopted by European institutions and bodies.

This provision has been interpreted and applied by the EDPS as an EDPS obligation to oversee the consultation performed by the DPOs. Indeed, although the EDPS encourages institutions and bodies to inform and consult the EDPS, the EDPS advises data controllers to consult their DPO as a first step. The matter can be submitted to the EDPS for consultation thereafter in cases of complexity or for subjects concerning appreciable risks to the rights and freedoms of the data subjects.[70]

The wording of Article 28.1 has been under discussion. The DPO network pointed out that Article 28.1 should say "consult" instead of "inform" as the obligation relates to the section of the Regulation dedicated to "Consultations». In this regard, the term "inform" seems closer to the practices of the EDPS acting to oversee the work performed by the DPOs and therefore, more appropriate than the term "consult". Stakeholders have underlined that the relationship between Article 28(1) and the prior checking mechanism may be unclear as the EDPS does not seem to accept Article 28(1) consultations where a subsequent prior checking will be necessary.

Effectiveness has increased through the building of guidelines by the EDPS and the reduction of the workload. According to the EDPS, DPOs and data controllers should verify whether the EDPS has already given advice on a similar or analogous subject. Should this be the case, the same recommendations (i.e. recommendations that the EDPS has already provided for same or similar subject) shall apply. In addition, the EDPS publishes opinions that provide novel interpretations of points of law that impact new technologies, or that are considered to be particularly relevant. Moreover, as a first step, administrative measures will be submitted to the DPOs. Only if the matter may not be resolved at the level of DPOs will it be escalated to the level of the EDPS. The DPO plays a key role. This allows time savings.

Conclusion

The term "inform" used in Article 28.1 is appropriate in the light of the current application of this provision by the EDPS.

The EDPS has effectively implemented and applied Article 28.1 of the Regulation. The EDPS has gained efficiency by intervening subsequent to the DPOs where its experience and knowledge in the field of data protection are required.

[70] https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Papers/PolicyP/2012-11-23_Policy_on_consultations_EN.pdf/

The EDPS also monitors and supervises the application of Regulation (EC) No. 45/2001 by conducting (i) biannual general surveys and (ii) compliance visits.

Although not specifically provided for in Regulation (EC) No. 45/2001, in the course of its supervision activities the EDPS has initiated two activities to ensure the compliance of institutions and bodies with the Regulation:

(i) Biannual general surveys;

(ii) Compliance visits.

(i) General monitoring and reporting surveys

Regulatory framework

This activity is not expressly provided for in Regulation (EC) No. 45/2001 but its legal basis can be found in Article 41(2) of the Regulation.

Implementation and Application

The EDPS carries out general surveys monitoring and reporting on the data protection activities of the EU institutions and bodies. So far, the EDPS has performed four general overview exercises and a survey on the status of Data Protection Officers (DPO). This monitoring tool allows the EDPS to identify shortcomings and to plan for the next steps towards compliance and targeted actions.

"Naming and Shaming" Tool

The general survey has proven to be an effective compliance tool by benchmarking the practices of the EU institutions and bodies and comparing them to their peers (i.e. analogous institutions or bodies).

A survey on the function of DPCs among institutions was also performed.

(ii) Compliance visits

Regulatory framework

Compliance visits are not directly provided for by Regulation (EC) No. 45/2001 but this task is detailed in the EDPS Rules of Procedure (Article 37).

Implementation and Application

Compliance visits are visits from the EDPS management to the management of an EU institution or body in order to foster compliance and increase knowledge. This is an open discussion which aims to "engage the commitment of the senior management of an institution or agency to comply with the Regulations" [71]controllers who have been identified by the EDPS as lacking maturity.

According to the EDPS, this exercise is an effective means to promote compliance. In the 2013 General Survey, the EDPS stated that *'"in a nutshell, these visits are "visits with courtesy, but not courtesy visits".*[72]

[71] EDPS Annual Report 2013, page 35.

[72] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2014/14-01-24_survey_report_EN.pdf.

The EDPS monitors the development of technologies and develops guidelines for them.

Regulatory framework

Pursuant to Article 46 (e) of Regulation (EC) No. 45/2001, the EDPS performs ongoing monitoring of the development of technologies that may affect the protection of personal information.

Implementation and Application

The EDPS implemented this obligation in Article 38 of the EDPS Rules of Procedure.

The EDPS effectively fulfils this obligation. The EDPS collects and uses publicly available information on new technology developments (white papers, conference papers, etc.) and meets with industry constructors, experts and technology professionals. As part of its technology monitoring activities, the EDPS checks the claims made and risks identified by the technology community concerning specific technologies and personal data protection. The EDPS ensures that all points of views are analysed, taken into consideration and put in perspective with technological facts in order to eliminate any misunderstanding. At the end of this process the EDPS delivers its recommendations and guidelines in the technical area.

The EDPS is currently working on developing guidelines for data protection for mobile technologies, cloud computing and websites.

Considering the rapid evolution in technology developments, the DPOs need responsiveness, as the guidelines are essential guidance in their day-to-day work.

Conclusion on the oversight activity of the EDPS

It follows from the foregoing that Regulation (EC) No. 45/2001 achieves its objective to confer upon the EDPS the task of monitoring and ensuring the application of Regulation (EC) No. 45/2001, but further improvements should be considered.

Over time, the EDPS has implemented and applied its obligations under the Regulation. Moreover, the Supervision and Enforcement unit has established efficient and powerful tools to oversee the application of the Regulation. This is particularly true for the processing of complaints and prior checks.

Stakeholders have underlined some drawbacks, notably with regard to the lack of awareness of operational needs and activities of the EU institutions and bodies and with regard to the quality of inspections. Increasing the number of inspections could also allow the EDPS to acquire a better understanding of these activities.

(3) Effectiveness of the EDPS' advisory role

In addition to its supervision and enforcement powers, the EDPS advises EU institutions and bodies on proposals for legislation and new policies, appears before the Court of Justice and cooperates with other authorities. The Policy and Consultation unit is thus divided into three main activities: (i) Legislative Policy, (ii) Litigation and Institutional Policy, (iii) International Cooperation.

The EDPS has fully implemented and applied this obligation but is not systematically consulted in the course of legislative process.

Regulatory framework

Pursuant to Article 28.2 of Regulation (EC) No. 45/2001, one of the main tasks of the EDPS is to examine the data protection and privacy impact of proposed new legislation. Regulation (EC) No. 45/2001 does not detail the consultation procedure but states that the European Commission "when it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, shall consult the European Data Protection Supervisor."

Moreover, the EDPS provides legal advice to EU institutions and bodies on the basis of Article 41(2).

The Regulation does not specify either the exact time for consultation or the legislation subject to consultation.

Implementation and application

The legislative consultation obligation is effectively implemented by the EDPS.

This obligation is implemented by the EDPS Rules of Procedure and the Policy paper on Consultation of June 2014[73], which interpret and provide a detailed procedure for legislative consultation. The EDPS Policy Paper on Consultation of June 2014 aims at interpreting its role with regard to legislative consultation and in particular, in terms of limitations in scope, working methods and main orientations.
The EDPS has developed a 'policy toolkit' – which includes general guidance to the legislator, for instance through thematic or sectorial guidelines – in order to raise awareness of institutions on data protection and privacy impacts.

A memorandum of understanding[74] with the three main institutions (European Parliament, Council of the European Union, and European Commission) is also envisaged by the EDPS.

This obligation is effectively applied by the EDPS but has raised several concerns.

Each year, the EDPS identifies the legislative and policy making proposals with the most impact for data protection on the basis of the European Commission work program. A meeting is usually organized in December when the European Commission has set the work program. In its policy inventory the EDPS lists the policy initiatives planned by the European Commission that it will comment upon or monitor. The EDPS provides advice to the legislator at all stages of the legislative process, from the Commission's draft to the definitive adoption of the text.

According to the EDPS[75], the consultation covers a wide range of legal instruments: legislative texts, but also other legal documents which are part of the legislative process (implementing acts, delegated acts, green papers, etc.).

There are different stages and tools for consultations:

1. According to Article 28.2 of the EDPS Rules of Procedure, formal legislative opinions are the main instruments used by the EDPS; they are issued in respect of proposals adopted by

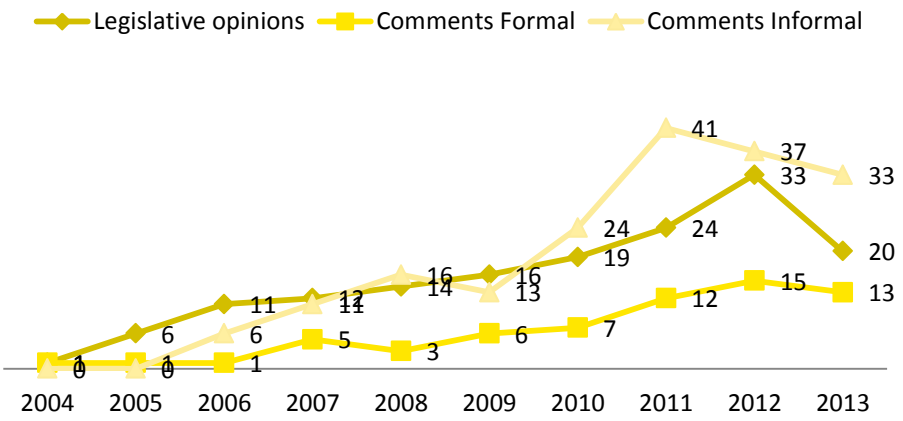
[73] Policy Paper "The EDPS as an advisor to EU institution on Policy and Legislation: building on 10 years of experience", June 2014.
[74] This memorandum would replace the 2008 note by EC Secretary-General.
[75] See EDPS Consultation Policy Paper 2014 and EDPS rules of procedures (article 26).

the Commission and include a full review of data protection related aspects of the proposal or other instrument. They analyze the impact of the text with regard to data protection and privacy. As a rule, the EDPS issues opinions on non-legislative texts only if data protection is a core element.[76]

2. Occasionally, formal comments are drafted on specific data protection issues.
3. Informal comments on the Commission's drafts for legislative proposals on which EDPS must be consulted by the Commission. The informal comments are confidential and they often precede formal consultation. These informal comments make it possible to take data protection requirements into consideration at an early stage.

The EDPS activity on providing legislative opinions steadily increased until 2012 although it decreased in 2013, in relation to the time spent on strategic priorities, including the review of the data protection framework.

Figure 20 – Number of legislative opinions and comments (formal and informal) provided by the EDPS in the last 10 years (source: EDPS annual reports)



The effectiveness of consultation is increased when the consultation is carried out at an early stage.

The consultation with the European Commission may take place at various stage of the legislative or policy-building process. At the stage of the Commission's draft, data protection issues may easily be taken into account in the proposal. Once the draft is published (just before Parliament and Council's review), it becomes more difficult for the EDPS to make its "data protection" case before the Parliament and Council.

The EU institutions may be reluctant to involve the EDPS in the legislative process.

The EDPS is not systematically consulted by the European Commission in the legislative processes that have an impact on data protection. This is partially due to the wording of Regulation (EC) No. 45/2001 that does not specify the time and the types of instruments subject to consultation. The wording of Article 28.2 only refers to "legislative proposal". Yet, the EDPS' implementing procedures result in the scope of consultation encompassing a broader range of texts than just "legislative proposals".

The European Commission is **not always aware of the types of instruments that trigger the consultation process.** The policy paper has been a cornerstone for the EDPS insofar as it takes

[76] EDPS Annual Report 2013.

stock of 10 years of experience and provides useful information relating to this interpretation of the provision. In the case of confidential information (such as negotiations for an international agreement such as safe harbor), the European Commission may appear reluctant to consult the EDPS. There is a resistance to consulting (due in particular to the confidentiality of the negotiations) and according to the EDPS this matter should be settled at the Regulation level. Nonetheless, the EDPS stated that there was no confusion between consultations on administrative measures pursuant to Article 28.1 and on legislative proposals pursuant to Article 28.2.

Moreover, Regulation (EC) No. 45/2001 does not specify the **exact timing for consultation.** In this respect, the consultation should be performed prior to the adoption of the text. In practice, the timing is highly dependent on the Directorate General in charge of the proposal.

An amendment of Regulation (EC) No. 45/2001 could be considered (see below); a common procedure could also be adopted. For this purpose, a draft memorandum of understanding between the EDPS and the European Commission, the European Parliament and the Council is in progress.

In the course of consultation, collaboration with the European Commission is constructive but could be further enhanced.

Relationships with the European Commission and in particular with the DG Justice are very constructive. The EDPS highlighted that overall, through bilateral contacts at staff level and awareness-raising events, it has built constructive cooperation with all DGs. Each year, the EDPS identifies the legislative and policy-making proposals with the most impact for data protection on the basis of the European Commission work program. The EDPS lists the priorities for legislative consultation for that year in its inventory.

The relationship between the European Commission and the EDPS also faces communication issues due to lack of awareness of some staff of the consultation process. Indeed, there are sometimes misunderstandings because officials of the European Commission believe that by ticking the box relating to consultation, the proposal will directly be transmitted to the EDPS (which is not the case).Some inter-institutional affairs units are not properly trained on the procedure agreed between the European Commission and the EDPS. Therefore, increased staff training could resolve this issue.

Relationships with the European Parliament are also considered to be very satisfactory.

It appears that there is a natural level of contact with the LIBE committee, notably in charge of matters of data protection. The EDPS provides the Parliament with its opinions and makes its best to keep the Parliament informed. The EDPS often presents its opinions before Committees of the European Parliament, and meets with rapporteurs in the Parliament to discuss relevant issues in ongoing legislative files.[77]

Relationships with the Council of the European Union should be enhanced.

The EDPS has various contacts with the secretariat and with teams dealing with presidency cooperation but the relationships are less cooperative. The EDPS must wait for official invitations to attend the meetings, which are only provided if the EDPS is expected to make a presentation. For instance, the EDPS could not attend all the meetings relating to the General Data Protection Regulation (GDPR). **In order to change this situation, the EDPS emphasizes that the EDPS should have a recognized a status in relation to the Council. The issue of this status is part of the draft Memorandum.**

[77] See EDPS policy paper 2014 for more details.

However, it should be stressed that the Council has several times invited the EDPS to participate in meetings and discussions even though it has no obligation to do so pursuant to Regulation (EC) No. 45/2001 and the Treaties.

Conclusion

The timeframe of the consultation and the legislative instruments subject to this procedure should be set out in further detail.

There are two available options to increase the effectiveness of the consultation obligation:

- **Hard Law:** amendment of Regulation (EC) No. 45/2001. Article 28.2 of Regulation (EC) No. 45/2001 could be amended to specify the consultation process and the types of texts subject to consultation. Informal consultations should be formalized.
- **Soft Law:** drafting of a Memorandum of Understanding. Indeed, an alternative option would be adopt a Memorandum of Understanding between the three legislative institutions (European Commission, Council of the European Union and European Parliament) and the EDPS.

The EDPS intervenes before the Court of Justice of the European Union; major drawbacks should nonetheless be stressed.

Regulatory Framework

Pursuant to Article 47 (1) (i) of Regulation (EC) No. 45/2001, the EDPS may intervene in actions brought before the Court of Justice of the EU (including the Court of Justice, the General Court, and the Civil Service Tribunal).

Implementation and Application

This power is implemented by the EDPS Rules of Procedure (Article 41). An internal manual has also been established and is used by the EDPS. The pleadings submitted at oral hearings (where applicable) are published on the EDPS website.

This power to intervene before the Court of Justice in accordance with Article 40 of the Statute of the Court of Justice of the European Union[78] is effectively applied by the EDPS, but limited as EDPS may intervene solely in proceedings designed to resolve a dispute in support of one party.

Applications to intervene are submitted on the basis of Article 47 (1) (i) of Regulation (EC) No. 45/2001 which provides that the Supervisor may intervene in actions brought before the Court of Justice. Under Article 40 of the Statute of the Court, an application to intervene shall be limited to supporting the form of order sought by one of the parties. This means that the EDPS has to choose which party to support, despite lacking access to the materials of the case, i.e. sufficient information. The Court held that the right to intervene does not extend to preliminary reference procedures under Article 267 TFEU (see order of the President in Case C-73/07)[79]. The EDPS

[78] OJ C 83/210.
[79] According to the Order of the President of the Court in case C-73/07 §11 & 12.

"11 Participation in the proceedings in the cases covered by Article 234 EC is governed by Article 23 of the Statute of the Court of Justice, which limits the right to submit statements of case or observations to the Court to the parties, the Member States, the Commission of the European Communities and, where appropriate, the Council of the European Union, the European Parliament and the European Central Bank, to the States, other than the Member States, which are parties to the Agreement on the European Economic Area, the EFTA Surveillance Authority and non-member States. By the expression

highlighted the necessity of being recognized as *amicus curiae* before the Court of Justice (and not only in support of one party) and to be provided with the possibility to submit observations during the preliminary reference procedure. In this regard, it should be noted that the Court of Justice has already invited the EDPS to attend a hearing in the course of preliminary ruling proceedings (pursuant to Article 24 of the Statute).[80]

In practical terms, once the leave for intervention has been granted by the Court of Justice of the European Union, the channels for communication are smooth thanks to the use of e-curia.

Efficient coordination exists within the EDPS between the Supervision unit and the Consultation unit. The channels of communication are effective. The two units always collaborate and coordinate to select the cases for interventions and the position of the EDPS.

Conclusion

The intervention power of the EDPS before the Court is implemented and applied. Some practical drawbacks have been underlined by the EDPS. However, with due regard to the independence of the Court of Justice of the European Union, the evaluator does not recommend tackling practical drawbacks by means of amendment of Regulation (EC) No. 45/2001.

Cooperation is very active although cooperation with non-EU countries is not explicitly provided for

Regulatory framework

Pursuant to Article 46 (f) and (g), the EDPS has the duty to:

- cooperate with national data protection authorities and the supervisory bodies established under the former third pillar (i.e. Joint Supervisory Bodies of EUROPOL and EUROJUST);
- participate in the activities of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (also known as the "Article 29 Working Party" established under Article 29 of Directive 95/46/EC).

Implementation and application

The EDPS' cooperation tasks are aimed at increasing the consistency of data protection in the EU. The implementation of cooperation efforts is laid down in Article 46 of the EDPS Rules of Procedure:

1. *"The EDPS shall take part with national supervisory authorities in the coordinated supervision of large scale IT systems, as provided under Union law.*
2. *The EDPS shall organize coordination meetings and provide the secretariat of the coordination groups.*

'parties', Article 23 refers only to the parties to the action before the national court (see, to that effect, the judgment in Bollmann, paragraph 4, and the order of the President of the Court in SGAE, paragraph 5).

12 Since the Supervisor is not expressly mentioned in Article 23 of the Statute of the Court of Justice, and since, in the main proceedings, he is not a 'party' for the purposes of that Article, he is not entitled to submit observations to the Court on the questions referred by the national court for a preliminary ruling."

[80] A recent example is case C-362/14, *Schrems*. The hearing took place on 24 March 2015.

3. *The EDPS shall cooperate with individual national supervisory authorities to the extent necessary and according to their priorities, with a view to ensuring coordinated supervision of the national and central parts of large scale IT systems."*

Cooperation with national data protection authorities

EDPS's main cooperation work with national data protection authorities occurs through the Article 29 Working Party, to provide the European Commission with advice on data protection issues and contribute to the development of harmonized policies for data protection in EU Member States (see below).

Direct cooperation of the EDPS with national authorities is an area of increasing importance in the context of the development of large-scale international databases such as EURODAC, the Visa Information System (VIS), the Schengen Information System II (SIS II) or the Customs Information System (CIS), which requires a coordinated approach to supervision.[81] There is special legislation applicable to these activities. The EDPS provides the secretariat for those Coordinated Supervision groups and has been the chair of some of these Coordinated Supervision Groups, for example, the EURODAC, VIS and CIS SCGs. The EDPS also organizes meetings. The supervision groups monitor the systems (compliance with special legislation and functionalities provided for in Regulation (EC) No. 45/2001) and draft recommendations (ensure the existence of appropriate security and confidentiality measures).

Participation in the activities of the Article 29 Working party on the protection of individuals

The EDPS participates in the work carried out within the framework of the Article 29 Working Party, as the EDPS is a member of the Article 29 Working Party. For instance, the EDPS takes part in various subgroup meetings and in drawing up opinions and texts, sometimes playing a key role in these groups (rapporteur or co-rapporteurs for the opinions).

Additional activities: EDPS participation in international and European conferences

Although this is not specifically provided for by Regulation (EC) No. 45/2001, the EDPS also participates in European and international conferences such as the Conference of Data Protection and Privacy Commissioners. Articles 44 and 45 of the EDPS Rules of Procedure provide for:

- exchanges of knowledge and cooperation with data protection regulators worldwide;
- the conditions for participation in Article 29 Working Party discussions and meetings.

The EDPS attends meetings of the Consultative Committee of Convention 108. In addition, the EDPS contributes to several panels and workshops on data protection in international organizations. At the international level, the EDPS also collaborates with data protection authorities from non-EU countries. This exchange of information at an international level ensures consistency in the field of data protection, mutual assistance for the protection of personal data and engagement in data protection activities. Cooperation on enforcement of data protection rules is also a priority.

Conclusions

The EDPS actively cooperates with national authorities, notably in the field of the development of large-scale IT systems and within the jurisdiction of the Article 29 Working Party. Additional cooperation actions are performed at its own initiative in order to monitor international discussions on data protection.

Regulation (EC) No. 45/2001 does not provide for the EDPS' role in international cooperation. In this regard, an amendment of Regulation (EC) No. 45/2001 would align the legislation with the current practices of the EDPS.

[81] EDPS Annual report 2013.

Relations between the EDPS and the Joint Supervisory Bodies will be analysed in the case study devoted to data protection in the field of police and judicial activities.

Conclusion on the EDPS' advisory role

Regulation (EC) No. 45/2001 meets its objective to entrust to the EDPS the task of effectively advising the EU institutions and bodies, as well as cooperating with other bodies.

The EDPS has implemented and applied its advisory obligations and has in many ways surpassed the obligations provided by the Regulation. As a result, its role is performed at a very high level of effectiveness.

Drawbacks and shortcomings of the wording of Regulation (EC) No. 45/2001 have been identified.

Regulation (EC) No. 45/2001 does not provide for procedures for EDPS consultation and cooperation duties. The general wording of Regulation (EC) No. 45/2001 leaves a large margin of interpretation to the EDPS. However, it also hinders the smooth application of the legislative consultation process.

The Regulation does not provide for the role the EDPS currently plays in the context of international cooperation.

GENERAL CONCLUSIONS ON OBJECTIVE 3

Regulation (EC) No. 45/2001 contributed to establishing a relevant, effective governance system, notably an independent supervisory system:

- DPOs are established in each EU institution and body and the tasks and powers conferred by the Regulation allows them to ensure that the provisions of the Regulation are applied and advise controllers to comply with their obligations, although various improvements could increase their effectiveness (notably reducing the scope of notification while introducing an obligation for DPOs to maintain records of data processing operations in an inventory)

- The Regulation establishes the EDPS as an independent supervisory authority and confers upon it the tasks and powers to effectively monitor and ensure the application of Regulation (EC) No. 45/2001, although further improvements should be considered. Over time, the EDPS has implemented and applied its obligations under the Regulation. Moreover, the Supervision and Enforcement unit has established efficient, powerful tools to supervise the application of the Regulation. This is especially notable for the processing of complaints and prior checking.

- The Regulation achieves its objective to confer upon the EDPS the task of effectively advising the EU institutions and bodies as well as cooperating with other bodies. The EDPS has implemented and fulfilled its advisory obligations and has in many ways gone beyond the obligations set out in the Regulation. As a result, the level of effectiveness of its role is very high.

4 Efficiency

To what extent is the overall governance of the Regulation (EC) 45/2001 efficient in ensuring appropriate application?

4.1 Methodology for answering the evaluation question

4.1.1 Understanding of the question

Two main types of analyses should be conducted to assess the efficiency of the application of Regulation (EC) No. 45/2001:

- The evaluation study assesses the impact of Regulation (EC) No. 45/2001 in terms of costs and administrative burden for Union institutions, bodies, offices and agencies and their evolution over time;
- The study also assesses the effectiveness of Regulation (EC) No. 45/2001, notably the effectiveness of its governance system (see evaluation question on effectiveness);

Assessment of effectiveness and the costs incurred by the governance system and application of the Regulation (1st point) and their evolution over time makes it possible to assess unnecessary costs and to draw conclusions on the efficiency of the whole system.

Proposed approach and limits

The approach to answering this evaluation question is based:

- Firstly, on quantification of the time spent on each activity related to the implementation of Regulation (EC) No. 45/2001, including EDPS staff members, DPO and DPC activities, and data controller activity relating to data protection;
- Secondly, on a qualitative analysis of the importance of each activity in relation to one another.

The objective is to determine whether the time spent and associated costs are appropriate, and identify recommendations to improve efficiency.

This cost analysis provides an initial estimate of the overall application cost of Regulation (EC) No. 45/2001 and should be viewed as a baseline scenario, although several limitations must be pointed out:

- quantification of the EDPS costs related to the Regulation has not been separated from those relating to EDPS responsibilities arising from other regulatory sources: the entire cost of the EDPS is considered to derive from the regulation. This approximation doubtless overestimates the costs of the EDPS.

- The staff costs of institutions and bodies are limited to an estimate of their salaries based on the total average cost provided by DG BUDGET[82], including the "*habillage*" (real estate expenses, office equipment, IT, etc.

Although provided for in the inception report, the standard cost model has not been applied due to the wide range of operations and insufficient data on EDPS activity costs.

[82] Circular from DG BUDGET to RUF dated 26 June 14

4.2 Implementation of the Regulation (EC) No. 45/2001 reached a total cost of 28 million euros in 2014, corresponding to 210 FTEs[83] performed by 1455 staff

The total costs relating to the implementation of Regulation (EC) No. 45/2001 can be calculated by adding together all the types of costs incurred:

1. Total budget of the EDPS;
2. Cost of DPOs and DPCs;
3. Cost of data controllers;
4. IT expenses (related to the protection of personal data): fees paid out to external contractors (initial design and annual maintenance);
5. Staff training expenses (if available).

The total budget of EDPS is available (EDPS annual report). However, staff costs (DPOs, DPCs, data controllers) have been estimated. Expenses for IT dedicated to protection of personal data and staff training expenses are not available, mainly because the share of the contract with IT services providers dedicated to data protection cannot be isolated. As training sessions are mainly provided by the EDPS, their costs are already included in the total budget of the EDPS. Additional costs (in particular, travel costs to attend DPO network meetings or training sessions) are difficult to assess but certainly negligible in relation to staff costs and EDPS costs.

Methodological note: estimating the staff costs of DPOs, DPCs and data controllers.

The staff costs of DPOs, DPCs and data controllers were calculated on the basis of:

- the time spent on data protection activities by DPOs and DPCs, as declared in the survey, extrapolated to the total number of DPOs and DPCs (provided by the European Commission), reflecting the proportion of time spent on data protection activities by respondents;

- the time spent on data protection activities by data controllers, as declared in the survey, extrapolated to the total number of data controllers, reflecting the proportion of time spent on data protection activities by respondents. The total number of data controllers by entity is based on the estimate provided by DPOs in the survey, and extrapolated to the total number of institutions and bodies.

The number of full time equivalents (FTEs) obtained is multiplied by the total average cost of an Official of the European Union in 2014, including the "*habillage*" (€132 000/year)[84].

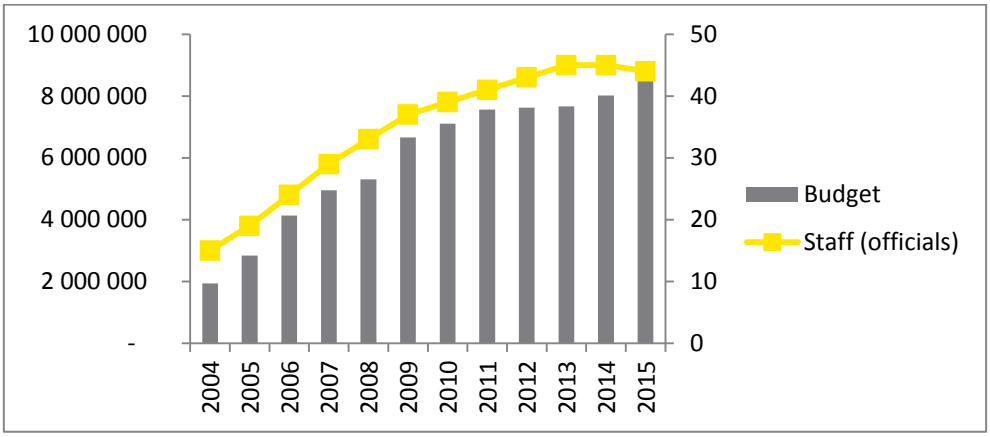
Total budget of the EDPS: an overall cost of 8 million euros in 2014

The overall budget of the EDPS rose from 2 million euros in 2004 to 7.5 million euros in 2011 and has remained fairly stable since then despite inflation, although the 2015 budget is slightly higher than the 2014 budget.

[83] Full-time equivalent
[84] Circular from DG BUDGET to RUF dated 26 June 14

In line with European Commission decision, the workforce has regularly increased by two people every second year in order to keep up with the increasing scope of the EDPS. From a start with 20 people at the outset, EDPS staff amounted to 42 officials and 14 contract agents in 2014.

Figure 21 - Changes in total EDPS budget and number of official staff since 2004 (source: EDPS)



Cost of DPOs and DPCs: an estimated cost of 11 million euros in 2014

The total cost of DPOs and DPCs is calculated as follows: *number of persons involved x time spent on data protection activities x average salary* where

- The number of DPOs and DPCs is based on figures provided by the European Commission;
- The time spent on data protection activities is based on an EY survey of DPOs and DPCs, for which results have been extrapolated to the entire group;
- Average salary corresponds to the total average cost of an Official of the European Union in 2014[85] (€132 000/year).
- 61 DPOs[86] and 113 DPCs are responsible for implementing the regulation in their institution or body (EUROPOL and EUROJUST are excluded from the scope, as the regulation is not implemented in these institutions). The list of DPOs and identified DPCs is provided in the annex hereto. Five institutions appointed DPCs to support DPOs in the execution of their duties; the European Commission, the Council of the European Union, the European Central Bank (ECB), the European External Action Service (EEAS) and the European Parliament. In addition, some DPOs rely on a team of staff members to assist them in the performance of their duties.

61 DPOs spent on average 35% of their time on data protection activities and are supported by another 0.35 FTE[87]

The survey of DPOs and DPCs allows collection of data on the time spent by DPOs in performing their duties and the number of staff members assisting them in their tasks.

One third of the respondents spent less than eight hours per week on data protection activities and 80% spend less than two days per week[88]. However, 12% of the respondents perform a full time job

[85] Circular from DG BUDGET to RUF dated 26 June 2014 Corresponding to the average cost including "*habillage*" (real estate expenses, office equipment, IT, etc.).
[86] No DPO from EDPS is included in the scope (already included in the total EDPS budget)
[87] Full time equivalent
[88] Analyses based on 50 respondents out of 61 DPOs

on these activities in the largest institutions[89]. The average time spent on data protection activities is 14 hours/week whereas the median is eight hours/week.

As a result, we may conclude that 61 DPOs are spending an average of 0.35 FTEs on data protection activities, i.e. 21.2 FTEs are dedicated to data protection matters.

Figure 22 On average, how much time do you spend on data protection matters as a DPO per week?

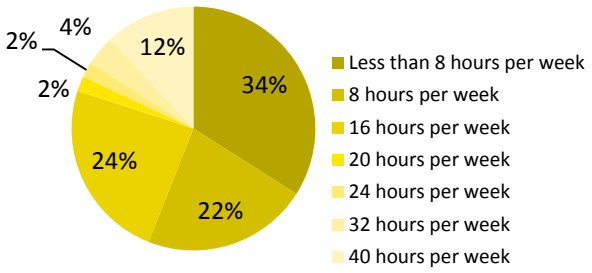
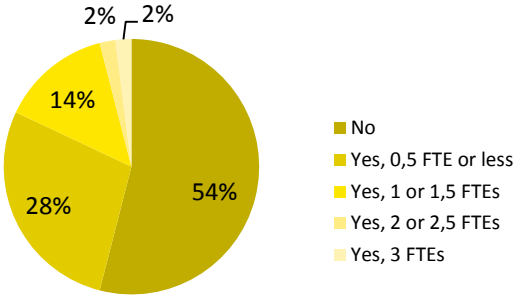


Figure 23 - In your capacity as DPO, do you have a team working for you (other than the DPCs)?



(Source: EY survey)

Most DPOs work alone and are not assisted by any team (54%) or are assisted only to a limited extent (82% are supported by 0.5 FTEs or less). However, the DPOs of the largest institutions[90] are assisted by one or more FTEs (18% of respondents).

On average, 0.35 FTEs assist DPOs in their duties, corresponding to 21.4 FTEs.

113 DPCs spend eight hours per week (on average) on data protection issues and are rarely assisted by a team (0.16 FTEs on average)

Similar to the observations on DPOs, most DPCs spend less than eight hours per week on data protection matters (64% of the respondents)[91]. However, some DPCs of the European Commission and the European Parliament state that they spend 2.5 to 5 days per week on data protection matters.

Most DPCs do not receive any support in the performance of their duties (77% of respondents) while others are assisted by a limited number of staff as detailed in the figure below. On average, we can assume that DPCs are assisted by 0.16 FTEs.

Figure 24 On average, how much time do you spend on data protection matters as a DPC per week?

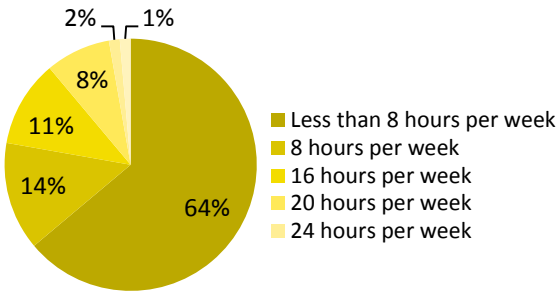
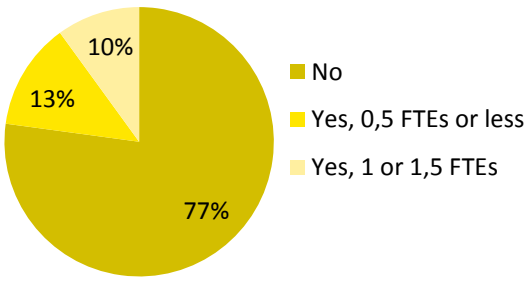


Figure 25 - In your quality as DPC, do you have a team working for you? (Source: EY survey)



[89] European Parliament, Council of the European Union, European Commission, EEAS, European Centre for the Development of Vocational Training (CEDEFOP), European Investment Bank (EIB), EU-LISA
[90] Court of Auditors, European Parliament, Council of the European Union, European Commission, European Centre for Disease Prevention and Control (ECDC), European External Action Service (EEAS), European Investment Bank (EIB), Court of Justice of the European Union, European Foundation for the Improvement of Living and Working Conditions (Eurofound)
[91] Analyses based on 72 respondents out of 113 DPCs

Thus, we can assume that DPCs are spending 0.2 FTEs on data protection matters, assisted by 0.16 FTEs, corresponding to an overall number of 40 FTEs dedicated to data protection activities.

An estimated cost of 11 million euros per year for DPO and DPC activities dedicated to data protection

Based on the average cost for Official Staff of the European Union provided by DG BUDGET[92], we can assume that the yearly cost of DPOs and DPCs is €132 000/year. With a monthly value of €11000, we can estimate the total cost of DPO and DPC time dedicated to data protection activities as described below.

Table 3 –DPO and DPC cost estimates

Activity	Number of FTEs per year	Estimated cost per year (in millions of euros)
Source	*Extrapolation from the survey*	*Estimate based on the circular from DG BUDGET dated 26 June 2014*
DPO activity on data protection	21,2	2.8
Support to DPO	21,4	2.8
DPC activity on data protection	22,6	3.0
Support to DPC	17,8	2.3
TOTAL	**82,9**	10.9

The estimated cost of DPOs (5.2 million euros) is approximately equivalent to the estimated cost of DPCs (5.3 million euros), i.e. five institutions use up half of the budget allocated to data protection management in institutions. This statement is consistent with the activity of these institutions and the staff size they represent.

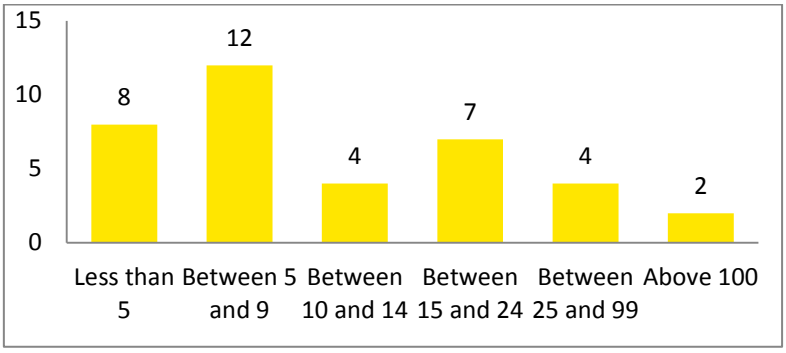
An estimated cost of 9.3 million euros for data controllers

Approximately 1214 data controllers involved in data processing activities…

The number of data controllers per institution depends on the size of the institution. Although the median figure given by DPOs and DPCs is eight[93], the largest institutions may have more than 50 data controllers, resulting in an average of 27 data controllers per institution. However, at the DPC level, the number of supervised data controllers generally goes down to 11.

[92] Circular from DG BUDGET to RUF dated 26 June14. Corresponding to the average cost including "*habillage*" (real estate expenses, office equipment, , IT, etc.).
[93] Analyses based on the 37 of 61 institutions for which DPOs or DPCs provided an answer to the question.

Figure 26 - Approximately how many data controllers are in your institution or body? (Source: EY survey)



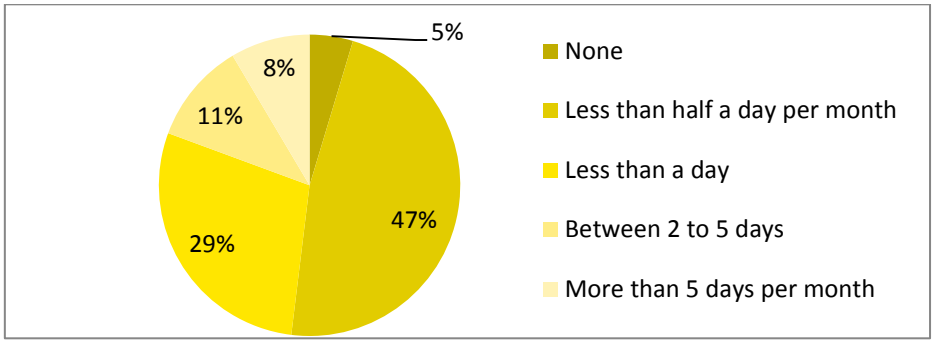
On the basis of this data, we can assume that the 62 DPOs or 113 DPCs are supervising approximately 1214 data controllers. For institutions and bodies for which no information was made available (24), the median value of eight data controllers was chosen.

…corresponding to approximately 70 FTEs on data protection activities, i.e. around 9.3 million euros per year

Although the total number of data controllers estimated is high, the time spent on data protection activities remains limited. The majority of respondents say that they spend less than half a day per month on data protection activities. 8% of respondents spend more than five days per month. The median number of days spent on data protection activities is less than half a day per month. However, 8% of respondents said they spend more than five days per month on these activities.

When applying these results to the total number of data controllers, we can assume that around 70 FTEs are performing data controller activities in the 62 institutions, corresponding to an overall budget of 9.3 million euros.

Figure 27 - On average, how much time do you spend on data protection activities? (Source: EY survey)



As a result, the overall estimated costs for data protection matters based on EDPS costs and data protection staff costs amount to 28 million euros (IT expenses and training expenses not included), of which EDPS costs represent 28% of total expenses, DPOs and DPCs 39% and data controllers the remaining 33%.

4.3 Breakdown of costs per activity

The total budget can be broken down per type of activity in order to assess the importance of each provision of the regulation in the overall budget.

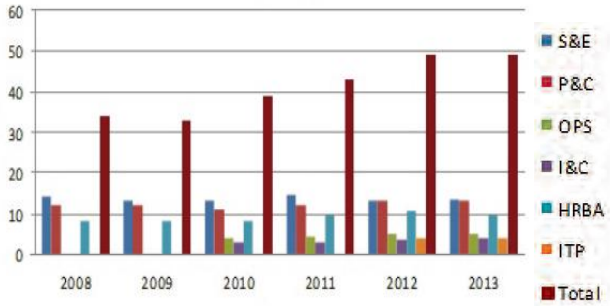
Breakdown of EDPS budget per activity: a cost accounting project to monitor the activity

The breakdown of EDPS' budget per activity is not available at this time but a new project is being implemented to determine the cost of each activity (activity-based project). As referred to above, the budget has been frozen since 2011 despite the growth in activity. As a result, the EDPS is now working on putting cost accounting in place in order to better monitor the activity and optimize resource allocation.

The Supervision and Enforcement unit and in the Policy and Consultation unit have similar staff numbers, which have been stable since 2008

Analysis of staff allocation per unit reveals that the number of official staff remained stable since 2008 in the following units: Supervision and Enforcement (S&E), Policy and Consultation (P&C) and Human Resources and Business Administration (HRBA), while other units were set up in the meantime (Information and Communication Sector, Information Technology Policy Sector and the Records Management Group), notably to provide support to the work done by the other units.

Figure 28 - Evolution of EDPS official staff by unit since 2008 (source: EDPS Annual report)



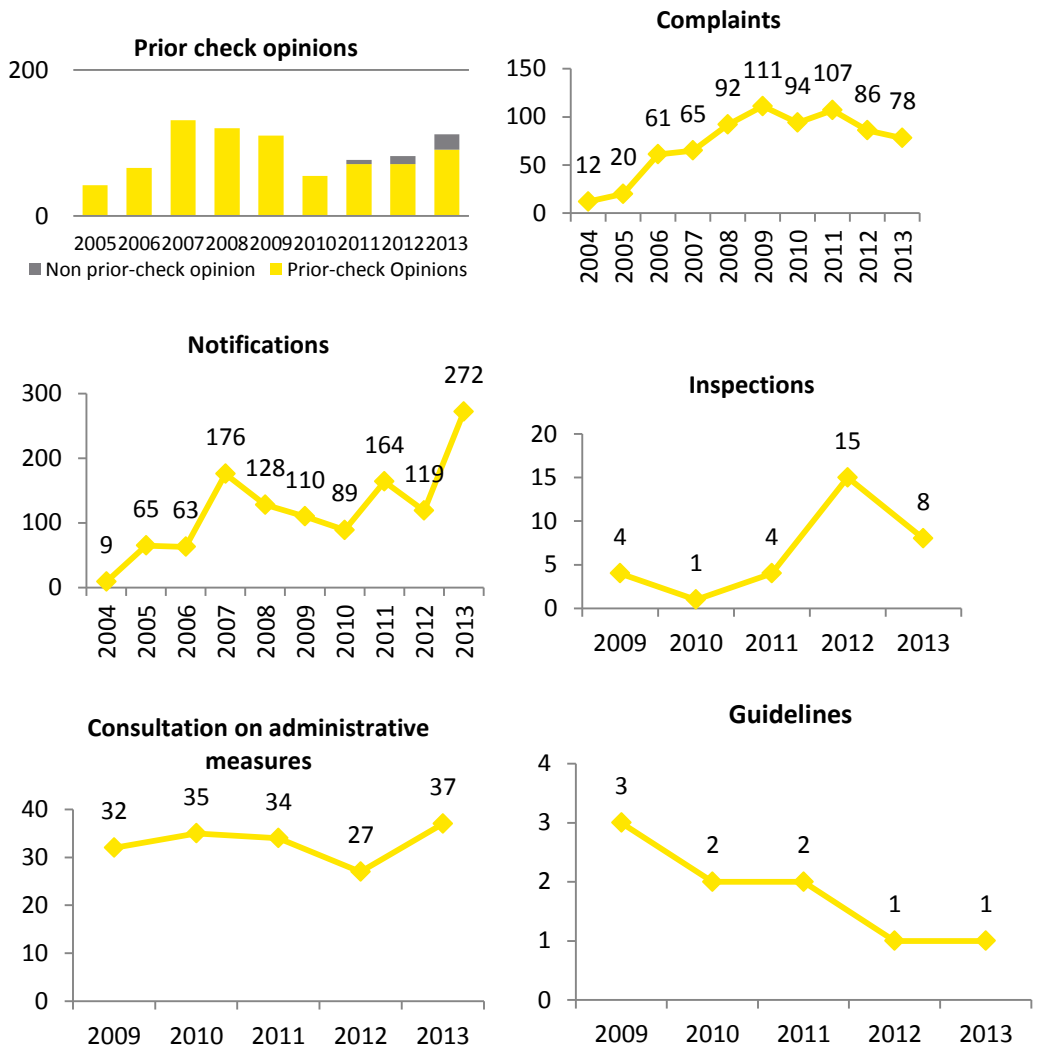
The Supervision and Enforcement unit accounts for one quarter of the staff costs, which is equivalent to the allocation of staff costs to the Policy and Consultation unit. Two thirds of the staff costs are concentred there, together with the Human Resources and Business Administration unit.

Efficiency gains in both units since 2008

Supervision and Enforcement

When considering the number of activities performed by the S&E unit since 2008, the stable staff number reflects the significant gains in efficiency in this unit. This is particularly notable with regard to the increase in the number of notifications received and inspections performed and the implementation of new tools to improve t support to institutions and bodies, such as compliance visits and the hotline for DPOs and data controllers. In particular, the regular development of guidelines has contributed to limiting the need for data controllers and DPOs to obtain support from the EDPS. Although the time spent on each activity can vary significantly between cases, the figures below illustrate the evolution of the level of activity of the unit.

Figure 29 - Changes in S&E unit activities since 2004 (source: EDPS annual reports)

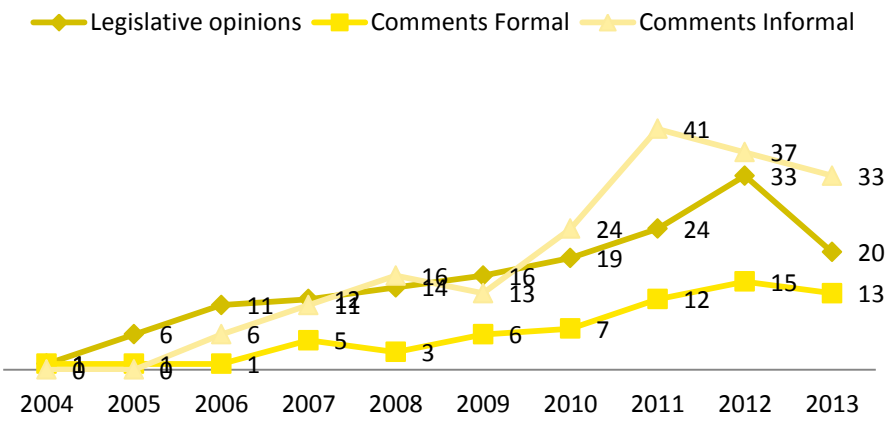


Policy and consultation

As regards the Policy and Consultation unit, the number of comments and opinions provided (one of the activities it performs) since the establishment of the EDPS regularly increased between 2004 and 2011 and has been fairly stable since then (although the 2013 reduction of activity corresponds to the significant amount of time dedicated to the reform of the GDPR[94]). The 2008 level represents roughly half of the 2013 activity, although the number of staff has been fairly stable since 2008. This effort reflects the efficiency gained by the unit, mainly generated by the skills improvement of unit members.

[94] Global Data Protection Regulation

Figure 30 - Trend in legislative opinions and comments provided by the EDPS since 2004 (source: EDPS annual reports)



The allocation of resources between the units appears to be unbalanced in comparison with the weight given to each of the underlying tasks set out in the Regulation

When placing these figures in relation to the importance assigned to each role (i.e. supervisory and regulatory roles) in the Regulation as presented hereabove, it appears that the S&E unit performing most of the supervisory tasks and the P&C unit performing most of the advisory tasks have the same staffing level, although in the Regulation priority seems to be given to the supervisory role of the EDPS.

This statement must be balanced by the fact that:

- the Information Technology Policy Sector, which comprised four official staff members in 2013 and six in 2015, also supports the EDPS' supervisory and advisory functions. In addition, other support or cross-disciplinary services (I&C, HRBA and OPS) also provide support to the two main policy units (S&E and P&C);
- the EDPS' advisory activities of the extend beyond the scope of Article 28.2 to embrace other sources (e.g. Directive 95/46 for activities related to WP29, specific regulations setting up large-scale IT systems VIS, SIS II, Eurodac, CIT, IMI for coordinated supervision activities, etc.) and are shared between the S&E (art 28.1 & 46 (d)) and P&C (art 28.2, 41, 46(d)) units.

The new EDPS strategy: giving priority to an enhanced cooperation and advisory role

The new EDPS strategy for 2015-2019 is structured on three orientations:

- **Data protection goes digital**: the role of digital technologies in ensuring data protection:
- **Forging global partnerships**: cooperation at international level on data protection issues:
- **Opening a new chapter for EU data protection**: development of EU data protection rules

This new strategy highlights EDPS's commitment to enhancing its supervisory role in data protection with the help of new digital technologies. The third orientation focuses on its willingness to promote the dialogue on new EU rules for data protection and to support the policy-making process, corresponding to its advisory role. The second orientation highlights the role the EDPS wishes to play in international discussions on data protection. Although this role was assigned to the

recently appointed European Data Protection Supervisor in the vacancy notice[95] (*representing at the highest levels and developing and maintaining effective relationships with a diverse community of stakeholders in other EU institutions, Member States, non-EU countries and other national or international organisations*), it does not seem to fully reflect the roles given to the EDPS as per the Regulation.

The primary role of the EDPS under the Regulation being the supervision of institutions and bodies, neither the allocation of resources nor the EDPS strategy appears to fully reflect this, bearing in mind that the EDPS' advisory activities extend beyond the scope of Article 28.2 to embrace other sources (e.g. Directive 95/46 for activities related to WP29, specific regulations setting up large-scale IT systems for coordinated supervision activities, etc.) and are shared between the S&E (art 28.1 & 46 (d)) and P&C units (art 28.2, 41, 46(d)), etc.). Either a reallocation of resources or an amendment of the Regulation could be considered to adjust the time the EDPS devotes to each activity. The implementation of the activity-based cost project (ongoing) will facilitate monitoring of resources in relation to the assigned objectives of the EDPS.

Breakdown of DPO activities: an important share of DPOs' time is spent on activities that deviate from the tasks assigned by the Regulation

The survey makes it possible to analyse the breakdown of time spent per activity per DPO. On average, their activity is well balanced between the various tasks, although two of the top five most time-consuming activities deviate slightly from their primary role.

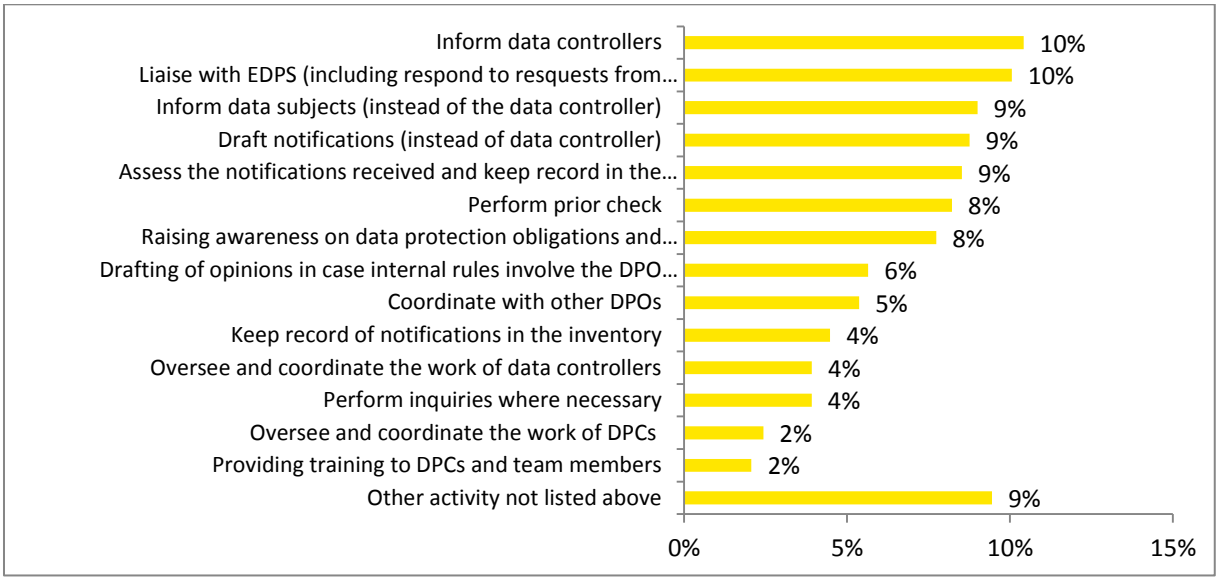
Surprisingly, apart from the two most time-consuming activities, which are fully in line with their role as DPO of (1) responding to requests for advice or information from data controllers and (2) liaising with the EDPS, the third- and fourth-most time-consuming activities are: (3) informing data subjects, although this task should be performed by data controllers and (4) drafting notifications (instead of data controllers doing this). 18% of their time is dedicated to activities they perform in place of the data controllers.

The other activities are more in line with the tasks assigned to DPOs by the Regulation: assessing notifications, performing prior checks and raising awareness.

Apart from the liaison with the EDPS, coordination activities with other DPOs, DPCs and data controllers are not perceived to be time-consuming.

[95] Vacancy notice for the European Data Protection Supervisor COM/2014/10354 (2014/C 163 A/02), OJ C 163 A/6 28 May 2014.

Figure 31 - On annual average, how much time do you spend as a DPO on each of the following data protection activities? (Source: EY survey)



It is noteworthy that 9% of their time is spent on activities that are not listed above, including the following tasks:

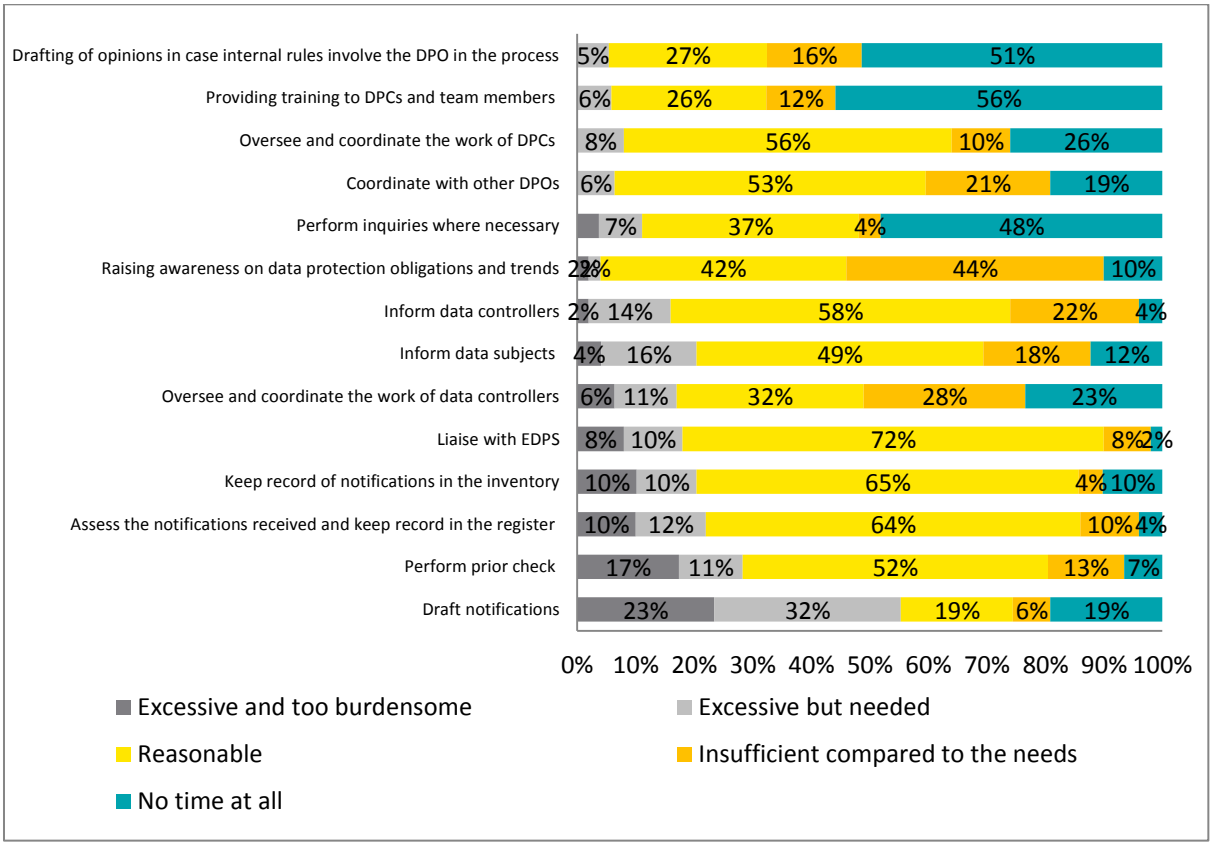
- Providing training to new arrivals;
- Prepare DPO network meetings or meetings with national DP authorities;
- Discuss data protection issues raised in complaints dealt with by the European Ombudsman;
- Work on data protection-related policies and procedures (e.g. video surveillance policy, contacts database policy, etc.).

DPO perception of the time spent on each activity: there is a serious need to better train and coordinate data controllers, which could help reduce the time allocated to drafting notifications

In addition to the direct interviews with DPOs, the survey made it possible to collect DPOs' perceptions of the time they devote to each activity.

There is a consensus among the majority of respondents in stating that the time spent on **drafting notifications (instead of data controllers doing this job)** is perceived as 'excessive', and 'too burdensome' for 23% of them.

Figure 32 - How would you consider the time you spend to performing each of these activities? (Source: EY survey)



Three other activities are perceived as 'excessive' for more than 20% of respondents and 'too burdensome' for more than 10% of the respondents including:

- Performing prior checks (i.e. notifying risky operations to EDPS and liaising with the EDPS);
- Assessing the notifications received and keeping record in the register;
- Keeping records of notifications in the inventory (if applicable).

However, more than 20% of DPOs state that the time spent on the following tasks is 'insufficient compared to the needs':

- Raising awareness on data protection obligations and trends (44%);
- Overseeing and coordinating the work of data controllers (28%);
- Informing data controllers (responding to requests for advice/ information regarding the exercise of data subjects' rights, etc.) (22%).
- Coordinating with other DPOs (21%).

These figures illustrate the need for an increased role for DPOs inn awareness raising for data controllers (in particular). This could help limit DPO involvement inn notification drafting and data subjects' information that they perform in place of the data controllers.

A poor perception of improvements among DPOs; quite satisfactory among DPCs

The trend in amount of time dedicated to each activity should have improved with the experience gained from the first years of implementation. However, DPO opinions are quite balanced between slight improvements and no real improvements for each of the activity. When considering the most

burdensome activities, DPOs' opinions of improvements on the time spent for each activity are mixed:

- Time dedicated to **drafting notifications** and **keeping record of notifications** in the inventory did not really improve for 57% and 52% of respondents, respectively;
- Time dedicated to **performing prior checks** (i.e. notifying risky operations to the EDPS) and **liaising with the EDPS** improved slightly for 55% and 59% of respondents, respectively;
- Time dedicated to **assessing the notifications** received and **keeping records in the register** improved for 51% of respondents, while it did not improve for 49%.

The strongest improvements are perceived for the **activities related to awareness raising, data subjects' information and data controllers' information** (above 60% positive perceptions), reflecting the progressive dissemination of a data protection culture within the institutions and in society more generally. The lowest improvements are perceived in performing inquiries (30% positive perception) and coordinating DPCs and data controllers (11% and 33%), corresponding to activities to which DPOs dedicate very little time.

When looking at DPC answers, it appears that very few of them (comparatively) consider that some of their tasks are 'excessive' and 'too burdensome'. A**ssistance to data controllers** (including drafting and submitting notification forms) is the only task that is rated as 'excessive' by a significant share of participants (30% of respondents). However, 24% of them consider that the time spent on raising awareness is insufficient compared to the needs, as did the DPOs. Similarly, the time dedicated to **overseeing the work of data controllers and examining data processing operations** is considered to be insufficient compared to the needs by 19% and 17% of respondents, respectively.

DPC respondents consider that the time dedicated to each of their activities improved over the years (59% on average).

DPCs seem to be more satisfied than DPOs with the time spent on each activity. This could be due to the fact that DPCs are appointed in largest institutions where data protection matters are appropriately managed and a full time DPO is appointed and organise the workload. However the assistance to data controllers in the notification process is, once again, perceived as a burdensome activity and the need to raise awareness is listed as a priority, although insufficiently considered.

Room for improvement identified in spite of persistent difficulties

In addition to what has already been presented above, DPOs have identified a list of other issues that remain problematic, including:

- the lack of **authority of the DPO** to ensure internal application of the provisions of the regulation ("*The biggest challenge is to raise awareness and achieve a prioritization of DP matters amongst colleagues and hierarchy"*);
- the lack of **capacity to perform security assessments on IT systems,** and the insufficient compatibility of common IT systems with data protection rules;
- the lack of **uniformity of EDPS recommendations** in the opinions (e.g. regarding data retention periods) and the impossibility of relying on the European Commission's forms and models;
- **Contradiction with other regulations** (see question on coherence);
- **Drafting opinions on internal rules** that can be challenging **for DPOs.**

Many DPOs have already identified areas for improvement. There are several commonly-shared views to improve the efficiency of their tasks:

- **Strengthen data controllers' accountability and responsibility**, and more generally gain support for raising awareness on data protection matters internally from the top management. *"Data protection is seen as the exclusive duty of the DPO";*
- **Provide uniform guidelines and general principles** from the EDPS which take a more pragmatic approach, also targeting non-legal and non-IT staff. Several DPOs call for improvements in simplifying notifications and prior check procedures, notably to limit the bureaucracy within the EDPS;
- Facilitate DPOs' tasks by **improving and standardizing data protection IT management tools** (inventory and registry database, notifications, communication with data controllers, claims, data breach incidents, etc.).

DPOs are required to be experts on data protection matters in order to foster its legitimacy. As mentioned previously, very few DPOs work full time and efficiency gains cannot be easily made in these areas. One option of interest[96] would be "*to have a full-time professional DPO shared among Agencies instead of a part-time DPO who does not have the means, time and the support from the hierarchy*", provided the staff regulation offers the possibility of working for different agencies.

[96] Suggested by a DPO in the survey

Figure 33 - Words cloud based on DPOs proposition to improve the activities (wordle.net)

DPCs also mentioned a list of difficulties they encounter in their tasks, consistent with the ones mentioned above by DPOs:

- The difficulty to **identify data controllers on new processing operations** as they do not want to take on additional responsibility on a matter they are not familiar with and, more generally, the lack of awareness on data protection matters;
- Their poor capacity to oversee the work of data controllers and perform inquiries **without appropriate IT skills** to ensure compliance with processing security;
- Data controllers' difficulty to **draft of notifications,** as they have poor legal backgrounds.

DPCs also identified several topics that would help to improve their tasks:

- **Improve governance of data protection matters** with appropriate IT tools which include relevant security requirements (in line with the privacy by design/by default principles established in the GDPR). This can be achieved through an early involvement of DPOs/DPCs in IT development in order to embed DP concerns.
- **Raise awareness among data controllers and more generally policy unit staff**, with standard training materials and clear and accessible guidelines (with concrete examples), targeting as a priority staff working on a daily basis with personal data.
- **Introduce "standard notifications"** for day-to-day activities shared among all services/institutions in order to reduce paperwork.
- **Clarify the formal roles and responsibilities of DPCs**.

DPCs are generally very satisfied with the collaboration they have with their DPOs. Many of them also point out the lack of resources to address all requests. DPOs are perceived as extremely busy and have difficulty addressing all requests in a timely manner. Strengthened coordination with other DPCs could help to resolve certain issues, as 21% of the DPCs respondents regret a lack (or absence) of coordination between them.

On the other hand, the network of DPOs is perceived as a valuable tool to improve DPO methods and share best practices. 83% of respondents are entirely or mostly satisfied with the time spent coordinating with other DPOs. It gives them the opportunity to share their views with peers and discuss specific topics.

A few improvements to the current functioning of the network were put forward as a means of improving the overall efficiency of the Regulation application:

- As most agencies tend to copy the European Commission's rules and policies, the DPO network meetings could provide an opportunity to present the tools they have developed.
- The number of DPO meetings could be reduced to one per year and the format of EDPS meetings could be improved to make it more interactive.
- A training session for newly-arrived DPOs would be useful.

Breakdown of data controller activity

Data protection principles and notification

Data controllers say that they spend approximately six hours on data protection issues. 34% of respondents consider that the time dedicated to notifications is not reasonable and a majority of respondents (64%) consider that notifications could be performed more efficiently). It must be noted that 76% of respondents state that they perform fewer than five notifications per year, which limits the capacity to get used to the notification procedure and thus gain efficiency over time. This leads to a situation where DPOs are performing notifications instead of data controllers.

Table 4 – Time spent by DCs on various data protection activities (source: EY survey)

Data protection activities	Average time spent (in hours)
Implementation of security and confidentiality measures	1.69
Notification or update of notification of data processing (including analysis of the compliance of the data processing operation with the data protection principles, i.e. accuracy of data, relevance of data, purpose limitations, limited data retention, compliance with data transfer requirements)	1.64
Responding to requests from EDPS (formal and informal requests, e.g. request(s) for information during notification process, cooperation, investigations, request(s) for allegations, etc.)	1.24
Drafting and updating information statements of data subjects	0.99
Response to requests from data subjects (notably processing of complaints)	0.79

Responding to requests of data subjects and information of data subjects

On average, responding to requests of data subjects takes barely more than half an hour for data controllers. 21% of respondents consider they spend excessive time on this activity.

Implementing security and confidentiality measures

22% of respondents consider that they spend excessive time on implementation of security and confidentiality measures, whereas they are 43% to consider it to be reasonable.

The proposed solutions to improve the efficiency of each task are in line with those of DPOs and DPCs:

- Create **standard templates for notifications** of common procedures (use of mail, HR systems, job application, etc.) and drafting and updating information statements of data subjects;

- Ensure that **IT tools embed data protection requirements**;
- Increase the **use of electronic forms** and promote IT tools in general;
- Increase **resources dedicated to data protection** internally (starting with the DPO);
- **Limit EDPS requests** to the Regulation requirements;
- **Strengthen synergies among institutions**, in particular to benefit from the work performed at the European Commission level on rules and guidance developments

In conclusion, the evaluation highlights that the application of the Regulation costs 28 million euros, with less than a third of the budget dedicated to EDPS, another third to DPO and DPC implementing the Regulation in their institution, with the remaining share corresponding to the costs of data controllers' activities on data protection.

Within the EDPS, the allocation of resources per objectives assigned is balanced between supervisory and advisory activities. Both units in charge of these roles have increased their activities in recent years, without increasing the number of staff dedicated to each unit. Both units benefit from efficiency gains made over the last five years, although further follow-up would be helpful to help DPOs raise awareness in institutions and bodies.

This allocation of staff does not fully reflect the importance placed on supervisory activities in the Regulation (Articles 41, 46 and 47) as compared to advisory activities (Article 28.2), bearing in mind that the EDPS' advisory activities extend beyond the scope of Article 28.2 to cover other sources (e.g. Directive 95/46 for activities related to WP29, specific regulations setting up large-scale IT systems for coordinated supervision activities, etc.).

An allocation of resources in favour of the Supervision and Enforcement unit could be envisaged in order to (1) intensify the existing supervision activities of the EDPS (inspections, compliance visits, guidelines) and (2) better reflect the weight given to supervision in the Regulation (subject to our comment above).

As regards the DPOs, the evaluation results show that many of them are struggling to perform all the tasks assigned to them by the Regulation, in the limited time they spend on data protection matters (generally part-time DPOs). They said they spend too much time on activities that should normally be performed by data controllers (Article 25 on drafting notifications, or Article 24 on data subjects' information). These activities represent 18% of their time spent working as a DPO.

A reallocation of these resources in favour of other activities aiming to raise awareness on data protection matters would contribute to better reflecting the tasks assigned to DPOs in the Regulation. In addition, it appears that a reinforced position for DPOs in institutions would also facilitate the implementation and application of the Regulation therein. Potential steps to achieve this could be (1) a higher position in the organisation chart and better support from the management, (2) a stronger focus on data protection matters for the DPO, i.e. full time DPOs instead of part time and (3) IT systems capacity to embed relevant security requirements.

Data controllers tend to agree these observations and many of them confirm that they spend too much time on notification drafting. Several suggestions have been made to increase the efficiency of these tasks (standard template for notification, IT tools embedding security requirements, synergies between institutions and bodies).

5 Relevance

5.1 Methodology to assess the evaluation question

This section aims at assessing the relevance of the provisions and mechanisms provided for by Regulation (EC) No. 45/2001 in order to fulfil the objectives set forth therein. The relevance analysis requires assessing to what extent the rules and principles enshrined in Regulation (EC) No. 45/2001 are suitable and relevant in order to meet the objectives.

This section focuses on the principles and rules that have been identified by the evaluator and/or the stakeholders as partially relevant or inadequate to meet the objectives of the Regulation. This purpose pf the analysis is closely linked to the analysis of the effectiveness of the provisions of the Regulation, where certain relevance issues have already been pointed out. As an example, the question that could be raised is: how appropriate is the performance of prior checking in order to ensure the protection of fundamental rights and principles?

5.2 Items identified whose relevance is questioned

Prior checking with the EDPS	▶ Prior checking is a relevant mechanism for protecting the personal data and privacy of individuals in the context of risky operations. ▶ Although the notification of processing pursuant to Article 27 of Regulation (EC) No. 45/2001 is burdensome for data controllers and DPOs, it should be underlined that this mechanism ensures that privacy risks are tackled by the EU institutions and bodies. ▶ Prior checking is therefore relevant in order to raise awareness of privacy risks associated with risky processing of personal data. Improvements should nevertheless be envisaged (see analysis of efficiency). Some stakeholders favor the introduction of a system of block exemption consistent with the current practice of adopting guidelines to facilitate the prior checking process. Nevertheless, it could be relevant to narrow the scope of the prior checking to core risky operations.
Notification of processing operations to DPOs	▶ While the notification of data processing operations was an important tool for compliance at one time, it appears that a level of maturity on data protection issues has been reached in a large majority of EU institutions and bodies. This system is excessively burdensome on data controllers and DPOs. ▶ In this context, the relevance of the notification is questionable, notably in the light of the GDPR. ▶ Therefore, it may be possible to consider reducing the scope of the obligation of notification and/or introducing an obligation to document processing operations in an inventory.
Change of purpose	▶ The relevance of this issue may be challenged as internal rules adopted by an EU institution or body may derogate from

	one of the main data protection principles (purpose limitation) although the wording of Article 6 provides that the provision applies without prejudice to Article 4. In this regard, the EDPS specifies that the change of purpose provisions apply only to secondary purposes and that the adoption of internal rules is an additional safeguard. Moreover, the fact that internal rules are not defined increases privacy related risks. ▶ Further, it appears that Article 6.2 is not applied and is inconsistent with the derogations provided to the purpose limitation principle enshrined in Article 20 1. ▶ The change of purpose provision is not relevant to fulfilling the objectives of the Regulation.
Confidentiality and Security	▶ Article 21 targets solely internal data processors. It would be relevant to broaden its scope in order to encompass the data processing operations carried out by external service providers.
Sanctions	▶ The range of powers provided to the EDPS in Article 47 is extensive although the Regulation does not provide for the obligation to impose pecuniary sanctions to the EU institution or body. ▶ According to the EDPS and a sizable number of DPOs, the most effective sanctions are the reputational ones targeting the institution or the body. The publicity relating to a violation of data protection rules seems to be powerful and appropriate to the EU institutional environment. This could significantly raise awareness among the management of EU institutions and bodies. Therefore, it could be relevant to introduce a specific sanction involving the power to order the publication of EDPS decisions that highlight a failure of an institution to comply with its obligations. .
Transfer of personal data	▶ The transfer of personal data within or between the EU institutions, to a recipient subject to Directive 95/46/EC and to recipients in non-EU are subject to specific conditions laid down by Articles 7 to 9 of the Regulation. The conditions are stricter for transfer outside the EU institutional scope and outside the European Union, as the risks associated with these transfer may be significant. ▶ The rules governing the transfer of personal data outside the EU (Article 9) are not appropriate insofar as they require that EU institutions and bodies assess the level of adequacy of third countries or international organizations. In practical terms, this analysis is not feasible as the EU institutions and bodies lack the appropriate skills and resources to do so.
Rights for data subjects	▶ The right of blocking corresponds to situations that could not be dealt by the right of erasure or other rights provided by the Regulation. In this regard, this right is consistent with Article 17.4 of the GDPR, which provides for a restriction/limitation of processing in limited circumstances.
Rules in the context of telecommunication	▶ Several stakeholders have underlined that the provisions relating to the presentation and restriction of calling and connected line identification are not relevant.

6 Coherence

6.1 Access to documents versus data protection

Please refer to case study

6.2 Coherence between Regulation (EC) No. 45/2001 *and the ePrivacy Directive*

Please refer to case study

6.3 Miscellaneous: coherence with further identified legislation

The online survey pointed out that several other laws may potentially contradict Regulation (EC) No. 45/2001[97]. The following legislation has been identified: (i) the Archives Regulation, (ii) the Confidential Documents Regulation, (iii) the Staff Regulations, (iv) the Financial Regulation, (v) the Clinical Trials Regulation. The issue of coherence was discussed during the interviews with stakeholders in order to identify the practical coherence issues.

6.3.1 The Archives Regulation

Article 15 of the Treaty on the Functioning of the European Union provides any citizen of the Union and any natural or legal person residing or having its registered office in a Member State with the right of access to European Parliament, Council and Commission documents.

The general principles and the limits governing the public's right of access to documents of EU institutions and bodies were laid down in Regulation (EC) No. 1049/2001[98] *(see dedicated case study)*. This Regulation provides for exceptions to the public's right of access, in particular that relating to documents where disclosure would undermine the protection of privacy and integrity of the individual, in accordance with legislation on data protection[99]. These exceptions are applicable for a maximum period of 30 years. Therefore Regulation (EEC, Euratom) No. 354/83 of 1 February 1983 as amended by Council Regulation (EC, Euratom) No. 1700/2003 of 22 September 2003[100] (hereinafter the "Archives Regulation") aims to ensure that documents of historical or

[97] Answers to question 69 of the online survey
[98] Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145 of 31 May2001, p. 43)
[99] Article 4(1)(e) of Regulation (EC) No. 1049/2001
[100] Regulation (EEC, Euratom) No. 354/83 of 1 February 1983 concerning the opening to the public of the historical archives of the European Economic Community (OJ L 43 of 15 Feb.1983, p. 1) amended by Council Regulation (EC, Euratom) No. 1700/2003 of 22 September 2003 amending Regulation (EEC, Euratom) No. 354/83 concerning the opening to the public of the historical archives of the European Economic Community (OJ L243 of 27 Sept.2003, p. 1)

administrative value are preserved and made available to the public by EU institutions and bodies after the termination of that period[101].

In this context, on the basis of the Archives Regulation, after a period of 30 years, public access would be given to documents containing personal data.

Nevertheless, the Archives Regulation also provides for exceptions. According to one of these derogations, **documents covered by the exception relating to privacy and the integrity of the individual as defined in Regulation (EC) No. 1049/2001, may be disclosed in accordance with Regulation (EC) No. 45/2001 on data protection, in particular Articles 4 on data quality and 5 on the lawfulness of processing[102].** This article specifies that this exception covers the files of staff members of EU institutions and bodies.

The difficulties result from the practical implementation and application of the Archives Regulation.

6.3.2 The legislation on EU classified information

Regulation (Euratom) No. 3 of 31 July 1958 implementing Article 24 of the Treaty establishing the European Atomic Energy Community[103] lays down provisions applicable to both EU institutions and bodies and Member States, on the classification of information resulting from research programs, whose disclosure is likely to harm the defense interests of Member States, or of information linked to nuclear matters.

Implementing Rules of Procedure of EU institutions and bodies[104] also provide for specific procedures relating to the classification of information which requires a degree of confidentiality within EU institutions and bodies.

In this context, it has been pointed out that security rules aimed at protecting EU classified information might justify the introduction, consistent with the exceptions and restrictions of Article 20(1) of Regulation (EC) No. 45/2001, of a restriction of the right of access of data subjects, pursuant to Article 13 of Regulation (EC) No. 45/2001.

6.3.3 The Staff Regulation

The online survey also raises the issue of Regulation No. 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community[105] (hereinafter the "Staff Regulations").

The Staff Regulations provide for many human resources management procedures that involve processing of personal data of staff members or candidates for staff member positions (i.e. recruitment, staff evaluation, administrative inquiries and disciplinary proceedings, administration and payment of individual entitlements, etc.). The main issues of the implementation and application of these procedures in accordance with Regulation (EC) No. 45/2001 relate to data

[101] Article 1 of the Archives Regulation
[102] Article 2.2 of the Archives Regulation
[103] Regulation (Euratom) No. 3 implementing Article 24 of the Treaty establishing the European Atomic Energy Community (OJ 406/58 of 6 Oct.1958)
[104] For example: Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 amending its internal Rules of Procedure (OJ 317/1 of 3 Dec.2001)
[105] Regulation No. 31 (EEC), 11 (EAEC), *laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community* (OJ 45 of 14 June 1962, p. 1385) as last amended by Regulation (EU, Euratom) No. 1023/2013 of the European Parliament and of the Council of 22 October 2013 (OJ L 287 of 29 Oct. 2013, p. 15)

retention. For more information on these issues, please refer to the case study dedicated to data retention in the context of human resources.

6.3.4 The Financial Regulation

Amongst others, Regulation (EU, Euratom) No. 966/2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No. 1605/2002[106] (hereinafter the "Financial Regulation") contains provisions on the budget of the Union and provisions on procurement.

Firstly, according to this Regulation, the Commission shall include information on borrowing and lending operations in an Annex to the EU budget and shall make available information on recipients of these operations and on the nature and purpose of the measure financed. It is specified that this information shall be made available in compliance with the rules governing the protection of personal data. [107].

For that purpose, in order to comply with data quality principles, particularly the principle of proportionality of the data collected[108], where natural persons are concerned, the Regulation limits the published information to the name and location of the recipient, the amount awarded and the purpose of the award. The disclosure of those data shall be based on relevant criteria such as the frequency of award, or the type or importance of the award.[109]

The Regulation apparently anticipates contradictions with regulation (EC) No. 45/2001, but the notion of "relevant criteria" could be clarified.

Secondly, pursuant to the Financial Regulation, the Commission shall publish in the Official Journal of the European Union all public contracts exceeding specific thresholds[110]. However, these contracts may contain personal data, so their systematic publication would interfere with data subjects' rights to privacy and to personal data protection.

Interviews with stakeholders did not indicate practical coherence issues.

6.3.5 The Clinical Trials Regulation

Regulation (EU) No. 536/2014 of 16 April 2014 on clinical trials on medicinal products for human use[111] (hereinafter the "Clinical Trials Regulation") aims to facilitate the application process for clinical trials on medicinal products for human use, especially for multinational trials. In the course of Clinical Trials, personal data of participants to the trial may be processed, included sensitive data such as health data.

In theory, pursuant to Article 10 of Regulation (EC) No. 45/2001, sensitive personal data cannot be processed except for in predefined situations; this is notably the case of prior consent of the person participating in the trial. Article 10 provides for additional derogations to the prohibition on processing personal data including "where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the

[106] Regulation (EU, Euratom) No 966/2012 of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No. 1605/2002 (OJ L 298 of 26 Oct.2012, p.1)
[107] Article 35 of the Financial Regulation
[108] Article 4 of Regulation (EC) No. 45/2001
[109] Article 35 of the Financial Regulation.
[110] Article 103 of the Financial Regulation
[111] Regulation (EU) No. 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158 of 27 May 2014, p. 1)

obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy."[112].

For that reason, in its opinion on the Commission proposal for the Clinical Trials Regulation, the EDPS stated that: "*The notion of informed consent is central in data protection law. However, the EDPS understands that consent, even if it is the basis for a patient's participation in the clinical trial, is not the basis for processing and storage of personal data under the proposed Regulation. He will therefore not comment on the specific provisions concerning informed consent in the proposed Regulation*".

Nevertheless, it has been pointed out that after the adoption of this opinion, Chapter V relating to "*Protection of subjects and informed* consent" of the proposed Clinical Trials Regulation has been modified such that the consent of participants becomes the basis of the collection and processing of personal data for the purpose of clinical trials. Because of this modification, the Clinical Trials Regulation requires collecting prior consent from the trial participants to use their data outside the protocol of the clinical trial, for example, when universities or other research institutions are able to collect data from clinical trials to be used for future medical, natural or social sciences research purposes[113].

According to stakeholders, this requirement is too restrictive since it could disrupt the appropriate flow of information on the safety and efficacy of medicinal products in the EU. According to these stakeholders, the prior consent of trial participants collected in highly protected circumstances should be sufficient to further processing of health data collected for preventive medicine.

In our opinion, this issue does not need to be tackled in the context of the amendment of Regulation (EC) No. 45/2001.

[112] Article 10(3) of Regulation (EC) No. 45/2001
[113] Recital 25(a) and Article 28(2)(a) of the Clinical Trial Regulation

7 Impact

As a preliminary remark, it should be underlined that Regulation (EC) No. 45/2001 is still relevant in numerous ways. A large number of principles and rules provided by the proposed GDPR were already included in Regulation (EC) No. 45/ 2001.

Within the context of the adoption by the European Commission of a proposal reform package including the General Data Protection Regulation laying down the EU framework for data protection and replacing Directive 95/46/EC, it is important to put Regulation (EC) No. 45/2001 into perspective with some of the key provisions of this text, in order to project the potential impact created by possible amendments.

Indeed, EU institutions and bodies engage in a wide range of data processing operations. In the performance of this processing, these bodies should be bound by data protection rules and principles that provide as much protection as those applicable to all Member States.

Specific GDPR rules and principles have been identified during the inception phase:

1. Clarification of the principle of data minimization;
2. Introduction of the transparency principle and the increased information obligation;
3. Introduction of the right to be forgotten and data portability
4. Enhancing accountability of data controllers and reinforcing security: obligation to perform Privacy Impact Assessments, introduction of certification schemes and codes of conduct, notification of personal data breach and data protection by design and by default.

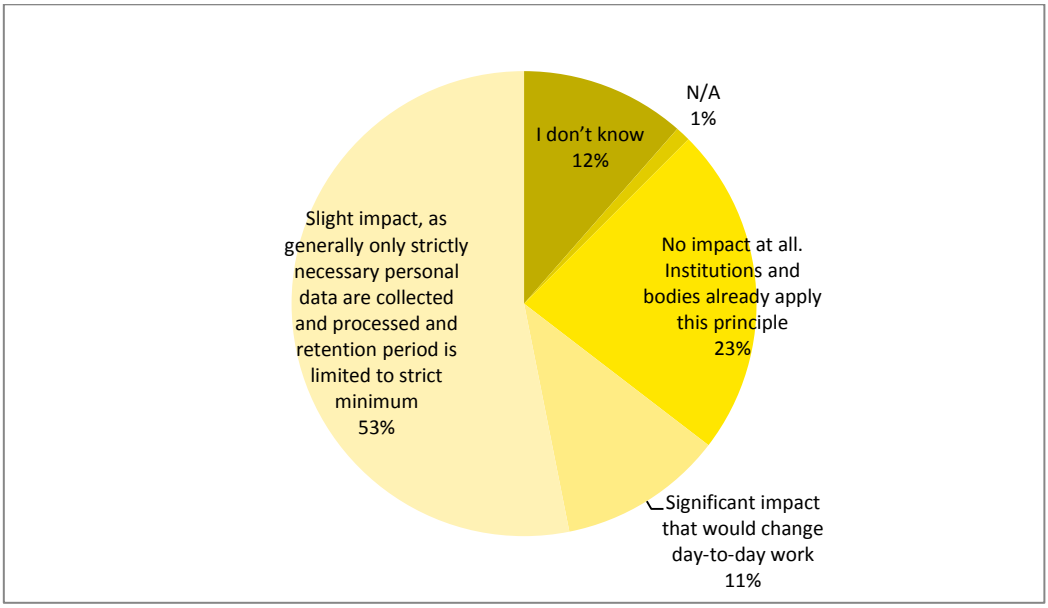
7.1 Clarification of the principle of data minimization

Article 5 (c) of the GDPR provides for the principle of data minimization whereby only the necessary minimum of personal data shall be collected in accordance with the purposes for which they are processed, replacing the words "*not excessive*" by the expression "*limited to the minimum necessary*".

The principle of data minimization is largely covered by Article 4 (c) of Regulation (EC) No. 45/2001.

The online survey shows that a large majority of DPOs and DPCs consider that this principle is highly relevant for EU institutions and bodies and already take it into consideration when designing processing of personal data. Similarly, a large majority of the respondents consider that introduction of the principle of minimization would result in minimal or even non-existent impact on EU institutions or bodies.

Figure 34 - What could be the impact of the implementation and application of such principle on your day-to-day work? (Source: EY survey)



7.2 Introduction of the transparency principle and increased information obligation

7.2.1 Introduction of the transparency principle

Article 5 of the GDPR also introduces a new principle of transparency, whereby personal data must be processed in a manner transparent for the data subject.

According to the online survey, increasing the transparency of processing activities would be an effective tool for improving accountability. The introduction of such a principle would not have a significant impact on EU institutions and bodies.

7.2.2 Increased information obligation

As a consequence to the introduction of the principle of transparency, the proposed GDPR provides for an increased obligation to inform data subjects. In addition to the obligations already provided for in Articles 10 and 11 of Directive 95/46/EC, the data controller shall provide information to the data subject on items such as the storage period, the right to lodge a complaint, international transfers and the source from which the data originate. Regulation (EC) No. 45/2001 already provides for an extensive obligation to inform data subjects (i.e. the obligation to provide information such as the legal grounds of the processing operation, time limits for storing the data, the right to have recourse to the EDPS at any time). The obligation to inform is already considered burdensome by data controllers and DPOs who draft the information notices. An increase in the level of information would increase the burden on data controllers and DPOs.

7.3 Introduction of the right to be forgotten and data portability

7.3.1 Introduction of the right to be forgotten

Article 17 of the proposed GDPR lays down data subjects' right to be forgotten according to specific conditions.

This right is already expressed in Regulation (EC) No. 45/2001 to a certain extent by the obligation to keep personal data for no longer than necessary for the purpose for which they were collected, combined with the right to erasure and the right to objectThe introduction of such a right to be forgotten in Regulation (EC) No. 45/2001 would not have a significant impact on EU institutions and bodies Indeed the right to block personal data already covers some of the provisions provided for in the proposed GDPR.

7.3.2 Introduction of the right to data portability

Article 18 of the GDPR provides for the data subject's right to data portability. This means that the data subject has the right to obtain transmission of its personal data in a structured, commonly-used electronic format, in order to transfer them from one electronic processing system to another without any possibility for the controller to prevent him from doing so.

Article 13 of the Regulation enshrines the right of access in an intelligible form (Article 13 (c)) which is very similar to the right enshrined in article 18 of the proposed GDPR. Our understanding is that the "electronic means" referred to in the GDPR are covered by the intelligible form as laid down in Article 13. The right to data portability could nevertheless be difficult to implement in the context of IT systems.

7.4 Enhancing accountability of data controllers and reinforcing security

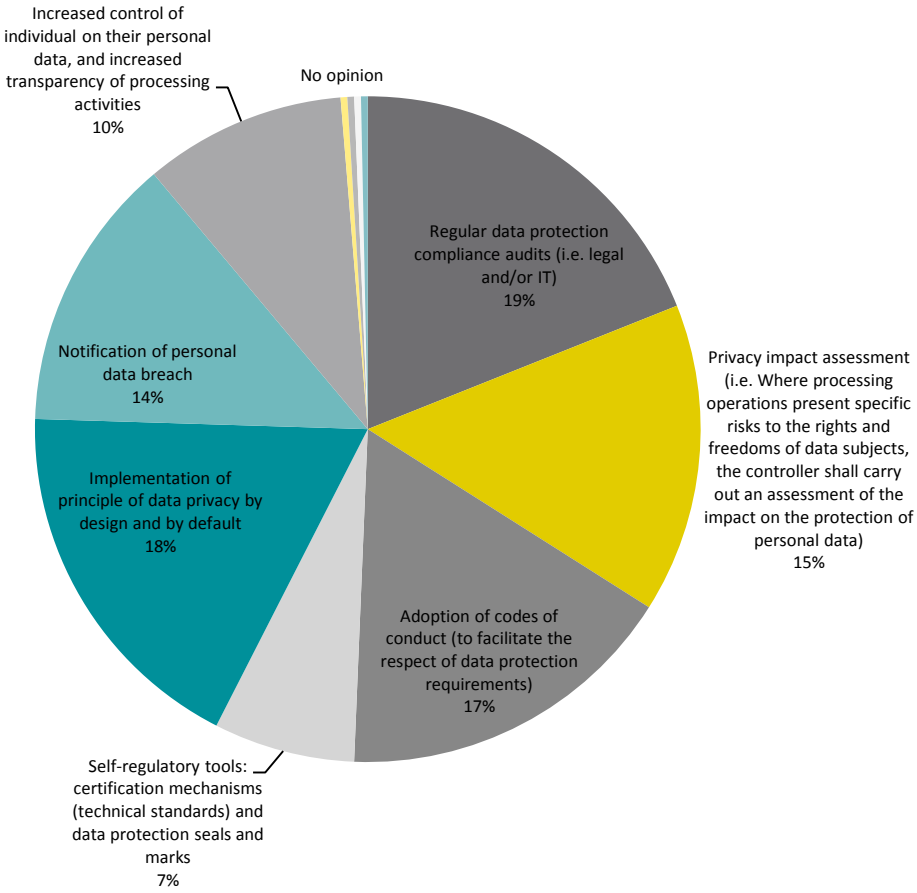
Article 22 of the proposed GDPR relates to the principle of responsibility and accountability of the data controller. Several tools are provided for such as an (i) the obligation to perform Privacy Impact assessments (PIA), (ii) certification schemes and codes of conduct, (iii) the notification of personal data breaches and (iv) the principles of data protection by design or by default.

As a preliminary remark, it should be underlined that the EDPS already applies the "risk-based approach" and principle of accountability in advising the EU institutions and bodies (on this point cf. the position paper on "Policy on consultations in the field of Supervision and Enforcement")[114].

DPOs and DPCs have expressed their views on the most suitable accountability mechanisms in the EU institutional environment.

[114] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/12-11-23_Policy_on_Consultations_EN.pdf.

Figure 35 - Which mechanisms would best improve accountability in the context of EU institutions and bodies? (Source: EY survey)



7.4.1 Obligation to perform Privacy Impact Assessments (PIA)

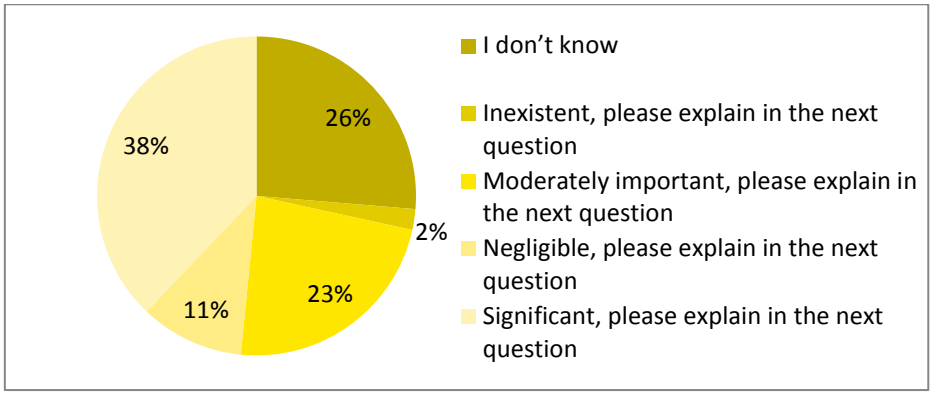
Article 33 of the GDPR introduced the obligation of controllers and processors to carry out a data protection impact assessment prior to the processing of operations which present specific risks.

It becomes clear from the online survey that the performance of PIAs would enhance the level of protection of personal data and it appears that PIAs are already performed in a few EU institutions and bodies (e.g. when new IT applications are implemented).

Nevertheless, stakeholders pointed out the performance of PIAs would involve consider reliance on DPOs, possibly with support from DPCs, and that it will significantly increase their administrative burden.

According to the majority of respondents, the impact of the introduction of the obligation to perform Privacy Impact Assessments prior to risky processing operations would be significant or at least moderately significant.

Figure 36 – What would be the impact of the introduction of the Privacy Impact Assessments prior to risky processing operations? (Source: EY survey)



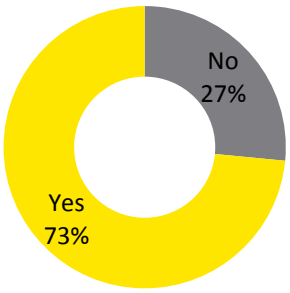
Should the Privacy Impact Assessment mechanisms be introduced in Regulation (EC) No. 45/2001, DPOs and DPCs underline that mitigation measures should be taken, such as a clear definition of the notion of risk and the creation of guidance and templates in order to standardize the procedure and official recognition of respective roles in the process.

7.4.2 Introduction of certification schemes and codes of conduct

Codes of conduct

The online survey shows that numerous DPCs and DPOs consider that it would be worthwhile to create codes of conduct on better protection of personal data and simplification of the work.

Figure 37 – Do you think it would be worthwhile to create a code of conduct in terms of better protection of personal data and simplification of the work? (Source: EY survey)



DPOs and data controllers note that these codes of conduct could facilitate access to information on data protection obligations. These codes of conduct should be practical (and not merely "legalistic").

Introduction of certification mechanisms

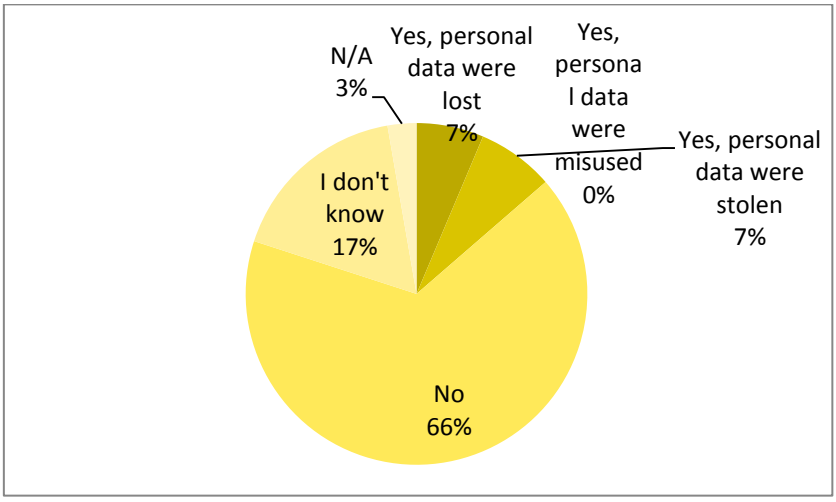
Article 39 of the GDPR introduces the possibility of establishing certification mechanisms and data protection seals and marks.

Such mechanisms are self-regulatory and could be seen as means to encourage EU institutions and bodies to comply with data protection requirements. Nevertheless, the online survey shows that DPOs and DPCs consider this tool to be the least relevant proposed.

7.4.3 Notification of personal data breach

In the context of EU institutions and bodies, it appears from the online survey that personal data breaches are not very frequent:

Figure 38 –Have you ever experienced personal data breaches? (Source: EY survey)



However it seems that in the few reported cases of data breaches, notification of data breaches were made. . Sometimes, personal breaches were reported to the EDPS but they were reported to DPOs more often. They were also occasionally reported to data subjects, but not systematically.

Nevertheless, DPOs and DPCs have differing opinions on such a mechanism.

Figure 39 - Do you think that this rule is useful and should be kept in future Regulation (EC) 45/2001? (Source: EY survey)

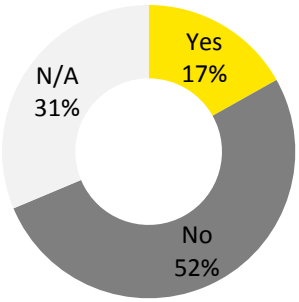
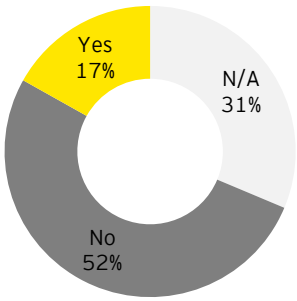


Figure 40 - Should you consider that the implementation and application of the obligation to notify data breaches would have an impact on your day to day work, do you know any mitigation measures that could be taken? (Source: EY survey)



Should such a mechanism be introduced in Regulation (EC) No. 45/2001, it should be determined whether personal data breaches would be notified to the EDPS or to DPOs. Systematic notification to the EDPS would increase its administrative burden. Therefore, it may be envisaged (i) to establish a risk *threshold* above which the breach would be notified to the EDPS and (ii) to notify all personal data breaches to the DPO. In any case it would be necessary to introduce an obligation to notify personal data breaches to data subjects concerned by the breach when the breach is likely to affect the protection of his personal data or privacy.

In the event a general obligation to notify personal data breaches is laid down in Regulation (EC) No. 45/2001, there would be no need to provide for an additional obligation to notify personal data breaches in the context of electronic communication (chapter IV).

7.4.4 Data protection by design and by default

Article 23 of the GDPR enshrines the principles of data protection by design or by default, which means that data protection safeguards should be built into products and services from the earliest stage of development and privacy-friendly default settings should be the norm.

According to the online survey, privacy by design and privacy by default would effectively play a role in improving accountability and should be the standard. Moreover, these principles are already in use in several EU institutions and bodies.

8 Key findings and recommendations

Regulation (EC) No 45/2001 remains, to a large extent, a highly relevant legal framework in order to meet the twofold objectives of ensuring the free flow of data while protecting fundamental rights. The appropriateness of this legal instrument is reflected in the fact that a sizable number of provisions of Regulation (EC) No 45/2001 have been introduced in the GDPR.

Although the provisions of the Regulation are not systematically and fully implemented through formalized processes and procedures, the Regulation is applied to a large extent and has contributed to the development of an effective and efficient data protection system within the EU institutional framework.

It follows from the foregoing that the Regulation and its application contribute highly to its general objectives. In particular, an effective and efficient governance system has been put in place and has gained in maturity over the past years.

Within this context, the evaluator has developed 10 main key findings and has drawn up several proposed recommendations[115]. In view of the future amendment in the light of the proposed GDPR, it is important to provide an equivalent level of data protection for EU institutions and bodies while respecting the particulars of the EU institutional framework.

8.1 An effective governance system, structured around two pillars: the DPO and the EDPS

The current Regulation describes the tasks, duties and powers of the DPO and the EDPS, acting as key governance stakeholders.

The Regulation provides for a satisfactory range of powers for the EDPS (although these are not fully applied) and for the DPOs (that are to be further specified in implementing rules).

- **The Regulation provides for an appropriate range of powers for DPOs and the EDPS….**

  The range of supervisory and enforcement powers conferred on the EDPS by Article 47 of Regulation (EC) No 45/2001 is extensive and appears satisfactory for the purposes of monitoring the application of the Regulation. This range of powers also includes the power to warn or admonish the controller, which has rarely been used in practice. As regards the DPOs, it stems from the evaluation that the list of tasks conferred by the Regulation is appropriate (Article 24 and Annex).

  The share of powers between DPOs and the EDPS is clear and well balanced. The share of powers and responsibilities is well balanced between the EDPS and DPOs. The DPO is in charge of ensuring the internal application of the provisions of the Regulation (Article 24.1

[115] N.B.: The findings are not presented in any particular order of importance. They are a synthesis of all the findings of the study.

b), whereas the EDPS monitors and ensures the application of the provisions of the Regulation by providing legal support to DPOs in the performance of their tasks, as well as supervising the level of implementation and application of the Regulation. In the exercise of its powers, the EDPS acknowledges the DPOs' key role in the monitoring of the internal application of the Regulation (e.g. in the processing of complaints or consultation before administrative measures are taken).

The evaluation acknowledges the utility of DPCs within institutions to improve the quality of compliance with data protection rules: they play a key role in transposing and relaying the rules within their units and departments. However, the evaluator's viewpoint is that the decision to establish a DPC network within an institution should be left to the institution itself in order to offer flexibility in a very heterogeneous context.

- **... Although some practical difficulties may arise in the exercise of the powers and duties:**

The DPOs may **lack the authority and support from their management** in **order to perform their tasks.** This is particularly relevant for the DPOs of small agencies. The DPOs of the largest institutions obtain valuable support from both their hierarchy and the DPCs. The roles and responsibilities of DPCs seem to differ from one institution to another in response to the specific needs and organisation of the institution. In practice, the evaluation shows that direct reporting to the highest management level (such as the Executive Director) and the allocation of a sufficient amount of time to data protection issues are key to enabling the effective application of the Regulation. **In this regard, the position of the DPC is crucial in order for the latter to be able to perform his or her tasks efficiently.**

The efficiency analysis identifies bottlenecks in the DPOs' activities: certain time-consuming activities prevent them from being able to perform all their tasks, including that of increasing the level of knowledge on data protection rules within their institution. In this context, the EDPS' supervisory role is central in order to provide assistance to DPOs in performing their tasks. The strengthening of the EDPS' supervisory and enforcement activities could also facilitate the DPOs' tasks, and as a result, ensure the satisfactory application of the provisions of the Regulation (see recommendation 8.2).

8.2 The system for the enforcement of the Regulation could be enhanced, notably through greater use of sanctions

Regulation (EC) No 45/2001 provides the EDPS with an extensive range of powers in order to monitor the application of the Regulation. Even though the EDPS has effectively and efficiently implemented and applied its supervisory tasks (prior checking, processing of complaints, inspections...), the EDPS has applied its sanctioning powers in a limited manner.

Indeed, the EDPS does not apply its power to impose sanctions upon EU institutions and bodies, even though the appropriateness of the range of powers provided by the Regulation is not questioned by the stakeholders. Within the institutional framework, the work of the EDPS has focused on cooperation with EU institutions and bodies towards compliance (e.g. compliance visits) and has rarely used its power to warn or admonish data controllers or to ban a processing operation. The mere existence of these powers may be dissuasive according to the EDPS. In this regard, the EDPS underlines that there is a high level of compliance when the EDPS takes action, even if such action does not involve enforcement measures (e.g. compliance visits), and sanctions

are only applied if other measures are not sufficient to ensure compliance (*"escalation strategy"*). In addition, offenders within an EU institution or body are never (or extremely rarely) sanctioned for failure to comply with the rules enshrined in the Regulation. This limited application of the sanctioning system may reduce the incentive for data controllers to comply with their data protection obligations.

Considering the limited level of awareness on data protection matters in many EU institutions and bodies, the **evaluator believes that the increased application of the enforcement powers of the EDPS (notably inspections and sanctions) towards institutions and bodies could be a relevant incentive to promote the implementation of data protection rules within the hierarchy of the EU institutions and bodies.**

However, the assessment study also shows that the application of enforcement actions within the EU institutional framework is unusual. In this regard, the alignment of this Regulation with the GDPR should take into consideration the particulars of the EU institutions and bodies. In particular, the proposed GDPR gives the supervisory authorities the power to impose pecuniary sanctions in the event of violation of the Regulation. The amendment of the Regulation should assess whether this power is relevant within the EU institutional framework.

8.3 Some of the Regulation's key requirements (e.g. on data retention or data security) need to be better implemented to achieve "real and operational" compliance

- **Several stakeholders perceive personal data security as being insufficient**

The overall level of implementation and application of the principles set out in Article 22 remains low. Some misinterpretations remain and prevent EU institutions and bodies from effectively assessing the risks associated with the processing of personal data. The evaluation points out that, on average, the level of security of IT systems with regard to data protection is low, except within the main EU institutions.

Old IT systems may hamper the capacity of the mechanisms in place for the exercise of rights, as in certain circumstances complex manual intervention may be required (in particular, the implementation of the data retention period in IT systems is perceived as being badly monitored). In this regard, it should be emphasised that new systems are usually designed to take into account data protection obligations in the light of the "privacy and data protection by design" principle.

In order to improve the level of implementation and application, several recommendations are made:

- **Introduction of a risk management approach: raise awareness of data controllers to perform privacy risk assessments before carrying out the processing operations.** During the last decade, the stress has been put on the performance of notifications and prior checking. While these mechanisms have shown significant benefits for the protection of personal data, **it is also critical to focus on real and operational compliance according to the risk-based approach promoted by the GDPR, making it possible to strengthen the responsibility and accountability of the data controller. Therefore, notification and prior checking procedures could be reshaped in order to allow DPOs to effectively work on raising awareness within the EU institutions and bodies.**

- Publication of specific guidance and provision of mandatory training by the EDPS or the EU institutions and bodies relating to the interpretation and application of Article 22, including the risk assessment/management methodology for staff involved in data protection and local information security officers
- **Performance of regular compliance checks and inspections by the EDPS in order to raise awareness on compliance.**

8.4 Effective communication channels between the EDPS and EU institutions and bodies, even if there is still room for improvement

Effective cooperation between the EDPS and EU institutions and bodies, but further improvements could be made

Articles 29, 30 and 31 of Regulation (EC) No 45/2001 provide for the obligations of the controller (i) to provide information to the EDPS in the cases provided by Article 46(h) (*e.g.* in the context of authorizations and exemptions) and (ii) to cooperate with and to react to allegations by the EDPS in the course of investigations.

These obligations are effectively implemented and applied by the EU institutions and bodies. The latter are cooperative and reactive in the course of investigations by the EDPS. In this regard, the DPOs play a key role in the preparation of the investigations. Nevertheless, it was pointed out that certain EU institutions and bodies sometimes delayed in responding to the EDPS. The quality of cooperation has increased over time, notably with regard to how EU institutions and bodies perceive inspections.

The answers provided by the EDPS when addressing a request from an institution or body are often perceived as too general and not clear enough for the controller. DPOs and data controllers expect the EDPS to provide more pragmatic answers with concrete examples.

Several aspects of communication between EU institutions and bodies and the EDPS could be enhanced:

- clearer and more specific communication by the EDPS to EU institutions and bodies;
- Greater use of and leverage on best practices and existing procedures in institutions and bodies to illustrate their opinions.

Effective exchange of information between EU institutions and bodies through the DPO network

The exchange of information on data protection between EU institutions and bodies is largely supported by internal cooperation between DPOs, notably thanks to the DPO network meetings. The DPO network has proven to be an important tool to strengthen compliance.

In this regard, the DPOs underline that communication between the EDPS and EU institutions and bodies during the DPO network meetings could be further improved, notably by the increased involvement of the EDPS (e.g. real discussions between DPOs and the EDPS, increasing the presence of the EDPS from half a day to a whole day).

8.5 The rules enshrined in chapter IV relating to the telecommunications sector are outdated

Chapter IV of the Regulation focuses on the protection of personal data and privacy in the context of internal telecommunications networks.

The current rules enshrined in Chapter IV are outdated in the light of the provisions of the ePrivacy Directive. In this regard, it should be noted that the European Commission has already implemented and applied the provisions relating to the use of cookies.

The ePrivacy Directive may need to be revised after the adoption of the GDPR and it is essential to coordinate the amendment of chapter IV of Regulation (EC) No 45/2001 and the revision of the ePrivacy Directive. Otherwise, the Regulation will be aligned with an outdated text.

Finally, several stakeholders pointed out that the provisions relating to calling and connected line identification are now outdated. Nowadays, the staffs of EU entities are accustomed to calling and connected line identification due to the widespread use of mobile phones where these features are enabled by default.

8.6 The principles and rules enshrined in the Regulation are to a large extent relevant to meet the objectives of the Regulation, although some core definitions lack clarity

The principles and rules laid down in Regulation (EC) No 45/2001 are to a large extent highly relevant (rights of data subjects, obligations of data controllers, etc.) in order to meet the twofold aim of ensuring the protection and the free flow of personal data.

Nevertheless, some core principles or definitions enshrined in the Regulation lack clarity and consistency throughout the Regulation.

The following definitions and principles raise interpretation and application issues.

*Please note that this **list is not exhaustive (other examples are given in the report, such as the notion of "change of purpo**se (…) permitted by the internal rules of the Community institution and body", the notion of fair processing or the right of blocking).*

- **Identification of data controller**

The identification of the controller is unclear and inconsistent throughout the Regulation. In Article 2(d), it seems that the controller is the institution/body or the unit/department/directorate within the EU institution or body. It is unclear whether the controller is the EU institution or body, the directorate, the unit or other operational entity Moreover, the name and address of the controller effectively indicated in the registers are the details of the natural person responsible for the processing operation. The future Regulation should identify the controller more clearly, as this significantly impacts the interpretation of the other provisions of the Regulation (e.g. article 7 of the Regulation on transfers within or between Community institutions or bodies, or the notification requirements provided by article 25).

– **Confidentiality of processing**

The wording of Article 21 targets only internal data processors who act under the instructions of data controllers, and not external data processors. The scope of this Article should be broadened to include the data processing operations carried out by external service providers.

Moreover, the current provision could be interpreted as stating that any person employed within an EU institution or body who processes personal data under the instruction of a data controller could be considered to be a data processor. This would mean that an official acting under the instruction of his head of unit would be considered to be a data processor. Should an official acting on the instruction of the data controller be considered to be data processor, the provisions of Article 23 would be applicable to that official and the provisions of Article 22 would have to be included in a written binding document. Moreover, this could also be considered as a transfer of personal data pursuant to Article 7. The EDPS considers that an EU official acting under the instruction of his or her hierarchy is not a processor.

– **Unclear Definition of recipient**

The definition of a recipient is unclear and raises interpretation issues. In particular, there is an issue regarding this definition as to which bodies should be considered as an *"authority which may receive the data in the course of an inquiry"*, notably in the light of the application of Articles 7, 8 and 9 on the transfer of Personal Data. Some EU institutions and bodies have interpreted this exception as also covering the rules on transfer. The EDPS takes the view that only Articles 11 and 12 on information on data subjects do not apply to authorities which receive data within the framework of a particular inquiry. The rules on transfers apply to these authorities.

Moreover, it is unclear whether the Article refers to EU bodies or to authorities that are subject to Directive 95/46/EC, or even authorities in third countries.

8.7 Data protection matters in EU institutions and bodies represent an overall estimated cost of 28 million euros, although the allocation of resources could be questioned

The evaluation estimates that the application of the Regulation costs EU institutions and bodies 28 million euros, with 28% of this budget dedicated to the EDPS, 39% to DPOs and DPCs implementing the Regulation in their institutions, and 33% corresponding to the cost of data controllers' data protection activities.

Within the EDPS, the allocation of resources per objective assigned is balanced between supervisory and advisory activities. Both units in charge of these roles have increased their activities in the last few years, without increasing the number of staff dedicated to each unit. Both units have benefited from efficiency gains in the last five years, although reinforcing the EDPS' supervisory role would help DPOs to raise awareness in EU institutions and bodies.

This allocation of staff could be analysed with regard to the significant weight given to supervisory activities in the regulation (Articles 41, 46 and 47) as compared to advisory activities (Article 28.2), bearing in mind that the advisory activities of the Policy and Consultation Unit go beyond the scope of Article 28.2 (e.g. providing the Secretariat for Coordinated Supervision Groups, dealing with litigation, cooperating with supervisory authorities within the framework of the Article 29 Working Party and participating in international forums).

- **As regards the DPOs**, many of them struggle to perform all the tasks assigned to them by the Regulation within the limited time they spend on data protection matters (generally part-time DPOs). In addition, they stated that they spend too much time on activities that should normally be performed by data controllers (Article 25 on the drafting of notifications, or Article 24 on the informing of data subjects). These activities represent 18% of their time spent on DPO duties.
- A reallocation of these resources in favour of other activities aiming to raise awareness on data protection matters would better reflect the tasks assigned to DPOs in the Regulation. In addition, strengthening the position of DPOs in EU institutions and bodies could also facilitate the implementation and application of the Regulation within the latter. This could be achieved by (1) giving DPOs a higher position in the organisation chart and better support from the management, (2) having DPOs focus more on data protection matters, i.e. full-time instead of part-time DPOs (DPOs shared between institutions) and (3) the capacity of IT systems to embed the relevant security requirements.

  Data controllers' responses are in line with these observations and many of them confirm that they spend too much time on the drafting of notifications.

- Several suggestions are made to increase the efficiency of these tasks: a standard template for notification, IT tools embedding security requirements, synergies between EU institutions and bodies.

8.8 The notification and prior checking system is excessively burdensome

Prior checks are effectively implemented and performed by the EDPS, although some drawbacks have been underlined. Given the importance of the time spent by the EDPS on this activity, the latter has developed several efficient means to facilitate and accelerate the performance of prior checks (such as the use of guidelines).

It follows from the foregoing that Articles 25.1, 27 and 46 (j) of Regulation (EC) No 45/2001 are effectively implemented and applied. However, some further improvements could be considered (and/or are already foreseen by the EDPS).

- **DPOs and data controllers focus their efforts on prior checking in order to prove compliance with Regulation (EC) No 45/2001.** In light of the "risk-based approach", emphasis should be put on the implementation of the prior checks opinions and recommendations and thus on compliance with the data protection principles and the rights of data subjects enshrined in Regulation (EC) No 45/2001 (see finding 8.2).
- **The performance of prior checks is time-consuming for the EDPS and for the DPOs in charge of drafting the notifications. The preliminary analysis of eligibility for prior checks contributes to the heavy burden represented by the prior check procedure. Further clarification of the scope of prior checking could help to reduce unfounded prior check notifications. This burden prevents the EDPS from focusing on the performance of the prior check itself.**
- Some stakeholders favour the introduction of a "block exemption" system in line with the current practices of adopting guidelines to facilitate the prior checking process. Nevertheless, it might be relevant to narrow the scope of prior checking to risky operations.
- Regarding the notification of data processing operations (Article 25.1), the scope of the notification could be **reduced while introducing an obligation for the DPO to keep a record**

of the data processing operations in an inventory, which would be in line with "the risk-based approach" promoted by the GDPR. It is crucial to stress that this option would only be effective if an adequate level of maturity towards data protection issues is achieved within EU institutions and bodies.

8.9 The articulation of access to documents and data protection has raised operational difficulties

These fundamental rights have been implemented respectively in Regulation (EC) No 45/2001, which regulates and guarantees the protection of individuals' data by EU institutions[116], and Regulation (EC) No 1049/2001, which recognises the right of access to EU documents that might contain those data[117]. However, these Regulations may have contradicting aims: whereas the objective of Regulation (EC) No 1049/2001 is to provide 'the fullest possible effect to the right of public access to documents'[118] ensuring transparency of the public decision-making process, Regulation (EC) No 45/2001 focuses on the protection of personal data and delimits their disclosure.[119] Therefore, a conflict may arise in cases where a document subject to an access-to-documents request contains data such as the names and other details of participants in a meeting organised by a Union institution or information on persons employed by the institution.[120]

The source of this tension lies in the conflict of the texts (and their application) between Article 6(1) of Regulation (EC) N°1049/2001 – which states explicitly that applicants for access to documents are not obliged to state reasons for the application – and Article 8(b) of Regulation 45/2001 – which states that the recipient must establish the necessity of having the data transferred. However, Article 4 1 (b) of the Regulation underlines that an EU institution must refuse access to a document where disclosure would undermine the protection of the individual's privacy and integrity, in particular in accordance with Community legislation regarding the protection of personal data.

The interpretation and application of these provisions have raised operational and practical issues.

The case law of the Court of Justice (Bavarian Lager and subsequent cases) has strived to identify a *modus vivendi* in the application of Regulation (EC) N°1049/2001 and Regulation 45/2001.It appears most likely that in the case law of the Court of Justice on the relationship between access to documents and data protection (Bavarian Lager), the *renvoi* theory will continue to prevail over the threshold theory.

The question has been raised as to whether the tension between access to documents and the protection of personal data should be resolved in the amendment of Regulation (EC) No 45/2001. Should this be the case, **the new, revised Regulation (EC) No 45/2001 could start from the**

[116] The Regulation implements Article 286 of the Treaty establishing the European Communities which requires the application of data protection rules to Community institutions and bodies, as well as the establishment of an independent supervisory authority. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12 January 2001, at 1- 22; (hereinafter: Data Protection Regulation).

[117] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31 May 2001, at 43-48; (hereinafter: Access to Documents Regulation)

[118] Access to Documents Regulation, Preamble 4

[119] Case T- 194/04 Bavarian Lager v. Commission, [2007] ECR- II 4523, para 98

[120] Although the debate on the conflict of access to documents and the protection of personal data already arose before the adoption of Regulation (EC) No 45/2001 and Regulation (EC) No 1049/2001, as shown by the events preceding the Bavarian Lager Case (Ombudsman Case 713/98/IJH, available via: http://www.ombudsman.europa.eu/en/cases/specialreport.faces/en/380/html.bookmark), this analysis will focus on these two Regulations as providing the current legislative framework for the debate.

premise that under Regulation (EC) No 1049/2001 – as interpreted by the Court in the Bavarian Lager case – data protection rules can limit access to documents (Article 4-1-b), and that an applicant must comply with Article 8 (b) of Regulation (EC) No 45/2001 and justify the necessity to obtain the personal data. Nevertheless, it is uncertain whether (i) Regulation (EC) No 45/2001 should address issues of coherence with other legislations, as Regulation (EC) No 1049/2001 already provides for an exception pertaining to the protection of personal data (and in particular, on what legal basis this could be achieved); (ii) the amendment of Regulation (EC) No 45/2001 would resolve the practical issues faced by EU institutions and bodies.

8.10 The transfer rules and mechanisms need to be clarified and simplified

Exchanges of personal data within or outside the EU institutions are developing fast. Solutions need to be put in place to facilitate the free flow of personal data while maintaining a high level of protection of personal data.

Regulation (EC) No 45/2001 sets out the rules governing the transfer of personal data within or between EU institutions and bodies (i) to recipients other than EU institutions and bodies subject to Directive 95/46/EC (ii) and to recipients other than EU institutions and bodies in third countries (iii).

Some stakeholders have questioned the relevance of the rules on the transfer of personal data within or between EU institutions and bodies. Moreover, the provisions relating to the transfer of personal data have raised interpretation issues and operational and practical difficulties.

Relevance of the rules on transfer:

- The transfer of personal data within or between the EU institutions to recipients subject to Directive 95/46/EC and to recipients in third countries are subject to specific conditions laid down by Articles 7 to 9 of the Regulation. The conditions are stricter for transfer outside the EU institutional remit and outside the European Union, as the risks associated with such transfer may be significant.
- The rules governing the transfer of personal data outside the EU (Article 9) are not appropriate insofar as they require that EU institutions and bodies assess the level of adequacy of third countries or international organisations. In practical terms, this analysis is not feasible, as the EU institutions and bodies lack the appropriate skills and resources. The assessment of adequacy is burdensome and difficult for EU institutions and bodies to perform. The use of standard contractual clauses (validated by the EDPS) could be a satisfactory way of facilitating international transfer and ensuring the free flow of data while maintaining a high level of protection of personal data.

Operational/practical difficulties

- Article 7 of Regulation (EC) No 45/2001 dealing with the transfer of personal data within EU institutions and bodies has given rise to interpretation issues regarding the notions of "transfers" and of the "competence" of the recipient. Data controllers have difficulty in assessing and qualifying transfer situations. This uncertainty may hinder the free flow of personal data.

- Article 8 of the Regulation only provides for rules applicable to the transfer of personal data requested by the recipient and does not include rules applicable when the transfer is initiated by an EU institution or body.
- EU institutions and bodies also experience difficulties in applying the criteria set out in Article 9 for transfer to third countries, in particular in the context of transfer to international organisations (where the use of standard contractual clauses may not be appropriate).

8.11 Shortcomings have been identified in the EDPS consultation process

- **The EDPS has fully implemented[121] and applied the obligation of consultation but it is not systematically consulted in the course of the legislative process.**

Pursuant to Article 28.2 of Regulation (EC) No 45/2001, one of the main tasks of the EDPS is to examine the data protection and privacy impact of proposed new legislation. Regulation (EC) No 45/2001 does not detail the consultation procedure but states that the European Commission "when it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, shall consult the European Data Protection Supervisor."
The evaluation study identifies certain drawbacks and shortcomings in the wording and the application of the provisions:

- **The Regulation specifies neither the exact timing for consultation nor the legislative instruments subject to consultation.**

As regards the timing of the consultation, it was underlined that the effectiveness of a consultation is increased when the consultation is carried out at an early stage. Indeed, consultation with the European Commission may take place at various stages of the legislative or policy-building process, just as it may occur at national level between data protection authorities and their legislator. At the stage of the Commission's draft, data protection issues may easily be taken into account in the proposal. Once the draft has been adopted (just before review by Parliament and the Council), it becomes more difficult for the EDPS to make its "data protection" case before Parliament and the Council.

As regards the legal instruments, some of the European Commission services are **not aware of the types of instruments that trigger the consultation process.** In this regard, the 2014 Consultation Policy paper has been a cornerstone for the EDPS insofar as it takes stock of 10 years of experience and provides useful information relating to this interpretation of the provision. Yet, it stems from the EDPS implementing procedures that the scope of consultation encompasses a broader range of texts than "legislative proposals".

- **The EU institutions may be reluctant to involve the EDPS in the legislative process.**

The EDPS is not systematically consulted by the European Commission in the legislative processes that have an impact on data protection. In some cases, there is resistance to consultation (due in particular to the confidentiality of the negotiations) and this matter should, according to the EDPS, be settled at the Regulation level.

[121] This obligation is implemented by the EDPS Rules of Procedure and the Policy paper on Consultation of June 2014, which interpret and provide a detailed procedure for legislative consultation.

Moreover, the EDPS underlines that it has to wait for official invitations to attend the meetings of the Council working groups, which are only provided if the EDPS is expected to make a presentation. For instance, the EDPS could not attend all the meetings relating to the General Data Protection Regulation (GDPR). **In** order to change this situation, the EDPS underlines that the EDPS should be recognized as a status with respect to the Council. However, it should be underlined that the Council has, several times, invited the EDPS to participate at meetings and discussions, even though it has no obligation to do so pursuant to Regulation (EC) No 45/2001 and the Treaties.

- **There are two available options in order to increase the effectiveness of the consultation obligation:**
  - **Hard Law:** amendment of Regulation (EC) No 45/2001. Article 28.2 of Regulation (EC) No 45/2001 could be amended to specify the consultation process and types of texts submitted for consultation.
  - **Soft Law:** drafting of a Memorandum of Understanding. an alternative option would be to adopt a memorandum of understanding between the three legislative institutions (European Commission, Council of the European Union and European Parliament) and the EDPS.

9 Annexes

9.1 List of DPOs and DPCs

Name of institution or body	DPOs	DPCs
European Central Bank (ECB)	1	10
European Parliament	1	12
European External Action Service (EEAS)	1	16
European Commission	1	36
Council of the European Union	1	39
Agency for Fundamental Rights (FRA)	1	
Agency for the Cooperation of Energy Regulators (ACER)	1	
ARTEMIS Joint Undertaking	1	
Body of European Regulators for Electronic Communications (BEREC)	1	
Clean Sky Joint Undertaking	1	
Committee of the Regions (CoR)	1	
Community Plant Variety Office (CPVO)	1	
Consumer, Health and Food Executive Agency (Chafea)	1	
Court of Justice of the European Union	1	
Education, Audiovisual and Culture Executive Agency (EACEA)	1	
ENIAC Joint Undertaking	1	
EU-LISA	1	
European Agency for Safety and Health at Work (EU-OSHA)	1	
European Agency for the Management of Operational Cooperation at the External Border (FRONTEX)	1	
European Anti-Fraud Office (OLAF)	1	
European Asylum Support Office (EASO)	1	
European Aviation Safety Agency (EASA)	1	
European Banking Authority (EBA)	1	
European Centre for Disease Prevention and Control (ECDC)	1	
European Centre for the Development of Vocational Training (CEDEFOP)	1	
European Chemicals Agency (ECHA)	1	
European Court of Auditors (ECA)	1	
European Defence Agency (EDA)	1	
European Economic and Social Committee (EESC)	1	
European Environment Agency (EEA)	1	
European Fisheries Control Agency (EFCA)	1	
European Food Safety Authority (EFSA)	1	
European Foundation for the Improvement of Living and Working Conditions (Eurofound)	1	
European GNSS Supervisory Authority	1	
European Institute for Gender Equality (EIGE)	1	
European Institute of Innovation and Technology (EIT)	1	
European Insurance and Occupations Pensions Authority (EIOPA)	1	
European Investment Bank (EIB)	1	

Name of institution or body	DPOs	DPCs
European Investment Fund (EIF)	1	
European Maritime Safety Agency (EMSA)	1	
European Medicines Agency (EMA)	1	
European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)	1	
European Network and Information Security Agency (ENISA)	1	
European Ombudsman	1	
European Police College (CEPOL)	1	
European Railway Agency (ERA)	1	
European Research Council Executive Agency (ERCEA)	1	
European Securities and Markets Authority (ESMA)	1	
European Training Fundation (ETF)	1	
European Union Institute for Security Studies (EUISS)	1	
European Union Satellite Centre (EUSC)	1	
Executive Agency for Small and Medium-sized Enterprises (EASME)	1	
Fuel Cells & Hydrogen Joint Undertaking	1	
Fusion for Energy	1	
Innovation and Networks Executive Agency (INEA)	1	
Innovative Medicines Initiatives Joint Undertaking	1	
Office for Harmonisation in the Internal Market (OHIM)	1	
Publication office	1	
Research Executive Agency (REA)	1	
SESAR Joint Undertaking	1	
Translation Centre for the Bodies of the European Union (CdT)	1	

9.2 List of consulted documentation

EDPS DOCUMENTS
- EDPS website (https://secure.edps.europa.eu/EDPSWEB/edps/EDPS)
EDPS Decisions
- Decision of 28 April 2009 laying down rules on the secondment of national experts to the EDPS and replacing European Data Protection decisions on the subject
- Decision 2013/504/EC of the European Data Protection Supervisor of 17 December 2012 on the adoption of Rules of Procedure, (OJ L 273 of 15 Oct. 2013, p. 41)
- Decision of 22 January 2013 concerning the provisions relating to the traineeships programme
EDPS Papers and Policies
- "The EDPS as an advisor to the Community institutions on proposals for legislation and related documents", Policy Paper, EDPS, 18 March 2005 (replaced by the Policy Paper of 4 June 2014)
- "Public access to documents and data protection", Background Paper, Series No.1, EDPS, July 2005
- "Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001", EDPS, 28 November 2005
- "Inspection policy and procedure", EDPS, version 2.0 – July 2009
- "Monitoring and Ensuring Compliance with Regulation (EC) 45/2001", Policy Paper, EDPS, 13 December 2010
- "Public access after Bavarian Lager", Background Paper, EDPS, 24 March 2011
- " Consultations in the field of Supervision and Enforcement", Policy Paper, EDPS, 23 November 2012
- "Inspections conducted by the EDPS", Policy Paper, EDPS, November 2013
- "The EDPS as an advisor to EU institutions on policy and legislation : building on ten years of experience", Policy Papers, EDPS, 4 June 2014
- "Transfer of personal data to third countries and international organisations by EU institutions and

	bodies", Position Paper, EDPS, 14 July 2014
-	"Stakeholders' Consultations - Future of Regulation 45/2001", Background Paper, EDPS
EDPS General Reports	
-	"Measuring compliance with Regulation (EC) 45/2001 in EU institutions and bodies (Spring 2007)", General Report, EDPS, Brussels, 14 May 2008
-	"Measuring compliance with Regulation (EC) 45/2001 in EU institutions and bodies (Spring 2009)", General Report, EDPS, 2009
-	"Monitoring compliance of EU institutions and bodies with Article 24 of Regulation (EC) 45/2001", Report on the Status of Data Protection Officers, EDPS, Brussels, 17 December 2012
-	"Measuring compliance with Regulation (EC) 45/2001 in EU institutions and bodies (Survey 2011)", General Report, EDPS, Brussels, 23 January 2012
-	"Survey on the Function of Data Protection Coordinators at the European Commission", General Report, EDPS, Brussels, 25 January 2013
-	"Measuring compliance with Regulation (EC) 45/2001 in EU institutions and bodies (Survey 2013)", General Report, EDPS, Brussels, 24 January 2014
EDPS Guidelines	
-	"Guidelines concerning the processing operations in the field of staff recruitment", EDPS, 10 October 2008
-	"Guidelines concerning the processing of health data in the workplace by Community institutions and bodies", EPDS, 28 September 2009
-	"Guidelines concerning the processing of personal data in administrative inquiries and disciplinary proceedings by European institutions and bodies", EDPS, 23 April 2010
-	"Guidelines concerning implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8)", EDPS, 29 July 2010
-	"Guidelines on evaluation of statutory staff in the context of annual appraisal, probation, promotion or regarding certification and attestation", EDPS, 15 July 2011 (2011-042)
-	"Guidelines concerning the processing of personal data in the area of leave and flexitime", EDPS, 20 December 2012
-	"Guidelines on the processing of personal data in the context of public procurement, grants and external experts", EDPS, 25 June 2013
-	"Inspection Guidelines", EDPS, November 2013
-	"Guidelines on the Rights of Individuals with regard to the Processing of Personal Data", EDPS, 25 February 2014
-	"Guidelines on data protection in EU financial services regulation", EDPS, 26 November 2014
-	"Guidelines on the processing of personal data with regard to the management of conflicts of interest in EU institutions and bodies", EDPS, 8 December 2014
EDPS Letters	
-	Letter by Christopher Docksey (EDPS, Director) to Paul Nemitz (DG JUST, Director Fundamental Rights and Citizenship), 2 July 2013
-	Letter by Marie-Hélène Boulanger (DG Justice, Head of Unit Data Protection) to Sophie Louveaux (EPDS, Head of Unit Supervision and Enforcement) and Hielcke Hijmans (EPDS, Head of Unit Policy and Consultations), "Consultation of DPCs on reform of Regulation 45/2001", 25 July 2013
-	Letter by Sophie Louveaux (EPDS, Head of Unit Supervision and Enforcement) and Hielcke Hijmans (EPDS, Head of Unit Policy and Consultations) to Marie-Hélène Boulanger (DG Justice, Head of Unit Data Protection), "Note on the application of Regulation 45/2001", 2 October 2013
-	Letter by Peter Hustinx (European Data Protection Supervisor) to Viviane Reding (Vice-President of Justice, Fundamental Rights and Citizenship in the European Commission), "Application of the proposed General Data Protection Regulation GDPR to EU institutions and bodies", 9 December 2013
-	Letter by Peter Hustinx (European Data Protection Supervisor), to Mr Maroš Šefčovič (Vice-President of the European Commission); Mr Juan Fernando López Aguilar (Chairman of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs) and to Ambassador Theodoros N. Sotiropoulos (Permanent Representative of Greece regarding the appointment of the European Data Protection Supervisor and Assistant Supervisor), 7 January 2014
EDPS Opinions	
-	Opinion on the notification for prior checking relating to internal administrative inquiries and disciplinary procedures within the European Commission, Brussels, 20 April 2005, Case 2004-187

-	Opinion on a notification for prior check on the system of "Recruitment, by competition, of permanent staff for the European institutions or for Community bodies, offices and agencies", Brussels, 24 February 2006, Case 2004-236
-	Opinion on a notification for prior Checking received from the Deputy Data Protection Officer of the European Commission on the "Management of personal data of Auxiliary Conference Interpreters (ACI) stored in Signalétique (application of the central database CORALIN)", Brussels, 22 December 2006, Case 2006-364
-	Comments by the European Data Protection Supervisor on the draft Common Conservation List (CCL), Brussels, 7 May 2007
-	Opinion on a notification for prior checking received from the Data Protection Officer of the Council on the "Selection procedure for trainees at the General Secretariat of the Council of the European Union", Brussels, 12 June 2007, Case 2007-217
-	Opinion on the notification for prior checking from the European Ombudsman's Data Protection Officer regarding the "disciplinary proceedings and administrative investigations" dossier, Brussels, 17 October 2007, Case 2007-0413
-	Opinion concerning recruitment of permanent, temporary and contract agents at European Maritime Safety Agency (EMSA), Brussels, 7 January 2008, Case 2007-566
-	Opinion on the « notification d'un contrôle préalable reçue du Délégué à la protection des données du Conseil de l'Union européenne à propos du dossier "Procédure d'embauche des fonctionnaires et autres agents du Secrétariat général du Conseil" », Brussels, 25 January 2008, Case 2007-194
-	Opinion on the notification for prior checking from the Data Protection Officer of the European Economic and Social Committee regarding the EESC internal administrative investigations and disciplinary proceedings, Brussels, 9 November 2009, Case 2008-569
-	Opinion on notifications for prior checking from the Data Protection Officers of certain EU agencies concerning the "processing of administrative inquiries and disciplinary proceedings", Brussels, 22 June 2011, Case 2010-072
-	Opinion on the updated notification concerning administrative inquiries and disciplinary proceedings within the Court of Justice of the EU, Brussels, 12 September 2011, Case 2011-0806
-	Opinion on the notification for prior checking from the Data Protection Officer of the Community Plant Variety Office concerning "Assessment and reporting on probationary periods" Brussels, 19 October 2011, Case 2011-0298
-	Letter from the EDPS to the DPO of the Court of Auditors, Brussels, 23 July 2012, Case 2011-0482
-	Opinion on a notification for prior check of the processing of personal data in the context of the selection and recruitment of Seconded National Experts ("SNEs"), trainees and interim agents the European Research Council Executive Agency, Brussels, 28 February 2013, Case 2012-0997
-	Opinion on the notification for prior checking received from the Data Protection Officer of the European Central Bank concerning the ECB's Underperformance Procedure, Brussels, 30 August 2013, Case 2013-0892
-	Opinion concerning the selection of the Chair of the Supervisory Board of the European Central Bank, Brussels, 20 September 2013, Case 2013-1007
-	Opinion on the notification for prior checking from the Data Protection Officer of the European External Action Service concerning annual appraisal, Brussels, 23 May 2013, Case 2013-0206
-	Opinion on a notification for prior check on the "staff assessment procedure" of the European Defense Agency, Brussels, 16 October 2013, Case 2013-0744
-	Opinion on prior-checking notification on the processing operations related to renewal of contracts for temporary and contract agents in the Innovation and Networks Executive Agency, Brussels, 12 June 2014, Case 2013-1288
-	Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2008/C 181/01

-	Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2009/C 128/04
-	Opinion on a notification for prior checking received from the Data Protection Officer of the European Union Agency for Fundamental Rights on the "the processing of personal data in the context of internships", Case 2013-0654
-	Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (OJ 2009, C 2/03)
-	Executive summary of the Opinion of the European Data Protection Supervisor on the Commission proposal for a regulation on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ C 253, 3.9.2013, p. 10.).
Other EDPS Documents	
-	EDPS Annual reports from 2004 to 2013
-	EPDS Strategic plan : "Strategy 2013 – 2014 : Towards excellence in data protection"
-	Remarks about "Implementing rules concerning tasks, duties and powers of the Data Protection Officer (Article 24.8)", EDPS
-	Presentation on "EU Data Protection Reform : The future of Regulation 45/2001", Sophie Louveaux, EDPS Head of Unit Supervision and Enforcement, European Commission – Data Protection Day, 28 January 2014
-	Revision of Regulation (EC) No. 45/2001, Contributions of DPO working groups, Working Group no. 1, EDPS
-	Revision of Regulation (EC) No. 45/2001, Contributions of DPO working groups, Working Group no. 2, EDPS
-	Revision of Regulation (EC) No. 45/2001, Contributions of DPO working groups, Working Group no. 3, EDPS
-	Revision of Regulation (EC) No. 45/2001, Contributions of DPO working groups, Working Group no. 4, EDPS
-	"Workshop 1 : Development of legal framework and future role of DPO", Moderator: Ph Renaudière, DPO European Commission, EDPS
-	"Perspectives of Independent Authorities : independence and more effectiveness", Peter Hustinx (European Data Protection Supervisor), in "The Independent Authorities in Modern democracy", Athens Concert Hall Conference, Megaron Plus, 2 April 2007
Article 29 Data Protection Working Party Documents	
-	Opinion 8/2006 of the Article 29 Data Protection Working Party on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive, 26 September 2006, 1611/06/EN, WP126
-	Opinion 1/2008 of the Article 29 Data Protection Working Party on data protection issues related to search engines, 4 April 2008, 00737/EN, WP 148
-	Opinion1/2009 of the Article 29 Data Protection Working Party on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy directive), 10 February 2009, 00350/09/EN, WP 159
-	Opinion 2/2010 of the Article 29 Data Protection Working Party on online behavioral advertising, 22 June 2010, 00909/10/EN, WP 171
-	Opinion 15/2011 of the Article 29 Data Protection Working Party on the definition of consent, 13 July 2011, 01197/11/EN, WP187
-	Opinion 04/2012 of the Article 29 Data Protection Working Party on Cookie Consent Exemption, 7 June 2012, 00879/12/EN, WP 194
-	Opinion 9/2014 of the Article 29 Data Protection Working Party on the application of Directive 2002/58/EC to device fingerprinting, 25 November 2014, 14/EN, WP 224
EU Documents	
EU Legislation	
-	Regulation (Euratom) No. 3 of 31 July 1958 implementing Article 24 of the Treaty establishing the

	European Atomic Energy Community (OJ 406/58 of 6 Oct. 1958)
-	Council Regulation (EEC, Euratom) No. 354/83 of 1 February 1983 concerning the opening to the public of the historical archives of the European Economic Community (OJ L 43 of 15 Feb. 1983, p. 1)
-	Directive 95/46/EC of the European Parliament and 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 of 23 Nov. 1995, p.3 1)
-	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 (OJ L24 of 30 Jan. 1998, p.1)
-	Charter of Fundamental Rights of the European Union (OJ C 364 of 18 Dec. 2000, p.1)
-	Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000, on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and the free movement of such data (OJ L 8 of 12 Jan. 2001, p.1)
-	Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use (OJ L 121 of 1 May 2001, p.34)
-	Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31 May 2001, at 43-48
-	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 of 31 July2002, p.37)
-	Council Regulation (EC, Euratom) No. 1700/2003 of 22 September 2003 amending Regulation (EEC, Euratom) No. 354/83 concerning the opening to the public of the historical archives of the European Economic Community (OJ L243 of 27 Sept. 2003, p. 1)
-	Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (repealed)
-	Consolidated version of the Treaty establishing the European Community (OJ No 321 of 29 Dec. 2006)
-	Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on universal service and users' right relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (OJ L 337 of 18 Dec. 2009, p.11)
-	European Parliament, Proposal for a regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (recast) (OJ C 87E , 1 April 2010, p. 362–380)
-	Regulation (EU, Euratom) No. 966/2012 of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002 (OJ L 298 of 26 Oct. 2012, p.1)
-	Regulation (EU) No 611/2013 of the European Commission of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications
-	Regulation No. 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community (OJ 45 of 14 June 1962, p. 1385) as last amended by Regulation (EU, Euratom) No. 1023/2013 of the European Parliament and of the Council of 22 October 2013 (OJ L 287 of 29 Oct. 2013, p. 15) (Consolidated version: 1962R0031-EN-01.01.2014-011.001)
-	Regulation (EU) No. 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158 of 27 May 2014, p. 1)
-	COM (2008) 229 final, European Commission, Proposal for a Regulation of the European Parliament

	and of the Council regarding public access to European Parliament, Council and Commission documents
EU Decisions relating to the EDPS	
-	Decision No. 1247/2002/EC of the European Parliament, of the Council and of the Commission of July 2002 on the regulations and general conditions governing the performance of the European Data-protection Supervisor's duties (OJ L 183 of 12 July 2002, p.1)
-	Decision 2004/55/EC of the European Parliament and of the Council of 22 December 2003 appointing the independent supervisory body provided for in Article 186 of the EC Treaty (European Data Protection Supervisor) (OJ L12 of 17 Jan. 2004, p. 47)
-	COM/2008/10070 Vacancies of the European Data Protection Supervisor and the Assistant Supervisor (OJ C 126 A/1 of 23 May2008)
-	Decision 2009/30/EC of the European Parliament and the Council of 14 January 2009 appointing the European Data Protection Supervisor and the Assistant Supervisor (OJ L 11 of 16 Jan. 2009, p. 83)
-	COM/2013/10338 Publication of a vacancy notice for the positions of European Data Protection supervisor and Assistant Supervisor (OJ C 219 A/1 of 31 July 2013)
-	COM/2014/10353 European Data Protection Supervisor - Vacancy for the Assistant Supervisor (OJ C 163 A/1 of 28 May 2014)
-	COM/2014/10354 European Data Protection Supervisor – Vacancy for the European Data Protection Supervisor (OJ C 163 A/2 of 28 May 2014)
-	Decision 2014/886/EU of the European Parliament and of the Council of 4 December 2014 appointing the European Protection Supervisor and the Assistant Supervisor (OJ L 351/9 of 9 Dec. 2014)
Other EU decisions and documents	
-	Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 amending its internal Rules of Procedure (OJ 317/1 of 3 Dec. 2001)
-	Commission Decision 2002/47/EC, ECSC Euratom of 23 January 2002 amending its Rules of Procedure (OJ L21/23 of 24 Jan. 2002)
-	Rules governing the official traineeships scheme of the European Commission – Commission decision of 2 March 2005 – C(2005)458
-	Implementation rules on the European Commission Decision of 16 August 2006, C (2006) 3602, concerning the security of information systems used by the European Commission
-	"Guide to the obligations of officials and other servants of the European Parliament", European Parliament, Code of Conduct adopted by the Bureau, July 2008
-	Rules on the secondment to the Commission of national experts and national experts in professional training – Commission decision of 12 Nov. 11.2008 – C(2008) 6866
-	SEC(2009)1643 Implementing rules for Decision 2002/47/EC, ECSC, Euratom on document management and for Decision 2004/563/EC, Euratom on electronic and digitised documents, adopted on 30.11.2009
-	PROTOCOL (No 3) on the statute of the court of Justice of the European Union (OJ C83/02, 30 March 2010)
-	« Liste spécifique de conservation PMO », European Commission, Ref. Ares(2011)1049880 – 04 Oct. 2011
-	Rules on document Management in the European Parliament, Bureau decision of 2 July 2012
-	Common Commission-Level Retention List for European Commission Files – First Revision, adopted on 17 December 2012, SEC(2012)713, first version adopted on 4 July 2007, SEC (2007) 970
-	"Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Key issues of Chapters I-IV", Council of the European Union, Interinstitutional File 2012/0011 (COD), Brussels, 31 May 2013
-	Ares(2015)182108 Guidelines on document management and access to documents, 16 Jan. 2015
-	DPO Network Working Groups' Follow-up Exercise, DPO Network Proposals in light of EC General DP Regulation Proposal and Reg. 45/2001
-	European Parliament, Data Protection Registry (http://www.europarl.europa.eu/data-protect)
-	European Commission, DPO Register (http://ec.europa.eu/dpo-register)
-	General Secretariat of the European Council, DPO Register

	(http://www.consilium.europa.eu/en/general-secretariat/corporate-policies/data-protection)
-	OLAF Personal Data Register (http://ec.europa.eu/anti_fraud/olaf-and-you/data-protection/olaf-register/index_en.htm)
-	List of all the Judgments/Case/Order referring to Regulation 45/2001
-	List of other EU legislation referring to Regulation 45/2001
Other legal documents	
-	Commission Nationale de l'Informatique et des Libertés (CNIL), Deliberation n°88-052 of 10 May 1988 on « adoption d'une recommandation sur la compatibilité entre les lois n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et n°79-18 du 3 janvier 1979 sur les archives »
-	CNIL, Deliberation n° 2006-228 of 5 October 2006 on the « recommandation relative à la mise en oeuvre par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives de fichiers dans le cadre de leurs activités politiques »
-	Arrêté du 21 décembre 2012 relatif à la composition du dossier individuel des agents publics géré sur support électronique (NOR: RDFF1239419A), after last amendment dated 2 January 2013
Other publications	
-	D. Adamski, How wide is "the widest possible"? Judicial interpretation of the exceptions to the right of access to official documents revisited, 46 Common Market Law Review (2009), pp. 521-549
-	D. Adamski, "Approximating a Workable Compromise On Access to Document: The 2011 Developments in the European Courts", 49 Common Market Law Review, pp. 521-558 (2012)
-	F. Banat-Berger, « Archives et protection des données personnelles », Revue Lamy Droit de l'Immatériel 2013/95, n°3177
-	D. Blas, Data protection at Eurojust – A robust, effective and tailor-made regime, Eurojust publication, 2011, 52 pages
-	D. Blas, "Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom", ERA Forum, 2010, p. 233 -250
-	N. Campagne, La protection « informatique et libertés » des données des personnes morales en Europe, Lamy Droit de l'Immatériel, 2014
-	D. Curtin "The role of judge-made law and EU supranational government: a bumpy road from secrecy to translucence" in M. Dougan, N.N. Shuibhne & E. Spaventa (Eds.), Empowerement and disempowerement of the European citizen (Modern studies in European law, 35) (Oxford: Hart, 2012), p. 101-127
-	E. De Capitani, "The Schengen system after Lisbon: from cooperation to integration", ERA Forum, 2014, p. 101–118
-	P. De Hert and V. Papakonstantinou, "The EDPS as a Unique Stakeholder in the European Data Protection Landscape, Fulfilling the Explicit and Non-Explicit Expectations", Data Protection Anno 2014: How to Restore Trust? Contributions in Honour of Peter Hustinx, European Data Protection Supervisor (2004-2014), H. Hijmans and H. Kranenborg (ed.), Brussels, Intersentia, 2014, p. 237–52
-	P. De Hert and V. Papakonstantinou, The data protection regime applying to the inter-agency cooperation and the future architecture of the EU criminal justice and law enforcement area, Study for the European Parliament, PE 510.001, November 2014
-	S. Gutwirth, Y. Poullet, P. De Hert (ed.), Data Protection in a Profiled World, 2014, Dordrecht Heidelberg London New York, Springer
-	S. Gutwirth, R. Leenes, P. De Hert (ed.), Reforming European Data Protection, 2015, Dordrecht Heidelberg, London New York, Springer
-	E. Haas, "International Integration : The European and Universal Process", International Organization, n° 15, 1961
-	I. Harden, Openness and Data Protection in the European Union, Queen's Papers on Europeanisation No, 9/2001, p. 19
-	H. Hijmans and A. Scirocco, "Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be expected to help?", Common Market Law Review, Vol. 46, 2009
-	P. Jeney, The Future of Eurojust, Study for the European Parliament, PE 462.461, April 2012
-	D. Korff , "EC Study on Implementation of Data Protection Directive 95/46/EC", 2002, 253 p. - Available at SSRN: http://ssrn.com/abstract=1287667
-	H. Kranenborg & W. Voermans, Access to information in the European Union – A comparative Analysis

	of EC and Member State Legislation, Groningen: European Law Publishing, 2005
-	H. Kranenborg, Access to Documents and Data Protection in the European Union: On the Public Nature of Personal Data, 45 Common Market Law Review (2008), pp. 1079-1114
-	C. KUNER, "The Baffling Case of the Headless EDPS", 15 January 2014 (https://privacyassociation.org/news/a/the-edps-mess/)
-	H. Labayle, Openness, transparency and access to documents and information in the EU, Note, European Parliament, DG for Internal Policies, Policy Department C – Citizen's Rights and Constitutional Affairs, 2013, p. 21
-	P. Leino, "Just a little sunshine in the rain: the 2010 case law of the European Court of Justice on access to documents", 48 Common Market Law Review 48 (2011), pp. 1215-1252
-	Y. Poullet, "EU data protection policy. The Directive 95/46/EC: Ten years after", Computer Law and Security Review: The International Journal of Technology and Practice, 2006, Volume 22, Numéro 3
-	S. Peers, The New Regulation on Access to Documents: A Critical Analysis, Yearbook of European Law (2001) 21 (1): 385-442
-	S. Van Rapenbusch, « La réforme institutionnelle du traité de Lisbonne : l'émergence juridique de l'Union européenne », Journal de Droit Européen, 2008
-	R. Wong, "The Data Protection Directive 95/46/EC: Idealisms and Realisms", International Review for Computers and Law, 2012
-	Network of Data Protection Officers of the EU institutions and bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001, 14 October 2010
-	Europol, Data Protection at Europol, Publication Europol, 2012
-	Court of Justice of the European Union, Press Release No 54/14, Luxembourg, 8 April 2014
-	Sénat (France), Europol et Eurojust: perspectives d'avenir, Rapport d'information fait au nom de la commission des affaires européennes, 17 April 2014
-	Symantec Response to Commission Communication: "A comprehensive approach on personal data protection in the European Union"
Case Law	
-	CJEC, 1 June 1994, Commission of the European Communities v Augusto Brazzelli Lualdi and others, Case C-136/92 P
-	CJEC, 11 October 1995, Baltsavias v Commission, Cases T-39/93 and T-553/93
-	CJEC, 17 June 1998, Svenska Journalistförbundet v Council, Case T-174/95
-	CJEC, 11 January 2000, Kingdom of the Netherlands and Gerard van der Wal v Commission, Joined cases C-174/98 and C-189/98
-	CJEC, 6 July 2001, Franchet and Byk v Commission, Joined Cases T-391/03 and T-70/04
-	CJEC, 7 February 2002, Aldo Kuijer v Council of the European Union, Case T-211/00
-	CJEC, 12 June 2003, Eugen Schmidtberger, Internationale Transporte und Planzüge v Republik Österreich, Case C-112/00
-	CJEC, 6 November 2003, Bodil Lindqvist, Case C-101/01
-	CJEC, 17 March 2005, European Parliament v Council of the European Union, Case C-317/04
-	CJEC, 1 February 2007, Sison v Council, Case C-266/05 P
-	CJEC, Order of the President of the Court, 12 September 2007, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy,Case C-73/07
-	CJEC, 12 September 2007, Kalliopi Nikolaou v Commission, C-259/03
-	CJEC, 8 November 2007, The Bavarian Lager v Commission of the European Communities, Case T-194/04
-	CJEC, 21 February 2008, Commission of the European Communities v Marie-Claude Girardot, Case C-348/06 P
-	CJEC, 10 February 2009, Ireland v. European Parliament and Council of the European Union, Case-301/06
-	CJEC, 11 March 2009, Borax Europe Ltd v Commission of the European Communities, Case T-121/05
-	CJEC, 11 March 2009, Borax Europe Ltd v Commission of the European Communities, Case T-166/05
-	CJEU, 23 April 2009, Falco Privatstiftung and Thomas Rabitsch v Gisela Weller-Lindhorst, Case C-533/07
-	CJEU, 16 September 2009, Fiorella Vinci v European Central Bank, Case F-130/07
-	CJEU, 9 March 2010, European Commission v Federal Republic of Germany, Case C-518/07
-	CJEU, 11 May 2010, Fotios Nanopoulos v European Commission, Case F-30/08 and confirmed on

appeal T-308/10 P
- CJEU, 15 June 2010, Dimitrios Pachtitis v European Commission, Case F-35/08
- CJEU, 29 June 2010, European Commission v Bavarian Lager Co. Ltd., Case C-28/08 P
- CJEU, Order of the President of the Court, 6 September 2010, British American Tobacco (Investments) Ltd v European Commission, Case T-170/03
- CJEU, 9 November 2010, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen and Bundesanstalt für Landwirtschaft und Ernährung, Cases C-92/09 and C-93/09
- CJEU, Order of the President of the 8th Chamber of the Court, 10 January 2011, Angel Coedo Suarez v Council of the European Union, Case T-3/08
- CJEU, Order of the General Court, 19 February 2011, Erasmia Kitou v EDPS, T-164/09
- CJEU, European Union Civil Service Tribunal, 5 July 2011, V. v European Parliament, Case F-46/09
- CJEU, 7 July 2011, Gregorio Valero Jordana v European Commission, Case T-161/04
- CJEU, 23 November 2011, Gert-Jan Dennekamp v European Parliament, Case T-82/09
- CJEU, 28 March 2012, Kathleen Egan and Margaret Hackett v European Parliament, Case T-190/10
- CJEU, Order of the President of the Court, 20 April 2012, Dimitrios Pachtitis v European Commission, Case T-374/07
- CJEU, 22 May 2012, Internationaler Hilfsfond v Commission, Case T-300/10, published in the electronic Report of Cases, para. 107 and 108
- CJEU, 16 October 2012, European Commission v Republic of Austria, Case C-614/10 : action against the European Commission for failure to fulfil obligations
- CJEU, 12 December 2012, Cerafogli v ECB, F-43/10
- CJEU, 13 September 2013, ClientEarth and PAN v EFSA, Case T-214/11. An appeal is currently pending before the Court of Justice (Case C-615/13 P).
- CJEU, 27 February 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-132/12
- CJEU, 8 April 2014, Digital Rights Ireland Ltd and Seitlinger and Others, joined Cases C-293/12 and C-594/12
- CJEU, 8 April 2014, European Commission v Hungary, Case C-288/12
- CJEU, Dennekamp v European Parliament, Case T-115/13, pending (pleading of the EDPS before the General Court, Luxembourg, 19 November 2014)
- CJEU, 17 July 2014, YS v Minister voor Immigratie, Integratie en Asiel; Minister voor Immigratie, Integratie en Asiel v M, S, Cases C-141/12 and C-372/12
- CJEU, P Strack v Commission, Case C-127/13, not yet published

- ECtHR, Amann v Switzerland, App. no. 27798/95, ECHR 2000-II
- ECtHR, Rotaru v Romania [GC], App. No. 28341/95, ECHR 2000-V

- European Ombudsman, Case 713/98/IJH, 25.09.2002, available via: http://www.ombudsman.europa.eu/en/cases/specialreport.faces/en/380/html.bookmark
- European Ombudsman, Case 713/98/IJH, Letter from the European Ombudsman to the President of the European Commission regarding data protection, 30 Sept. 2002, available via: http://www.ombudsman.europa.eu/en/cases/correspondence.faces/en/3539/html.bookmark
- European Ombudsman, Case 1368/2004/GG against the European Commission, 15 Dec. 2005, available via: http://www.ombudsman.europa.eu/cases/decision.faces/en/2193/html.bookmark