

ANNEXES TO THE IMPACT ASSESSMENT

Annex 1: Current EU Legal instruments on data protection

Annex 2: Evaluation of the implementation of the Data Protection Directive

Annex 3: Data protection in the areas of police and judicial co-operation in criminal matters

Annex 4: Summary of replies to the public consultation on the Commission's Communication on a Comprehensive Approach on Personal Data Protection in the European Union

Annex 5: Detailed Analysis of Impacts

Annex 6: Detailed Assessment of Impacts of the Introduction of Data Protection Officers (DPOs) and Data Protection Impact Assessments (DPIAs)

Annex 7: Analysis of the Impacts of Policy Options on Fundamental Rights

Annex 8: Consultation of SMEs

Annex 9: Calculation of Administrative Costs in the Baseline Scenario and Preferred Option

Annex 10: Impacts of the preferred option on competitiveness

ANNEX 1

CURRENT EU LEGAL INSTRUMENTS FOR THE PROTECTION OF PERSONAL DATA

1. EU CHARTER OF FUNDAMENTAL RIGHTS

Article 8 of the Charter of Fundamental Rights of the European Union enshrines the fundamental right to the protection of personal data of every individual in a legally binding nature, and defines the basic principles for the protection of personal data.

2. DATA PROTECTION DIRECTIVE 95/46/EC

Directive 95/46/EC¹ is the central legislative instrument in the protection of personal data in Europe. Directive 95/46/EC is the legislative basis for two long-standing aims of European integration: the *Internal Market* (in this case the free movement of personal data) and the *protection of fundamental rights and freedoms of individuals*. In the Directive, both objectives are equally important.

Directive 95/46 was a milestone in the history of the protection of personal data as a fundamental right, along the path paved by Council of Europe Convention 108 of 28 January 1981. Legislation at EU level was essential because differences in the way Member States approached this issue impeded the free flow of personal data among the Member States. Its legal base was thus Article 100a/Article 95 of the EC Treaty.

The Directive applies to and has been implemented by all **27 EU Member States**, as well as the three *EEA/ EFTA States*: Iceland, Liechtenstein and Norway. *Switzerland* has also implemented the Directive for the Schengen relevant areas. In line with the Copenhagen criteria, all *candidate countries* are committed to transposing Directive 95/46/EC by the time of accession.

The Directive develops and specifies *data protection principles* in order to achieve harmonisation throughout the EU. The principles of the protection of the rights and freedoms of individuals vis-à-vis processing activities, notably the right to privacy, which are contained in Directive 95/46, give substance to and amplify those contained in the Convention (and its additional protocol on cross border data flows and independent supervisory authorities, added only in 2001 after the implementation of the Directive). The Directive stipulates general rules on the lawfulness of the processing of personal data and the rights of the people whose data are processed ('data subjects'). The Directive also provides that at least one independent supervisory authority in each Member State shall be responsible for monitoring its implementation. The Directive also regulates transfers of personal data to third countries: in general, personal data cannot be exchanged with a third country unless the latter guarantees an adequate level of protection. The Directive is *technologically neutral*, and its principles and provisions are sufficiently general, therefore its rules can continue to apply appropriately to new technologies and new situations.

¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

The Directive applies to both the public and the private sectors. Directive 95/46/EC does not apply to the processing of personal data in the course of police and judicial cooperation in criminal matters.

3. "E-PRIVACY" DIRECTIVE 2002/58/EC

Directive 2002/58/EC² particularises and complements Directive 95/46/EC with respect to the processing of personal data in the *electronic communication sector*, ensuring the free movement of such data and of electronic communication equipment and services in the Union. It has been partially amended by the Data Retention Directive 2006/24/EC.

This Directive has also been *recently amended* by Directive 2009/136/EC³ as part of the overall review of the regulatory framework for electronic communications, introducing in particular a mandatory personal data breach notification.

This Directive, also, applies to and has been implemented by all **27 EU Member States** as well as the three *EEA EFTA States* Island, Liechtenstein and Norway.

4. DATA PROTECTION REGULATION (EC) NO 45/2001

Combining the relevant features of Directives 95/46/EC and 2002/58/EC, Regulation No 45/2001⁴ regroups the rights of the data subjects and the obligations of those responsible for the processing into one legal instrument for the Institutions and bodies of the EU. It also establishes the European Data Protection Supervisor (**EDPS**) as an independent supervisory authority for the EU institutions (see also Decision 1247/2002). The legal basis was Article 286 EC.

With *the entry into force of Article 16 TFEU* (replacing the former Article 286 EC), the *scope of application of Regulation (EC) No 45/2001 extends automatically* to all data processing activities of Union institutions within the scope of Union law. The latter now contains both former third pillar and second pillar activities. Consequently, there is no legal need to formally update Regulation 45/2001 at present, but this cannot be excluded in the future, for legal certainty.

5. PROTECTION OF PERSONAL DATA IN THE AREA OF THE COMMON FOREIGN AND SECURITY POLICY

Currently there is no specific EU legislation for the protection of personal data for Member States in the area covered by the common foreign and security policy. Specific rules for the

² 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 2002 L 201/ 37).

³ 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 2009 L 337/11.

⁴ 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 2001 L 008/1.

protection of personal data may be laid down according to the *newly introduced Article 39 TEU for Common Foreign and Security Policy (CFSP)* issues, but for *Member States* only. The Commission applies, for all of its activities, the provisions of Regulation (EC) 45/2001. For all measures that fall within the sphere of the Union, such as Union action implementing restrictive measures/sanctions, Member States apply the national provisions resulting from implementing the Directive 95/46/EC.

6. PROTECTION OF PERSONAL DATA IN POLICE AND JUDICIAL COOPERATION IN CRIMINAL MATTERS

For the area of police and judicial cooperation in criminal matters alone, the current data protection framework in the EU can only be described as a patchwork that is, consisting of different rights and obligations for Member States and individuals, and creating several data protection supervisory authorities⁵. Several instruments exist with specific data protection regimes or with data protection clauses.

Since 2008 *Council Framework Decision 2008/977/JHA*⁶ aims at creating an EU general legislative framework for the protection of personal data in police and judicial cooperation in criminal matters. Implementation of the Framework Decision was due in November 2010. It applies fully to the UK and Ireland, as well as Iceland, Norway and Switzerland, because it is a development of the Schengen acquis. It does not, however, replace the rules applicable to Europol, Eurojust, Schengen and the Customs Information System, and it does not create a single independent supervisory authority. This Framework Decision does not affect the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Additional Protocol to that Convention of 8 November 2001⁷, which therefore remains relevant for some EU instruments relating to police and judicial cooperation which contain specific data protection regimes or data protection clauses.

Protocol 36 on Transitional provisions annexed to the Treaty of Lisbon provides that in the case of the existing former third pillar acquis, the principle is the preservation of all legal acts so long as they are not repealed, annulled or amended (Article 9).

The Commission has no infringement powers in the case of former framework decisions (Article 10). Also, the powers of the Court of Justice are to remain the same with respect to those acts in the field of police cooperation and judicial cooperation in criminal matters which were adopted before the entry into force of the Treaty of Lisbon. These transitional measures are to cease to have effect five years after the date of entry into force of the Treaty of Lisbon.

Declaration 50 concerning Article 10 of the Protocol 36 attached to the treaties invites the institutions, within their respective powers, to seek to adopt, in appropriate cases and as far as possible within the five-year transitional period, legal acts amending or replacing existing third pillar acts.

⁵ For example: the DPAs at national level, the EDPS, and the Joint Supervisory Board for Europol, Customs, Schengen (with a common secretariat), plus Eurojust and its Supervisory Body.

⁶ Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters; OJ 2008 L 350/60.

⁷ See below under 2.7

ANNEX 2

EVALUATION OF THE IMPLEMENTATION OF THE DATA PROTECTION DIRECTIVE

1. CONTEXT OF THE EVALUATION

The Commission's reports on the implementation of the Data Protection Directive 95/46/EC⁸ found in 2003⁹ and in 2007¹⁰ that the Directive did *not manage to fully achieve its internal market policy objective*, or to remove differences in the level of data protection actually afforded in the Member States. *Enforcement* was also identified as an area where improvement was needed.

This evaluation focuses on the implementation of *key provisions of the Data Protection Directive* since then. It is carried out in the context of the reform of the current *acquis* on the protection of personal data in the European Union. To address the question whether existing EU data protection legislation can still fully and effectively cope with the challenges, posed particularly by globalisation and new technologies, the Commission launched a review of the current legal framework on data protection, starting with a high-level conference in May 2009.

The conclusions in the present document are based on findings in this review as regards the implementation of Directive 95/46, including the analysis of Member States' legislation transposing the Directive into national law, on the basis of studies¹¹, of opinions of the Article 29 Working Party,¹² and of a survey launched by the Commission in relation to certain aspects of the Directive, to which 22 Member States responded.

⁸ Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

⁹ Report from the Commission - First Report on the implementation of the Data Protection Directive (95/46/EC), 15.5.2003, COM (2003)265final.

¹⁰ Communication on the follow-up of the Work programme for a better implementation of the Data Protection Directive, 7.3.2007, COM (2007)87final.

¹¹ Comparative study on different approaches to new privacy challenges, particularly in the light of technological developments, January 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf); European Agency on Fundamental Rights, Data Protection in the European Union: the role of National Data Protection Authorities – Strengthening the fundamental rights architecture in the EU II, 2010, available at http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf; Study on the economic benefits of privacy enhancing technologies, London Economics, July 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf); Study for an impact assessment for the future legal framework for personal data protection by GHK Consulting Ltd., February 2011, launched by the Commission to support the IA process; Case law on the circumstances in which IP addresses are considered personal data, by time.lex CVBA, October 2010; Allocation and Use of IP Addresses, by Vigilio Consult, 2010; Privacy and Trust in the Ubiquitous Information Society, by Fraunhofer ISI et al., March 2009; Legal Analysis of a Single Market for the Information Society: New rules for a new age?, by DLA piper, 2009.

¹² Working Party on the Protection of Individuals with regard to the Processing of Personal Data, established by Article 29 of the Directive; the opinions of the Working Party are accessible under: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm.

2. KEY PROVISIONS OF DIRECTIVE 95/46/EC

2.1. Definitions and concepts

2.1.1. *The concept of "personal data" - Article 2(a)*

The *concept of "personal data"* is one of the key concepts in the protection of individuals by the current EU data protection instruments and triggers the application of the obligations incumbent upon data controllers and data processors. The definition of "personal data" covers all information relating to an identified or identifiable natural person, either directly or indirectly. This deliberate technique to define "personal data" used by the legislator in 1995 has the advantage of providing a high degree of flexibility and the possibility to adapt to various situations and future developments affecting fundamental rights. However, although the definition of "personal data" and "data subjects" are almost literally transposed by the majority of the Member States into their national laws¹³, this broad and flexible definition leads to some diversity in the practical application of these provisions. In particular, the issue of objects and items ("things") linked to individuals, such as IP addresses, unique RFID-numbers, digital pictures, geo-location data and telephone numbers, has been dealt with differently among Member States.

For instance *IP addresses*, which identify computers on networks, are considered as personal data by some Member States, while by others they may be qualified as such only under certain circumstances.¹⁴ Only a few Member States have taken a clear regulatory approach assessing the status of IP addresses. Austria considers IP addresses as being personal data in the Austrian Security Policy Act. Laws in Cyprus, Italy and Luxembourg suggest the same, but within the context of electronic communications. According to the Bulgarian and Estonian Electronic Communications Acts, only a combined set of data which includes IP addresses constitutes, as a whole, personal data. Hence, public authorities in charge of Network and Information Security and Critical Information Infrastructure Protection as well as Computer Security Incident Response Teams (CSIRTs), Internet Service Providers and the security industry have expressed concerns about legal uncertainty regarding the handling and exchange of IP addresses and e-mail addresses across organisations and borders to ensure the overall security of networks and information systems (e.g. to mitigate spam, botnets or Distributed Denial of Service attacks).

In the absence of clear regulatory provisions, many national Data Protection Authorities (DPAs) provided guidelines and opinions on the matter. Some of them took the view that the processing of IP addresses does not fall within the scope of legislation implementing the Directive, as long as the addresses themselves are not linked to individuals or to PCs of individuals (e.g. Belgium, UK). The majority of DPAs point to the fact that sophisticated means allow, in most cases, the re-identification of users, and consider, in their opinions on this issue, that IP addresses themselves are personal data (e.g. Denmark, France, Germany,

¹³ National laws of all Member State replicate the definitions of "personal data" and "data subjects" including, in some cases, the elements of recital 26 of the Directive¹³ (e.g. France, Slovenia, Spain) or other minor amendments.

¹⁴ Case law on the circumstances in which IP addresses are considered personal data, by time.lex CVBA, October 2010;

Hungary, Latvia, Lithuania, Netherlands, Poland, Spain). Estonian, Slovenian and Swedish DPAs state that IP addresses are considered as personal data in combination with other data, which could allow linking a dynamic or static IP address to an individual subscriber. The Austrian DPA recognised dynamic IP addresses (which are assigned automatically, as opposed to static IP addresses) as personal data.

National courts tend to consider IP data as personal data (e.g. in Austria, France, Germany, Italy, Poland, Spain, Sweden, UK); only few courts found that IP addresses were not personal data since they allowed identification of a computer but not its user (e.g. some courts in France¹⁵, Ireland¹⁶). ECJ case law on the confidentiality of electronic communications¹⁷ does not refer to the status of IP addresses.

Another major area of divergent interpretation relates to the circumstances in which data subjects can be said to be "**identifiable**", if they have been made "anonymous", so that data can no longer be related to the individual, or "pseudonymised", where data can only be linked to the individual if one is in possession of a decoding "key". In this regard, recital 26 of the Directive states that "the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable". However, the assessment whether the data allow re-identification depends on the circumstances, available means and technological development. In several Member States, DPAs consider encoded or pseudonymised data as identifiable – and thus as personal data – in relation to the actors who have means (the "key") for re-identifying the data, but not in relation to other persons or entities (e.g. Austria, Germany, Greece, Ireland, Luxembourg, Netherlands, Portugal, UK). In other Member States all data which can be linked to an individual are regarded as "personal", even if the data are processed by someone who has no means for such re-identification (e.g. Denmark, Finland, France, Italy, Spain, Sweden). However, DPAs in those Member States are generally less demanding with regard to the processing of data that are not immediately identifiable, taking into account the likelihood of the data subject being identified as well as the nature of the data.

Digital pictures of properties held in a database are considered, in the Netherlands for example, as personal data, if used for valuation or taxation purposes. In Sweden, telephone numbers were considered as personal data, but in one case, under the previous law, subject to the condition that not more than one specific person used the phone.¹⁸ There are also cases where the notion of "personal information" referring to professional activities as personal data was challenged.

Responding to these divergent approaches, the Article 29 Working Party issued an opinion on the concept of "personal data"¹⁹, clarifying, particularly, the elements of "any information", "relating to", and "natural person", and pointing to recital 26 of the Directive as an essential

¹⁵ SCPP / Marie-Thérèse O. TGI Montauban, 9 March 2007; Anthony G./SCPP, Appeal Court of Paris, 13th Ch., sect. B, 27 April 2007; Sacem v. Cyrille Saminadin, Supreme Court, Criminar Ch., 13 January 2009.

¹⁶ EMI records & Ors-v-Eircom Ltd, 2010, IEHC 108

¹⁷ E.g. C-275/06, *Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU*, 29.1.2008. C-557/07, *LSG-Gesellschaft v. Tele2Telecommunications GmbH*, 19.2.2009.

¹⁸ See also the definition of "traffic data" in Article 2(b) of the ePrivacy Directive 2002/58/EC, OJ L 201, 31.7.2002, p. 37.

¹⁹ Opinion 4/2007 on the concept of personal data (WP 136).

means for interpretation. On the specific issue whether IP addresses are to be considered as "personal data", the Working Party concluded that IP addresses should be considered as personal data particularly in those cases where they were processed for the purpose of identifying the users of the computer. This position is referred to by DPAs in several Member States (e.g. Latvia, Lithuania, Luxembourg, Malta, Poland, and Romania).

Although the present definition of "personal data" encounters divergent applications in Members States in some situations, especially as regards things linked to individuals, it would seem counterproductive to change the definition of personal data. Specific issues such as IP addresses and geo-location data should be tackled on the basis of this proven concept, taking into account – as said in recital 26 of the Directive - of "all the means likely reasonably to be used either by the controller or by any other person to identify the said person". Detailed references to specific technologies would jeopardise the proven technological neutrality of the Directive and risk gaps when technology advances.

2.1.2. *The concepts of data "controller" and "processor" - Article 2(d) and (e)*

The concepts of data controller and data processor play a crucial role in the application of the Directive, particularly for determining the responsibility for compliance with data protection rules, the exercise of the rights of data subjects, the applicable national law and effective enforcement by the Data Protection Authorities. The definition of data "controller" in the Directive refers to the natural or legal person or body which - alone or jointly with others - determines the purposes and means of processing. "Processor" is defined as the natural or legal person or body which processes personal data on behalf of the controller. However, apart from rules relating to confidentiality or security of processing and for the controller's responsibilities as regards the data subject's rights, the Directive contains no comprehensive or detailed set of obligations and responsibilities for controllers and processors.

A number of national laws (e.g. Belgium, Denmark, France, Luxembourg, Netherlands and Sweden) closely follow the definition of the "**controller**". Other laws provide for some variations: for instance, focusing on the determination of the "purposes" of the processing, either without any reference to the "means" (e.g. Austria) or with reference to the "contents and use" of processing instead of the "means" (e.g. Spain). Irish law defines the controller as the person who determines the "scope and manner" of the processing, without referring to the purposes, while Italian law provides a detailed definition of the controller as "either the entity as a whole or the department or peripheral unit having fully autonomous decision-making powers in respect of purposes and mechanisms", and also expressly "related to security matters". German law defines the controller as "any person or body which collects, processes or uses personal data for itself, or which commissions others to do the same".

The definition of "**processor**" has been implemented by most national laws. Austrian law provides that if a processor carries out processing "other than as instructed", he/she has to be regarded as the controller in respect of that processing. Some Member States do not provide a definition of "processor", but cover this processing in definitions of "third party" or "recipient". German law covers in more detail processing "on behalf of the controller" and "on instructions".

These divergences run counter the objective of the Directive to ensure the **free flow of personal data within the internal market**. This is true for a large number of sectors and contexts, e.g. when processing personal data in the employment context or for public health

purposes. Different interpretations and a lack of clarity of certain aspects of these concepts has led to uncertainties with regard to responsibility and liability of controllers, co-controllers and processors, the actual or legal capacity to control processing, and the scope of applicable national laws, causing negative effects on the effectiveness of data protection.

The lack of harmonisation is one of the main recurring problems raised by private stakeholders, especially economic operators, since it is an additional cost and administrative burden for them. This is particularly the case for data controllers established in several Member States, who are obliged to comply with the requirements and practices in each of the countries where they are established. Moreover, the divergence in the implementation of the Directive by Member States creates legal uncertainty not only for data controllers but also for data subjects, creating the risk of distorting the equivalent level of protection that the Directive is supposed to achieve and ensure. Also the provision on liability in the Directive (Article 23) focuses on the controller, without addressing the liability of the processor.

The lack of harmonisation is especially pertinent where *more than one controller and/or processor* are involved in processing operations located in different Member States that apply different rules for controllers and/or processors. In practice, due to the complexity of the environment in which data controllers and processors operate, and particularly due to a growing tendency towards organisational differentiation in both the private and the public sectors as well as the impact of globalisation and new technologies, these concepts became increasingly complex. Sometimes numerous controllers and/or processors are involved in the same processing operations. An example for this is behavioural advertising, where publishers rent website-advertising space and network providers collect and exchange information on users. Such "joint controllership" is covered by the definition of the "controller" ("jointly with others"). However, in such cases there is a need to clarify the sphere of responsibilities, including the duty of informing the data subject that his/her data are accessible by others and conditions of access to personal data. In case the controller is located outside the EU, additional problems arise in view of the determination and enforcement of the applicable law (*see section 2.3*) and the transfer of data to third countries (*see section 2.11*).

These problems are amplified in the context of "*cloud computing*", whereby software, shared resources and information are on remote servers ("in the cloud"). In the context of cloud computing, a cloud user can delegate to a cloud operator the supply of storage, infrastructure, software and security. The internet makes it much easier for data controllers and processors established outside the EU to provide such services from a distance and to process personal data in the online environment. It is often difficult to determine the location of personal data, which is frequently replicated on all continents in order to improve its accessibility, and to enforce data protection rules particularly in situations where the controller targets services to EU residents but has no establishment or representative in the EU. This may involve the loss of individuals' control over their potentially sensitive information when they store their data with programs hosted on someone else's hardware. Cloud providers usually consider themselves as data processors; however, whether the cloud provider is to be regarded as a controller or processor depends on the circumstances. Due to the current limitations of encryption technologies, it is expected that the cloud provider will very often have full access to most personal data controlled by its customers. Also, the concrete implementation of the rights of the individuals, such as modification and deletion of the personal data, is frequently operated by the cloud provider's subcontractors. It is, therefore, important to clarify which controller in such situations is responsible for ensuring that the data subjects using online

services can exercise their rights, independently from the place where the processing occurs, whether in a European or an international cloud.

On 16 February 2010 the Working Party adopted an opinion on the concepts of "controller" and "processor"²⁰, in which it assessed these concepts in detail, concluding that clarification of these concepts was called for in order to ensure effective application and compliance in practice, but also found that the current distinction between controllers and processors was relevant and workable.

Although the definitions and concepts of "controller" and "processor" remain themselves relevant, they need to be clarified and detailed in specific provisions as regards the obligations, responsibilities and liability of both controllers and processors. Harmonised rules on the responsibilities of data controllers and processors, including the obligation to demonstrate compliance with their obligations, would foster legal certainty. Including in the case of more than one controller and/or processors being involved, it must be clear for the data subject whom to address to in order to exercise his or her rights.

2.1.3. *The concept of "consent" - Article 2(h)*

The definition of "the data subject's consent" in the Directive builds on the elements of "any freely given specific and informed indication" of the data subject's wishes signifying the agreement to the processing of personal data relating to him/her. Whereas national law in most Member States reflects these elements, several Member States require the consent to be "unambiguous" (e.g. Portugal, Spain, Sweden), given "expressly" (e.g. Cyprus) or "explicit" (e.g. Greece, Luxembourg). In some Member States, the consent for data processing must be, in principle, in writing (Germany, Italy). Poland requires a "declaration of will", which "cannot be alleged or presumed on the basis of the declaration of will of other content", but does not particularise the elements "free, specific and informed". On the contrary, some other Member States (e.g. France, Ireland, Romania and UK) do not provide a definition of "consent" in their national data protection laws. In practice, this leaves room for considering, in certain circumstances, that "consent" to the processing of (non-sensitive) data is implied, as it is the case in the UK. In some cases it is not even clear what would constitute freely given, specific and informed consent to data processing.

These different approaches among the national systems – *ranging from written consent to implied consent* – create considerable discrepancies, which are relevant for ensuring "informed consent" of the data subject (*see section 2.7*). This situation is particularly problematic in cross-border situations, including the internet. "Consent" obtained under the law of one country and valid under that law, could be regarded as insufficient for subsequent processing in another Member State because it might not meet (additional) requirements of that law for considering "consent" as a valid legal basis. The scope of application of "consent" also needs clarification, particularly in relation to the requirement of "free consent" in specific situations where there is an imbalance between the position of the data subject and the controller, in particular in the employment context, due to the relationship of the subordination of the employee to the employer, or in the public sector. The opinions issued by the Article 29 Working Party cover specific situations such as cross-border data flows,²¹

²⁰ Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169).

²¹ Working Document on a Common Interpretation of Article 26(1) of the Directive, 25.11.2005 (WP 114).

employment²², schools,²³ and the medical sector²⁴, but do not solve the problem of divergent national approaches.

These discrepancies are brought into sharper focus in the *online environment*, where individuals are generally less aware of or certain about their rights, and are hence less capable of giving informed and meaningful consent to data processing. A critical question in this respect is whether the settings (default or otherwise) of most commercially available web browsers can actually be considered to deliver the informed consent within the meaning of the Directive. In the light of this debate and the discrepancies between Member States' national rules, the Article 29 Working Party issued, in June 2010, an opinion on behavioural advertising²⁵, in which it states that "the settings of currently available browsers and opt-out mechanisms only deliver consent in very limited circumstances" and calls on "advertising network providers to create prior opt-in mechanisms requiring an affirmative action by the data subjects indicating their willingness to receive cookies or similar devices and the subsequent monitoring of their surfing behaviour for the purposes of serving tailored advertising."

In view of the divergent approaches among national laws and the consequences deriving from these, there is a need to clarify and determine in more detail the conditions and rules on consent, in order to guarantee informed consent and to ensure that individuals are fully aware that they are consenting to a specific data processing.

2.2. "Household exemption" - Article 3(2), second indent - and Freedom of information - Article 9

2.2.1. The 'household exemption'

Member States, businesses and individuals see online services as creating one of the main challenges to personal data protection. The internet makes processing easier and consequently vastly increases the audience and the volume of data processed; this also results in the increased risks for data subjects when using such applications. Surveys show that most European users feel uneasy when transmitting their personal data over the internet, but only a minority of users said they used tools and technologies that increased data security.²⁶

In this context, one issue of major concern is the application of the Directive to online *social network services (SNS)*. While the social network providers are controllers (since they determine the purposes and the means of processing personal information on their online communication platforms) the situation is less clear as regards the users of such platforms. The Directive does not apply to the processing of personal data by a natural person in the context of a purely personal or household activity. However, the role of the users may go

²² Opinion 8/2001, 13.11.2001 (WP 48).

²³ Opinion 2/2009, 11.2.2009 (WP 160).

²⁴ Working Document on the processing of personal data relating to health in electronic health records, 15.2.2007 (WP 131).

²⁵ Opinion 2/2010, 22.6.2010 (WP 171).

²⁶ See Flash Eurobarometer No 225 – Data Protection in the European Union:
http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

beyond such context. Personal data are often retained and disclosed without the person concerning being informed and/or having given his/her consent on this.

*ECJ case law*²⁷ - referring to the "correspondence and the holding of records of addresses"²⁸ – has clarified the scope of this exemption. The court ruled that the exemption does not apply "with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people". This means that users of social networks, disclosing personal data of other individuals, act as controllers and therefore cannot rely on the complete exemption from the scope of the Directive, even if the processing relates to purely non-economic, charitable and religious purposes. On the other hand, the Court clarified that the information appearing on a computer in a third country does not constitute a transfer of data by the users themselves, and also, that Member States are not prevented from extending the scope of their national law to areas not included in the scope of the Directive.²⁹

In practice, in most Member States the Data Protection Authorities focus on the *responsibility of the service providers*, without dealing with the question of whether users of such sites, who make personal data available to others, become subject to the law as controllers. In France, the Data Protection Authority excludes bloggers from the notification requirement and advises internet users who create a personal website for a circle of family or friends to impose access restrictions, to inform the individuals concerned, to disseminate the data to third parties only within the context of private activities, to give the data subject the opportunity to object to it and to ensure a proportional retention period. By contrast, in the UK, the Data Protection Authority has not even addressed the responsibilities of the SNS providers and has restricted itself entirely to issuing guidance to individual users, without addressing the issues that arise on the processing of information about other individuals.

In view of these serious discrepancies between the Member States, the Article 29 Working Party issued, in June 2009, an opinion on social networking³⁰. It clarified that the "household exemption" applies to users who operate within a purely personal sphere, contacting people as part of the management of their personal, family or household affairs. The opinion advocates robust security and privacy-friendly default settings and focuses on the obligations of providers in its recommendations, including the obligation to inform data subjects on the different purposes for which they process personal data, and to take particular care with regard to the processing of the personal data of minors. It recommends that information on other individuals should only be uploaded by a SNS user with that individual's consent.

2.2.2. *Freedom of expression*

According to the Directive, should it be necessary to reconcile the right to privacy with the rules governing freedom of expression, Member States shall provide for exemptions or derogations in the national laws for the processing of personal data for solely journalistic purposes, artistic or literary expression (Article 9). However, the Directive does not provide guidance on what is "necessary" in order to reconcile the right to privacy with the rules

²⁷ ECJ, Case C-101/01, *Bodil Lindqvist*, 6.11.2003, and the Satamedia Case C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy*, 16.12.2008, para. 44.

²⁸ Cf. recital 12 of the Directive.

²⁹ ECJ, Case C-101/01, *Bodil Lindqvist*, 6.11.2003.

³⁰ Opinion 5/2009, 12.6.2009 (WP 163).

governing freedom of expression. As regards this exemption, also, the ECJ held that processing of personal data must be considered as "solely for journalistic purposes" if the sole object of those activities is the *disclosure of information, opinions or ideas to the public*, and that also personal data files which contain solely, and in unaltered form, material that has already been published in the media, fall within the scope of application of the Directive.³¹ In its case law, the ECJ stressed the margin for manoeuvre of Member States to determine how, in any particular case, a fair balance between freedom of expression and privacy should be achieved, provided that the right to freedom of expression and freedom to receive and impart information is taken into account, and that any such national decision would have to be proportionate in relation to those rights.³²

In practice, this provision is applied quite differently in the Member States. The need to *extend the exception to everyone and not just to journalists*, artists or writers is recognised particularly clearly by Denmark and Sweden, where the data protection law does not apply to the extent of violating the freedom of expression. On the other hand, Luxembourg's law contains the caveat that "without prejudice to the rules in the legislation on mass communication media", thus focussing on the mass media rather than on non-journalists. It provides specific rules on informing the data subject, on the right of access, on transfers to third countries and – to the extent that they relate to matters "manifestly made public by the data subject" – on the processing of sensitive data. Italian law provides that data on private matters may only be reported if there is a "substantial public interest", unless the data subject has made the data public, or if their publication is justified in view of the public conduct of the data subject.

Austrian law focuses on whether it is "necessary to fulfil the information-providing task of media companies, media service providers and their employees". Spanish law does not refer to freedom of expression, but contains certain provisions relaxing its rules with regard to the processing of data derived from "publicly accessible sources". In France, there are a number of exemptions for the media and for literary or artistic expression, explicitly stressing that these exemptions are without prejudice to the rules in civil and criminal law of defamation. In Germany, the "media privilege" does not exempt the media from the data protection requirements, but recognises that the interests of data subjects and controllers must be balanced differently in this context. In other Member States (e.g. Belgium, Netherlands, Portugal), the exemptions relate to a more limited range of provisions. Belgian law spells out that issues such as the protection of sources, or whether the normal rules would hamper the collection of information, should be taken into account. The UK and the Irish law impose the requirement that the controller "reasonably believes" that the processing is "in the public interest", thus leaving, in practice, the emphasis on self-regulatory control of the press. In Greece, the law only grants an exemption from the obligation to inform data subjects, and then only if the data subjects are "public figures". Apart from these widely different approaches in national legislation, in several Member States "non-professionals" such as SNS users and "bloggers" are not covered by exemptions in relation to freedom of expression, despite the fact that their "user-generated" information will, to a significant extent, provide information to the public.

³¹ ECJ, Case C-73/07, *Satamedia*, 16.12.2008.

³² ECJ, Case C-101/01, *Bodil Lindqvist*, 6.11.2003.

As regards the disclosure of information to the public or to third parties, the ECJ³³ has made it clear that no automatic priority can be conferred to the objective of transparency over the right of personal data, and that the disclosure of documents involving personal data would require demonstrating the necessity for their disclosure on compelling legitimate grounds.

Both the "household exemptions" and exemptions in relation to freedom of expression create increasing uncertainty in particular as regards the processing of data by users of social networks. The limitations of "purely personal or household activities" and the application of data protection rules for disclosing to the public information, opinions or ideas, in relation to the freedom of expression should be clarified.

2.3. The applicable law - Article 4

The Commission's first report on the implementation of the Data Protection Directive³⁴ in 2003 already highlighted the fact that the provisions on applicable law were "deficient in several cases, with the result that the kind of conflicts of law Article 4 seeks to avoid could arise". The situation has not improved since then, as a result of which it is not always clear to data controllers and data protection supervisory authorities which law is applicable where data processing in several Member States is involved.

The linking of the applicable law to *any establishment of the controller* leads to the consequence that the same controller has to comply with different national laws which apply for each of its establishments. This is particularly the case for data controllers established in several Member States and obliged to comply with the – sometimes divergent – requirements and practices in each of these Member States. Moreover, the divergence in the implementation of the Directive by Member States creates legal uncertainty as to which legal obligations apply. This is not only relevant for data controllers, but also for data subjects, creating the risk of distorting the equivalent level of protection that the Directive is supposed to achieve and ensure. This may lead to situations of different levels of protection, e.g. when Member States follow different interpretations of the "household exemption", or of the concept of freedom of expression. Data Protection Authorities frequently provide guidance to controllers on how to comply with their law on the internet, but rarely on the question of when their law applies to these activities. Generally, they do not seek to apply their national laws to processing operations of controllers established in other Member States (*see point 2.12.6*).

Uncertainties exist also on the issue as to which national law applies to the processing *activities of controllers located outside the EU*, in particular when the data controller is not established in the EU but provides its services to EU residents in several Member States. The application of the Directives for such controllers is linked to the "use of equipment, automated or otherwise, situated on the territory" of the Member State, unless used for purposes of transit. However, already the notion of "equipment" itself is not clear and widely interpreted in the sense of "means". This is in particular relevant given the growing complexity due to globalisation and technological developments: data controllers increasingly operate in several Member States and jurisdictions, providing services and assistance around the clock. The

³³ Joint cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert v. Land Hessen*, 9.11.2010; C-28/08, *Commission v. The Bavarian Lager Co Ltd*, 29.6.2010.

³⁴ Report from the Commission - First Report on the implementation of the Data Protection Directive (95/46/EC) - COM(2003)265.

internet makes it much easier for data controllers established outside the EU to provide services from a distance and to process personal data in the online environment, and it is often difficult to determine the location of personal data and of equipment used at any given time (e.g., in “cloud computing” applications and services). Whereas, for example, in most Member States, the Data Protection Authorities regard the use of "cookies" – in line with the opinion of the Article 29 Working Party³⁵ - as sufficient to bring the processing of data by a non-EU controller within the scope of their laws, investigating violations on the internet and enforcement of the data protection rules becomes difficult where servers are located outside the EU. In some Member States (e.g. in France), the views of national courts and Data Protection Authorities differ from each other. The "*transit*" criterion is applied by several Member States (including Belgium, Finland, Ireland, UK) only to the Member State in question, or without clarifying whether this means transit through their territory or transit through the EU (e.g. Greece, Netherlands and Spain).

Divergent approaches exist also in relation to the obligation to appoint a *representative* for a non-EU based controller. In many Member States it is not known how many controllers not established on EU territory and making use of equipment situated on their territory have designated a representative, as required by Article 4(2) of the Directive. Thus this obligation to designate a representative is hardly enforced in practice. This situation creates the serious risk of depriving individuals of the protection to which they are entitled under the EU Charter of Fundamental Rights and EU data protection legislation.

In December 2010, the Article 29 Working Party issued an opinion³⁶ aimed at clarifying the concept of applicable law. It notes, *inter alia*, that several Member States' laws could become applicable when establishments of the same controller are located in several Member States. The "use of equipment" provision should apply in those cases where there is no establishment on EU territory, or where the processing is not carried out in the context of such establishment. The opinion recommends simplifying the rules for determining applicable law, and applying the 'country of origin principle' on the basis of comprehensive harmonisation of national legislation, so that the same law applies to all establishments of the controller, regardless of the location of the establishments. Where the controller is established outside the EU, it recommends, *inter alia*, to developing 'targeting criteria' when processing is targeted at individuals in the EU, and to apply the equipment criterion in a limited form.

Uncertainties and different approaches as regards applicable law demonstrate the need for a revision of the provisions on applicable law, in order to improve legal certainty and ultimately provide for the same degree of protection of EU data subjects, regardless of the geographic location of the data controller.

2.4. Data Protection Principles - Article 6

The data protection principles are in general considered, both by Member States and stakeholders, as being sound and valid. However, the wording of the *purpose-limitation principle* leaves it open to divergent application, ranging from "reasonable expectations" of

³⁵ Opinion 1/2008, 4.8.2008 (WP 148).

³⁶ Opinion 8/2010, 16.12.2010 (WP 179).

the data subject, to "fairness" or the application of various "balance tests". In some countries, the principle is subject to exemptions, particularly for the public sector. In others, purposes are sometimes defined in excessively broad terms. The rules concerning the ***change of purpose*** for the processing of non-sensitive personal data without the consent of the data subject, including for research and statistical purposes, vary considerably, as they do as regards the requirement of safeguards. Some Member States do not provide any safeguards, and others only minimal, insufficient safeguards.

Also, the vague terminology that personal data must be "not excessive" in relation to the purposes for which they are collected and/or further processed, leaves room for divergent interpretations and does not guarantee ***data minimisation***, i.e. limiting the extent of processing to the minimum necessary in relation to its purposes. This is relevant e.g. in view of the collection and storage period for personal data or of privacy-friendly default settings which could enhance data protection. Currently, default settings are often overly complex and not user friendly; also, the method of changing them can be unclear or imprecise.

While the Directive requires that personal data be processed "fairly" and provides for certain information requirements, it does not explicitly express the "***principle of transparency***" in the sense that the data must be processed in a manner that is transparent to the data subject. The specific inclusion of such a principle would emphasise that transparency is a fundamental condition for enabling individuals to exercise control over their own data and to ensure effective protection of their personal data, which could serve as a basis for improved information requirements (*see section 2.7.*).

Another issue is the need to clarify the role of data controllers in ensuring compliance with these principles, as required by Article 6(2) of the Directive. The Working Party concluded, in its opinion of 13 July 2010 on the ***principle of accountability***³⁷, that there is a need to strengthen this concept by requiring data controllers to implement appropriate and effective measures to ensure that the principles and obligations of the Directive are complied with, and demonstrate this to the Data Protection Authorities upon request. Such a principle on the comprehensive responsibility of data controllers would need to be clarified and accompanied by the elaboration of detailed provisions, specifying the concepts of controllers and processors.

While the key data protection principles have proven to still be valid and sound, the principles of data minimisation, transparency should be added, as well as the principle of comprehensive responsibility of the data controller to ensure and demonstrate compliance with data protection rules. Clarification is also needed particularly on the conditions for the change of purpose of the processing of personal data, which are collected for another purpose, and on the processing of personal data for statistical and research purposes.

2.5. Lawfulness of processing - Article 7

In several Member States the criteria set out in Article 7(a) to (f) of the Directive are transposed as alternative grounds for lawful processing on equal footing (e.g. in Belgium, Denmark, Finland, Ireland, Luxembourg, the Netherlands and Sweden). In Austria, Germany and Spain, consent and processing based on a law or to fulfil a legal obligation are given primary status, the other criteria being seen as exceptions. In other countries (including the

³⁷ Opinion 3/2010, 13.7.2010 (WP 173).

Czech Republic, France, Greece and Portugal) processing on the basis of consent is the sole primary criterion. In Italy this is the case only for the private sector.

As regards processing on the basis of *consent*, the legitimacy of processing depends on the concept of "consent", which is understood and applied differently from Member State to Member State (*see point 2.1.3*). Apart from that, uncertainties arise as to how far data processing in the public sector and other specific sectors, such as employment, may rely on the consent of the data subject.

In relation to processing on the basis of a *legal obligation*, the ECJ³⁸ and the European Court of Human Rights³⁹ clarified the issue of whether such legal obligation might be justified by reasons of substantial public interest such as those laid down in Article 8 of the European Convention on Human Rights and the requirement of necessity and proportionality for this purpose. However, different standards in the quality of laws cause problems particularly in the cross-border context, both in the private and public sector. This may lead to the situation that the Member State in which the data are further processed does not meet the requirements of the law of the Member State in which the data are collected. Another uncertainty is whether the legal obligation or the public interest as a legal basis for processing is to be determined by the national law to which the controller is subject, or by the national law of any EU Member State, which might then require the data collection and disclosure by a controller residing in another Member State. As regards a third country requesting the transfer of data collected in a Member State, the Article 29 Working Party indicated that an obligation imposed by a third country's legal statute or regulation requiring a controller in a Member State to undergo processing activities cannot qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate⁴⁰.

The implementation of the "*balance of interest*" criterion (Article 7(f)) differs substantially between Member States. In the UK it is largely left to controllers to conduct the assessment and to determine whether they can process personal data on this basis. In the Netherlands, the explanatory memorandum to the data protection law sets out guidance on what issues should be taken into account when applying this criterion. Given its vagueness, several Member States (including Belgium, Ireland and UK) have envisaged issuing further rules for the application of this criterion, but have not yet adopted such rules. DPAs have provided guidance in their opinions interpreting the law. In some countries, it is explicitly indicated that the balance test applies only to the private sector (e.g. Germany) or in cases specified by the Data Protection Authority (Italy) or on the basis of the permission of the national data protection supervisory authority in a specific case (Finland). Other countries (including Greece and Spain) impose stricter requirements on processing on the basis of this criterion. Thus, by its nature, this criterion gives the Member States latitude to adapt its application to specific situations.

In view of divergent approaches in the Member States, the criteria on lawfulness of processing on the basis of consent, of a legal obligation and of the 'balance of interest' criterion need clarification and specification.

³⁸ Joint cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert v. Land Hessen*, 9.11.2010; C-524/06, *Heinz Huber v. Germany*, 16.12.2008; C-139/01, *Rechnungshof, Österreichischer Rundfunk et al.*, 20.5.2003.

³⁹ See e.g. *S. & Marper v. UK*, 4.12.2008 (Application Nos. 30562/04 and 30566/04).

⁴⁰ See Opinions 1/2006 and 2/2006 (WP 117 and 118).

2.6. Sensitive data - Article 8

- The Directive is based on the premise that certain categories of personal data, as distinct from all other personal data, require extra protection and may be processed by private and public bodies only for specific purposes and under special conditions. Therefore, the Directive prohibits, as a general rule, the processing of exhaustively listed special categories of data, the so-called 'sensitive data', i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life, unless under certain conditions and safeguards. Without qualifying them as such special categories of data, the Directive sets out that for data relating to offences, criminal convictions or security measures, Member States may provide specific safeguards.
- When implementing this provision, some Member States go beyond the *categories of "sensitive data"* set out in the Directive and have added genetic data (e.g. Bulgaria, the Czech Republic, Estonia, Luxembourg, Portugal) and biometric data (e.g. the Czech Republic, Slovenia and Estonia). Portugal regards "private life" as sensitive data, Poland "party membership" (in addition to trade-union membership) and "addictions". Some Member States have also included data from the judiciary in their catalogue of special categories of personal data, for example information about previous convictions or criminal behaviour (e.g. Cyprus, the Czech Republic, Estonia, Slovenia, Spain, the Netherlands, Poland). On the other hand, some national laws do not include information on ethnic origin, political opinions or philosophical beliefs. Belgium provides a specific provision for health data in line with the Directive.

Genetic data are not expressly mentioned by the Directive in the list of 'sensitive data'. However scientific progress made over recent years in the field of genetic research has given rise to new data protection issues in relation to genetic tests and more generally to the processing of genetic data. Genetic data show characteristics which make them unique. The judgement of the European Court of Human Rights, in *S and Marper v United Kingdom*⁴¹, stated that there could be little, if anything, more private to the individual than the knowledge of his genetic make-up⁴². The fact that some Member States have listed genetic data as 'sensitive data' in their data protection law with associated restrictions and safeguards, whereas in most Member States the issue of the processing of genetic data is not regulated as such, leads to the consequence that an individual's fingerprints, cellular samples and DNA profiles may be processed for different purposes from one Member State to another, with different data protection rules and standards applying.

- Beyond sensitive data, France considers specific categories of treatments as "risky". Such "*risky treatments*" include for instance genetic data, biometric data and information about criminal records. Processing such data is not prohibited as such but is subject to prior authorisation from the data protection supervisory authority.
- Differences in the interpretation of the categories in the Directive may also be observed: e.g. "*health data*" may range from information about a simple cold to information

⁴¹ *S. and Marper v. the United Kingdom*, judgment of 4 December 2008, applications nos. 30562/04 and 30566/04.

⁴² For a more detailed analysis, see the Article 29 Working Party "Working Document on Genetic Data" (WP 91).

about illnesses or disabilities. Furthermore, the term "*racial origin*" (in addition to "ethnic origin") is often differently understood. Photos and images of persons, such as those published on the Internet or taken by traffic monitoring or other surveillance cameras, are especially problematic, since they can reveal information about an individual's ethnic origin or health status. Finally, there are differences in applying certain categories of sensitive data in Member States, because the degree of sensitivity may be seen in one Member State differently than in another Member State, e.g. with regard to the category "trade-union membership".

As regards the *exceptions from the general prohibition* of processing 'sensitive data', even less harmonisation than for the categories of 'sensitive data' has been achieved. Member States have used their discretion in a different fashion with the result of significant differences in the implementation of Article 8 (2) – (5). Some Member States impose additional requirements for the processing of sensitive data. The Netherlands provides specific exemptions for each category of sensitive data. The UK provides specific exemptions and conditions for processing genetic data. France allows processing under additional conditions, if justified by the purpose of the processing. For the exception based on explicit consent, about half of the Member States (including Belgium, Cyprus, France, Germany, Greece, Hungary, Italy, Latvia, Poland, Slovakia, Slovenia, Spain) require, as an additional condition, that the consent is given in writing. Some Member States stress, in addition to their general rules on consent, that the consent for processing sensitive data must not be obtained illegally or contrary to accepted moral values (Cyprus, Greece). Other Member States, such as Italy and Sweden, do not accept consent as a legitimate basis for processing sensitive data.

- The provision on the processing of sensitive data for specified *health-related purposes* has been implemented by most Member States; in some with corresponding provisions, in others with either more stringent or less stringent conditions. For example, in Cyprus and Denmark this exception is restricted to health professionals only, whereas in the Czech Republic and in Slovakia the exception is extended also to health insurance. In the other Member States, which do not recognise such extension to insurance, processing for the purpose of health insurance contracts is normally based on the exception of explicit consent; this leads, for example, to the use of blanket declarations by insurance companies, which might be doubtful both as regards "informed" and "free" consent. DPAs noted the problems in national data protection with regard to the term "health professionals". In practice health data are processed for various purposes and it is often not clear who belongs to the category of health professionals or the group of persons obliged to comparable secrecy obligations. Nor are there currently explicit grounds under Article 8 of the Directive justifying the processing of sensitive personal data in case of injuries, when health data are transmitted by non-medical personnel, e.g. at schools.

The possibility for Member States to add further exemptions for reasons of *substantial public interest* has led to a broad range of exceptions allowing for the processing of sensitive data for different purposes. These purposes are mostly related to public security (e.g. in Germany, Spain, UK), social security and welfare (e.g. Austria, Czech Republic, Ireland, Latvia, Spain), research and statistics (e.g. Austria, Belgium, Denmark, France, Germany, Malta, Netherlands, Poland, Spain, Sweden), journalistic and artistic purposes (e.g. Belgium, Spain, UK), the administration of justice (e.g. Ireland, UK), the functioning of government (Ireland), protection of public health and fiscal control (Spain) and obligations under international law (Netherlands). Some national laws refer to regulations made for reasons of "substantial public interest" (Ireland) or, for certain categories of data, to the "general interest" (Spain). However,

in the national laws of several Member States provisions on suitable safeguards are missing. Consequently, the Article 29 Working Party noted a need to formulate more precisely the exception for the processing of sensitive data “for reasons of substantial public interest”.

The provision on data relating to *offences, criminal convictions or security measures* is also transposed in various ways, partly by including it in the categories of "sensitive data" (e.g. Czech Republic, Hungary, Greece, Netherlands, Slovenia, Spain) or by a special legal framework (e.g. Belgium, Bulgaria, Germany, Italy, Luxembourg), but in many Member States suitable safeguards are not provided. As far as these categories are included in the definition of sensitive data, this has consequences such as that explicit consent may serve as a legitimate basis for data processing.

In many cases the provision on the *notification of derogations* from Article 8(1) of the Directive to the Commission has not been transposed. This is demonstrated by the fact that, for example, in 2009 the Commission received notifications of derogations only from four Member States (Denmark, Finland, Netherlands, UK). As in practice the obligation to notify is not always met by Member States it is difficult for the Commission to provide an EU-wide overview of those derogations.

Only some Member States (including Bulgaria, Denmark, Finland, Hungary, Latvia, Malta, Netherlands, Romania, and Sweden) have determined the conditions under which the *national identity number* can be transposed, with different basic approaches to the use of this identifier, ranging from a widespread exchange between public authorities to more restricted use. Some countries allow the use of such a number in the private sector, whereas others are restrictive in this regard.

Divergent approaches about what categories of data are considered as being "sensitive data" and under what conditions such data may be processed call for an examination of the concept of sensitive data, including the categories and their possible extension e.g. on genetic data and for further harmonising the conditions under which such data may, exceptionally, be processed.

2.7. Information to data subjects - Articles 10 and 11

Articles 10 and 11 of the Directive oblige the controller or his representative to inform the data subject as to the identity of the controller, the purposes of the processing and to provide any further information "in so far as such further information is necessary". Despite the examples of such information listed in those provisions, this open wording leads to uncertainties whether such information might or might not be necessary in a specific situation. Moreover, the *application of the information requirement* itself is not always ensured on in practice. For example, a survey conducted by the Commission among Data Protection Authorities and Member States in the case of hotel registrations revealed that not in all Member States national law obliges hotels to inform travellers about the purposes of the processing of their personal data when completing hotel registration forms. Whereas such an obligation exists e.g. in Belgium, the Czech Republic, Denmark, Estonia, Finland, Luxembourg, Latvia, Netherlands, Poland, Portugal, Romania, Slovenia, Slovakia, in other Member States the hotels are not required to provide such information (e.g. in Austria, Bulgaria, France, Germany, Greece, Hungary, Spain). Some Member States argued that the

information requirement is fulfilled by expressly laying down in the law the purposes of the registration as well as other information.⁴³

Despite being particularly relevant for individuals for exercising their rights, Articles 10 and 11 currently do not require informing the data subject of the competent Data Protection Authority and its contact details nor do these provisions specify how long the data will be retained. Moreover, the information provided by the controller is often *not easily accessible and difficult to understand*. Especially in the online environment, quite often privacy notices are unclear, difficult to access, non-transparent⁴⁴ and not always in full compliance with existing rules. A case where this might be so is online behavioural advertising, where both the proliferation of actors involved in the provision of behavioural advertising and the technological complexity of the practice make it difficult for an individual to know and understand if personal data are being collected, by whom, and for what purpose.

Despite *children* deserving specific protection, as they may be less aware of risks, consequences, safeguards and rights in relation to the processing of personal data⁴⁵, there are no specific requirements in the Directive. The lack of clear and understandable information of the data subjects also affects the validity of consent, which requires, as a fundamental condition, "informed consent" (*see point 2.1.3 on the concept of consent*).

Data breaches, in particular of large companies' customer databases, are increasing. Security failures may lead to harmful consequences for individuals, ranging from undesired spam to identity theft⁴⁶. The recent revision of the e-Privacy Directive⁴⁷ introduced a mandatory personal data breach notification, which covers, however, only the electronic communications sector. Given that risks of data breaches also exist in other sectors (e.g. the financial sector), the consultation carried out by the Commission in 2010-2011 confirmed the need to extend the information of data subjects to a general obligation of the controller to inform Data Protection Authorities and, in defined circumstances, also of data subjects when their data are accidentally or unlawfully destroyed, lost, altered, accessed by or disclosed to unauthorised persons.

⁴³ Despite the Commission's request, the Article 29 Working Party did not include this issue in its Working Programme and thus has not provided an opinion so far.

⁴⁴ A Eurobarometer survey carried out in 2009 showed that about half of the respondents considered privacy notices in websites 'very' or 'quite unclear' (see Flash Eurobarometer No 282 : http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

⁴⁵ See the Safer Internet for Children qualitative study concerning 9-10 year old and 12-14 year old children, which showed that children tend to underestimate risks linked to the use of Internet and minimise the consequences of their risky behaviour (available at: http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

⁴⁶ Interesting figures on recent data breaches and losses can be found at: <http://datalossdb.org> (*data not verified*).

⁴⁷ Directive 2002/58/EC of the European Parliament and of the Council of 12.7.2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37, as amended by Directive 2009/136/EC, OJ L 337, 18.12.2009, p. 11.

To ensure that individuals are well informed in a transparent way, data controllers should be obliged to inform data subjects about how and by whom their data are collected and processed, for what reasons, for how long and what their rights are if they want to access, rectify or delete their data. This information should be provided in an easily accessible and understandable way, using clear and plain language. Data controllers should be obliged to notify data breaches to Data Protection Authorities and, under defined circumstances, also to data subjects.

2.8. Rights of the data subjects - Article 12

The Directive provides for a set of rights for individuals. These include individuals' rights *vis-à-vis* those processing their personal data such as the right to access, rectify, block and delete their own data. These rights are, however, expressed in general terms and the way they can actually be exercised is not clearly specified. Nor does the Directive impose any deadlines for responding to data subjects' requests or any indication of the level of fees for exercising the rights to rectification, erasure and blocking; the condition "without excessive delay or expense" applies only to the right of access.

All Member States guarantee the right of the data subject **to access his/her own data**, although also in that respect there are differences in the implementation in national law. In some countries (e.g. Greece, Spain and Sweden) the controllers are required to inform the data subject, on request, about the source of the data, the processor or of any developments in processing since the last access request. In the Netherlands the law stipulates that the controller must contact other individuals if their data are involved and decide, in the light of the response, whether to disclose this data. UK follows a similar approach, but with an exemption concerning information given in confidence to the controller for certain purposes, including employment. In Germany the right of access is extended to data held in unstructured files, if the data controller, e.g. a credit reference agency, processes the data professionally for the purpose of providing the data to others. Other countries provide specific rules relating to such purposes. Austrian law provides that, on the data subject's request, the data may not be deleted for a period of four months. ECJ case law clarified that the Directive requires Member States to ensure the right of access, not only in respect of the present, but also in respect of the past, and to provide for access to that information on the basis of a fair balance between the interests of the data subject and the burden for the controller.⁴⁸

All Member States guarantee in their laws the right of data subjects to obtain **rectification** of personal data relating to them, but also with some differences. In Greece, this right extends to all contested processing, whereas in other Member States this is linked to incomplete or incorrect data. The laws in Austria and Germany provide that documents retained for historical purposes need not be rectified, but the data subject has the right to have comments added. Austrian law stipulates also that regularly issued compilations, such as address lists, should be corrected in the subsequent regular issue.

The right to request the **deletion of data** is provided by the Directive, but in practice it is difficult for an individual to enforce this right *vis-à-vis* the data controller. Recent reported

⁴⁸ C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, 7.5.2009, European Court reports 2009 Page I-03889

cases about people seeking to have their data deleted from a social network are a telling example of the practical difficulty to exercise this right especially in the online environment⁴⁹.

It is also not always clear who owns the personal data supplied by a user to a service provider. The Directive provides no explicit right for the individual *to withdraw his/her own personal data* (e.g. his/her photos or a list of friends) from an online-service, so that the individual may transfer data to another application or service.

The way in which these rights can be exercised differs from country to country, so that exercising them is actually easier in some Member States than in others. All Member States except Spain give data subjects the right to obtain an actual copy of the data. In some Member States (e.g. Austria, Finland, UK) the law expressly provides that, if the data subject agrees, the controller may, as an alternative, offer access on its premises or online rather than by hard copy. In other Member States this alternative is at the discretion of the controllers, at least when a copy in permanent form is not feasible or would involve a disproportionate effort (e.g. Ireland). In France, access to data on criminal convictions, "penalty points" on a driving licence and certain medical data is restricted to the inspection of the data, without providing the right to obtain a hard copy. In some Member States individuals have to pay a fee to access their data, while in others it is free of charge⁵⁰. Some Member States impose a deadline on data controllers to respond to access requests, while others do not.

Clarification and enhancement of the individual's control over his or her "own data" is needed, including the right to have the data deleted or to retrieve data from online service providers. Also, the conditions and modalities for the actual exercise of the rights of access, rectification and deletion of data need to be improved and harmonised, taking into account electronic means which facilitate access to their data and the exercise of these rights.

2.9. Notification of processing and Data Protection Officers - Article 18

2.9.1. Notification

Article 18 of the Directive imposes a *general notification requirement*, but leaves *considerable room for manoeuvre* to Member States to determine exemptions from and simplifications of notification requirements and the procedures to be followed. Accordingly, Member States adopt very different approaches. Some national laws (e.g. Bulgaria, Czech Republic, Denmark, Estonia, Greece, Hungary, Latvia, Spain, Romania, and UK) require all controllers to notify. In several Member States the controllers are required to notify when the processing is carried out by automated means (e.g. France, Malta, Netherlands, and Sweden). Other national laws require hardly any controllers to notify, except in limited circumstances on the basis of a positive list (e.g. Austria, Finland).

Moreover, the details and the *use of the information* provided by the notifications vary from Member State to Member State. The most frequent use of notifications is for inspections and audits, and for contacting the controllers. Most DPAs consider the purposes of the processing and data categories to be the most useful information, whereas the description of security procedures is considered as less useful for their purposes. Some DPAs use the notifications

⁴⁹ See <http://online.wsj.com/article/SB10001424052748703396604576087573944344348.html>.

⁵⁰ EB 2011.

for prior checking; some only use it to contact organisations in cases of a complaint, for enforcement purposes.

In several Member States, Data Protection Authorities collect *notification fees*, whereas others do not. The fees collected for a single notification range from about 23 EUR to about 599 EUR. In some Member States the fee varies depending on: whether the data controller is a natural or legal person; if processing is in the public or private sector; the numbers of staff and turnover; or by the method of notification, i.e. paper or online (e.g. Belgium). Some Member States charge a fee for amendments to the notification. In other Member States the fees are a one-off charge or an annual charge. Among those DPAs who collect fees, most receive income to their budget; this ranges from just over 1.2 % of their budget up to 100%, i.e. providing their complete budget (UK DPA). In few Member States the fees are paid into general revenue and do not benefit the DPA's budget.

There is general consensus amongst data controllers that the current general obligation to notify all data processing operations to the Data Protection Authorities is a rather cumbersome obligation which does not provide, in itself, any real added value for the protection of individuals' personal data, but rather creates an additional administrative and financial burden. This is particularly the case, as a consequence of the rules on the applicable law, where a controller is established in several Member States and has to comply with *divergent notification systems*.

According to the Article 29 Working Party's Advice paper on notification, a *public register* held by a DPA is no longer the best and most appropriate way for individuals to understand what an organisation is doing with their personal data, and who to contact when things go wrong.

2.9.2. *Data Protection Officers*

Most Member States made use of the possibility to exempt from the notification requirement in case that the controller ensures internal control of data processing operations by appointing a Data Protection Officer (DPO). However, only the national laws of about one third of the Member States (including France, Czech Republic, Germany, Hungary, Latvia, Luxembourg, Malta, Netherlands, Poland and Slovakia) contain *specific provisions on the expertise or the independence* of the DPO regarding the exercise of his/her functions.

While the appointment of a DPO is optional for the controller in other Member States, in Germany the appointment of a DPO is *mandatory*: for the public sector and – with a specified threshold of, in principle, ten employees permanently employed in the automatic processing – for the private sector. This does not necessarily lead to the recruitment of additional staff; often the assignment is given as an additional task to an existing staff member where the DPO function does not require a full-time, dedicated staff member. Other controllers outsource this task to external DPOs which provide services to various clients.

Existing studies point to the fact that larger corporations, especially multinationals, usually already have appointed data protection officers. The same is true for many public data controllers in a number of Member States. The Article 29 Working Party noted that the *successful experience* of the mandatory introduction of Data Protection Officers in Germany abolished not only the centralised system of notification and public register, but contributed

also to the development of sector-specific best practices in data processing and protection.⁵¹ This has been confirmed by stakeholders who expressed strong support for such concept, seen as a key element to demonstrate "accountability".

Given the different approaches of Member States to the notification requirements and on the exemptions there from, and the administrative burden for operators in the internal market to comply with different rules and concepts, a revision of the current notification system is needed. Harmonised conditions and standards are also needed for Data Protection Officers.

2.10. Remedies and Sanctions - Articles 22 and 24

2.10.1. Remedies

All Member States guarantee, as a fundamental principle of the rule of law, the right to seek **redress and corrective action through the courts**. Data subjects are therefore entitled by ordinary administrative or civil law to go to court. In some Member States, data protection law either creates a special tort, or adds such a special right to the general law. The forum and the procedures are also determined by the ordinary court procedural law. However, under the applicable rules in the Directive, the courts may have to apply the substantial law of the country in which the controller is located.

The substantial law differs to a certain extent from Member State to Member State, but in principle, the applicable administrative or civil law provides, in line with the Directive, that the controller is liable for **compensation**, unless he/she can prove that he/she is not responsible for the event causing the damage. In Ireland, under certain conditions, there is some lessening of the controller's burden of proof in view of alleged inaccuracy. UK law is more restrictive concerning non-material damage, for which compensation can only be awarded if material damage has also been proved. Belgium, Italy and Greece give data subjects the option of settling disputes either through the courts or by lodging a complaint to the Data Protection Authority in a quasi-judicial procedure.

Despite the fact that many cases where an individual is affected by an infringement of data protection rules also affect a considerable number of other individuals in a similar situation, in many Member States **judicial remedies, while available, are very rarely pursued** in practice. This seems to be related to a general reluctance to bring an action to court, often related to the lack of information and the financial risk for the individual, when he/she is obliged to bear the costs of an unsuccessful claim for a judicial remedy, or when the damage is limited, e.g. in the case of unsolicited mails. Whereas the Directive spells out that each supervisory authority shall hear claims also when lodged by an **association representing the individual**, such possibility that associations represent data subjects in court cases is not provided by the Directive. On the other hand, stakeholders expressed reluctance as regards a 'class action' style procedure, fearing that this would increase the cost of services.

⁵¹ Report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of data protection officers in the European Union, 18.1.2005 (WP 106).

2.10.2. Sanctions

The Directive obliges Member States to "lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive", but does not detail the categories of sanctions or whether and, if so, what sanctions could be imposed by Data Protection Authorities or by other authorities or by the courts. Accordingly, the implementation of this general provision by the individual Member States has given rise to significant variations. In most Member States, both the DPAs and the judicial authorities have the **power to impose sanctions**, in others the sanctioning power is only for judicial authorities. Administrative fines are imposed by the DPAs in most Member States, but not in all (e.g. not in Austria, Belgium, Denmark, Lithuania, Hungary and UK). Criminal sanctions have been imposed by judicial authorities in most Member States, but not in e.g. Bulgaria, the Czech Republic, Spain and Latvia. Hungary does not provide for administrative or criminal sanctions for the violation of data protection rules at all, but merely establishes liability under civil law. Slovakia in addition to administrative fines introduced disciplinary fines which may be imposed by the DPA.

The degree of precision of the infringements which are subject to **administrative sanctions** diverges considerably between the countries. Some countries define the infringements in general terms, for instance 'processing of personal data in violation of the Data Protection Law' (e.g. Lithuania). Others enumerate long and very detailed lists of infringements, such as: failure to specify the purpose, means or manner of processing; processing of inaccurate personal data; collecting or processing of personal data in a scope or manner which does not correspond to the specified purpose; preservation of personal data for a period longer than necessary for the purpose of processing; processing of personal data without the necessary consent of data subject; failure to provide the data subject with information in the scope or in the manner provided by law; refusal to provide the data subject with the requested information; failure to adopt or implement measures for ensuring security of personal data processing; failure to fulfil the notification obligation (e.g. Czech Republic).

Administrative fines in most Member States are established by specifying the minimum and maximum amount of money, while some others also make a reference to the percentage of gross turnover for the latest financial year in case the data controller is a legal entity (e.g. France). The upper limits for violating data protection laws range from €290 in Lithuania up to €120,000 in Italy, €300,000 in Germany and €601,000 in Spain. Some Member States differentiate the fines according to the type of the data controller, distinguishing natural and legal persons (e.g. Estonia, Czech Republic, France, Portugal), whether there is a repetitiveness of the offence or not (e.g. France, Lithuania), or have specific provisions to take into account negligence or intent (e.g. Poland, Portugal). In a few Member States the attempt to commit an offence is subject to penalty (e.g. Austria).

Criminal sanctions are not imposed in all Member States (e.g. not in Bulgaria, Czech Republic, Latvia). In almost two thirds of the Member States detention has been imposed for serious violations of the data protection rules. The maximum period for imprisonment ranges from 4 months (e.g. Denmark and Portugal), one year (e.g. Austria) and two years (e.g. Germany, Sweden) up to three years (Spain and Poland). Several Member States do not impose criminal sanctions at all. The amount of criminal fines also differs significantly between Member States.

In a number of Member States the level of fines is seen as too low. Fines are imposed too infrequently to have a dissuasive effect, or because supervisory bodies have not developed a practice of imposing them. In some countries prosecutions and sanctions for violation of data protection law are extremely limited.

In order to facilitate the application of remedies, the right to bring an action in court might be extended to civil society associations representing data subjects. There is also the need for strengthening the existing provisions on sanctions, including by explicitly obliging the Member States to impose criminal sanctions in cases of serious data protection violations.

2.11. Data transfers to third countries – Articles 25 and 26

2.11.1. Adequacy

Article 25 provides the principles for the transfer of personal data on the basis of an adequacy decision, either on the basis of national law or by the Commission.⁵² However, the condition that the third country must provide an *adequate level of protection* to the data being transferred is implemented by Member States in different ways. Some allow the data controller itself to conduct the adequacy check, while others reserve it for national authorities, in particular the DPAs. This leads to divergent approaches and uncertainties on the interpretation of "adequate level of protection", and varying interpretations of this concept between Member States, the DPAs and data controllers for declaring that the level of protection of a third country is adequate for the purposes of transfers to that country.

As regards the *Commission's adequacy decisions*, the effect of such unilateral recognition by the Commission that a given third country ensures an adequate level of data protection is to allow the free flow of personal data from EU Member States to that third country. The Commission may unilaterally launch the procedure with a view of assessing a third country's data protection legislation. In some cases, the Commission has adopted partial adequacy findings covering not all but only specific transfers of personal data to a particular third country.⁵³

In the course of its adequacy findings the Commission has encountered various failings in the data protection system of third countries, for example, failure on the part of public authorities to respect data subject's rights to privacy and the lack of independent data protection institutions.

At the same time, adequacy findings constitute a real opportunity for the Commission to engage in dialogue with third countries, promoting an EU compatible data protection model. Indeed, in today's world, characterised by constant and rapid development of new technologies where international data flows take place easily and quickly, traditional measures might not ensure sufficient protection of EU individuals.

Furthermore, the Commission's adequacy decisions are perceived by some third countries as a means to promote their strategy for a digital economy and a modern information society. These countries consider that adequacy decisions will allow them to become actively involved

⁵² See CRIDS (University of Namur), Assessment of the application of Article 25 of Directive 95/46, July 2011.

⁵³ See for the Commission decisions on the adequacy of third countries' data protection: <http://ec.europa.eu/justice/policies/privacy/thridcountries/>

in international flows of personal data and they will thus become internationally recognised as offering an adequate infrastructure and adequate means for processing personal data received from the rest of the world.

Nevertheless, current practice has shown its limits. Apart from the fact that adequacy findings involve a complex, lengthy and detailed exercise, Commission adequacy decisions are accorded a "**direct effect**" *in only a minority of Member States*. In most cases there are preliminary legislative and administrative formalities before such decisions can take effect. Depending on the Member State concerned, Commission decisions must be ratified legislatively, notified by the ministry to the national data protection supervisory authority, adopted by the supervisory authority, or notified in advance to, and authorised by, the supervisory authority.

2.11.2. *Standard contractual clauses*

International transfers may also take place to a third country which does not offer an adequate level of protection where the controller adduces adequate safeguards, particularly by means of **standard contractual clauses**, which are included in contracts that allow data transfers from a data controller established in the EU to data controllers and processors in third countries. The Commission standard contractual clauses were updated in February 2010⁵⁴, to cover subsequent sub-processing activities and provide a single contractual framework for all processing activities related to a given transfer.

Contractual clauses are seen as a useful instrument for international transfers involving a limited number of organisations or companies. However, these are also implemented differently. In some Member States, the DPA still needs to authorise the transfer, whereas in other Member States such authorisation is not required.

2.11.3. *Binding Corporate Rules (BCRs)*

The use of "**Binding Corporate Rules**" (BCRs), i.e. internal rules followed by a multinational corporation for transfers of personal data between the groups of companies belonging to the same multinational corporation, has been developed without being explicitly mentioned by the Directive.⁵⁵ Data Protection Authorities in 16 Member States (Austria, Belgium, Bulgaria, Cyprus, Czech Republic, France, Germany, Ireland, Italy, Latvia, Luxembourg, Malta, Netherlands, Slovenia, Spain, UK) and three EEA countries (Iceland, Liechtenstein, Norway) have agreed on a **mutual recognition procedure** aimed at speeding up the procedure of analysis and approval of BCR so as to ensure that they provide the necessary data protection safeguards. This procedure, which has been in place since 2008 and in which one of those DPAs acts as lead authority in each case, has accelerated the adoption of BCRs, on average, from 18 months previously to less than six months.

However, the use of BCRs also differs. Apart from the fact that not all DPAs participate in this mutual recognition scheme, several Member States still require an authorisation for the use of BCRs even though they have been approved by DPAs of other Member States. The adoption and authorisation of BCRs therefore remains **complex and time-consuming**.

⁵⁴ Commission Decision 2010/87/EU of 5.2.2010, OJ L 39, 12.2.2010, p.5.

⁵⁵ BCRs have been developed as a matter of practice by data protection authorities and by the WP29 on the basis of an extensive interpretation of Article 25(2) of the Directive. - See the overview on BCR: http://ec.europa.eu/justice/policies/privacy/binding_rules/index_en.htm.

Considerable time is often necessary for the dialogue between the multinationals concerned and the lead DPAs, as well as to allow the companies to present modified proposals, since this requires the regular involvement of the company's board.

While welcoming the approach of the BCRs and pointing to its increased significance, stakeholders in the private sector consider that the implementation of BCRs remains too lengthy, particularly due to the fact that they are a complex instrument which must address several issues, and that Data Protection Authorities have often no sufficient resources to approve BCRs promptly. This has limited the number of companies using this tool⁵⁶ and discouraged several other companies, potentially keen on using them⁵⁷. Economic stakeholders also expressed uncertainties about the notion of 'group of companies' and the lack of the inclusion of processors in the application of BCRs, and stressed the need to lay down legal rules on BCRs and to improve and simplify the "mutual recognition procedure".

Given divergent approaches and complex and lengthy procedures, there is a need to improve and streamline the current procedures for international data transfers, including providing a clear legal basis for "Binding Corporate Rules. The adequacy procedure should also be clarified, particularly as regards the criteria and requirements for assessing the level of data protection in a third country.

2.12. National Data Protection Authorities and enforcement - Article 28

2.12.1. 'Complete independence' of the National Data Protection Authorities - Article 28(1)

The requirement of "**complete independence**" has been clarified in a recent ECJ ruling⁵⁸, which stresses particularly that independence implies a decision-making power independent of any direct or indirect external influence on the supervisory authority, precluding not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task. The Court ruled therefore that making a DPA subject to state scrutiny is not in compliance with the requirement of "complete independence".

In Greece and Portugal an independent supervisory authority is explicitly established even by the Constitution. In other Member States DPAs are provided with a distinct legal personality (e.g. Malta, Spain) and by the power to bring an action in the Constitutional Court (e.g. Slovenia). In a number of Member States concerns arise as to the **effective capability** of the DPAs to perform their tasks with complete independence. These concerns are partly due to the fact that staff are appointed exclusively by the government (e.g. Ireland, Luxembourg, UK) or by the Minister of Justice (Denmark, Netherlands), whereas, in contrast, in other Member States Data Protection Commissioners are elected by legislative assemblies (e.g. Germany, Slovenia), sometimes pursuant to procedures which require consensus between the majority and the opposition (e.g. Greece), or in combined procedures involving executive, legislature, judiciary and organised societal groups (e.g. France, Spain, Portugal).

⁵⁶ According to information provided by the WP29, 14 BCRs have been approved by DPAs so far, about 25 companies have provided DPAs with a first draft of BCRs and another 26 are being prepared.

⁵⁷ According to stakeholders' feedback, only the biggest companies can afford to adopt BCRs, due to the complexity of the procedure and the related costs, which are € 20,000 on average but can amount – for very large companies with many subsidiaries - to €1 million.

⁵⁸ C-518/07, *European Commission v. Germany*, 9.3.2010.

In some countries the DPA is attached to the Ministry of Justice. In some Member States (e.g. Slovenia, Poland) the dismissal of Data Protection Commissioners has to follow the same procedures as their appointment, and only in specified cases. In other countries, government can directly remove them from office (e.g. Ireland).

Understaffing and lack of financial resources also pose problems in several Member States, restricting DPAs in the proper exercise of their tasks. Despite increases in the staff of most DPAs in recent years, the level of resources available to DPAs continues to remain limited in the majority of Member States with regard to their needs. In most Member States the DPAs receive their financial resources from the State's budget, and often from the budget allocated to the Ministry of Justice. In some Member States, these resources are increased through the revenues obtained from notifications and/or the financial sanctions imposed as a penalty for the infringement of data protection rules (e.g. Luxembourg, Malta). However, in the UK the DPA notification fees are the only financial source of the DPA (*see section 2.9 on notifications*). In a large number of Member States the lack of resources represents a significant challenge to the effectiveness of the national supervisory systems. In several Member States, DPAs do not have enough staff to handle all complaints. Furthermore, due to this lack of resources, some DPAs cannot regularly attend the meetings of the WP29.

The concept of "complete independence" of Data Protection Authorities needs to be clarified on the basis of the recent Court of Justice ruling, including the requirement to provide sufficient resources for the effective performance of the tasks of the Data Protection Authorities.

2.12.2. Investigative powers - Article 28(3), first indent

In all Member States the Data Protection Authorities hear and review ***claims or complaints*** and are charged with investigating possible infringements of the data protection law within their jurisdiction. This includes that they are vested with powers to request and access all necessary information in relation to processing operations and filing systems and therefore usually demand full access to relevant sites and materials. A range of DPAs practice a selective approach, i.e. selecting particular issues or sectors for particular attention, because of the importance of the processing in the sector concerned, the sensitivity of data, or because of the level of complaints received about the sector. In such cases especially, investigations tend to be detailed and in-depth, including discussions with the data controllers, but less so with the data subjects or their representatives.

In most Member States the DPAs are empowered to ***search premises*** without judicial warrant. In Belgium, DPA staff has the status of Officers of Judicial Police when carrying out on-site investigations, empowering them to demand, *inter alia*, the disclosure of documents and access locations. But in other Member States (e.g. France, Malta, Romania and UK), the DPA cannot enter premises without first obtaining a judicial warrant.

In some Member States the investigative powers are not clearly spelt out in the legal text, being expressed as duties rather than as an express reference to powers, or without clarification of the relationship to other legislation.

2.12.3. Powers of intervention - Article 28(3), second indent

The DPAs' powers of intervention differ from Member State to Member State. In most Member States the DPAs have the power to **authorise processing operations** likely to present specific risks, but not in others (e.g. Cyprus, Latvia, Spain and the UK). Experience shows that a major problem with these "prior checks" is that they are very time-consuming and demanding on human resources, and that too often they are carried out too late to be of any benefit in restructuring processing systems fundamentally, focussing instead on the minor details of such systems.

In all Member States, the DPAs may issue a warning to or reprimand the controller, and, except in Belgium, issue decisions binding upon the controller to **suspend data processing operations**. In most Member States the DPAs are also empowered to **order the erasure or destruction of data** (but not e.g. in Belgium, Germany or the UK). In Germany, the DPA is empowered to demand the dismissal of a Data Protection Officer, if he/she does not possess the required specialised knowledge and demonstrate the necessary responsibility. In several Member States the law provides that such binding measures should be preceded by recommendations, opinions or warnings (e.g. Austria, Bulgaria, Denmark, France, Greece, Ireland, Latvia, Lithuania, Slovakia).

In most Member States, the DPA has the **power to impose sanctions**, which mostly consist of imposition of administrative measures and/or financial sanctions/fines, however with considerable variation as to what constitutes an infringement and severity of sanctions (*see section 2.10*). Most DPAs report infringements to competent police and judicial authorities; in several Member States, such obligation is expressly laid down in data protection law (e.g. Cyprus, France, Lithuania, Netherlands and Slovenia). French law provides that the DPA may publish its warnings and, in certain situations, the penalties imposed. In several Member States the DPAs may refer the matter to national Parliament (including Belgium, Estonia, Finland, France, Germany, Greece, Italy, Lithuania, Malta, Netherlands and Sweden).

In all Member States formal actions and sanctions are, in practice, **used as a last resort**. In general, the DPAs see themselves more as advisors, facilitators and conciliators. In more than half of Member States, DPAs have issued guidelines to assist in the proper application of the data protection rules, including sector specific guidance. In cases of violations of data protection rules, DPAs in general first issue warnings, reminders or recommendations. In complex cases, DPAs often try to reach a compromise acceptable to the DPA and the controller. Such "soft measures" seem to be more effective where they are backed-up by effective enforcement powers available to the DPA in the event of non-compliance with the agreed measures.

2.12.4. Power to engage in legal proceedings - Article 28(3), third indent

In many Member States, national laws provide the immediate right to DPAs **to bring an action to court**. But in some Member States this is limited to the private sector or to specific situations. In Sweden, for instance, the right to bring an action in court is limited to the administrative courts for applications of the DPA to erase personal data which have been processed in an unlawful manner. In other Member States, DPAs have only the power to bring violations of the data protection rules to the attention of judicial authorities (e.g. Austria, Latvia and Ireland). In Slovenia, the DPA has the right to bring an action before the Constitutional Court to assess the constitutionality of legislation. In some Member States,

DPA's have the right to join in court proceedings which are initiated by other parties. In practice, also in many Member States, even where the DPAs have the power to engage in legal proceedings, the DPAs rarely commenced legal proceedings or intervened in legal proceedings on behalf of a data subject. In other Member States, the number of interventions ranged from 2 to a maximum of 143 cases per year.

In several Member States, Data Protection Authorities are not endowed with the full range of powers to conduct investigations, intervene in data processing operations and engage in legal proceedings. The divergence in powers and approaches to enforcement taken by the individual DPAs causes problems not only for the data subjects who do not enjoy the same level of enforcement in each Member States, but also uncertainties for controllers, particularly when operating in several Member States.

2.12.5. Appeals against decisions of supervisory authorities - Article 28(3)

As regards the right to appeal **against decisions of the Data Protection Authorities**, Danish law stipulates that no appeals may be brought before any other administrative authority against the decisions of the DPA, but does not clarify whether there is a right to go to court against those decisions. In Slovenia the law provides that there shall be no appeal against a decision or ruling of the DPA, but that an "administrative dispute" shall be permitted. Some Member States have no specific provision in their data protection law, but provide a general right to judicial review against any act of a public authority, on the basis of general court procedural law or, e.g. in Germany, on the basis of the Constitution.

Competent courts are either the ordinary courts or administrative courts. In some Member States the competent court is the Supreme Administrative Court (e.g. Austria, Portugal) or the general Court of Appeals (e.g. Greece, Sweden), in France the *Conseil d'Etat* and in Malta a specific Data Protection Appeals Tribunal. In several countries judicial review is limited to certain acts of the DPA (e.g. Ireland, Luxembourg, UK), or to the grounds of "illegal conduct" of the DPA (Hungary). The competence and procedure of the courts and the conditions for a right to appeal follow the general national rules of their judicial systems. Cases in which data subjects or data controllers have appealed in courts against decisions taken by the national data protection supervisory authority are rather limited.

Nearly all Member States guarantee in their national legislation the right to bring an action to court against decisions of the Data Protection Authority, either in data protection law or in general laws on judicial review.

2.12.6. Cooperation of Data Protection Authorities - Article 28(6)

Article 28(6) provides the competence of Data Protection Authorities to exercise their powers on the territory of their Member State, whatever national law is applicable, and the duty to exercise their powers on request of another DPA and to cooperate with each other "to the extent necessary for the performance of their duties".

Some Member States have provisions which specifically allow them **to act on the request of the DPA in another Member State** (e.g. Denmark, France, Portugal, UK) or to also exercise, on its own territory, its powers in cases where the law of another Member State applies (e.g. Denmark, Netherlands, Portugal). Whereas several national laws do not contain any related provision, other Member States have transposed in their national law only the mandate to

cooperate with DPAs in other Member States or generally with "foreign" DPAs (e.g. Cyprus, Czech Republic, Estonia, Greece, Italy, Luxembourg, Malta, Romania, and Spain).

In practice, DPAs liaise and/or *cooperate with authorities of other Member States* mainly in the context of the Article 29 Working Party or in the mutual recognition procedure for BCRs (see point 2.11.3). There has also been separate cooperation as between Nordic countries, as well as on the part of Central and Eastern Europe Data Protection Commissioners. Other forms of cooperation concern the participation in the Article 31 committee, the Working Party on Police and Justice, fora such as the Spring Conference of Data Protection Authorities and joint supervision for SIS, Europol, Eurojust, Eurodac and the Customs Information System. Some DPAs have designated, within their organisation, a contact point for such cooperation. DPAs have also some experience in joint investigations, where each applies its own law in its own jurisdiction.

However, the situation is more complex when *jurisdiction and applicable law do not coincide*. This concerns not only the legal aspect in terms of the applicable law to be followed, but also procedural aspects as regards the respective roles, responsibilities, powers and practices of each DPA involved. Thus, when a controller is established in more than one Member State or in other similar situations, the approaches taken by DPAs could considerably differ from one Member State to another.

Despite the fact that the Directive creates the duty of mutual cooperation and information exchange, there is *no cooperation mechanism established by the Directive* to provide an effective cooperation in such situations. This is amplified by the lack of harmonisation with regard to investigation powers and the absence of a legal obligation to reply and to inform of the outcome of proceedings, while current cooperation seems to be based on "good will", and deadlines are difficult to respect. There is hardly any experience on the application of the national law of another Member State; difficulties could arise in enforcing the data protection law of another Member State especially for small DPAs which have limited resources for cooperation on such a scale. Due to the lack of detailed rules in the Directive, some DPAs apply the provisions on mutual assistance in the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data⁵⁹. However such an approach, as well as existing non-binding mechanisms and structures in the framework of the WP 29, are insufficient to ensure the consistent application of data protection rules across the EU (see point 2.13). This situation often leads to divergent decisions of DPAs *vis-à-vis* the same data controller for the same data processing. No one single DPA has a complete overview of the processing activities of companies that are established (or, if based outside the EU, have appointed a representative) in several Member States.

Cooperation between DPAs is insufficient and does not ensure consistent enforcement of the common rules within the EU, in spite of the fact that the Directive creates the duty of mutual cooperation and information exchange. To improve the cooperation and coordination between Data Protection Authorities a cooperation mechanism should be introduced which ensures the consistent application and enforcement of the data protection rules in all Member States where this concerns issues with cross-border dimension.

⁵⁹ ETS No. 108.

2.13. Article 29 Working Party

The Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of the Directive with *advisory status*⁶⁰ - the so-called "Article 29 Working Party" (WP29) - is mandated to contribute to the uniform application of the Directive, to give the Commission an opinion on the level of protection in the EU and in third countries, on codes of conduct drawn up at EU level and advise the Commission on any amendment of the Directive and on any measures related to the protection of the rights and freedoms of natural persons with regard to the processing of personal data.

Since its creation, the Working Party has adopted 187 *opinions* (as at July 2011) and a variety of other documents. The opinions of the Working Party have dealt with topics including certain key concepts of the Directive, such as the opinions on the concept of personal data, the concepts of 'controller' and 'processor' and applicable law and on consent, as well as to the transfer of data to third countries and the level of protection in third countries or to specific issues.

Although in some cases the opinions of the Working Party have a certain impact national legislation and practice – some Member States amended their data protection legislation, once or twice, as a result of the work of the Working Party⁶¹ – the continuing divergent application and interpretation of EU rules by Data Protection Authorities has not been resolved sufficiently. This is largely due to the fact that often DPAs are *not in a position to enforce in their own national jurisdiction* the very same principles they advocate at European level. Apart from the fact that the Working Party's opinions are not legally binding, this may be often caused by legal restraints particularly as regards the DPAs' competences and powers, which vary widely among Member States and the lack of a mechanism at EU level to ensure a coordinated application and enforcement of data protection rules (*see section 2.12*).

Moreover, the fact that the Commission also ensures the *secretariat of the WP29* leads to uncertainties as to the demarcation between the role of the Commission as an Institution, on the one hand, and its role as secretariat, on the other hand, particularly when the WP29 adopts opinions which are critical of the Commission's position. As member of the Working Party (albeit without voting rights) the Commission promotes its priorities, its views and requests for advice. In its role as secretariat, it is its role to assist the Working Party according to the Working Party's own priorities and approaches.

The non-binding opinions of the Article 29 Working Party are insufficient to ensure the consistent application and interpretation of EU rules by Data Protection Authorities. The two-fold role of the Commission, being member in the Working Party and providing at the same time its secretariat, bears the risk of "conflicts of interest".

⁶⁰ The Article 29 Working Party is an advisory body composed of one representative of Member States', Data Protection Authorities, the European Data Protection Supervisor (EDPS) and the Commission (without voting rights), which also provides its secretariat. See: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm .

⁶¹ In Member States' replies to the survey, particular reference was made to the opinions on the concept of personal data (WP 136), on the concepts of data controller and data processor (WP 169), on online social networking and on processing by video surveillance (WP 89).

3. THE MAIN RESULTS: THE NEED FOR A NEW LEGAL FRAMEWORK

The findings of this evaluation on key provisions of the Directive show that the problems encountered in the Commission's 2003 and 2007 implementation reports have not been solved since then. On the contrary, the problems in *fully achieving its internal market policy objective*, removing differences in the level of data protection actually afforded in the Member States and in ensuring effective *enforcement* across the EU have become more acute in particular due to fast and far-reaching development of digital technologies and online services.

While the two-fold objective of ensuring an equivalent level of data protection amongst Member States and removing obstacles to the free movement of data as well as the key data protection principles remain valid, divergent approaches and gaps in the Directive and its application in Member States have led to legal fragmentation and uncertainty with negative consequences for businesses, individuals and the public sector and increasing difficulties for individuals in keeping control of their personal data. Since the Directive does not provide for sufficient protection in a fast-developing information society and globalised world, the increasing problems call for a *new legal framework for the protection of personal data in the EU*.

As confirmed by the findings of this evaluation of key provision, the fragmentation and uncertainties in the implementation of the Directive 95/46/EC and new challenges require the EU to adapt the legal framework for the protection of personal data in the European Union.

ANNEX 3

DATA PROTECTION IN THE AREAS OF POLICE AND JUDICIAL CO-OPERATION IN CRIMINAL MATTERS

4. FRAGMENTATION OF THE EU LEGAL FRAMEWORK FOR THE PROTECTION OF PERSONAL DATA IN THE AREAS OF POLICE COOPERATION AND JUDICIAL COOPERATION IN CRIMINAL MATTERS

4.1. Directive 95/46/EC does not apply in these areas

The general **Data Protection Directive 95/46/EC**⁶² applies to public and private data controllers and all sectors but does not apply to the processing of personal data in the areas of judicial cooperation in criminal matters and police cooperation.⁶³ Furthermore, Article 13(1) of the Directive allows for exemptions and restrictions of some important provisions of the Directive (relating to data quality, information, access, and publicising), *inter alia* for safeguarding national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.⁶⁴ The exclusion of the area of judicial cooperation in criminal matters and police cooperation led to the adoption of specific rules at EU level for police and judicial co-operation in criminal matters⁶⁵. Given the lack of a single EU instrument on data protection in this area until the adoption of Framework Decision 2008/977/JHA in 2008, these specific rules generally refer either to national legislation of the Member States, or to the Convention of the Council of Europe (ETS 108)⁶⁶ and – for those Member States which have ratified it – to the Additional Protocol to that Convention (ETS 181)⁶⁷, as well as to the principles of the non-legally binding Recommendation No. R (87) 15 of the Council of Europe regulating the use of personal data in the police sector (Police Recommendation)⁶⁸, which sets out the principles of Convention 108 for the police sector.

⁶² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('Directive') (OJ L 281, 23.11.1995, p.31).

⁶³ See Article 3(2), first indent, of Directive 95/46/EC: "This Directive shall not apply to the processing of personal data: - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law".

⁶⁴ The majority of Member States apply the Directive to the activities of police, customs, judicial and other competent authorities concerned with the prevention of and the fight against crime (see Commission Staff Working Document SEC(2005) 1241 as well as the replies of Member States to the Commission's questionnaire on the implementation of the Framework Decision).

⁶⁵ See the list at the end of this annex.

⁶⁶ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.: 108), ('Convention 108').

⁶⁷ Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows ETS No.: 181, ('Additional Protocol').

⁶⁸ Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, ('Police Recommendation').

4.2. Gaps and shortcomings in Framework Decision 2008/977/JHA

4.2.1. Limited scope of application of Framework Decision 2008/977/JHA

Framework Decision 2008/977/JHA⁶⁹ had to be implemented by Member States by 27 November 2010 (Article 29(1)).⁷⁰ It applies to personal data which for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties are transferred between different Member States (Article 1 (2)(a)), or which, after having been transferred between different Member States are subsequently transferred to a third country or international organisation (Article 13). It furthermore applies to personal data which are or have been transmitted or made available by Member States to authorities or to information systems established on the basis of the former Title VI of the Treaty on European Union ('Police and judicial cooperation in criminal matters') (Article 1(2)(b)), or are or have been transmitted or made available to the competent authorities of the Member States by authorities or information systems established on the basis of the former Treaty on European Union or the former Treaty establishing the European Community (Article 1(2)(c)).

- **No application to domestic data processing:**

As a first consequence of the scope as described in Article 1 (2)(a), the Framework Decision **does not apply to domestic processing operations** by competent judicial or police authorities in the Member States, or to **direct transfers** from a Member State to a third country or an international organisation.

Example 1: Exchange of personal data with Interpol

The Council Common Position 2005/69/JHA⁷¹ on exchanging certain data with the International Criminal Police Organisation (Interpol) obliges Member States to take the necessary measures to allow for the exchange of data between their competent law enforcement authorities and Interpol.

The Framework Decision does not apply to **direct exchanges** of personal data by Member States with Interpol.

However it would apply once personal data had been exchanged between Member States **and then** transferred to Interpol (Article 13 of the Framework Decision).

This distinction between personal data to be transferred or exchanged, and personal data being processed at domestic level only, exists neither in the relevant Council of Europe instruments, nor in the Directive. Both instruments apply without distinction to the processing of data carried out within Member States and when transferred from a Member State to a third country.⁷² As held by the ECJ in a number of cases⁷³, the rules on the protection of

⁶⁹ Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60) ('Framework Decision').

⁷⁰ See separate implementation report, COM(...).

⁷¹ Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol, (OJ 2005 L 27, 29.1.2005, p. 61).

⁷² See, e.g. Directive 95/46/EC Articles 3 and 4, and Articles 25-26.

⁷³ See Joined Cases C-465/00, C-138/01 and C-139/01 Rechnungshof, paragraphs 41-43 (op cit); Case C-376/98 Germany v. Parliament and Council, paragraph 85; Case C-491/01 British American Tobacco and Imperial Tobacco, paragraph 60.

individuals with regard to the processing of personal data and the free movement of such data apply regardless of whether or not there is a cross-border dimension.

Moreover, this distinction is difficult to make in practice: personal data which have been gathered in a purely domestic context can hardly be factually distinguished from data that have been subject to cross-border transmission. *A priori*, any purely domestically processed data may be subject to cross-border transmission. It can complicate the actual implementation and application of the Framework Decision and other legal instruments at EU level: good co-operation between Member States requires there to be mutual trust regarding the data protection of information received from other Member States. Such a high degree of trust can only be achieved if the protection (and the ensuing reliability) of all data which – at a later stage – may be transferred to other Member States, is fully ensured.

This distinction also may lead, in these areas, to different levels of data protection in different Member States between personal data to be transferred or exchanged or personal data being processed at domestic level only. Neither Article 8 of the Charter of Fundamental Rights of the European Union nor Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms excludes any situation or sector from the scope of protection.⁷⁴

This distinction also creates legal uncertainty – both for data subjects and for competent authorities – as to which rules should apply when personal data are processed by police and judicial authorities.

This limited scope of the Framework Decision already leads to legal and practical deficiencies for the protection of personal data at EU level: more and more EU legislation creates harmonised legal obligations upon private or public sector data controllers requiring the processing and exchange of personal data for purposes of prevention, investigation, detection or prosecution of criminal offences, without providing for correspondingly harmonised and/or comprehensive provisions for the protection of personal data, as the Framework Decision does not apply to the domestic processing of personal data in these situations.

This shortcoming of the Framework Decision has been pointed out also by several Member States during an expert meeting in February 2011 on the implementation of the Framework Decision. It has also been criticised by the European Data Protection Supervisor.⁷⁵ The European Parliament⁷⁶, the Conference of Data Protection Authorities⁷⁷, and the Council of Europe's T-PD Consultative Committee – consisting of data protection representatives of European governments – have all made clear in various occasions that the non-applicability of the Framework Decision to domestic processing of personal data is a key weakness.

- ***Application only to ‘competent authorities:’***

The Framework Decision applies to the processing of personal data by ‘competent authorities’ (or ‘information systems’) which transfer or make available personal data to other competent police or judicial authorities. In that context, ‘competent authorities’ means “agencies or

⁷⁴ In the second subparagraph of Article 16(2) TFEU a distinction is only made as far as a specific legal instrument for the Common Foreign and Security Policy is concerned.

⁷⁵ European Data Protection Supervisor, third opinion of 27 April 2007 on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, OJ 2007 C 139, p.1.

⁷⁶ European Parliament legislative resolution of 7 June 2007 on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (renewed consultation) (7315/2007 – C6-0115/2007 – 2005/0202(CNS)).

⁷⁷ See in particular: Declaration adopted by the European Data Protection Authorities in Cyprus on 11 May 2007 and the Common position of the European Data Protection Authorities on the use of the concept of availability in law enforcement Cyprus, 10. - 11. May 2007.

bodies established by legal acts adopted by the Council pursuant to Title VI of the Treaty on European Union, as well as police, customs, judicial and other competent authorities of the Member States that are authorised by national law to process personal data” within the scope of the Framework Decision (Article 2 h));

However, as a second consequence of the limited scope as described above, the Framework Decision **does not apply to activities by data controllers, which are not competent police or judicial authorities**, but which are transferring personal data within "a framework established by the public authorities that relates to public security", as described by the case law of the ECJ and are therefore in some way connected with the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or enforcement of criminal law.

This is the case e.g. for air carriers providing travellers information to police authorities of third countries, or internet service providers which have retained communication data for the purpose of fighting serious crimes, as required by Directive 2006/24/EC on data retention⁷⁸. The Framework Decision therefore fails to address this legal uncertainty.⁷⁹

4.2.2. Low level of harmonisation of the Framework Decision

The Framework Decision provides for a **low level of harmonisation**. It allows national laws providing for the protection of personal data at national level to impose **higher safeguards** than those established in the Framework Decision (Article 1(5)). As a consequence, national processing restrictions in place in one Member State have to be met by the other Member States (Article 12). The higher safeguards may also result from legal instruments adopted at EU level its Article 28 also states: “*where in acts adopted prior to the date of entry into force of this Framework Decision and regulating the exchange of personal data between Member States [...] specific conditions have been introduced as to the use of such data by the receiving Member State these conditions shall take precedence over the provisions of this Framework Decision*” (see below § 1.3).

Furthermore, the Framework Decision also ‘does not affect’ Convention 108 and its Additional Protocol (recital 41), thereby leaving it open for interpretation if its level of protection is ‘at least equal’ to the one of the Convention 108.

By contrast, other former third pillar instruments require Member States explicitly to adopt national data protection provisions in order to achieve a level of protection of personal data ‘at least equal’ to that resulting from the Convention 108 (Schengen Implementing Convention Article 126) or additionally to the Additional Protocol with the Police Recommendation (Prüm Decision Article 25).

4.2.3. No powers of EU institutions vis-à-vis the Framework Decision

As to the powers of the EU institutions, Protocol 36 on Transitional provisions annexed to the Treaty of Lisbon provides that the Commission has no infringement powers in the case of the Framework Decision (Article 10). Also, the powers of the Court of Justice are to remain the same with respect to those acts in the field of police cooperation and judicial cooperation in

⁷⁸ 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 (OJ L 105, 13.4.2006, p. 54).

⁷⁹ See the Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive (OJ C 255, 27.10.2007, p. 1). See also the EDPS Annual Report 2006, p. 47.

criminal matters which were adopted before the entry into force of the Treaty of Lisbon. Till these transitional measures cease to have effect five years after the date of entry into force of the Treaty of Lisbon, this legal status of the Framework Decision has implications to the extent that current rules for data controllers are not uniform and coherent across the EU. Furthermore, the Commission does not have implementing powers and there is no competence for the Article 29 Working Party composed by DPAs aiming at fostering common interpretation.

4.3. The Framework Decision's relationship with other legal instruments

4.3.1. *Unclear rules of precedence*

The Framework Decision did not replace or specifically amend the various existing sector-specific legislative instruments for police and judicial co-operation in criminal matters with data protection provisions. The articulation between the Framework Decision and these other data protection provisions contained in ex third pillar legal acts is not always clear.

Article 28 of the Framework Decision spells out a **rule of precedence** of acts adopted prior to the date of entry into force of the Framework Decision (19.1.2009).

However, some **former third pillar acts have been adopted after the entry into force of the Framework Decision**. This includes:

- Framework Decision 2009/315/JHA on **criminal records exchange**⁸⁰, which states that its specific data protection rules complement the general data protection rules in force, but with no specific reference to Framework Decision (recital 13 in the preamble);
- Decision 2009/316/JHA on the establishment of the **criminal records system ECRIS**⁸¹, which implements Framework Decision 2009/315/JHA on this issue, states that the Framework Decision 'should' apply in the context of computerised exchange of data between Member States, while allowing Member States to set higher levels of protection (recital 18 in the preamble);
- Decision 2009/371/JHA establishing **Europol**⁸², which replaced the prior Europol Convention and Protocols as from 1 January 2010, equally provides that the Framework Decision on data protection applies to the processing by Member States of the data to Europol, but that as regards Europol as such, the data protection rules in the Europol Decision replaced the general rules of the Framework Decision because of the 'particular nature, functions and competences of Europol' (recital 12 in the preamble); the same applies to two implementing decisions on Europol analysis work files⁸³, and on Europol's

⁸⁰ Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93 7.4.2009, p. 23).

⁸¹ Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93, 7.4.2009, p. 33).

⁸² Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), (OJ L 121, 15.5.2009, p. 37).

⁸³ Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files (OJ L 325, 11.12.2009, p. 14).

relations with partners, including the exchange of personal data and classified information⁸⁴;

- Amending Decision 2009/426/JHA to the Decision establishing **Eurojust**⁸⁵ specifies that the Framework Decision on data protection applies to the processing by Member States of the data transmitted between the Member States and Eurojust, but that the data protection rules applying to Eurojust as such (as amended by this later Decision) are not affected by the Framework Decision, because of the ‘particular nature, functions and competences of Eurojust’ (recital 13 in the preamble);
- Framework Decision 2009/829/JHA on the **recognition of pre-trial supervision orders**⁸⁶ also states that the Framework Decision applies to personal data exchange within its scope (recital 19 in the preamble);
- Decision 2009/917/JHA establishing the **Customs Information System (CIS)**⁸⁷, which replaces the CIS-Convention and its Protocols as from 27 May 2011 (Art 34), contains a number of specific references to the Framework Decision, which applies to the CIS unless otherwise provided for in the Decision (Art 20);
- Framework Decision 2009/948/JHA on **conflicts of jurisdiction**⁸⁸ states that the Framework Decision applies to personal data exchange within its scope (recital 18).

As regards the **acts adopted prior to the entry into force** of the Framework Decision, Article 28 does not clarify whether "**specific conditions** as to the use of such data by the receiving Member State" should also relate to general principles for the protection of personal data, such as guaranteeing lawful processing or supervision by independent data protection authorities or if they are only to be understood as being limited to conditions of use, e.g. a prohibition to process personal data supplied for the prevention of criminal offences for a major event with a cross border dimension for other purposes.

Recital 39 lists some existing measures which are deemed to set out a “**complete and coherent set of rules**” regarding data protection and remain unaffected by the Framework Decision. This creates legal uncertainty, in particular, because there is no exhaustive list of legal instruments that are to remain unaffected. As a consequence, it is left to the interpretation on a case-by-case basis which rules apply to a concrete situation. Furthermore, despite explicit references in the recital (but not in the legal text itself), it is not entirely clear whether the specific rules in these measures mentioned apply entirely instead of the rules in the Framework Decision or if the Framework Decision could apply e.g. in case of possible gaps in the legal instruments cited.

⁸⁴ Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol’s relations with partners, including the exchange of personal data and classified information (OJ L 2009, L 325, 11.12.2009, p. 6).

⁸⁵ Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (‘Eurojust Decision 2009’) (OJ L 138, 4.6.2009, p. 14)

⁸⁶ Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention (OJ L 294, 11.11.2009, p.20).

⁸⁷ Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes (OJ L 323, 10.12.2009, p 20).

⁸⁸ Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (OJ L 328, 15.12.2009, p. 42).

As regards measures targeted by recital 40 of the Framework Decision which have “more limited data protection rules”, they apply instead of the Framework Decision if the conditions imposed – as to the use or further transfer of personal data - on receiving Member States are ‘**more restrictive**’ than the Framework Decision, but otherwise the Framework Decision applies. Again, this leaves a large room for interpretation and therefore does not provide legal certainty neither for individuals nor for police and other competent authorities.

4.3.2. Differences in content between the Framework Decision and the other legal instruments with specific data protection provisions

A comparison of the substantive rules contained in the Framework Decision with the abovementioned other legal instruments with data protection relevance, in particular Directive 95/46/EC, shows differences in content, some of which are presented below.

- **Definition of ‘personal data’:**

The definition of ‘personal data’ (Article 2 (a) Directive) can equally be found e.g. in the Framework Decision (Article 2 (a)), while the definitions used for the SIS II Decision (Article 3 (d), or the CIS Decision (Article 2 No. 2) are only identical as to the main part of the definition, and do not describe further what is to be understood under an ‘identifiable person’. The Prüm Decision adds that “processing within the meaning of this Decision shall also include notification of whether or not a hit exists” (Article 24 (1) a)).

- **Limitations to the purpose limitation principle:**

The Directive requires personal data to be collected for specified, explicit and legitimate purposes and prohibits further processing in a way incompatible with those purposes (Article 6(1)(b)).

While the Framework Decision does lay down similar principles in its Article 3, it leaves it explicitly to the Member States to determine more precisely at national level which other purposes are to be considered as incompatible with the purpose for which the personal data were originally collected (recital 6). It also provides for further exceptions from the purpose limitation rule, as regards data received from other Member States (Article 11), including further processing for “any other purpose”, with the prior consent of the transmitting Member State or with the consent of the data subject, given in accordance with national law (Article 11 (d)). Equally, the Prüm Decision provides that although processing of personal data by the receiving Member State is ‘permitted solely’ for the purposes for which the data have been originally transferred, processing ‘for other purposes’ is admissible with prior authorisation of the Member State administering the file and subject to the national laws of both receiving and administering Member State (Article 26). A similar provision exists in the CIS Decision (Article 8).

In consequence, a provision permitting processing ‘for other purposes’ means that in practice any personal data, including sensitive data, processed by a competent police authority in one Member State and transmitted to another Member State may be processed for different purposes other than those for which they were originally collected and then transmitted and thereby emptying the purpose limitation principle of its value. In this context, the “consent” or “authorisation” of the transmitting authority cannot be considered under any circumstances as providing a valid legal ground to derogate from the purpose limitation principle.

- **Periodic review of personal data processed:**

The periodic review provided for by Article 5 of the Framework Decision refers to review of the need for the storage of the data but does not ensure the periodic verification of data quality

and does not ensure that police files are purged in practice of superfluous data and kept up to date.⁸⁹ The importance of such review is important both to ensure individuals' rights and for the efficient operation of police services.

- **Information to the data subject:**

Under the Framework Decision (Article 16), Member States have to ensure that their competent authorities inform data subjects of processing, unless national law provides otherwise or in cases of transfer to another Member State where that Member State has requested that the data subject is not to be informed. The Framework Decision does not specify form, content and modalities of that information and leaves this to national law. Under the Europol and Prüm Decisions it is established that when a data subject is informed it must be in an 'intelligible' or 'comprehensible' form. Under the Prüm Decision it must be free of charge.

- **Right of access:**

Under the Framework Decision (Article 17), a data subject has the right to obtain, without constraint or excessive delay or expense, either:

- (a) at least a confirmation from the controller or from the national supervisory authority as to whether or not data relating to him have been transmitted or made available and information on the recipients or categories of recipients to whom the data have been disclosed and communication of the data undergoing processing, or
- (b) at least a confirmation from the national supervisory authority that all necessary verifications have taken place.

This information or confirmation can either be provided directly by the competent authority ("direct access") or by the supervisory authority ("indirect access")⁹⁰. Member States may legislate restrictions to this right of access, in order to avoid obstructing official or legal inquiries, investigations or procedures; prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties; protecting public security; protecting national security; and protecting the data subject or the rights and freedoms of others (Article 17 (2)). Any refusals on behalf of the controller to provide this information must be made in writing (Article 17 (3)).

Both the 2002 Eurojust Decision (Article 19) and the Europol Decision (Article 30) provide for a specific right of access in a detailed provision. Other than these instruments, out of 26 other instruments, only six provide for a specific right of access in a specific provision: the Schengen Implementing Convention (Article 109), the SIS II Decision (Article 58), the Naples II Convention (Article 25), the Prüm Decision (Article 31), the VIS access Decision⁹¹ (Article 14) and the CIS Decision (Article 22). All these instruments require the right of

⁸⁹ As foreseen by principles 3 and 7 of the Police Recommendation. See the Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive (OJ C 255, 27.10.2007, p. 1). See also the EDPS Annual Report 2006, p. 47.

⁹⁰ This latter possibility is destined for those Member States which have provided for the right of access of the data subject in criminal matters through a system where the national supervisory authority, in place of the data subject, has access to all the personal data related to the data subject without any restriction and may also rectify, erase or update inaccurate data. In such a case of indirect access, the national law of those Member States may provide that the national supervisory authority will inform the data subject only that all the necessary verifications have taken place. This seems to apply, in particular, in France and Belgium.

⁹¹ Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (OJ L 218, 13.8.2008, p. 129).

access to be exercised in accordance with national law (in the case of the CIS Decision, implementing the Framework Decision) and some allow the national supervisory authority to decide whether and how that right can be exercised (SIC, SIS II, VIS Access Decision). The involvement of other MS before granting access is expressly foreseen (SIC, SIS II, Naples II, VIS access). Only the Prüm Decision lays down further details as to which information is to be given (e.g. which data are being processed, legal basis for the processing, etc.). All lay down grounds for refusal for access, but while similar use different grounds and differently wording.

- **Rights to correction, deletion and blocking of data:**

Under the Framework Decision a data subject has the right to obtain, without constraint or excessive delay or expense, confirmation of data processing (Article 17(1)). Any refusals on behalf of the controller to provide this information must be made in writing (Article 17 (3)). The data subject also has the right to request rectification, erasure or blocking of personal data (Article 18(1)). Each Member State will decide whether the request must be made to the data controller or to the national supervisory authority. Any refusals on behalf of the controller to rectify, erase or block data must be made in writing to the data subject (Article 18(1)). Under other legislative acts with access rights provisions, concrete time limits have been established by which requests made by data subjects must be dealt with. Under the Europol Decision, a subject requesting the deletion or correction of data will be informed of the outcome of their request within a maximum of three months (Article 31(5)). Under the Eurojust Decision, requests of access must also be dealt with within a maximum of three months and access to data are free of charge (Article 19(2)). Under Schengen legislation and the VIS Decision, requests for deletion must be dealt with within 60 days.

- **Transfers to third countries or international organisations:**

The Framework Decision establishes that personal data may be transferred to competent authorities in third States or to international bodies. This is generally allowed if ‘adequate protection’ is provided, and it is necessary for the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and with the prior authorisation of the original Member State (Article 13). The assessment of adequacy is left to the Member States on the basis of indicative criteria (see the text of Article 13 (4) DPF). There are also several exceptions to this rule, in particular when the national law of the transferring Member States so provides because of ‘legitimate prevailing interests’ (Article 13(3)). These specific rules on the transfer of data to third states or international bodies differ significantly from those applicable under the Directive (Articles 25, 26).

Example 2: Third country data transfers

Member State A considers that a third country X with which it has a bilateral data transfer agreement ensures an ‘adequate’ level of protection.

Member State B did not conclude a similar bilateral agreement with the same third country X and does not consider that country X ensures an ‘adequate’ level of protection.

Under the rules of the Framework Decision, Member State A is able to transfer personal data of individuals from Member State B, if transmitted to it by Member State B previously, to third country X – in emergencies without Member State B’s authorisation.

Had third country X requested this personal data directly from Member State B, third country X would not have received the data directly from Member State B as Member State B considers X as not ensuring an ‘adequate’ level of protection and would prohibit the transfer.

Other instruments also allow for the transfer of data to third countries or international organisations: by way of example, under the SIS II Decision, data cannot be transferred to third countries or to international organisations except for stolen, misappropriated, lost or invalidated passports, which may be exchanged with members of Interpol by establishing a connection between SIS II and the Interpol database on stolen or missing travel documents. The VIS Decision Article 8(4) says that VIS data shall not be transferred or made available to a third country or to an international organisation. However, in an exceptional case of urgency such data may be transferred or made available to a third country/international organisation exclusively for the purposes of the prevention and detection of terrorist offences and of other serious criminal offences subject to the consent of the originating MS.

The Framework Decision is furthermore 'without prejudice' to existing obligations and commitments incumbent upon Member States or upon the Union by virtue of bilateral and/or multilateral agreements with third States existing at the time of its adoption (Article 26), e.g. to the Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the surrender procedure between the Member States of the European Union and Iceland and Norway⁹² or the Agreement between the European Union and Iceland and Norway on the application of certain provisions of the Prüm Decision⁹³. However, future agreements have to comply with the rules on exchanges with third States: Article 26 provides for the application of conditions of Article 13 (1)(c) or (2) when falling within the scope of the Framework Decision.

- **Supervisory authorities**

As in the Directive, the Framework Decision recognises that the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of personal data processed within the framework of police and judicial cooperation between the Member States. It also allows that the supervisory authorities already established in Member States under the Directive to assume such responsibility (recitals 33, 34). The Prüm Decision also refers specifically to a supervisory authority within the meaning of the Directive (Article 31).

The Framework Decision does not establish rules related to the existing joint supervisory authorities. The instruments concerning Europol, Eurojust and CIS make specific provisions for the establishment up of a joint supervisory authority. The Europol Decision obliges an Independent Joint Supervisory Body to be set up to review the activities of Europol in order to ensure that the rights of individuals are not violated through the storage, processing and use of the data held in Europol.⁹⁴

⁹² OJ L 292, 21.10.2006, p. 2.

⁹³ Council Decision of 21 September 2009 on the signing, on behalf of the European Union, and on the provisional application of certain provisions of the Agreement between the European Union and Iceland and Norway on the application of certain provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, and the Annex thereto (2009/1023/JHA), (OJ L 353, 31.12.2009, p.1).

⁹⁴ According to Eurojust legislation the Joint Supervisory Body comprises a judge appointed by each Member State who is not a member of Eurojust, whereas under the CIS Decision, a Joint Supervisory Authority consists of two representatives from each Member State's respective independent national supervisory authority. For the SIS, Europol and the CIS, there is a Joint secretariat. See Council Decision of 17 October 2000 establishing a secretariat for the joint supervisory data-protection bodies set up by the Convention on the Establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention) (OJ L 271, 24/10/2000, p.1).

The Framework Decision does not establish any provisions concerning the European Data Protection Supervisor (EDPS). In this respect, the CIS Decision stipulates that the EDPS is to supervise the activities of the Commission regarding the CIS. The SIS II Decision (when it will be applicable) envisages that the EDPS will supervise processing activities of the Management Authority of SIS II; the same is the case also for the VIS decision. The VIS Regulation further stipulates that the EDPS is responsible for checking that personal data processing activities of the Management Authority are carried out in accordance with the VIS Regulation. The EDPS is also to ensure that data processing activities carried out by the Management Authority are audited. Under the SIS II Decision the EDPS is to act as a mediator between Member States in disputes regarding the correction or deletion of data.

5. FUNDAMENTAL RIGHTS AND OTHER STANDARDS

The protection of personal data is recognised as a fundamental right and has been interpreted by the jurisprudence of the European Court of Justice (ECJ) and the European Court of Human Rights (ECtHR).

5.1. Fundamental Rights Standards

5.1.1. Case law interpreting Article 8 of the EU Charter of Fundamental Rights

Important **case law** provided guidance for the interpretation of this fundamental right by the European Court of Justice (ECJ) in particular in the following cases: *Commission v Federal Republic of Germany*⁹⁵, concerning the lack of independence of the national supervisory authorities, and *Schecke et al.*⁹⁶ As underlined by the ECJ in the latter decision, the fundamental right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society. Article 8(2) of the Charter thus authorises the processing of personal data if certain conditions are satisfied. It provides that personal data ‘must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law’.

5.1.2. Article 8 of the European Convention of Human Rights of the Council of Europe (ECHR)

Under **Article 8** of the ECHR European Convention of Human Rights of the Council of Europe (ECHR), “everyone has the right to respect for his private and family life, his home and his correspondence.” Data protection emerges from the jurisprudence of the European Court of Human Rights in Strasbourg as an aspect of privacy protection. The case law is particularly relevant for the police and judicial cooperation in criminal matters.

The ECtHR has found in Article 8 ECHR not only negative obligations for the Member States to abstain from interfering with the right to privacy, but also positive obligations, that entail ‘the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals themselves’.⁹⁷ In *M.S. v. Sweden*⁹⁸, for instance, the ECtHR made clear that ‘the protection of personal data [...] is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention’.

⁹⁵ C-518/07, European Commission v. Germany, 9.3.2010.

⁹⁶ Joint cases C-92/09 and C-93/09, Volker und Markus Schecke GbR, Hartmut Eifert v. Land Hessen, 9.11.2010.

⁹⁷ See X and Y v Netherlands, judgement of 26 march 1985, para 23.

⁹⁸ M.S. v Sweden, judgment of 27 August 1997.

The collection of information by officials of the State about an individual will always concern his or her private life and will thus fall within the scope of Article 8 (1) ECHR. This includes for example: an official census which includes compulsory questions relating to the sex, marital status, place of birth and other personal details⁹⁹; the recording of fingerprinting, photography and other personal information by the police¹⁰⁰ even if the police register is secret¹⁰¹; the collection of medical data and the maintenance of medical records¹⁰²; the compulsion by state authorities to reveal details of personal expenditure (and thus intimate details of private life)¹⁰³; records relating to past criminal cases¹⁰⁴; information relating to terrorist activity¹⁰⁵, collecting personal information in order to protect national security¹⁰⁶.

5.1.3. *Possible limitations to the fundamental right to personal data protection and to private life*

Limitations on the right to privacy and data protection may be applied only when certain conditions are met. Article 8(2) of the European Convention on Human Rights accepts interference only where it is "*in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*".

Article 52(1) of the Charter accepts limitations only where they are "provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others". These are the provisions that serve as a frame of reference for the Court of Justice, which follows the lead of the European Court of Human Rights (Court of Human Rights) on this matter, when examining the compatibility of a data-processing measure with the rights in question¹⁰⁷.

Once an interference or infringement of the rights has been established, then, in application of the Court of Human Rights criterion that "*[t]he mere storing of data relating to the private life of an individual amounts to an interference*",¹⁰⁸ the grounds for that interference must be examined, which involves three cumulative conditions¹⁰⁹ that the interference or infringement must:

- (1) be **in accordance with the law**, which requires in particular:

⁹⁹ Appl. No. 9072/82, *X v. the United Kingdom*, 6 Oct. 1982, 30 DR 229.

¹⁰⁰ *Murray v. the United Kingdom*, judgment of 28 Oct. 1994, Series A no. 300-A.

¹⁰¹ *Leander v. Sweden*, judgment of 26 March 1987, Series A no. 116.

¹⁰² Appl. No. 14661/81, 9 July 1991, 71 DR 141.

¹⁰³ Appl. No. 9804/82, 7 Dec. 1982, 31 DR 231.

¹⁰⁴ *Friedl v. Austria*, Comm. Rep., 19 May 1994, p. 20.

¹⁰⁵ *McVeigh, O'Neill and Evans v. the United Kingdom*, 18 March 1981, DR 24 p. 15.

¹⁰⁶ *Leander v. Sweden*, judgment of 26 March 1987, para. 59.

¹⁰⁷ See the aforementioned *Volker* judgment. See also the judgment of 20 May 2003 (*Österreichischer Rundfunk*) in Joined Cases C-465/00, C-138/01 and C-139/01 (ECR 2003, p. I-4989).

¹⁰⁸ Judgment of the Court of Human Rights, *Marper*, dated 4 December 2008, 30562/04 and 30566/04, paragraph 67.

¹⁰⁹ See paragraph 62 of the aforementioned *Volker* judgment and paragraph 76 of the aforementioned *Österreichischer Rundfunk* judgment. On the case-law of the Court of Human Rights, see also the aforementioned opinion of the Legal Service 10146/01.

- that the measure "should have some basis in domestic law, but also refers to the quality of the law in question, [which] should be accessible to the person concerned and foreseeable as to its effects"¹¹⁰;
- rules involving negative consequences for individuals should be clear and precise and their application predictable for those subject to them¹¹¹;
- that the measure must be foreseeable, i.e. drawn up with sufficient precision to enable the individual to regulate his conduct"¹¹². It is "*essential [...] to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness*"¹¹³.
- States "*do not enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance*" and must provide adequate and effective guarantees against abuse".¹¹⁴

(2) meet a general-interest objective recognised by the Union (legitimate aim):

Article 52(1) of the Charter requires that the restrictions imposed on the exercise of the rights *in question* "*genuinely meet objectives of general interest recognised by the Union*"¹¹⁵.

Article 8(2) of the ECHR lists the various legitimate goals, including national security, public safety and the prevention of crime".

(3) be necessary and respond effectively to a general-interest objective:

This condition presupposes a review of proportionality according to settled case-law of the Court of Justice "the principle of proportionality, which is one of the general principles of European Union law, requires that measures *implemented* by acts of the European Union are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it".¹¹⁶

The objective pursued must in effect be reconciled with the fundamental rights set forth in Articles 7 and 8 of the Charter.¹¹⁷ It is thus necessary to balance on the one hand "*the European Union's interest*" in improving security through the prevention and combating of crime and, on the other hand, "*the interference with the right of [individual data subjects] to respect for their private life in general and to the protection of their personal data in particular*".¹¹⁸

¹¹⁰ See paragraph 52 of the aforementioned Rotaru judgment.

¹¹¹ see ECJ, Case C-110/03 *Belgium v Commission* [2005] ECR I-2801, paragraph 30; Case C-76/06 P *Britannia Alloys & Chemicals v Commission* [2007] ECR I-4405, paragraph 79; and Case C-226/08 *Stadt Papenburg* [2010] ECR I-0000, paragraph 45.

¹¹² See paragraph 95 of the aforementioned Marper judgment. See also paragraph 77 of the aforementioned judgment of the Court of Justice on *Österreichischer Rundfunk*.

¹¹³ See paragraph 99 of the aforementioned Marper judgment.

¹¹⁴ Judgment of the Court of Human Rights, *Klass*, dated 6 September 1978, No 5029/71, paragraphs 49 and 50. - See also the Judgment dated 4 April 2006 of the German Constitutional Court (BvR 518/02) which overturned a decision authorising searches by electronic profiling, through cross-checking data in a number of databases.

¹¹⁵ See paragraph 67 of the aforementioned Volker Judgment (C-92/09 and C-93/09).

¹¹⁶ See paragraph 74 of the aforementioned Schecke Judgment (C-92/09 and C-93/09).

¹¹⁷ See paragraph 76 of the aforementioned Schecke Judgment.

¹¹⁸ See paragraph 77 of the aforementioned Schecke Judgment.

As they constitute exceptions to the fundamental rights, grounds for interference are "to be interpreted narrowly"¹¹⁹ and "must apply only in so far as is strictly necessary"¹²⁰.

A limitation imposed on the rights in question, is justified only if it is "proportionate to the legitimate aim pursued"¹²¹ and "necessary in a democratic society" to attain a legitimate aim, and, in particular, that it is "proportionate to the legitimate aim pursued and [that] the reasons adduced by the (...) authorities to justify it are relevant and sufficient".¹²² The authorities "enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved".¹²³

It is therefore necessary to examine whether any proposed measure does not "go beyond what [is] necessary for achieving the legitimate aims pursued, having regard in particular to the interference with the rights guaranteed by Articles 7 and 8 of the Charter".¹²⁴

It is apparent from the case-law of the Court of Human Rights that a measure authorising "so-called exploratory or general surveillance" would contravene Article 8 of the ECHR¹²⁵. Similarly, "the blanket and indiscriminate nature of the power of retention" of data (fingerprints, biological samples and DNA profiles) "of persons suspected but not convicted of offences", which are "retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender" and without restriction of time, "overstep[s] any acceptable margin of appreciation in this regard [and] constitutes a disproportionate interference with the [...] right to respect for private life"¹²⁶.

ECHR case law:

In *Leander v Sweden*¹²⁷, the Court held that the storing of information relating to an individual's private life in a secret register and the release of such information amounted to an interference with his right to respect for private life as guaranteed by Article 8(1).

In *Rotaru v Romania*¹²⁸, the ECtHR reiterated that the storing by a public authority of information relating to an individual's private life and the use of it amount to interference with the right to respect for private life and added that such an interference occurred also from the refusal to allow an opportunity for the personal data to be refuted.

In *Amann v Switzerland*¹²⁹, the Court found that the storing of a card containing data relating to an individual's private life and stored by an authority storage itself amounted to an interference with the right to respect for his private life.

¹¹⁹ Judgment of the Court of Human Rights, *Rotaru*, dated 4 May 2000, 2841/95, paragraph 47.

¹²⁰ See paragraph 77 of the aforementioned *Schecke* judgment.

¹²¹ See paragraph 71, *Schecke* judgment.

¹²² See paragraph 101 of the aforementioned *Marper* Judgment. See also paragraph 83 of the *Österreichischer Rundfunk* Judgment.

¹²³ See paragraph 83 of the aforementioned *Österreichischer Rundfunk* judgment.

¹²⁴ See paragraph 79 of the aforementioned *Schecke* Judgment. See also point 86, 88 and 90 of the *Österreichischer Rundfunk* Judgment.

¹²⁵ See paragraph 17 above and the penultimate subparagraph of paragraph 5 of the opinion of the Legal Service 10146/01.

¹²⁶ *Marper* judgment, paragraphs 119 and 125.

¹²⁷ *Leander v. Sweden*, judgment of 26 March 1987, para. 48.

¹²⁸ *Rotaru v Romania*, judgment of 4 May 2000, para 43.

¹²⁹ *Amann v Switzerland*, judgment of 16 February 2000, para 70.

In *S. and Marper v. United Kingdom*¹³⁰ the ECtHR ruled on the lawfulness of the retention of fingerprints, cellular samples and DNA profiles after criminal proceedings against the applicants were terminated by an acquittal or discharge and despite the applicants had requested their destruction. The retention of both cellular samples and DNA profiles amounted to an interference with the applicants' right to respect for their private lives. The Court reiterated that as for the storing and use of this personal information, it was essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards. The protection afforded by Article 8 would be unacceptably weakened if the use of modern scientific techniques in the criminal justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.

The Court found that it amounts to a violation of Article 8 that fingerprints, cellular samples and DNA profiles could be retained by police authorities irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; if the retention was not time-limited; and if there existed only limited possibilities for an acquitted individual to have the data removed from the nationwide database or to have the materials destroyed. It expressly found that the retention of unconvicted persons' data could be especially harmful in the case of minors such, given their special situation and the importance of their development and integration in society

5.2. Other standards (Council of Europe)

Additionally, certain standards included in Recommendation No R (87) 15 of the Committee of Ministers of the Council of Europe are also useful benchmarks in this area, in particular:

- The need to ***distinguish personal data according to their degree of accuracy and reliability***, or whether they are based on facts or on opinions or personal assessments. The lack of such a requirement could actually undermine the data being exchanged between police authorities as they will not be able to ascertain whether the data can be construed as 'evidence', 'fact', 'hard intelligence' or 'soft intelligence'. This could have the consequence of hampering security operations and of making it more difficult for courts to secure convictions;
- The need to ***distinguish between different categories of data subjects*** (criminals, suspects, victims, witnesses, etc.), and to provide in particular for specific guarantees for data relating to non-suspects. Again, these distinctions are on the one hand necessary for the protection of the concerned individuals and on the other hand for the ability of the recipient law enforcement authorities to be able to make full use of the data they receive¹³¹.

¹³⁰ *S. and Marper v. the United Kingdom*, judgment of 4 December 2008, applications nos. 30562/04 and 30566/04.

¹³¹ Similar provisions are also included in the Decision related to Europol (Articles 12, 14) and Eurojust (Article 15),

LIST OF EU INSTRUMENTS IN THE FIELD OF POLICE AND JUDICIAL COOPERATION IN CRIMINAL MATTERS CONTAINING SPECIFIC DATA PROTECTION PROVISIONS

- (1) Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (OJ L 239, 22.9.2000, p. 19);
- (2) Council Decision of 17 October 2000 establishing a secretariat for the joint supervisory data-protection bodies set up by the Convention on the Establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention) (OJ L 271, 24.10.2000, p. 1);
- (3) Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism (OJ L 68, 15.3.2005, p.44);
- (4) Commission Decision 2006/758/EC of 22 September 2006 on amending the Sirene Manual (OJ L 317, 16.11.2006, p. 41).
- (5) Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63);
- (6) Commission Decision 2008/334/JHA of 4 March 2008 adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (OJ L 123, 8.5.2008, p. 39).
- (7) Council Act of 18 December 1997 drawing up, on the basis of Article K.3 of the Treaty on European Union, the Convention on mutual assistance and cooperation between customs administrations (OJ C 24, 23.1.1998, p.2).
- (8) Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union ([OJ C 197, 12.7.2000, p 1](#)).
- (9) Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (OJ L 271, 24.10.2000, p. 4).
- (10) Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States ([OJ L 190, 18.7.2002, p. 1](#)).
- (11) Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol ([OJ L 27,29.1.2005, p. 61](#))

- (12) Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union ([OJ L 386, 29.12.2006, p. 89](#)).
- (13) Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime (OJ L 332, 18.12.2007, p. 103).
- (14) Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1);
- (15) Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12).
- (16) Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences ([OJ L 218, 13.8.2008, p. 129](#)).
- (17) Council Framework Decision 2008/947/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions (OJ L 337, 16.12.2008, p. 102).
- (18) Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters ([OJ L 350, 30.12.2008, p.72](#)).
- (19) Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States ([OJ L 93 7.4.2009, p. 23](#)).
- (20) Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA ([OJ L 93, 7.4.2009, p. 33](#)).
- (21) Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention ([OJ L 294, 11.11.2009, p.20](#)).
- (22) Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes ([OJ L 323, 10.12.2009, p 20](#)).
- (23) Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings ([OJ L 328, 15.12.2009, p. 42](#)).

As regards the processing of personal data by **Eurojust**:

- (1) Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63, 6.3.2002, p. 1);
- (2) Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime ('Eurojust Decision 2009') ([OJ L 138, 4.6.2009, p. 14](#)).

As regards the processing of personal data by the **European Police Office (Europol)**:

- (3) Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009, p. 37).
- (4) Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information ([OJ L 2009, L 325, 11.12.2009, p. 6](#)).
- (5) Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files ([OJ L 325, 11.12.2009, p. 14](#)).

ANNEX 4

SUMMARY OF REPLIES TO THE PUBLIC CONSULTATION ON THE COMMISSION'S COMMUNICATION ON A COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION

Following the adoption of the Commission's Communication of 4 November 2010 on "A comprehensive approach on personal data protection in the European Union" a public consultation was launched on the ideas therein. The deadline for replies to the consultation was 15 January 2011. The Commission received 305 responses, of which 54 from citizens, 31 from public authorities and 220 from private organisations, in particular business associations and non-governmental organisations. The full text of these responses is available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm, except where respondents asked to remain anonymous or to have their entire contribution treated as confidential.¹³²

This document provides a factual and objective summary of the contributions received during the public consultation. While the summary is structured along the issues identified in the Commission's abovementioned Communication, the views and opinions expressed are not necessarily those of the Commission.

1. STRENGTHENING INDIVIDUALS' RIGHTS

1.1. Ensuring appropriate protection for individuals in all circumstances

The Commission will consider **how to ensure a coherent application of data protection rules, taking into account the impact of new technologies on individuals' rights and freedoms and the objective of ensuring the free circulation of personal data within the internal market.**

– Coherence

The coherent application of data protection rules was considered particularly important by large private companies, who insisted on having a coherent and uniform framework. Across industry, stakeholders felt that the current lack of harmonisation is detrimental to economic activity within the EU. Many stakeholders also pointed out that data protection rules should be coherent with existing sectoral regulation, such as the rules in the media sector (freedom to inform, journalistic rights and exemptions), the police and justice sector (specificities regarding access to data rights), the history and archiving sector (access to historical documents), the communications sector (security of networks, services and information), the health sector (collection of data for pharmacovigilance), and the research sector (recognition of scientific purposes as a substantial public interest, exemptions and safeguards for further processing of personal data).

¹³² 288 out of the 305 responses are available on the website.

Many contributors referred to the challenges to data protection posed by technological developments, such as cloud computing or social networks, and urged the legislator to respond to these in a concrete and coherent manner. Some propose to introduce sectoral legislation to specifically address these issues (following the model of e-Privacy directive). Similarly, a number of citizens complained about the apparent lack of regulation of the internet as far as personal data is concerned. A consistent privacy experience online is seen as vital in order to have trust in the internet.

Some stakeholders, including citizens, mentioned that a coherent application of the rules is only possible if definitions are clear, especially the definitions of "personal data", "data controller" and "processor". Some contributors suggested to change the current core definitions. For instance, some proposed to foresee that identification is not the only element in defining personal data and suggested to keep the personal data definition broad in order to anticipate possible evolution of new technologies and behavioural profiling. A group of researchers suggested to exclude from the definition of personal data any information whose processing does not interfere with the values of privacy, fairness and non-discrimination. Some DPAs wished to reconsider the categories of sensitive data by possibly moving towards a definition of the content which might be considered sensitive instead of prescribing an exhaustive list of sensitive data. A more radical proposal consisted of eliminating the general prohibition to process sensitive data and foreseeing instead a special obligation to ensure appropriate safeguards for such processing. Some public research institutions touched upon the need for further clarification and harmonisation of the existing definitions, especially the concepts of personal data, anonymous data and encoded data.

DPAs insisted on the need for coherent enforcement mechanisms in order to ensure the coherent application of data protection rules. Some pointed out the need to make use of existing rules and strengthen self-regulation or self-enforcement. Indeed, a number of public authorities argued that the issue at hand is less the strengthening of rights but rather the proper application of the existing Directive. Other stakeholders, including business associations, consider that in order to reach greater coherence of the data protection legal framework, an obligation of mutual recognition of the national data protection regimes between Member States should be introduced.

According to some public authorities and citizens more competition between internet providers, and hence less dependency on providers with a dominant market share, could strengthen internet users' self-determination and exercise of their rights. Currently, some services depend on a specific platform or there is no data portability (possibility for individuals to take their data with them when they move from one (social) network to another).

Some DPAs felt the need to shift the focus of regulation from all data processing operations to risky data processing in order to take into account today's technological reality. Accordingly, rules for daily, harmless data processing (such as processing of an unstructured documents like ordinary email or publication of personal data in running text on the internet) should be simplified, by permitting such processing without any additional requirements, unless it leads to an inappropriate encroachment of the individual's privacy. The focus on the areas which involve specific risks would increase respect and compliance with the regulation.

In this context, some stakeholders expect the new legal framework to explicitly state that the right to data protection will sometimes need to be balanced with other equally important fundamental rights.

1.2. Increasing transparency for data subjects

The Commission will consider:

- introducing a **general principle of transparent processing** of personal data in the legal framework;
- introducing **specific obligations** for data controllers on the type of information to be provided and on the **modalities** for providing it, including in relation to **children**;
- drawing up one or more **EU standard forms** ('**privacy information notices**') to be used by data controllers.

Transparency

Stakeholders generally agree on the importance of the principle of transparent processing. Many respondents, in particular businesses, noted that the notion of transparency is already an integral part of the present legal framework through Articles 10, 11, 12, 15 and 6.1(a) of the Directive. While some respondents argue that an inclusion of an explicit transparency principle would increase legal certainty, others consider it more important to reinforce the existing provisions.

One citizen proposed a standard obligation whereby (online) companies should once a year send an e-mail summary of all personal information held linked to a given e-mail address. Another citizen proposed creating a special icon on internet browser screens to inform individuals about the data processing (e.g. profiling, behavioral advertising), indicate the type of information collected and the identity of the processor. A similar suggestion is submitted by a group of privacy experts. This system would enable consumers to know about the processing of their data and give a meaningful consent prior to the collection of tracked data.

Children

Citizens are generally very concerned about privacy risks entailed by childrens' online activities and support age verification and other controls or additional protection mechanisms. Several stakeholders insisted on clearly defining what a child is (age) and establishing specific requirements for the processing of children's personal data. One NGO argued that children should be able to exercise their own privacy rights (distinct from their parents) and that privacy notices and consent forms should to be adapted to the level of awareness of the child.

DPA's and civil society organisations strongly agree that more consideration should be given to privacy-related children's issues. Some support additional legal provisions related to requirements for information provided to children, protection from behavioral advertising, categories of data which can never be collected, age threshold, parental consent to be included in the revised legal instrument. By contrast, some others – pointing to the diverse rules for defining a child across the EU, different levels of maturity and understanding of children of the same age, as well as practical difficulties related to age verification and mechanisms for obtaining consent – do not support detailed provisions on children. Several respondents indicated that a gradual approach regarding the responsibility of the child should be taken based on different national age limits for criminal, administrative and civil responsibility.

Though some restrictions may be needed for children especially regarding sharing of information online and exposure to behavioural advertising, some contributors argued that teenagers sometimes have a better understanding of online privacy challenges than their parents.

Privacy information notices

Some organisations, in particular large companies, support a standard EU form as a practical means to inform stakeholders, while others would prefer general guidance based on best practices. Organisations that support the introduction of EU standard forms argue that the varying requirements across the EU regarding privacy notices create administrative burden for data controllers and little added value for consumers.

Public authorities endorse the Commission's view that transparent processing requires the availability to data subjects of clear, easy to understand privacy information notices. However, some authorities are not convinced that EU standard forms are the best way to meet this need due to the specificity of the context and possible particular needs of the data subjects at whom they are aimed. Therefore, some institutions propose to develop forms of general nature or forms which serve as recommendations or guidelines.

The Commission will:

- examine the modalities for the introduction in the general legal framework of a **general personal data breach notification**, including the addressees of such notifications and the criteria for triggering the obligation to notify.

Data breach notifications

There is general support that data breach notifications need to be extended beyond the Telecom sector and the e-Privacy Directive, especially from public authorities. Data breach notifications are seen as a key element of transparency and accountability. Information is crucial for the individual to exercise his or her rights, for instance to claim financial compensation.

As far as the thresholds are concerned, respondents argue that a pragmatic approach should be foreseen, lessons from the experiences of the telecom sector should be drawn and overnotification should be avoided, in the interest of both businesses and data protection authorities. Some contributions highlight that data breaches in the public sector should be covered, as well as data breaches occurring in foreign countries, when they impact EU citizens.

Industry argues that no administrative burden should be created for riskless / insignificant breaches. For instance, the banking sector argued that data breaches are already reported on a voluntary basis, where appropriate, and that an obligatory requirement should be limited to serious cases.

Archives institutions argue that their special circumstances should be acknowledged; they consider it impracticable to attempt to ascertain the current contact details of the very large number (millions) of data subjects featuring in archives in the event of a data breach.

1.3. *Enhancing control over one's own data*

The Commission will therefore examine ways of:

- strengthening the **principle of data minimisation**;
- **improving the modalities** for the actual **exercise of the rights of access, rectification, erasure or blocking of data** (e.g., by introducing deadlines for responding to individuals' requests, by allowing the exercise of rights by electronic means or by providing that right of access should be ensured free of charge as a principle);
- clarifying the so-called '**right to be forgotten**', i.e. the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. This is the case, for example, when processing is based on the person's consent and when he or she withdraws consent or when the storage period has expired;
- complementing the rights of data subjects by ensuring '**data portability**', i.e., providing the explicit right for an individual to withdraw his/her own data (e.g., his/her photos or a list of friends) from an application or service so that the withdrawn data can be transferred into another application or service, as far as technically feasible, without hindrance from the data controllers.

Data minimisation

Many citizens report a widespread practice of collection of excessive (beyond the specific purpose) personal information on the internet. They also expect more options to remain anonymous in the virtual environment.

Public institutions, in particular DPAs and advisory bodies, agree with the importance of data minimisation, which can provide effective data protection, guarantee the rights of data subjects and promote best practise by data controllers. However, some respondents underlined that the principle should be clearly defined in order to ensure adequate implementation.

Service providers and industry noted that data processing can be beneficial to consumers and in particular business sectors (e.g. finance, insurance) and business models and therefore, not all the personal data need to be minimised. Some industry representatives, including trade organisations, considered that the data minimisation principle is already expressed in the Directive. Some expressed concerns that the principle of data minimisation might conflict with other industry legal requirements to retain data for official legally sanctioned purposes.

Some stakeholders in the service area (healthcare/advertising) fear that reinforcing data minimisation rules would lead to further restrictions on secondary use of data, which could restrict their professional activities. Also some business stakeholders fear that this would lead to additional costly anonymisation efforts.

Civil society organisations argue that the data minimisation principle should become a cornerstone of any modern approach to data protection. Data controllers should think in terms of data minimisation at the very beginning of the design of products and services. Privacy organisations suggested that anonymisation could help to meet a principle of data minimisation.

Improving the actual exercise of the rights of access, rectification, erasure or blocking of data

Many citizens consider that they do not have enough control over their personal data put online. A number of respondents underlined specific dangers related to the publication of personal data (in particular pictures) by data subjects themselves - or the uploading by others

of, *inter alia*, slanderous images and sensitive data – on social networking sites. They emphasised the necessity to harmonise and strengthen the right of access to personal data by decreasing the legal barriers, simplifying compulsory procedures and formalities, facilitating the determination of applicable law in cross-border cases and strengthening the role of DPAs.

A number of other contributors, in particular businesses and public authorities, argued that rights of access, rectification and erasure or blocking are already part of the existing legal framework and advocated that further detailing of those rights in sectoral codes could be more appropriate, so that they can be better enforced in practice

A group of academics noted the need to reconcile data subjects' right of access and the freedom of private communications, citing as an example the personal data restrictions of university email use. They also encouraged considering a limitation to the right of access to one's personal data based on the ground of disproportionate resource burden.

"Right to be forgotten"

Several contributors stressed that the "right to be forgotten" and the existing right to delete one's own personal data are similar. Many stakeholders, especially technology companies, industry and trade alliances, service and content providers argued that the right to be forgotten is already explicitly guaranteed by the principles of purpose and use limitation and the right to erasure. These stakeholders therefore think that existing rules in this regard should be implemented better and their stronger harmonisation across the EU should be reached. Therefore, a clear distinction between the two rights would have to be made by defining clear requirements for the rights and specifying against whom the rights may be enforced. Most businesses also argued that the most fundamental challenge will be to define a "right to be forgotten" clearly, since it is not established or widely understood.

Nevertheless, the right to be forgotten and the possibility to recuperate or delete personal data uploaded on internet websites was stressed as an absolute necessity by many citizens. They wished the legal framework to provide for such a possibility especially as regards under-age internet users.

Industry alliances, service and content providers and legal and related companies argued that there should be exceptions to the right in some contexts and situations, such as preventing fraud or crime or for journalistic purposes. They were concerned that a right to be forgotten does not add value for businesses or customers and may cause industry to incur significant cost or administrative burdens. Service and content providers also noted that a right to be forgotten could negatively impact the services or products offered to customers. Some technology companies suggested that anonymisation can replace deletion as a means of protecting and enhancing this right.

Service and content providers as well as international justice and trade organisations were also concerned that a right to be forgotten might conflict with other industry legal requirements to retain data for official legally sanctioned purposes. Stakeholders in the healthcare sector mentioned that they are sometimes obliged to keep patient data for a very long time, for example for the monitoring of undesirable effects of medicine.

Some stakeholders highlighted that the right to be forgotten may also mean that consent should only be given for a reasonable and limited period, and that data should be deleted after

the expiry of such period. Some stakeholders specifically suggested introducing a mechanism of automatic data deletion after the storage period ends. Some public authorities and DPAs fear that the right to be forgotten could have a very limited application in practice and ask for clarifications on the extent to which this right can be effective and on its costs. The EDPS suggested that the right to be forgotten might only be a solution in a digital environment.

Civil society organisations supported the right to be forgotten. However, they also asked for clarification as to the meaning and principles associated with a right to be forgotten and that the right should be of substance rather than a slogan with no meaningful benefit to customers or industry. Privacy related organisations noted that alongside the right to be forgotten there is a need to educate and raise awareness among data subjects that they have such a right which can be exercised. Consumer organisations noted that there is a need for such a right to be harmonised across the EU.

Data portability

A number of citizens have argued that they should be able to retain control over their personal data, including by moving it from one online application to another. Some stakeholders consider that data portability is redundant with the existing right of access. Others doubt its feasibility both in technical terms and as regards copyright and protection of intellectual property. Online service providers argued that user data should be clearly distinguished from data created by the service; in their view only user data could be portable. An alternative proposal was to introduce in the privacy notice mandatory information on what data can be retrieved from the online service and make this a voluntary practice.

1.4. Raising awareness

The Commission will explore:

- the possibility for **co-financing awareness-raising activities on data protection** via the Union budget;
- the need for and the opportunity of including in the legal framework **an obligation to carry out awareness-raising activities** in this area.

Awareness-raising

Some contributors indicated that the national DPA is the appropriate body to be tasked with awareness raising activities. Citizens in particular expect national DPAs to play a greater role in raising awareness of data protection norms amongst citizens and newly emerging data controllers who often have little knowledge of data protection compliance.

There are diverging views on whether an obligation to carry out awareness-raising activities needs to be included in the legal framework. Some public authorities believe that Member States should take their own measures and DPAs should be allowed to choose their own approach. Some others note that awareness-raising is expensive and if this task is to be given to DPAs, it requires an explicit legal basis. Moreover, some DPAs suffer from insufficient funding in their Member State and welcomed any initiatives that would improve their financial situation.

Some contributors argued that Data Protection should be a mandatory field of study in universities, for instance in fields of studies where the manipulation of sensitive data such as health data is inevitable.

1.5. *Ensuring informed and free consent*

The Commission will examine ways of **clarifying and strengthening the rules on consent**.

There is a general consensus among public authorities, DPAs and EDPS on the need to clarify the notion of consent to avoid the risk of misinterpretation and to apply the rules uniformly and consistently across the EU. The specific dimension of consent and the link to the purpose should be maintained. In their view, an opt-in approach is the most supportive of the right to privacy of data subjects vis-à-vis data controllers. Some DPAs expressed concern that always requiring explicit consent may be unworkable and present an undue burden on DPAs in ensuring sector-wide and industry compliance.

A number of technology companies and industry alliances expressed support for a clarification of the definition and the rules around consent, but noted that the changes to consent should not negatively impact business and industry. Several business stakeholders consider that consent may be implied from individuals' behaviour and note that requiring explicit consent in all circumstances could be detrimental to many business models and industry procedures. Some argue that a certain degree of flexibility as regards rules on consent is important in order to take into account certain business contexts (new business models, new technologies), social and cultural differences in understanding consent. Some contributors also highlight that privacy notices are not the best way to secure user's consent. A shared view among industry is that too much emphasis on consent will undermine privacy as individuals will become used to always agreeing to a stated purpose without necessarily understanding what is being asked of them

Civil society organisations also supported an explicit, informed and opt-in approach to consent. However, some consumer organisations recognised that consent might be difficult to achieve and the need to explore the best possible way to ensure that consumers are aware of the consent they give. A need to raise awareness amongst consumers, and particularly children, about the consent and its implications in terms of their personal data was mentioned by many organisations.

In addition, some citizens pointed out situations when the data subject is not in a position to give 'informed' and 'free' consent, such as a situation when the consent becomes part of a larger transaction or contract, "bundled" with a service sought by the customer, or the user is refused a service or charged a higher price unless he consents the processing of personal data or disclosure of such data to third parties. Some contributors proposed to oblige personal data controllers, whenever they intend to store or process personal data beyond the fulfilment of ordinary transactions, to explicitly specify those terms and conditions pertaining to consumer personal data and its compensation according to contract law, calling the result a "personal data contract".

Citizens also mentioned the limited freedom to consent to personal data processing in the context of employment or unequal professional-consumer relations.

Moreover, many citizens think that data subjects should be entitled to revoke their consent at any time and using online channels. The revocation should take effect immediately and not be circumvented by contract terms, refusal of services or higher price. Citizens also favoured opt-out by default from direct marketing services and placing the burden of proof on data controllers in opt-out cases.

1.6. *Protecting sensitive data*

The Commission will consider:

- whether other categories of data should be considered as '**sensitive data**', for example **genetic** data;
- further clarifying and **harmonising the conditions** allowing for the processing of categories of sensitive data.

There is a general consensus on harmonising the conditions related to the processing of sensitive data across the EU. Also many stakeholders support including genetic data in the list of sensitive data to be considered, especially pointing to the possible discriminatory use of genetic data. However, a big extension of the list is not favoured, several contributors preferring to stick with a short harmonised list of prohibited processing, allowing for some contextual exceptions.

Some DPAs instead suggested putting more emphasis on the risk (e.g. significant damage or stress for individuals) that particular processing poses in particular circumstances while assessing sensitivity of personal data. Some public authorities highlighted that there is sometimes a need to process sensitive data, such as ethnic data in order to evaluate the benefits of some positive discrimination policies. Therefore exceptions need to be provided.

The increase in biometric data is a common worry among citizens and respondents want it to be addressed in the new legal framework. One citizen underlined the lack of effective protection of health data in relation to new technologies in the health sector (e.g. ICT implants).

A group of researchers noted that due to the broad definition of sensitive data many academic institutions are restricted in activities they may carry out as the majority of social investigations involve the processing of such data. This practise may diminish academic freedom and result in loss of important forms of knowledge production.

1.7. *Making remedies and sanctions more effective*

The Commission will therefore:

- consider the possibility of **extending the power to bring an action before the national courts** to data protection authorities and to civil society associations, as well as to **other associations representing data subjects' interests**;
- assess the need for **strengthening the existing provisions on sanctions**, for example by explicitly including criminal sanctions in case of serious data protection violations, in order to make them more effective.

Right to bring an action

Some public authorities and citizens noted that present Directive offers limited help to individuals whose privacy has been violated and who need to obtain redress.

A fairly large number of citizens asked to introduce the right of action for consumer and privacy associations extending injunctions for the protection of consumers' interest to data protection violations. Collective redress mechanisms empowering groups of data subjects to combine their claims and bring a single action against data controllers are supported by the DPAs and the EDPS. As far as civil society associations are concerned, some contributors fear that 'class action' style of actions would increase the cost of services.

Some businesses argued that out of court settlements and mediation by DPAs can be more efficient than judicial redress.

Citizens emphasised the need to prohibit disadvantageous treatment of data subjects who exercise their rights under data protection legislation.

– Powers of DPAs

DPAs are in favor of strengthening and harmonising their powers, an idea that is generally welcomed by citizens and privacy associations, whereas a number of business stakeholders argued that existing legislation gives sufficient powers to DPAs

Sanctions

Several public authorities considered that while administrative sanctions such as fines could be harmonised, they do not support the harmonisation of criminal sanctions as far as data protection is concerned. Others, however, argued that if the Commission considers the introduction of criminal sanctions, these should be a real deterrent to the unlawful trade in personal data and should be applied also against individuals who act maliciously.

Some DPAs argued that the cost of reputational damage, is frequently higher than fines for companies.

Citizens strongly supported a personal data security breach regime with strict accountability principles and corresponding remedies. Some underlined the accountability of manufacturers and proposed to introduce the liability for data safety in defective products as well as liability of data controllers for data protection breaches independently of their fault or negligence. Others supported the introduction of heavy criminal sanctions for systematic or reckless failure to meet the data protection requirements.

According to some contributors the fines for data protection violations should be determined according to the scale and nature of the business of the data controller. Many citizens desired to see a fixed minimum compensation for victims of privacy violations established in the revised directive.

2. ENHANCING THE INTERNAL MARKET DIMENSION OF DATA PROTECTION

2.1. *Increasing legal certainty and providing a level playing field for data controllers*

The Commission will examine the means to achieve **further harmonisation of data protection rules at EU level.**

Most citizens and many private stakeholders support further EU-level harmonisation of the data protection rules. Especially businesses operating in a number of Member States called for harmonised rules, which would simplify their operations. Some business associations called for the mutual recognition of decisions by national DPAs. Some business argued that harmonisation can only be accepted if it does not lead to more stringent and burdensome rules. On the other hand, privacy associations argued that harmonisation and EU level should not lead to an overall reduction of data protection standards in the EU.

According to one contributor the revised legislative act should be easier to understand and avoid excessively complex structure and terminology, as this may affect the implementation and help in gaining a wider public acceptance.

2.2. *Reducing the administrative burden*

The Commission will explore different possibilities for the **simplification and harmonisation of the current notification system**, including the possible drawing up of a **uniform EU-wide registration form.**

Reducing the administrative burden is welcomed by most organisations and stakeholders, particularly businesses.

Many DPAs see the existing notification system as administratively burdensome, requiring allocation of great resources for its administration and not accompanied by an equivalent improvement in data protection as notification are not necessarily useful for the DPAs' supervisory activities. Therefore, the majority of public authorities support either the elimination or simplification of the current notification procedure. One of the possible simplification options, proposed by some contributors, is to change the existing all-encompassing general notification requirement to a more targeted system.

One DPA noted that changes in the notification system could adversely impact the current fee-based funding model (i.e. not funded by their government but through notification fees paid by data controllers). The elimination of notification requirements is also strongly supported by a group of academics who perceive the existing system as entirely disproportionate and serving no useful purpose.

However several companies indicated to the Commission that third party control and possibly certification (by the DPA or another independent organisation) is needed throughout the 'data processing lifecycle' (from the conception to the deployment, operations and later on dismantling) in order to guarantee a good level of privacy. They argued that self certification is ineffective, as many flaws in the data protection design may remain unnoticed.

A comprehensive approach reviewing the notification of processing and the data breach notification would be welcomed by most stakeholders. Several stakeholders insist on the need to fully harmonise and simplify notifications, and introduce the proposed EU-wide registration system.

2.3. *Clarifying the rules on applicable law and Member States' responsibility*

The Commission will examine how to **revise and clarify the existing provisions on applicable law**, including the current determining criteria, in order to improve legal certainty, clarify Member States' responsibility for applying data protection rules and ultimately provide for the same degree of protection of EU data subjects, regardless of the geographic location of the data controller.

Some contributors proposed to improve the area of territorial application of the Directive, especially as regards multinational companies carrying out personal data processing in different Member States and companies established outside the EU but collecting personal data from EU citizens on a large scale.

2.4. *Enhancing data controllers' responsibility*

The Commission will examine the following elements to enhance data controllers' responsibility:

- making the appointment of an independent **Data Protection Officer** mandatory and harmonising the rules related to their tasks and competences, while reflecting on the appropriate threshold to avoid undue administrative burdens, particularly on small and micro-enterprises;
- including in the legal framework an obligation for data controllers to carry out a **data protection impact assessment** in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance;
- further promoting the use of PETs and the possibilities for the concrete implementation of the concept of '**Privacy by Design**'.

– **Data Protection Officers (DPOs)**

There is overall support for introducing DPOs under certain threshold conditions among DPAs, public institutions and the EDPS. However, some DPAs noted the financial and administrative burden associated with mandatory DPOs and called for research to be conducted into this area seeking to minimise any negative impacts, especially on SMEs. Other DPAs noted that mandatory DPOs may not address the problems currently experienced in Europe due to a lack of expertise and skills as well as the specific nature of the problems.

Industry organisations and companies in general preferred a voluntary and flexible DPO system as mandatory DPOs would impose a significant and unwarranted costs on some companies, particularly SMEs. While some service and content providers supported the use of DPOs perceiving them as key elements in order to demonstrate accountability, industry alliances were concerned whether mandatory DPOs will be more effective than raising awareness and standards for data protection within organisational structures, procedures and operations. Several industry representatives, including service and content providers, doubt that internal DPOs can realistically be independent, given that, as employees of the company, they have to help it achieve its business goals. Some industry alliances also worried that requiring mandatory DPOs could be an unwarranted intrusion into internal company's operations and procedures.

The majority of civil society organisations expressed the need for the role, duties, responsibilities and powers of DPOs to be harmonised across the EU as well as the mandatory requirement being consistently enforced within all Member States. Both consumer and privacy related organisations called for DPOs powers to be outlined, specifically to prevent DPOs from being limited to awareness raising and other education activities within organisations.

– **Data Protection Impact Assessment (DPIA)**

Data protection impact assessments (DPIA) are seen as very useful tools to reinforce privacy and are supported by many contributors. DPAs supported the use of DPIAs as these might lead to greater self-regulation in terms of protecting privacy and data. Furthermore, DPAs suggested that the use of DPIAs might be incentivised for companies by foregoing other notification requirements where DPIAs have been conducted and their results made public. A few contributors however are not yet persuaded of the need to introduce a legal obligation for all data controllers to conduct data protection impact assessments, in the absence of a proper assessment of the subsequent benefits and additional burdens for data controllers and DPAs.

Civil society organisations overwhelmingly supported the use of DPIAs. They introduced some specific recommendations, for example, DPIAs should be used where sensitive data is involved and when new databases are created. Many organisations also noted that mandatory DPIAs might represent undue burdens for some companies of smaller sizes, and that these difficulties should be taken into account. Consumer organisations argued that there is a need for DPIAs to be harmonised across the EU and standardised across business sectors.

A number of responses across the industry, expressed concern about the costs associated with mandatory DPIA's for business and industry, in particular SMEs. Many respondents preferred a voluntary or flexible DPIA system, which provides incentives and is encouraged by national DPAs. However, some respondents agreed that a mandatory DPIA might be appropriate in the case of sensitive data. Some industry respondents suggested that DPIAs should be considered in tandem with requirements for DPOs.

– **Privacy by design**

Many citizens support the introduction of the privacy by design principle.

DPAs also explicitly welcome the promotion of Privacy-enhancing technologies (PETS) and implementation of the concept of 'privacy by design', which could offer excellent prospects for strengthening accountability, security and individual rights. DPAs consider that the principle can be introduced without incurring any additional burden on the controller as such measures would focus on pre-establishing safeguards and mechanisms. Germany noted that privacy-by-design rules are already included in its legislation and argued that European privacy-by-design rules should not be too detailed to leave sufficient scope for different situations.

Data protection institutions from the third countries also strongly support the Commission communication's approach on 'privacy by design' and consider 'privacy by design' a significant standard for data protection internationally which will foster simultaneous protection and innovation.

By contrast, many stakeholders from the private sector consider privacy by design too vague a concept and difficult to measure if it has to remain technology neutral, whereas public administrations generally support it and see it as an approximation to OECD and APEC principles.

Some stakeholders underline that they would agree to privacy by design, as long as it is not understood as 'privacy by default'. Some stakeholders suggested the creation of some check lists, in order to assess the level of accountability and privacy by design. These check lists could be made publicly available in a register.

2.5. *Encouraging self-regulatory initiatives and exploring EU certification schemes*

The Commission will:

- examine means of **further encouraging self-regulatory initiatives**, including the active promotion of Codes of Conduct;
- explore the feasibility of establishing **EU certification schemes** in the field of privacy and data protection.

– **Self-regulatory initiatives**

Many sectoral private organisations supported the development of self regulatory initiatives.

The majority of DPAs referred to the need of encouraging self regulatory initiatives. Some mention that a self-regulation system should guarantee the representation of the sector, be credible and ensure that self-regulatory provisions are up to date and relevant. Internal control of compliance systems should be introduced, but it should not replace a possible inspection by a DPA or its sanctioning regime.

– **Certification schemes**

Certification schemes are widely supported by the industry, several industrial companies arguing that products that are awarded a seal should have a faster access to the market, and that some of the administrative burden should be lifted for those products. The 'Europrise' seal is quoted as a good reference by several stakeholders. More than one citizen encourage to establish a European sign which could assure data subjects that data protection was carried out in accordance with the data protection standards.

A few stakeholders argued that certification schemes should not be made mandatory, as this would create additional administrative burden.

3. REVISING THE DATA PROTECTION RULES IN THE AREA OF POLICE AND JUDICIAL COOPERATION IN CRIMINAL MATTERS

The Commission will, in particular:

- consider the **extension of the application of the general data protection rules to the areas of police and judicial cooperation in criminal matters**, including for processing at

domestic level while providing, where necessary, for harmonised **limitations** to certain data protection rights of individuals, e.g., concerning the right of access or to the principle of transparency;

- examine the need to introduce **specific and harmonised provisions** in the new general data protection framework, for example on data protection regarding the processing of **genetic data** for criminal law purposes or distinguishing the various categories of data subjects (witnesses; suspects etc) in the area of police cooperation and judicial cooperation in criminal matters;

- launch, in 2011, a **consultation** of all concerned stakeholders about the best way to **revise the current supervision systems in the area of police cooperation and judicial cooperation in criminal matters**, in order to ensure effective and consistent data protection supervision on all Union institutions, bodies, offices and agencies;

- assess the need to **align**, in the long term, the **existing various sector specific rules adopted at EU level for police and judicial co-operation in criminal matters in specific instruments**, with the new general legal data protection framework.

There is general support among the DPAs and public institutions for extending data protection rules to the areas of police and judicial cooperation in criminal matters and for the harmonisation of any specific provisions considered necessary in this area.

Law enforcement authorities should be subject to clear rules on the protection of personal data and they should be broadly comparable to the standards that apply in other sectors. However, as noted by several DPAs and national public authorities, special rules and derogations which duly take into account the specificity of the police and justice sector should be foreseen. Thus, specific needs of law enforcement authorities should be catered for within the legal framework (e.g. consent is unlikely to be readily forthcoming from those engaged in criminal activities).

As regards harmonised limitations on data protection rights of individuals, they have to be necessary, proportionate and not change the essential elements of the right itself. The EDPS emphasised that the Directive currently applies to "law enforcement" in various areas (such as taxation, customs, antifraud) that are not fundamentally different from many activities in the area of police and criminal justice.

In Eurojust's view, the new instrument should define the general principles applying to all sectors while specific provisions will still be applied to the area of police and judicial cooperation in criminal matters. Given the specificity and sensitivity of the processing operations in this area, detailed tailor-made provisions would provide a higher level of protection than general ones. The exclusion of Eurojust and Europol from the scope of application of the Framework Decision 2008/977/JHA on Data Protection should be maintained.

Voices from industry seek clarifications on how organisations can disclose data without breaching data protection obligations where data are requested from international or national law enforcement authorities. Moreover, clarity is needed both on the applicable law and jurisdiction question as well as on the process of responding to requests received from law enforcement authorities.

Some contributions argue that the EU should not introduce data protection safeguards that are so restrictive that they might stop law enforcement authorities from protecting the public. On

the other hand, specific safeguards should be put in place in order to give data subjects additional protection in an area where the processing of personal data may be more intrusive. This is well illustrated by citizens' replies who are worried about the amount of data collected by the police and law enforcement authorities and transfers of such data to third countries.

4. THE GLOBAL DIMENSION OF DATA PROTECTION

4.1. *Clarifying and simplifying the rules for international data transfers*

The Commission intends to examine how:

- to **improve and streamline the current procedures** for international data transfers, including legally binding instruments and 'Binding Corporate Rules' in order to ensure a **more uniform and coherent EU approach** vis-à-vis third countries and international organisations;
- to **clarify the Commission's adequacy procedure** and better specify the **criteria and requirements** for assessing the level of data protection in a third country or an international organisation;
- to define **core EU data protection elements**, which could be used for all types of international agreements.

Respondents from all of the different types of industry organisations recommended increased harmonisation, consistent enforcement and uniform application of data protection rules. BCRs, notification requirements and other administrative burdens should be reduced in order to increase competitiveness of European companies, however these reductions in compliance burdens could be offset by the creation of new regulations. Despite the concerns about compliance costs, service and content providers and technology companies all recognised that strong data protection rules can increase consumer trust and provide a competitive advantage. Responses from international trade organisations also argued that a lack of harmonisation across Member States and globally disrupts business significantly and a harmonised approach would support competitiveness and benefit all businesses.

Several companies, industry organisations and service and content providers all note that any changes to the directive should promote prosperity alongside privacy protection and recognise that restrictions and administrative burdens could give business operators based outside the EU serving customers in the EU an unfair advantage in not complying with the regulations applicable to EU companies. This is particularly true in relation to developing new technologies or services.

Like industry, privacy related civil society organisations stated that the EU data protection framework should be considered in a global context and that the EU should take a lead in dialogue surrounding cross border data transfers. Privacy organisations also argued that sanctions should be imposed on organisations that move data processing across borders in order to avoid the burden or costs associated with compliance of EU legislation.

– Adequacy

Adequacy provisions are considered not satisfactory currently, as there is a need for clarification and streamlining. The current mechanisms are deemed to be bureaucratic, impractical, complex and not related to commercial realities. Cloud computing and the exponential growth in the use of the internet have moreover changed the nature and dynamics of international data transfers.

The adequacy procedure as it is applied nowadays has been more a test of similarity or equivalence with the EU regime and has caused tensions with other countries whose enforcement mechanisms will naturally differ.

According to the responses, the Commission should consider the possibility of granting sector-specific adequacy determinations, so that data of a certain type transferred to another country and subject to sector-specific laws or regulations may be found to be adequately protected.

Adequacy assessments must focus on the outcomes of the regime being analysed and not on the list of prescriptive provisions in the legal regime. The procedure should move from prescriptive rules to a risk-based model of accountability with adequacy of specific transfers rather than of a country in focus. More attention should be paid to the competence and adequacy of the body handling data rather than to the territory where data is held.

A recurring industry view was that adequacy should be replaced by the extension of the accountability principle to international data transfers. This would place the emphasis on both data controllers and processors to ensure that data is adequately safeguarded regardless of location.

The adequacy procedure should be more transparent so that businesses can anticipate favourable determinations and put in place appropriate arrangements in advance. One should also study the possibility of carrying out sectoral adequacies, for instance to cover certain part of a third country data protection regime (for instance, only the banking sector, or only the IT subcontracting sector, for countries that have sectoral legislation)

According to industry, controllers (in the context of accountability) should have the flexibility to make their own adequacy determinations. The revised framework should include clear criteria for controllers to guide them through this process.

In industry's view data processors should be reflected in the proposal – a processor that acts on behalf of a controller should not be treated as a third party (of course if a processor applies EU rules for data protection). As well, contractual options should allow transfers from data processors to sub-processors, provided that their obligations under the Directive are passed on in contract.

Representatives of the academic community also supported a much more flexible approach and proposed to implement a risk-based model which would be built on data controller's obligation to evaluate all relevant factors (e.g. the nature of the data, how long the data will be in the third country, whether the data will remain under the control of the data controller etc.). In this case they accept that data transfer can take place even in situations where the general legal regime governing data protection is not similar to that as within the EU, but reasonably effective in protecting individuals' core rights and interests.

A citizen working in the IT field, proposed to introduce a certification scheme as a measure to comply with adequacy requirements in the context of international data transfers.

Respondents argued that any international agreement between EU and a third country should reflect a high level of data protection.

– **Binding Corporate Rules (BCRs)**

Respondents argued that the authorisation process for establishing BCRs is currently inefficient: too slow, bureaucratic and complex. Thus, a clearer, more harmonised approach to BCRs is needed and direct reference to BCRs should be made in EU legislation. Recognizing BCRs as a suitable way of providing appropriate protection measures will give BCRs a status equivalent to standard contractual clauses. However, BCRs should be better adapted to modern practices (e.g. cloud computing).

BCRs could easily serve as a more flexible and less formalistic approach to data transfers by means of robust internal policies and procedures and internal oversight and auditing. They can constitute an alternative to adequacy.

In respect of BCRs, the notions of both "accountability" and "group of companies" were referred to very often. BCRs provide a good framework for a variety of inter-group transfers for multinational companies. The prevailing opinion of the industry is that transfers within the same "group of companies" need to be radically simplified. They should also apply to data processors when transferring personal data (such expansion of scope would be beneficial to EU businesses).

To make BCRs more attractive and effective, the mutual recognition scheme needs to be expanded to include all MS (for one single regulatory approval to have effect in EU-27). One stakeholder proposed a new approach to BCRs – creation of Binding Global Codes (BGCs) for multinational organisations built on foundation of accountability. They would take form of a set of binding rules demonstrating compliance with data protection principles on a worldwide basis. The Code would cover policies, procedures, technology and human/organisational issues, not just legal compliance, with clear governance arrangements and identifiable internal responsibility.

4.2. *Promoting universal principles*

The Commission will:

- continue to **promote the development of high legal and technical standards of data protection** in third countries and at international level;
- strive for the **principle of reciprocity of protection** in the international actions of the Union and in particular regarding the data subjects whose data are exported from the EU to third countries;
- **enhance its cooperation, to this end, with third countries and international organisations**, such as the OECD, the Council of Europe, the United Nations, and other regional organisations;
- **closely follow up the development of international technical standards by standardisation organisations** such as CEN and ISO, to ensure that they usefully complement the legal rules and to ensure operational and effective implementation of the key data protection requirements.

In the majority of contributions, the Commission was encouraged to continue its work on promoting development of international data protection standards. However this should not

take form of simply imposing EU standards on third countries. Constructive and open dialogue is required.

Current revisions of the EU, Council of Europe, and OECD frameworks should lead to ensure greater convergence and enhanced protection for individuals.

Modernisation of cross-border transfer of data between law enforcement authorities constitutes one of the areas where international standardisation could be beneficial.

A global harmonised approach towards data protection is deemed indispensable especially bearing in mind the growing popularity of cloud computing services. Some stakeholders called for a multilateral binding agreement within the G8 or G20.

There were several references, especially in contributions from the industry, to the Madrid resolution as a good step in establishing common standards.

Some contributions called for capacity building support for third countries to promote the development of data protection standards.

5. A STRONGER INSTITUTIONAL ARRANGEMENT FOR BETTER ENFORCEMENT OF DATA PROTECTION RULES

The Commission will examine:

- how to **strengthen, clarify and harmonise the status and the powers of the national Data Protection Authorities** in the new legal framework, including the full implementation of the concept of ‘complete independence’;
- ways to **improve the cooperation and coordination between Data Protection Authorities**;
- how to ensure a more consistent application of EU data protection rules across the internal market. This may include **strengthening the role of national data protection supervisors, better coordinating their work via the Article 29 Working Party (which should become a more transparent body), and/or creating a mechanism for ensuring consistency in the internal market under the authority of the European Commission.**

The majority of views are that the coordination between DPAs should be enhanced in order to achieve a harmonised approach within the EU. Some emphasise that the role and competences of DPAs should be clarified and harmonised across the EU. Strengthening DPAs' powers should imply being able to bring actions before court and have the power to impose sanctions on controllers.

Only few contributions suggested that there is no need for strengthening the DPAs as they have already sufficient powers. Instead the enforcement of provisions by them should be improved.

In addition, a wish for the enhanced cooperation not only between DPAs but also between DPAs and market regulatory authorities at Member States and EU level, for instance between the Art.29 WP and ENISA was expressed. The role of ENISA as far as data protection is concerned should also be clarified.

As regards the full implementation of the concept of ‘complete independence’, the German Federal Government noted that Member States should be provided a way to reconcile the

concept of 'complete independence' for data protection supervision with their constitutional traditions. On the other hand, the EDPS referred to the decision in Case C-518/07 and insisted on the need to clarify the notion of independence of DPAs and suggested to codify explicitly the elements of the 'absence of any external influence' and 'instructions from anybody' in the new legal instrument.

The role of Art.29 WP in this respect in clarifying DP norms and standards is generally perceived as vital. Many respondents (especially from industry) argue that Art.29WP should be more engaged with stakeholders from public, private and NGO sector through consultations before it reaches the decision or publish an opinion. There are many calls for greater transparency of Art.29 WP activities. Some private stakeholders and organisations support a single point of contact at EU level.

In order to make opinions of the Art.29 WP more authoritative the EDPS recommended to include an obligation for the DPAs and the Commission to take "utmost account" of opinions and common positions adopted by the Art.29 WP, based on the model adopted for the positions of the Body of European Regulators for Electronic Communications in the Regulation No. 1211/2009. Furthermore, according to the EDPS proposal the new legal instrument could give the Art.29 WP the explicit task to adopt "interpretative recommendations".

The EDPS underlined a need to preserve and maybe improve coordination between the Art.29 WP and the EDPS, to make sure that they work together on the main data protection issues, for instance by coordinating agendas on a regular basis and by ensuring transparency on issues which have a more national or specific EU aspect.

ANNEX 5

DETAILED ANALYSIS OF IMPACTS

1.	Policy Option 1: Soft action.....	2
1.1.1.	1.1. Problem 1: Barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement.....	2
1.1.2.	1.2. Problem 2: Difficulties for individuals to stay in control of their personal data	6
1.1.3.	2. POLICY OPTION 2 - MODERNISED LEGAL FRAMEWORK.....	7
1.1.4.	2.1 PROBLEM 1 - Barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement.....	7
1.1.5.	2.2. Problem 2: Difficulties for individuals to stay in control of their personal data	15
1.1.6.	2.3. Problem 3: Inconsistencies and gaps in the protection of personal data in the field of police and judicial cooperation in criminal matters	21
1.1.7.	3. POLICY OPTION 3: DETAILED LEGAL RULES AT EU LEVEL	22
1.1.8.	3.1. Problem 1: Barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement.....	22
1.1.9.	3.2. Problem 2: Difficulties for individuals to stay in control of their personal data	24
1.1.10.	3.3. Problem 3: Inconsistencies and gaps in the protection of personal data in the field of police and judicial cooperation in criminal matters	26

6. POLICY OPTION 1: SOFT ACTION

6.1.1. 1.1. Problem 1: Barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement

(see section 6.1.1, a) and c) of the Impact Assessment)

1) Adoption of interpretative Communications by the Commission in order to clarify the existing rules

The Commission would issue Communications to add more clarity on the interpretation of the provisions of the data protection instruments. While these Communications would not have a legally binding value, they would provide an authoritative and consistent interpretation of EU law, providing more clarity for both Member States and other stakeholders (data controllers, individuals) on key provisions of the Directive. However, the current practice with (non-binding) Article 29 opinions on various aspects of the Directive has shown that the impact of such soft law on Member States' - and DPAs' – practice is quite limited. Furthermore, it needs to be taken into account that a Commission interpretation is not binding for the courts and that national courts and the ECJ in particular may come to different conclusions than the Commission. Therefore, interpretative Communications cannot sufficiently address the problem linked to the lack of legal certainty.

2) Further encouraging self/co-regulation

The Inter-Institutional Agreement on Better Law Making of 2003 (IIA) between the Commission and the legislator provides for the use of self- and co-regulation as alternatives to EU legislation and lays down criteria and principles to apply regarding these instruments. The Data Protection Directive provides for self-regulation by explicitly encouraging the creation of codes of conduct and the assessment of their legal compliance and their endorsement by supervisory authorities at national level or by the Article 29 Working Party at EU level. This procedure incorporates elements of co-regulation within the meaning of the IIA.

Since the entry into force of the Directive, the possibility to have codes endorsed by the Article 29 Working Party has been used in a very limited number of cases¹³³. In a fast moving economic and technological environment, there could be an opportunity for self regulation to become a more meaningful and useful instrument, so that the encouragement for EU level self regulation should be assessed. In 2008, the Commission published a study on self regulation, which provided recommendations and a check list for self regulation initiatives based on a screening of 61 self- and co-regulation initiatives in SANCO policy areas¹³⁴.

A successful self-regulation or co-regulation process is not necessarily of shorter duration than a legislative procedure. This is due to the fact that a meaningful agreement must achieve

¹³³ As an example, see the European Codes of practice for the use of Personal Data in direct marketing by FEDMA, including an annex on online direct marketing: <http://www.fedma.org/index.php?id=56>. It took several years to have the annex to the Code finalised, due to discussions with the supervisory authorities and WP29 (see the opinions issued, one in 2003 and one in 2010): http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp174_en.pdf and http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp77_en.pdf.

¹³⁴ Self-Regulation Practices in SANCO Policy Areas, http://ec.europa.eu/dgs/health_consumer/self_regulation/docs/self-reg-SANCO-final.pdf

a balance of all relevant interests as must the ordinary legislative procedure, however, the actors in self-regulation are not subject to a similar mandate as the EU legislator and are not subject to similar time constraints and procedural deadlines.

A self- or co-regulation procedure draws less on the resources of the institutions than a legislative initiative; it can be launched much faster than a legislative initiative, focus much more narrowly and provide much more precise rules than legislation, so that in the end it can make a considerable contribution to improving legal certainty for economic operators and more effectively protecting individuals' rights with respect to those activities and actors within its scope. It also may engage stakeholders more than the legislative procedure and may create a higher level of awareness due to their active participation in the process

Effectiveness requires that such codes are monitored systematically and equipped with an enforcement mechanism which includes statutory enforcement of the underlying legislation as the last resort.

Self regulation at EU level can only work properly when all participating actors have a common legal basis. Divergences in implementation and application of legal provisions between Member States make EU level codes of conduct unworkable or reduce their scope considerably. National level self regulation can only have limited effect for the EU Single Market as they cannot address cross-border issues; and in some cases it could contribute to making cross-border activities more difficult when national codes differ in substance.

Stronger harmonisation of legal implementation and application of data protection rules may therefore be the key factor to increase the effect of self-regulation and lead to a broader use of this instrument in the data protection domain, but self regulation cannot address the lack of harmonisation itself.

All in all, self-regulation at EU level, if it is accepted by all stakeholders and recognized by the competent authorities, may increase legal certainty and practical harmonisation for all stakeholders, but it can achieve this effect only when a clear and harmonised legal framework serves as a basis. It cannot, by itself, overcome fragmentation of national transposition, as evidenced by the current situation.

3) Standardisation

Standards developed by recognized standardisation bodies and addressing technological and organisational aspects of data protection could provide practical guidance for data controllers on setting up data protection compliant practices in their organisations. The well developed system of security standards and existing sectoral standards for privacy demonstrate the feasibility and the benefits of this approach. The standardisation process allows for the involvement of all relevant stakeholders and participation of DPAs, so that a broad reflection of all relevant views can be expected.

Nevertheless, successful EU level standardisation requires that legal requirements are clear and consistent. Standardisation cannot solve by itself obstacles created by divergent requirements in Member States.

4) Interpretative Clarification regarding DPA powers, resources and independence

Considerable divergences exist with respect to the powers actually entrusted to DPAs for investigation and intervention, as well as their available resources. The Commission could spell out in more detail the requirements resulting from the current framework. Independence of DPAs is already enshrined in the current Directive and the recent ECJ case-law on the matter (case C-518/07) has clarified the requirements to ensure full independence. The strengthening of DPAs independence would allow them to better play their role in supervising

data protection legislation at national level, and decide autonomously their enforcement priorities. A Communication could outline the Commission's plans on how to ensure that all Member States comply with the Court's findings on independence and a time schedule. As regards independence, the legal conditions have been clarified by the Court and provide the Commission with a basis to assess DPA independence in all Member States and use its instruments to ensure full compliance of all Member States. More concrete information would help the Member States to prepare any adjustments of their national laws where necessary. As regards DPA powers and resources, an interpretative Communication by the Commission is not likely to have strong effect on national transposition legislation. Member States generally consider it necessary to adapt enforcement and monitoring systems to the overall structure of their legal, administrative and enforcement environment where no precise binding rules are provided by the Union *acquis*. Commission advice regarding resources allocated to DPAs may not have strong effect, given budgetary constraints in many Member States.

5) Strengthened coordination tasks for WP29 vis-à-vis national DPAs and tools

Under this option, the catalogue of tasks of the WP29 would be extended to include the provision of advice to national DPAs and the exchange and preparation of best practices. DPAs would have additional practical IT tools, to improve the exchange of information, cooperation and mutual assistance between them. This, together with the strengthened role of WP29 in providing advice to DPAs and the encouragement of staff exchanges between DPAs, should help the development of more consistent enforcement practices across the EU. This would be beneficial to businesses, in particular, but also to individuals.

The cost of three concrete elements supporting this enhanced co-operation are assessed below:

- The cost of setting an IT system for collaboration have been estimated to be up to € 2 million one off costs¹³⁵, plus annual running costs of € 300 000 and additional costs in terms of human resources. The system would allow the secure exchange of documents between DPAs, and include a workflow to follow up that documents are reviewed and validated in due time if required for the cooperation procedures. Before setting up such a system, an in-depth analysis of the reusability of existing systems would need to be made, in order to minimize both initial and running costs;
- A budget for a programme supporting exchange of experts between DPAs, in order for them to work better in a network and to reinforce cooperation should also be provided. Depending on the number of participants, it can be estimated empirically that between € 500,000 and € 1 million per year could be devoted to an exchange program between DPAs (covering training, travel expenses and daily allowances of staff working in another DPA than his own).
- The Secretariat of the Art. 29 WP would need to be reinforced to cover the additional work. A 30% increase of the Secretariat budget to cover the additional workload could be estimated; based on current costs for the workload of Art 29 WP, this would amount to about € 0.5million.

6) Harmonised notifications forms – Single (online) platform

¹³⁵ Based on the costs of other information exchange systems developed by DG JUST, such as the e-Justice portal.

The setting up of a central platform with an online form, whereby data controllers submit only one form and mark the countries they need to notify – as one of the options proposed by the WP29 in its Advice paper on the matter¹³⁶ – would help reducing and simplifying the administrative formalities and burden linked to notifications. This would be welcome by Member States, as they could keep their current – differentiated – regime for notifications and exceptions/derogations. On the other hand, this option presents several shortcomings. The setting up of such a platform – be it by the Commission or by one or several DPAs – would be technically complex and costly, given the need to take account of the different requirements of the various Member States. For reference, the Commission has the experience of setting up information systems which provide for exchange of information between public authorities; such systems include IMI (internal market information system), Eurodac, the SIS system (information about wanted persons), the CPCS system, and the e-justice portal (information about the judicial system). Costs and implementation times of the systems vary greatly (time to set up from 18 months to several years, and costs from € 1 million to multiples of € 10s of millions, depending on the number of authorities involved, and the volume and complexity of the data). Experience shows that the complexity and cost of setting up such a system grows especially when the national laws defining how to collect and process the data in the Member states are not sufficiently harmonised, which would be the case in policy option 1.

The added value of such considerable investment would be limited as it would only reduce part of the burden – i.e., it would reduce the paper formalities by providing a unique and centralised electronic interface – while leaving the current differences in substantial requirements and the related costs unaffected. This solution is unlikely to be perceived by stakeholders as reducing sufficiently the costs and the administrative burden linked to notification requirements.

7) Legal amendments clarifying provisions on international transfers

Clarifying and detailing the criteria for adequacy and providing a clear legal basis for Binding Corporate Rules (BCRs) – which have developed as a matter of practice, thanks to the input of WP29 – would bring more legal certainty as regards international transfers and would benefit data controllers and individuals as well as the third countries concerned. However, this would not address all issues raised by business stakeholders about the limits of the current BCRs model, i.e. on the length and complexity of the procedure, which often requires several authorisations at national level even when the BCR has been validated by the "lead" DPA.

6.1.2. 1.2. Problem 2: Difficulties for individuals to stay in control of their personal data

(see section 6.1.1, b) and c) of the Impact Assessment)

8) Awareness-raising activities (information to individuals, particularly children)

The Fundamental Rights and Citizenship programme will continue to fund awareness-raising activities related to data protection, targeting children in particular. Current funding (about € 800 000 for the period of 2009-2010 under the Fundamental Rights Programme) could be increased by 25% in order to expand such activities further.

9) Promotion of PETs, privacy-friendly default settings, uptake of privacy seals

136

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex2_en.pdf

The EU already promotes and supports the research and development of privacy enhancing technologies, privacy by design and privacy by default settings through research priorities in FP 7. More than 13 EU projects related to privacy enabling technologies are currently funded by the EU budget. An additional call for projects related to security and privacy has been published in July 2011 with a budget of € 80M¹³⁷. Some additional funding for studies under the Fundamental Rights Programme could be envisaged to promote specific objectives, such as an "EU privacy seals for international transfers".

These measures would provide support to increased application of the principle of "Privacy by Design" in the industry. As a recent survey carried out by the Commission has shown¹³⁸, privacy by design is favoured by a large majority of the security industry who believes that it should be a mandatory obligation, 77% of the respondents from the industry would even favour introducing the privacy by design principle in the legislation. As regards sector specific trust marks and seals, they are generally viewed favourably by industry, but would not welcome a horizontal certification program.

Continuing and strengthening current support through EU programmes will maintain the current level of engagement of stakeholders, mainly in research and technological development. However, as the experience from several years of this support shows, it does not create an incentive for broad endorsement in business practices when rolling out new commercial or public services.

10) Introduction of explicit transparency and data minimisation principles

The introduction of an explicitly stated transparency principle for the controller - while not adding specific additional obligations - would build on the existing provisions to provide the necessary information to the individuals concerned before the processing of their personal data not only in specific cases, but extend this to processing in general. This would strengthen the data subjects position as this would enable him/her to have more and earlier insights into the processing of his or her personal data provided by the controller in the specific case and lay the foundation for his or her consent (if and where necessary).

It would equally strengthen the data controller in relation to the data subject as he would demonstrate upfront to the data subject his way of processing the personal data in question and thereby generate the necessary trust. While the implementation by controllers may generate some initial additional costs, these would be offset by the potential benefits for the controller controlling data flows and for the development of e-commerce.

Data minimisation, i.e. processing and storing only those personal data that are necessary for a legitimate purpose, is becoming more and more important when technical limitations to storage, processing and transfer capacity are quickly disappearing, and when at the same time security risks and data breaches are becoming more prevalent. Security and data protection experts have underlined that data that is not stored or processed cannot be misused as a consequence of a breach. The principle is already provided for by the current provisions; however, it is not always fully understood how to interpret in practice. An explicit explanation of the principle in the legal instrument will provide data controllers with more clarity and improve the protection of individuals; and it will have no effect on legitimate data processing. It would strengthen the existing provisions on data quality, explicitly stressing that data processed should be limited to the minimum necessary in relation to the purposes for which they are collected and/or further processed.

¹³⁷ FP 7, call 8, Objective ICT-2011.1.4 Trustworthy ICT

¹³⁸ Survey conducted in Q1 2011 by DG ENTR with companies representative from the security industry.

Explicit recognition of the principle would be beneficial to data subjects as they will not be exposed to excessive data collection, which will better ensure their protection. Also this will limit the negative impact of data collected while not necessary (e.g., function creep, reputational risk, aggressive marketing and surveillance). As regards the impact on data controllers, data minimization requires full understanding of the data one possesses in order to be able to delete with confidence. Data minimisation is a sound principle of data management. It helps avoiding data overflow and mitigates the risks in case of security breaches. Moreover, data loses its value over time, and it would reduce costs associated with the use of outdated data and increase compliance with data quality requirements. Finally, if data subjects do not feel that their data protection right is violated by excessive collection of data, e.g. for online services, consumer trust will increase, thereby potentially having a positive effect on the development of e-commerce.

6.1.3. 2. POLICY OPTION 2 - MODERNISED LEGAL FRAMEWORK

6.1.4. 2.1 PROBLEM 1 - Barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement

(see section 6.1.2 of the Impact Assessment)

1) Further harmonising the substantive data protection rules

This would be achieved by a combination of measures, namely:

a) Clearer and more detailed substantive provisions

More precise and detailed rules would harmonise the implementation and application in Member States, thus greatly reducing the current cost of legal fragmentation (estimated to amount – only in terms of administrative burden – to **almost € 3 billion per annum**). These costs are incurred by economic operators processing personal data several Member States to which different national rules are applicable.

Replacing the current Directive by a Regulation or by a maximum harmonisation Directive – together with a clarification of rules on applicable law and other simplification measures (*see below*) - would have the effect of eliminating most, if not all, of these costs and drastically simplifying the regulatory environment. The resulting economic benefits for the internal market would be considerable as:

- In the short run, economic operators would no longer be faced with the disincentive of high legal costs when considering whether to expand their business cross-border. The enhanced legal certainty could therefore encourage greater cross-border investment within the internal market and also boost the competitiveness of EU economic operators internationally.
- In the medium-run, more cross-border offers in the internal market would boost competition within the Member States, increase consumer choice, and hence put a downward pressure on prices.
- In the long-run, savings in legal costs may result in more funds being devoted by economic operators to research and development, hence boosting innovation in the internal market
- Also in the long-run, the streamlined regulatory environment with one set of clear and consistent rules applying across the internal market would make the EU a more

attractive place for business, for multinational companies considering expansion into the EU.

This approach – and particularly the Regulation option, being directly applicable upon Member States without the need for transposition into different national laws - is strongly supported by the great majority of economic operators, which consider it essential to ensure the desired legal certainty and simplification within the internal market. On the other side, a Regulation would have an important impact on Member States, given the fact that most of them have developed an extensive and detailed national legislation implementing the Directive, covering both the private and the public sector.

Additionally, entrusting the Commission with powers to adopt **implementing measures or delegated acts** in specific cases would increase consistency of the EU data protection framework. In particular, detailed harmonised rules could be adopted for specifying technical aspects that require uniform conditions of implementation (e.g. detailed security measures in various situations).

The implementing powers to be given by the legislator to the Commission would follow the rules and general principles concerning mechanisms for control by the European Parliament and the Member States of the Commission's exercise of implementing and powers¹³⁹, thereby guaranteeing for a procedural involvement, whilst leaving the possibility for the European Parliament or the Council to be able at any time to indicate to the Commission that, in its view, a draft implementing act exceeds the implementing powers provided for in the basic act, taking into account their rights relating to the review of the legality of Union acts.

2) Revising the rules on applicable law and on DPA competence (one single law and "one-stop-shop")

In case of a Directive, the applicable law would be the law of the Member State of main establishment of the controller. In case of a Regulation, the EU legal instrument would be the single and directly applicable law across EU Member States.

In both cases, the *clarification and simplification of rules and criteria on applicable law*, would be highly beneficial to data controllers with several establishments in the EU, as it would remove conflicts of application, provide more legal certainty and reduce existing unnecessary costs since the controller would shift from a distributive application of different national laws to a centralised application of a single legislation in all Member States¹⁴⁰.

In addition to the single applicable law, the fact of entrusting one single DPA with the competence to deal with a controller operating across the EU would respond to the strong demands for simplification and consistency of the current enforcement system, leading to a *"one-stop-shop"* for data controllers and processors. Together with the increased substantive harmonisation of the rules and the simplification of rules on applicable law, this would contribute to reducing the costs linked to fragmentation. Due to the much higher degree of harmonisation of the data protection rules the effective application of the "main establishment" principle – both for the applicable law (if it is a Directive) and for DPA competence - would not result in 'forum shopping' in favour of Member States whose legislation would be considered as less strict in terms of data protection requirements.

¹³⁹ Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, OJ L 055 , 28/02/2011 P. 013 – 018.

¹⁴⁰ Within the territory of the EU the need for more precision in the legal framework and a simplified criterion to determine the law applicable has been emphasised by the Article 29 Working Party in a recent opinion (Opinion 8/2010 on applicable law, WP 179).

From the point of view of the data subject, the impact would bring about equally legal certainty as to what rules apply to the processing of his or her personal data. And in any case, the data subject would retain the right to complain to a data protection supervisory authority of his/her choice (e.g. his/her residence). Strengthened *administrative sanctions* available to DPAs against non-compliant data controllers will contribute to ensure that individuals' rights are actually respected and enforced.

3) Replacing notifications with a generalised basic registration system

A basic registration for all data controllers would simplify formalities and allow certain DPAs to continue financing themselves with a fee-based system¹⁴¹. However, if the registration system would be a general requirement and not allow for derogations of the same level as the current notification rules, it would impose additional – albeit - reduced administrative burden to data controllers in those Member States that have made extensive use of the current possibilities for exemptions and derogations (e.g. Sweden, Germany). On the other hand, maintaining this kind of margin would again open the possibility of divergence in Member States, contrary to the main policy objective pursued (i.e. simplification and reduction of undue administrative burden).

However, it would fall short of the expectations of the large majority of economic stakeholders for which this represents an (unnecessary) administrative burden, without providing any actual added value for the data subject. Indeed, DPAs themselves acknowledged that the current register – available at DPAs premises on the basis of notifications received - "is no longer the best and more appropriate way for individuals to understand what an organisation is doing with their personal data, and who to contact when things go wrong"¹⁴².

If this system is estimated to cost 50% of the current costs of notifications to DPAs (including the additional burden in those Member States that largely exempt from notifications today), then it can be assumed that its overall cost would amount to approximately €65 million per annum across the EU.

4) Notification of data breaches to DPAs and individuals

Technical and organisational measures to ensure the security of the processing of personal data, appropriate to the risk connected to the processing and taking account of the state of the art and the cost of the measure, are already a legal obligation for data controllers under existing legislation, Directive 95/46/EC and Directive 2002/58/EC. Systematic monitoring and enforcement of these obligations is, however, difficult, as it would require a thorough assessment of internal conditions and procedures of the data controller by the enforcement authority. In practice, inadequate security measures are only discovered in cases where breaches of security occur and come to the knowledge of the authorities of the public.

In some jurisdictions, obligations to notify security breaches which compromise personal data have been introduced. Experience has shown that these obligations have indeed a positive effect on data security measures taken by data controllers. This is due to a number of reasons: breach notifications provide a systematic feedback about the actual risk and the actual weaknesses of existing security measures; they enable authorities and consumers to assess the

¹⁴¹ This concerns, in particular, the UK DPA (ICO), which is currently exclusively funded by notification fees. ICO argues that a fee-based funding model is the application of the 'polluter pays' principle (in that those processing personal data are the ones who make it necessary for there to be a system of supervision, regulation and advice and guidance services provided by data protection authorities, and they therefore are the ones who should pay for it).

¹⁴² See Advice Paper of WP29 on notifications, p.6.

relative capabilities of data controllers with respect to data security; they force data controllers to assess and understand their own situation regarding security measures. Data security issues become relevant for the management level of an organisation, which may be even further encouraged to apply systematic procedures by the objective to avoid reputational damage in the case of an avoidable breach.

Member State legislators and administrations have started to implement notification obligations for data breaches. In order to avoid diverging Member State rules, the Union has to provide for a harmonised system of breach notifications across the EU. As a first step, a breach notification obligation was introduced with the review of the electronic communications framework in the e-Privacy Directive. As requested by the European Parliament, the current review of the general data protection framework is now the opportunity to create an all encompassing obligation to notify personal data breaches. Under the e-Privacy Directive, all personal data breaches occurring at providers of electronic communications services have to be notified to the competent national authority. In addition, breaches that are likely to adversely affect the privacy or personal data of individuals are to be notified to these individuals concerned. A recital of the amending Directive lists cases that are considered examples for creating adverse effects, i.e. if the breach may lead to identity theft or fraud, physical harm, significant humiliation or damage to reputation. The Directive empowers the Commission to adopt implementing measures on the circumstances, format and procedures of breach notifications in a comitology procedure, including stakeholder involvement and consultation of ENISA, the EDPS and the Article 29 Working Party. US experience – as well as the responses from stakeholders – suggests that the definition of the threshold for notification to the data subjects is a key factor to determine the immediate cost impact of breach notification obligations on data controllers, including the administrative burden. The proper setting of this threshold is also necessary to achieve the intended effect on improving the protection of individuals with regard to possible misuse of their personal data. If the criteria are set too strict and the threshold too high, data subjects may not be informed about breaches concerning their data and may lose the opportunity to protect themselves against damaging consequences. If the threshold is set too low and criteria are too loose, data subjects might receive many notifications that do not actually require any action from their side. This could lead to a so-called notification fatigue, with the result that data subjects do not pay attention to notifications and miss cases that would require action on their part. This is why following the same approach as in the e-Privacy Directive - i.e. defining the core elements of the notification system and leaving the definition of details on circumstances (including criteria to assess the likelihood of adverse effects), procedures and formats to Commission implementing measures, appears as the best solution to ensure consistency across sectors. When the amendments of the ePrivacy Directive were discussed, the EU legislator chose this approach as it found that the use of implementing measures allowed more detailed, precise and flexible rules than could be integrated in the basic legal act itself. These considerations were conducted with a broader application than the electronic communications sector in mind, as the legislator also noticed that data breaches in some other areas, in particular online business, could result in similar or even more serious damage than in that sector. An additional advantage of technical implementing measures would be that they would allow for differentiation of sectors where appropriate, what would not be possible within the sector agnostic general data protection instrument. Implementing measures would allow for a comparably fast and easy way to adjust rules based on experience with first practical application of breach notification rules in the EU and to ensure that its practical application can remain in line with technological development. Notably, the experiences with breach notifications in the electronic communications sector could be fully exploited for a more general solution. It results that the approach of leaving the

definition of details regarding circumstances, formats and procedures of notifications to implementing measures is more effective regarding the achievement of the political objectives of simplification and improving individuals' exercise of their rights than the attempt to provide for full details in the basic act. The approach also allows for better involvement of stakeholders and better balancing of the different interests at stake.

While the legal instrument should provide for the possibility of defining details of breach notifications through implementing measures, it must set certain basic characteristics of the procedures by itself. It has been suggested in particular that setting a more precise time frame for a notification could provide more legal clarity to data controllers and reassure data subjects. While the ePrivacy Directive provides that notifications should be made without undue delay, a 24-hour deadline to notify the supervisory authority, where feasible, from the establishment of the breach and the identification of who is affected could be expected to provide more precision.

The impact of such a concrete deadline needs to be assessed. Firstly, it needs to be clarified which event should trigger the start of the time interval. Such an event would be the detection of the breach by the data controller. To be more precise, it would be the moment when the data controller records in its files that an event that triggered a first investigation has been identified as a personal data breach. This event could be a security breach discovered in-house, or an alert received from an outside entity. It should be noted that the actual breach itself may have taken place much earlier, or may have been ongoing for a while before it was detected. Secondly, it should be considered that a notification is the more useful the more precise and comprehensive information about the nature of the breach and the data concerned can be provided. A 'quick and dirty' notification rushed out to meet a deadline, which then requires updates and corrections will cause more insecurity concern and loss of confidence of data subjects than it provides benefits to users. Thirdly, the notification can only be provided if the individuals concerned and a workable channel for the communication of the notification have been identified. Fourthly, as already recognized by the amended ePrivacy Directive, the breach may require additional criminal and forensic investigations which could be compromised if the general public, including the perpetrators, receives early information about the detection of the breach. Any deadline for notifying a breach must in practice consider these elements and should not create an incentive for the data controller to delay the recognition and recording of a breach in order to avoid consequences of a formally delayed notification.

Nevertheless, the legal instrument could provide the clarification that a first notification of the detection of a personal data breach should be delivered to the competent authority, where feasible, within 24 hours after the establishment of the breach, followed where appropriate by more detailed information as it becomes available. The data controller shall provide the competent authority on its request with the precise reasons if the delay exceeds 24 hours. Individuals would only be notified, without undue delay, where the data breach is likely to adversely affect the protection of the personal data or privacy of the data subject. This would ensure that "over-notification" – even when there is no harm to the individual - is avoided. As regards criteria for determining the seriousness of a breach, it should be taken into account that quantification is generally not possible due to the vast differences of breach cases that can occur. The number of individuals concerned by a breach cannot be used as a severity criterion, as the possible risk for any individual is not dependent from the number of others that are concerned by the same incident. In some circumstances damage may even be more likely when less individuals are concerned, e.g. if a hacker obtains only a few credit card records, each one may have a much higher probability to be used for fraud than when several million records are stolen.

Annex 9 estimates the cost of this measure in terms of administrative burden to amount to € 20 million per annum, based on UK figures and extrapolating from those for the rest of the EU, factoring in a cost of € 400 per notification.

5) Strengthened and simplified rules on international transfers

Simplifying the rules on international transfers would generally have a positive impact both on relations with third countries and on non-EU businesses and will boost the competitiveness of EU economic operators internationally, as they will find it easier to transfer personal data outside of the EU. In particular (*in addition to measures foreseen in Policy Option 1, see above*):

- Giving the Commission a monopoly on adequacy findings would reduce uncertainty and inconsistency that would arise from potentially contradictory decisions from Member States, which are both prejudicial to data controllers;
- Abolishing the system of prior authorisations in Member States when standard tools (e.g. contractual clauses or BCRs) are used, would also be beneficial to data controllers as it would shorten and simplify the procedure for authorising a transfer, thus reducing costs;
- Extending the use of BCRs to "data processors and "groups of undertakings", together with the simplification of the procedure of "mutual recognition" between DPAs, would extend and facilitate their use, while at the same time ensuring a high level of data protection. This would considerably reduce the time (currently 6 months to 2 years) and the money spent on – nowadays - long and burdensome procedures (up to € 1 million for large companies as reported in the course of the public consultation by some of these companies with BCR experience).
- Allowing data controllers, under certain circumstances, to conduct their own assessment under their responsibility - and adducing appropriate safeguards - as regards specific transfers will increase flexibility.

6) New governance system – Better monitoring and enforcement

a) Strengthening national DPAs

The strengthening of DPAs independence would be highly beneficial to data subjects, as it would help them exercise their data protection rights: DPAs would have more powers and resources to investigate complaints, assist individuals in having access to their data etc. Data controllers are also likely to benefit since DPAs will have more resources to provide advice and assistance to them.

The harmonisation of tasks and powers of DPAs is essential to ensure that they can effectively perform their monitoring and investigation tasks, as well as for the proper working of the cooperation and consistency mechanism described below.

As regards costs, the requirement of providing DPAs with sufficient resources to be able to fulfil their tasks would require additional financial means for some Member States. This additional cost is difficult to estimate in general, given the current differences in the size, available resources, means of funding, tasks and powers of national DPAs. It is likely that the costs will be higher for smaller Member States and/or those Member States where DPAs have limited resources at the moment, taking into account that the abolition of notification requirements will freed resources.

Ensuring proper resources for DPAs is also key to ensure good cooperation between them. Some DPAs face recurrent financial difficulties, limiting their ability to cooperate with others.

b) Strengthening cooperation and mutual assistance between DPAs – Mutual recognition of decision and "consistency mechanism"

Together with the revision of provisions on applicable law (*see above*), these measures would **further enhance the internal market dimension of data protection**, increase harmonisation and legal certainty and reduce the current costs linked to fragmentation and inconsistent enforcement.

As regards the impact on Member States' data protection authorities, they will no longer have a direct role in cases where the data controller's main establishment would be in another Member State and thus outside their direct supervision. However, they would remain competent to supervise the implementation of the data protection legislation on the territory of their Member State e.g. to verify and intervene on a processing operation that is taking place on its territory by a controller with a main establishment in another Member State. This would have to be done in close coordination with the supervisory authority in that Member State, which would take a final decision against the controller. This decision would have to be enforced by all concerned DPAs on their own territory.

The *new cooperation and consistency mechanism* between DPAs will ensure that their concerns are taken into account as they would be able to intervene in cases concerning their citizens and or affecting their country. The strengthened role of the Commission would ensure the overall consistency and compliance with EU rules on data protection.

This mechanism would also entail additional costs (including administrative burden) for:

- **National DPAs**, as they would need to foresee additional resources to adequately cooperate and exchange information with other DPAs, in particular to:
 - Carry out checks, inspections and investigations as a result of requests from DPAs in other Member States, as part of the mutual assistance mechanism established;
 - Have additional staff and mechanisms in place to investigate enforcement requests from DPAs in other Member States;
 - enforcement of the decisions taken by DPAs in other Member States as part of the "one-stop shop" system of supervision

It is expected that DPAs will need at minimum 2 or 3 staff members working for the EU cooperation to ensure a proper functioning of the proposed consistency mechanism. This may pose problems for the DPAs of small Member States, whose financial and human resources are already more scarce. On the other hand there is a trade-off, as parallel procedures by several DPAs will be eliminated by the clear assignment of a single DPA for the controller. It is difficult to establish the balance between these effects as this will depend very much on the current size and resources of DPAs, the cases they will have to be involved in etc.

- **The EU budget**, since additional human, financial and technical resources should be foreseen to:
 - a) Handle notifications of cases handled by DPA that have a European impact. In other policy areas similar mechanisms (e.g. telecom, technical standards), require between 15 and 20 staff to handle the notification system managed by the Commission, together with adequate technical means (databases, communication system, translations etc). The data protection consistency mechanism requires resources particularly from the EDPS, which will provide the secretariat of the European Data Protection Board and operate the IT system required for quick and standardised communication between national DPAs and the Board. Together with the general

tasks of the board secretariat, these tasks will require 10 FTE posts (in addition to the EDPB Chair). Overall, the EDPS budget will have to be increased by approximately € 3 million on average for the first six years of operation.

- b) Establish an information exchange system to facilitate communication between DPAs, the Commission and the *European Data Protection Board which will be replacing the WP29*.

(see section 6.1.2, b) of the Impact Assessment)

6.1.5. 2.2. Problem 2: Difficulties for individuals to stay in control of their personal data

7) Clarifying substantive rules and key concepts

a) Definition of personal data (online identifiers):

A recent study¹⁴³ analysing case law relating specifically to IP addresses found that in the vast majority of cases analysed the courts had identified these identifiers as personal data in the cases under decision, by applying the interpretation provided in recital 26 of the data protection directive on whether or not a person is identifiable. In 84% of the relevant 48 cases courts considered IP addresses personal data on the basis that they relate to an identifiable individual, in particular when the data controller has the intention to identify the individual, when other data elements were present that made identification easier or when the court applied a principle of caution regarding identifiability. The interpretation of identifiability depends to some extent on how the national legislator has used the explanation provided in recital 26 in its national legislation. Several Member States have integrated the explanation of identifiability in the national legislation as part of the definition of personal data, thus providing a more stringent basis to national courts than the Directive itself. Differences in national interpretation regarding online identifiers can accordingly be explained to some degree by differences in national transposition laws, which also include other modifications of the definition¹⁴⁴. By moving the explanation of the term 'identifiable person' from the recital to a substantive provision and by further clarifying the related recital, diverging interpretation will be avoided and more harmonised interpretation ensured.

This will have a beneficial impact on individuals, which will have enjoyed increased and effective protection of their personal data across all Member States.

In order to assess the impact of these clarifications on data controllers, it must be taken into account that no substantial change of the legal situation is envisaged, but a clarification of existing rules. Data controllers are not faced with new obligations, but with a clarification of existing already applicable law. Considering the Article 29 WP has already for a long time recommended to treat online identifiers as personal data as concerns the rules applied to their processing¹⁴⁵, those data controllers who followed this advice would not have to take any additional measures and would thus not experience any changes of their processing and not suffer any additional costs of administrative requirements. This interpretation has recently been confirmed by the ECJ in its ruling of 24 November 2011¹⁴⁶.

¹⁴³ Timelex study on case-law regarding IP addresses [...]

¹⁴⁴ [Examples to be added]

¹⁴⁵ Art 29 opinion on Internet of /19992000

¹⁴⁶ ECJ judgment in Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM).

b) Definition and modalities of consent

As also pointed out in the opinion adopted by WP29 on consent, it seems essential to clarify that valid consent requires the use of mechanisms that leave no doubt of the data subject's intention to consent, while making clear that – in the context of the on-line environment - the use of default options which the data subject is required to modify in order to reject the processing ('consent based on silence') does not in itself constitute unambiguous consent. This would give individuals more control over their own data, whenever processing is based on his/her consent. As regards impact on data controllers, this would not have a major impact as it solely clarifies and better spells out the implications of the current Directive in relation to the conditions for a valid and meaningful consent from the data subject.

In particular, to the extent that 'explicit' consent would clarify – by replacing "unambiguous" – the modalities and quality of consent and that it is not intended to extend the cases and situations where (explicit) consent should be used as a ground for processing, the impact of this measure on data controllers is not expected to be major.

The current requirement for unambiguous' consent has been translated in the various languages quite differently (in some cases even with the word 'explicit'¹⁴⁷) and subject to a variety of interpretations. 'Explicit' consent ensures, on the other hand, that consent is clearly expressed by the individual concerned – not necessarily and not solely in writing, it is not the purpose of imposing one specific modality - where consent is required as a legal ground for processing personal data. Additional legal certainty would be provided by specifying in a recital that consent must result at least from a "clear affirmative action" of the data subject and that data controllers must be "in a position to demonstrate that consent has been obtained". This is, on substance, in line with WP29 opinion on consent¹⁴⁸.

Individuals would greatly benefit from the clarification of consent and from a strengthening of the modalities for consent, as this would allow them to be more aware that they indeed indicate their wishes in relation to the processing of their personal data and better informed about what they are consenting to 'ex ante', if consent is required. They would also be enabled to ask the controller ex-post for a proof of their consent in cases where they contest having given their consent or the extent of their consent. Thus the control of the data subject over their own data would be strengthened.

As regards controllers, this can bring significant benefits in terms of responsibility and the effective protection of personal data, as it is made sure that only consent that is construed in a solid way is taken as such and can be relied upon by controllers. 'Explicit' consent helps the controller to demonstrate that the individual has given his/her consent and to comply with their burden of proof. This would enhance legal certainty also for the controller that he could rely on the individual's consent has a legal ground for processing his/her personal data.

What is also important to clarify is that consent cannot be a valid ground for processing when there is a clear imbalance between the data controller and the data subjects (e.g. in the employment context).

The administrative burden linked to this obligation is included in the estimate for measuring the general obligation for the controller to demonstrate compliance with data protection law (see Annex 9).

c) Data portability

The possibility to move data from one service provider to another would increase competition in some sectors, e.g. between social networks, and could also make data protection an element

¹⁴⁷ For example, in the Greek version of the Directive and in EL national law.

¹⁴⁸

in this competition, when users decide to move away from a service they do not consider appropriate in terms of data protection.

Given that the transfer of data about users is usually already possible through other interfaces, e.g. for third party application developers or for exchanges with affiliated companies, the costs for implementation are minimal. In fact, use of existing interfaces for these purposes may allow the development of portability functions very quickly.

d) "Right to be forgotten"

The clarification of the right to be forgotten would strengthen users' control on their own data by enabling individuals to decide whether or not to share personal information as well as to impede the continued use of their data by data controllers, data processors or third parties. The adverse effect of data retained and retrieved after a long time has lapsed (e.g. in employment area, where a prospective employer may be prevented from hiring someone on the basis of information on political opinions which may have changed in the meantime) would be avoided.

Therefore, the reinforcement of the right to be forgotten would greatly benefit the data subjects, especially (but not exclusively) in online environments, such as social networks or cloud computing platforms: the data subject's right to remove his/her personal data from such a service would be more clearly stated in data protection rules.

As far as the data controllers are concerned, as with data minimisation, the right to be forgotten will avoid the retention of data that are outdated and often useless for the data controller. Another advantage is that this will stimulate innovation in this area.

On the other hand, this right, if it is carried out in an automatic way will imply some technological changes, necessary to affix an "expiry date" on data or sets of data. This will involve costs for data controllers.

The "right to be forgotten" will, however, not apply to activities subject to exemptions and derogations provided for under the provisions for processing for private purposes ("household exemption") and under processing for journalistic and literary purposes; it would therefore be ensured that the right to be forgotten does not affect freedom of expression and is used by individuals to attempt to alter or disappear from the public record. The media's role in keeping such public record will therefore not be affected.

e) Adding genetic data to the category of sensitive data

The explicit inclusion of genetic data as a special category of personal data requiring specific safeguards ("sensitive data") would bring about an important positive impact for individuals as it would address the particular concern that genetic data is properly and securely dealt with in all Member States. Equally, the harmonised approach would bring about positive impacts for those controllers who process genetic data as they could enjoy legal certainty for this processing in all Member States.

f) Children data

When services are specifically addressed to children, the information provided and the tools to control the protection of personal data must be adapted to the target group's expected capabilities. Privacy notices that are written for lawyers and complex privacy setting mechanisms that require deep understanding of the functioning of IT and online services cannot be considered appropriate. Appropriate information and mechanisms would greatly improve the possibility for children to exercise their data protection rights more effectively. The additional burden for data controllers would be limited if from the very beginning, products and services are designed to include children-friendly privacy information and settings ("data protection by design"). In relation to rules on consent in the online environment for children below 13 years – for which parental authorisation is required – it should be noted that they build on existing US regulations and practices (see in particular the Children Online Data Protection Act of 1998) and are not expected to impose undue and

unrealistic burden upon providers of online services and other controllers. This would also not interfere with Member States' contract laws, which would remain unaffected. The methods and modalities to obtain verifiable consent would be left to Commission's implementing measures.

e) Clarification of the rules applying to data processing by individuals for private purposes: Under this option, the current "household exemption" contained in Article 3 (2) first indent of the Directive would be clarified to exclude purely domestic processing addressed to a 'definite' number of individuals. This would reduce to zero the burden of data protection compliance costs when relating to activities which are solely carried out in the course of private or family life of individuals (which is not the case with the processing of personal data consisting in publication publicly available on the internet so that those data are made accessible to an indefinite number of people).

Article 9 of Directive 95/46/EC, however, would be reformulated in a way that it would cover all activities which aim at the disclosure to the public of information, opinions or ideas and protected by the right to freedom of expression, irrespective of the medium which is used to transmit them and of the person transmitting them, i.e. not linking the exceptions and derogations to "journalism" only. Doing so would bring private individuals engaged or claiming to be engaged in informing the public online via blogs, YouTube, Twitter, etc. under the scope of Article 9 of Directive 95/46/EC.

Under this solution, the situation of data subjects would change compared to the current situation. Private individuals who disclose information, opinions or ideas to the public – e.g. through blogs, YouTube or Twitter, protected by the freedom of expression – would be treated the same way like media professionals which process personal data “solely for journalistic purposes or the purpose of artistic or literary expression” and thus have to be exempted by Member States from certain provisions of data protection requirements if necessary to reconcile the right to data protection with the rules governing freedom of expression. In contrast to the current situation following the “Lindqvist” case¹⁴⁹, data subjects would not be able to rely anymore on the full set of data protection rights and remedies against private individuals that process their personal data on the internet accessible by an indefinite number of people. However, these possible exemptions from data protection laws would not deprive data subjects from their right to protection of private life. Data subjects will continue to be able to rely on civil and criminal law remedies developed under national law to enforce their right to private life against private bloggers, twitterers, etc.

8) Benefits for individuals from strengthened DPAs and more consistent enforcement

(See above under 2.1)

9) Strengthened remedies:

a) role of associations

In those cases where an individual is affected by an infringement of data protection rules, a considerable number of other individuals in a similar situation might be equally affected. Actions on behalf of individuals which might be brought by a representative entity (e.g. ombudsman, consumer or civil society association), should encourage beneficial remedies against infringement of the data protection rules, in particular by allowing savings for the parties involved and increasing the efficiency of both judicial and out-of-court redress with the supervisory authorities.¹⁵⁰

¹⁴⁹ ECJ, Case C-101/01, *Bodil Lindqvist*, 6.11.2003, ECR [2003] I-12971.

¹⁵⁰ Consumer organisations (e.g. BEUC, Consumer Focus) and non-governmental organisations (e.g. Privacy International) have expressed strong support for the establishment of collective redress mechanisms, both at

b) strengthened sanctions:

Experience in Member States shows that administrative sanctions, such as fines, serve as an important incentive for controllers and processors for compliance. Individuals could be ensured that a data protection violation would not be sanctioned differently from one Member State to the other. At the same time, further harmonised rules on administrative sanctions would bring about major benefits for controllers and processors as these sanctions for breaches of applicable data protection law within any European jurisdiction would cease to vary depending on the approach taken by the applicable regulator, and thus, provide for more business predictability.

10) Introduce a general obligation for data controllers to demonstrate compliance with data protection law (including through evidence that data subjects' consent was sought and obtained wherever necessary, as well as DP Impact Assessments and Data Protection Officers, where applicable)

Under this option data controllers will be obliged to demonstrate their compliance with data protection rules in cases of audit by data protection authorities. Annex 9 estimates the net administrative burden of this obligation to amount to € 600 million per annum, assuming 100% compliance by data controllers. The need not to impose an undue burden on SMEs is taken duly into account when formulating these obligations, in particular in relation to DPOs and DPIAs, and including in the empowerment of the Commission to adopt delegated acts where the principle of "think small first" is integrated.

a) Additional information obligations

The introduction of mandatory information requirements relating to the quality of information provided to data subjects, as part of the enhanced transparency, will positively strengthen the information of data subjects about the processing of personal data relating to them. This is a pre-condition to give the data subject a say in the processing of personal data, 'ex ante', i.e. prior to processing and for exercising their data protection rights in general.

For controllers, further information requirements can bring significant benefits in terms of accountability and the effective protection of personal data. Though the introduction of further mandatory information requirements for controllers entails an additional administrative burden for data controllers (estimated to be approximately € 180 million per annum in Annex 9, assuming 100% compliance by data controllers), the cost can be justified in terms of enhanced accountability and compliance and should be seen in the context of the drastic reduction of other *ex-ante* controls from DPAs (e.g. simplification of notifications). This additional compliance cost must therefore be balanced with the eliminated costs of notification obligations.

b) More responsibility for processors

New and harmonised provisions which clarify the legal obligations for the processor, irrespective of the obligations laid down in the contract or the legal act with the controller, as well as the application of the "data protection by design" principle, the need for data protection impact assessments in some cases, and an obligation to cooperate with supervisory authorities will bring about benefits for the individual, as this will ensure that outsourcing and delegation by controllers to processors do not result in lowering the standard of data protection.

national and European levels, as an efficient tool for data subject's empowerment and business compliance. The European Economic and Social Committee is equally of the opinion that consideration should be given for business and professional organisations and trade unions to represent individuals and bring an action before courts.

While these measures might entail some initial additional compliance cost for the processors, the cost can be justified in terms of enhanced accountability and compliance, making it easier in the long run for controllers to choose a processor providing sufficient guarantees for processing.

c) DPOs – see detailed assessment in Annex 6

d) DPIAs – see detailed assessment in Annex 6

e) Data protection by design

Data protection by design is a measure aimed at reducing the risks of infringements of the data protection legislation. This would not be a requirement targeting designers and developers but data controllers, which should implement it when defining their data protection and privacy policies, especially but not solely in the field of security. It can be estimated to a few percentage points of the total development cost of the product or service. It shall also be considered that – as confirmed by a recent study conducted by the Ponemon Institute¹⁵¹ - the cost of compliance is much lower than the cost of non compliance. Recent incidents, such as a data breaches that occurred in major companies and where personal data about millions of individuals have been stolen, have shown that the cost of non compliance, or poor compliance are huge. Data protection by design can help reducing such risks and thus be beneficial both to the data controller and the individuals concerned.

No administrative burden would be incurred by either public authorities or data controllers as a result of the introduction of the data protection by design principle.

6.1.6. 2.3. Problem 3: Inconsistencies and gaps in the protection of personal data in the field of police and judicial cooperation in criminal matters

Policy Option 2

11) Extending the scope of data protection rules in the area of police cooperation and judicial cooperation in criminal matters

Measures under this option would have **positive impacts** on data protection in the area of police cooperation and judicial cooperation in criminal matters, both for individuals and law enforcement authorities, as they would entail:

- The elimination of gaps, in particular by the fact of extending the scope of rules also to 'domestic' data processing, thus ending the artificial and unpractical distinction between cross-border and non-cross border data processing. This would be fully in line with Article 16 TFEU;
- The extension of general data protection principles to this area would have a positive impact on the standards of protection, and thus on individuals' data protection rights, in particular by strengthening the rules on right of access, transparency and on purpose limitation;
- Benefits for police and judicial authorities due to more legal certainty and consistency of the rules in this area, which would facilitate exchanges of personal data between authorities of different Member State.

The additional specific safeguards to be put in place will be beneficial to data subjects by giving them additional protection in an area where the processing of personal data may be

¹⁵¹ Study is available here:
http://www.ponemon.org/local/upload/fckjail/generalcontent/16/file/ATC_DPP%20report_FINAL.pdf

more intrusive. The increased harmonisation of the conditions for access to one's own personal data, or the distinction to be made between various categories of data subjects (criminal suspects, victims, witnesses, etc.) would strengthen data subjects' legal position vis-à-vis police authorities.

This would have some, but limited impact on police and criminal authorities in the Member States: today's data protection principles, in particular the principle of data quality but also the principle of necessity and the principle of proportionality, already require a controller to distinguish between different categories of data subjects, as this is relevant inter alia for the use and storage of that data. In the police sector, the distinction between a suspect of a criminal activity and a non-suspect comes particular to mind as well as a data classification between verified and unverified information.

Moreover, the exemptions and limitations foreseen to the rights of the data subject (of information, access etc) allow taking into account the specific needs of law enforcement authorities, in line with Declaration N° 21.

As regards international transfers, the increased harmonised approach would provide additional legal certainty for both individuals and competent authorities, which is currently lacking¹⁵².

Additional obligations upon competent authorities – such as the appointment of a DPO – have been tailored to the nature of the activities of such authorities and are proportionate to the objective pursued, i.e. to ensure a high level of data protection, without hindering police activities. As regards the DPO, this function can easily be performed at central level (central police authority) and is not meant to impose an undue burden on each police office/department.

12) Addressing fragmentation

The increased harmonisation of the rules and the extension of the scope of the Framework Decision, as described above, would also reduce fragmentation and increase legal certainty in this area for both individuals and competent authorities. A certain degree of fragmentation would nevertheless remain as the other "former third pillar instruments" are not specifically amended. This would, however, be counterbalanced by the evaluation to be carried by the Commission that would help identifying any possible incompatibility and propose amendments where necessary.

6.1.7. 3. POLICY OPTION 3: DETAILED LEGAL RULES AT EU LEVEL

6.1.8. 3.1. *Problem 1: Barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement*

1) **Increasing harmonisation - Detailed rules for specific sectors (e.g., employment, health, scientific and historical research)**

By providing for further harmonisation of rules for specific sectors (health/medical and employment) the internal market dimension would be further improved and the free flow of data would be favoured, with more legal certainty and reduced costs for data controllers, currently exposed to different requirements.

However, a high level of detail and sectoral specificity would increase the risk of the rules becoming outdated and ineffective very quickly in view of rapid technological and economic development, so that frequent revisions of the instrument would be required to maintain the effectiveness of the provisions. An approach allowing for more flexible adaptations, e.g. by implementing acts, could be much more beneficial.

2) **Abolition of the notification requirements**

¹⁵² See the Implementation report of the Framework Decision (COM...)

The abolition of the general notification obligations for data controllers would entail a significant reduction of the current administrative burden for data controllers - particularly those operating cross-border and hence incurring the cost of notifications in more than one Member State - and would simplify the regulatory environment, without having a negative impact in terms of the protection of data subjects, given its limited added value in that respect. Annex 9 estimates the cost to data controllers to be EUR 200 *per notification*. It is estimated that there are approximately 650,000 notifications in the EU per year, therefore resulting in an approximate cost of € 130 million per annum, incurred by data controllers. The abolition of notifications would therefore eliminate these costs, as well as the costs linked to notification fees (not included in the calculation of the administrative burden).

There is an almost unanimous support from stakeholders – particularly economic operators - for radically simplifying the current system and, in some cases, for abolishing notifications altogether.

This change would have, however, a negative impact on those DPAs that are funded by the fees to be paid when notifying a data processing¹⁵³.

3) Development of an EU-wide certification/standardisation scheme (privacy seal)

Such a measure could be beneficial for both controllers, in the EU and in 3rd countries, as it could make their compliance more 'visible', and for individuals, who would be reassured that their data are effectively protected.

However, the cost of certifying products by third parties is high. For instance, in the existing voluntary certification program Europrise, the cost of certifying a single product or service varies from 10 man days of work of a data protection expert, for a very simple product to up to 100 man days of work for complex products or services. Therefore, making a standardisation scheme mandatory of all processing would have a significant cost, superior to the existing compliance costs.

4) Setting up of a central EU Data Protection Authority (via a new EU agency) responsible for the supervision of all data processing with an internal market dimension or with an effect on the European area of freedom, security and justice

Enforcement would be considerably improved thanks to the setting up of a pan-European Authority /regulatory Agency competent to issue binding decisions on Member States. This option would, however, entail significant costs for the EU budget.

Examining other institutional bodies with a similar mandate and objective in order to identify comparison benchmarks, reveals that an EU regulatory Agency would require a substantial budget allocation, within the range of EUR 7-15 million. In the current economic climate, such an economic burden is not likely to be welcome by Member States or the European Parliament.

Indicatively:

- The overall 2011 budget for the European Data Protection Supervisor (EDPS) amounts to EUR 7,6 million
- For the EU Fundamental Rights Agency (FRA) the 2008 budget amounted to EUR 15 million (and is expected to reach up to EUR 22 million by 2013) and

¹⁵³ This concerns, in particular, the UK DPA (ICO), for which notifications represent currently by large the main source of funding. They consider that a fee-based funding model for DPA is the most suitable to ensure the actual independence of the DPA from the Government.

- For the European Network and Information Security Agency, EUR 8,1 million for 2011.

In addition, this could be against EU law as an Agency cannot exercise genuine discretionary powers.

5) Establishing minimum rules with regard to the definition of criminal offences and sanctions in the area of personal data protection

EU minimum rules with regard to the definition of criminal offences and sanctions in the area of personal data protection, to be implemented by Member States, would foster the confidence of individuals as regards the processing of their personal data through a more efficient fight against crimes involving personal data. Such rules would also lessen the incentive and possibility for criminal controllers or processors to choose the Member State with the most lenient legal system as a certain approximation of the national laws prevents the existence of such "safer havens". Additionally, common rules strengthen mutual trust between the supervisory authorities, and judiciaries of the Member States. This facilitates cooperation and mutual recognition of judicial measures. On the other side, criminal investigations and sanctions may have a significant impact on individuals' rights and have a 'stigmatising' effect. However, this would be a very far-reaching measure – to be based on a specific legal basis (Article 83 TFEU) – that would encounter strong resistance from Member States.

6.1.9. 3.2. Problem 2: Difficulties for individuals to stay in control of their personal data

6) Extension of categories of sensitive data to: children, biometric and financial data

The extension of special categories of “sensitive data” to those relating to biometric identifiers and of financial data, coupled with detailed rules on when processing would be lawful, would vigorously improve the level of protection for those data and this option would have a very high positive impact. In relation to the rights of the child, this option would increase the protection of children.

Inclusion of financial data would be more controversial given its impact on the financial sector, whose processing would have to be generally adapted to the new data protection requirements.

7) Introduction of specific provisions on online identifiers and geo-location data

Under this PO specific Articles would regulate a specific regime for online identifiers and geo-location data. While this could have the advantage of allowing for more flexibility, it would affect the technological neutrality of the Directive, which would risk of becoming rapidly obsolete.

8) Making (explicit) consent as the primary legal ground for processing

This measure would sensibly change the current model in the Directive, based on six different grounds for processing and where consent does not have a primary role but is just one of them. This could be justified given that Article 8 of the Charter explicitly mentions only "consent" (and not other legal grounds).

However, this would create a very rigid system which would be both very costly for data controllers to use – as they would be obliged to base their processing more often on consent, and be able to prove it - and not necessarily in the interest of individuals. An 'abuse' of consent as a legal ground for processing can, on the contrary, rather lead to a much poorer quality of it.

9) Specific thresholds and criteria for notifying data breaches to data subjects

This measure would provide more legal certainty for data controllers. However, it would risk being rejected by stakeholders if not based on sound evidence and analysis of the implementation of existing legislation. Reports and studies are being prepared on the implementation of the e-Privacy Directive, which could be used to define specific obligations consistently across all sectors.

10) Collective redress

Where breaches of EU law (and in particular, data protection law) harm a large group of individuals and businesses, individual legal actions are often not an effective means to stop unlawful practices or to obtain compensation for the harm caused by these practices: individuals and businesses are often reluctant to initiate private lawsuits against unlawful practices, in particular if the individual loss is small in comparison to the costs of litigation. As a result, continued illegal practices cause significant aggregate loss to individuals and businesses. In addition, as acknowledged by the Digital Agenda for Europe, enforcement of EU Law in the Digital Environment appears sometimes to be difficult because of the lack of clarity on the applicable rights especially for consumers. Uncertainty and perceived difficulty to access redress is one important factor undermining confidence and thus constitutes an obstacle to the development of cross-border electronic commerce. Moreover, where breaches of EU law do trigger multiple individual lawsuits, the procedural laws of many Member States often leave the courts ill-equipped to deal with the case load efficiently and within reasonable delay. This can be true for injunctive collective redress, but in particular for claims to obtain compensation. For these reasons, mechanisms of collective redress are being considered in order to remedy the current shortcomings in the enforcement of EU law¹⁵⁴.

Not only are collective actions important for ensuring full compensation or other remedial action; they also perform indirectly a deterrence enhancing function. The risk of incurring expensive collective damages in such actions would multiply the controllers' incentives to effectively ensure compliance. In this regard, an enhanced private enforcement by means of collective redress mechanisms would complement public enforcement.¹⁵⁵

Nonetheless, given that the Commission has conducted a wide public consultation on the issue of collective redress¹⁵⁶ in order to explore policy options for a coherent European approach and consider possible further action, it would not be prudent to pre-emptively introduce provisions relating to collective redress in the data protection reform package.

6.1.10. 3.3. Problem 3: Inconsistencies and gaps in the protection of personal data in the field of police and judicial cooperation in criminal matters

11) More prescriptive and stringent rules

The fact of providing for very prescriptive rules (i.e. imposing direct access) would not take into account the need to leave some flexibility to Member States in an area which remains

¹⁵⁴ From Commission Staff Working Document "Towards a Coherent European Approach to Collective Redress" (SEC(2011)173 final), available at http://ec.europa.eu/justice/news/consulting_public/0054/sec_2011_173_en.pdf

¹⁵⁵ This innovation is also supported by the Data Protection Authorities in the WP document on the Future of Privacy (op cit). And the EDPS in his opinion on the Commission's Communication COM (2010) 609 final, OJ C 181, 22.6.2011, p.1

¹⁵⁶ http://ec.europa.eu/justice/news/consulting_public/news_consulting_0054_en.htm

sensitive. Including biometrics amongst the sensitive data would also be disproportionate given the needs of law enforcement authorities to use fingerprints etc in their routine work. Equally, carrying out a DPIA – even if only for processing of data into large scale systems, when the processing is likely to be risky - would impose a disproportionate obligation upon police and other law enforcement authorities – who already act under the legality principle – and could hinder the performance of their tasks.

12) Maximum coherence and consistency of the rules in the former third pillar

In addition to measures foreseen in Policy Option 2 - which are highly beneficial to individuals and enhance data protection in this area – under this policy option consistency and coherence of the rules would be maximised by amending other ex-third pillar instruments, to the extent that they would be incompatible with the new rules.

This would, however, have an important impact on existing forms of (police and judicial cooperation) as regulated in the specific instruments that would be affected and should not be attempted without serious evaluation.



ANNEX 6

DETAILED ASSESSMENT OF IMPACTS OF THE INTRODUCTION OF DATA PROTECTION OFFICERS (DPOs) AND DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

7.

Introduction

A central objective of the data protection reform package is to increase the effectiveness of data protection rights, by enhancing the responsibility and accountability of data controllers. Two particular measures included in the preferred policy option which aim to achieve this objective are the introduction of Data Protection Officers (DPOs) and Data Protection Impact Assessments (DPIAs).

This Annex provides a detailed analysis of the expected impacts of new provisions on DPOs and DPIAs. In general terms, the two proposed changes are expected to have some economic impacts on data controllers, particularly in terms of compliance costs. For this reason, in the course of the public consultation some stakeholders were opposed to the introduction of such obligations. However, while it may be easy to overestimate the potentially negative cost-related impacts of these measures, the benefits they can portend if a targeted, threshold-based approach is adopted, should not be overlooked.

Data Protection Officers

○ *Background*

The designation of data protection officers is an issue on which several stakeholders have provided input in the context of the public consultation, some highlighting potentially negative impacts in terms of compliance costs.

Some of the stakeholder responses raised questions as to which type or size of organisation would have to designate a data protection officer. Germany already mandates a DPO for organisations with more than 10 employees. Existing studies point to the fact that larger corporations, especially multinationals, usually already have data protection officers. The same is true for many public data controllers in a number of Member States. The evidence from the German example is that introduction of DPOs has been successful, due to the development of best practices in specific sectors and the streamlining of administrative costs due to exemptions from centralised notification requirements.

Some stakeholders argued that the requirement to designate DPOs should not be extended to SMEs because of the costs that would be incurred. Others argued that if DPOs were mandated, then concessions should be made, specifically to exempt data controllers from some reporting obligations.

Furthermore, it can be expected that some organisations, perhaps a majority, will use existing staff to perform the function of a DPO; they will not recruit additional staff, rather they will assign an additional responsibility to an existing staff member, especially where they believe that the DPO function will not require a full-time, dedicated staff member. Yet other

organisations may not seek to designate a DPO to their respective organisations; instead, they will seek to draw on independent DPOs who provide services various clients. External contracting of work related to the responsibilities of a DPO, while still incurring some costs, might reduce labour and compliance burdens overall.

o ***Envisaged measures in Policy Option 2***

Policy Option 2 envisages the introduction of the mandatory appointment of Data Protection Officers (DPOs) for public authorities, for companies above 250 employees and those whose core business involves risky processing. Conditions would be set to ensure the independence of the DPO from the data controller as regards the performance of his/her duties and tasks.

It will also be clarified that where the controller or processor is a public authority or body the DPO can be appointed for several of its entities, taking account of the organisational structure of the public authority or body. Even in cases where a DPO is not required, a register on data processing activities should be kept by the data controller.

It is a reasonable assumption that, as with other professionally provided services, such as accounting, general legal advice etc., a rate of € 250 per hour will be an EU average in terms of employing external contractors to perform DPO-related compliance activities.

As such it is envisaged that most data controllers – other than larger organisations better equipped or already having a substantive expenditure on DPOs or employees performing such duties as part of the normal terms of their employment – will make use of a mixture of means to ensure compliance with compulsory aspects of the proposed changes to the data protection regulatory framework in the EU.

These elements could be:

1. Use of existing staff, with training, to perform duties and responsibilities envisaged for DPOs.
2. Use of external contractors to perform these duties and responsibilities.
3. Hiring new staff to perform these duties and responsibilities.

The same considerations would apply for the public sector, especially considering that Policy Option 2 allows the flexibility of appointing one DPO for several entities within the same organisational structure.

The benefits of having either a DPO or some element which will perform the duties and responsibilities for the DPO in a data controller can be assumed to be the following:

1. Protecting the rights of data subjects and being a conduit between the data controller and data subjects
2. Reducing compliance and administrative costs
3. Reducing losses associated with data breaches

According to Commission Recommendation 2003/361/EC, enterprises are distinguished by size according to the following specific criteria:

Category	Employees	Turnover- or	Balance Sheet Total
Medium sized	<250	< €50 million	< €43 million
Small	<50	< €10 million	< €10 million
Micro	<10	< €2 million	< €2 million

Eurostat figures indicate that the majority of EU enterprises are small and micro sized enterprises.¹⁵⁷

	Total	SMEs	Micros	Small	Medium	Large
Number, millions	19.65	19.60	18.04	1.35	.21	.04
% of total	100.0	99.8	91.8	6.9	1.1	0.2

○ *Sub-options as regards the designation of Data Protection Officers*

- - For **public data controllers**: a general obligation to designate a DPO, without exceptions, but with flexibility allowing the appointment of the same DPO for several entities under the same organisational structure.
 - For **private sector** data controllers, three sub-options are considered:
 - a. SUB-OPTION 1: DPOs should be designated when processing is carried out by large enterprises (more than 250 employees) and when processing is likely to present specific risks to the rights and freedoms of data subjects; **OR**
 - b. SUB-OPTION 2: DPOs should be designated when the processing is likely to present specific risks to the rights and freedoms of data subjects); **OR**
 - c. SUB-OPTION 3: DPOs should be optional, while providing incentives to data controllers that do designate a DPO in terms of the supervision they undergo by national authorities.

○ *Expected impacts*

The compulsory requirement to designate a DPO for public authorities would entail a cost for **Member States' public authorities**. It is difficult to estimate such costs given that many public authorities already have DPOs (this varies between Member States) and that organisational structure and data processing varies between public authorities. Moreover, it would be reasonable to expect that the role of DPO would be assumed by existing civil servants in public authorities, who will be suitably trained to perform the function, and that no additional staff would need to be recruited. Additionally, the fact that it is possible to appoint a DPO for several entities of a public administration will limit the burden even further. Therefore it can be expected that the financial cost of introducing this obligation would not be disproportionate to the risks involved in the processing of personal data by public authorities.

As regards the private sector, the impacts of each sub-option are expected to be the following:

¹⁵⁷ Eurostat 2008 figures, available at http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-08-031/EN/KS-SF-08-031-EN.pdf

For Sub-Option 1:

- The exclusion of economic operators with less than 250 employees (i.e. excluding all SMEs and micro enterprises) is intended to facilitate the business environment for comparatively smaller operators by reducing the burden of data protection compliance costs.
- Exempting micro, small and medium sized enterprises from the provisions would exclude 99.8% of EU enterprises.
- In some specific instances enterprises of this size might however be reasonably assumed to fall under the provisions of this requirement, where the processing might present specific risks to the rights and freedoms of data subjects. These might include, for instance:
 1. High-tech start-up enterprises working in particular fields, e.g. health.
 2. Enterprises whose processing of personal data involves an evaluation of personal aspects relating to the data subject, including his or her ability, efficiency and conduct;
 3. Enterprises processing children's, genetic, biometric, financial or location data
 4. Enterprises processing data obtained from video surveillance

In Sub-Options 2 and 3 it can be assumed that in most cases the larger enterprises' DPO would have a role in ensuring compliance with sub-contractors. Assuming that 100% of large enterprises will be data controllers, this would entail 40,000 large size enterprises having to designate a DPO. It is reasonable to assume that the vast majority of large organisations processing personal data already have employees with the responsibilities to perform the duties of DPOs. From stakeholder feedback during the impact assessment study the total labour cost associated with recruiting an additional employee as a full-time DPO was estimated at €80,000 per annum.

Number of large enterprises involved	40,000
% Rate of DPO designation	100%
DPO required	40,000
Total Labour Cost	€3.2 billion (per annum)

This table assumes that all large enterprises will have to designate a DPO. This would entail a total annual cost of €3.2 billion. However, this probably significantly overstates the outcome since many enterprises of this size already comply with current data protection regulations. That being the case, it would be reasonable to assume that a majority already have DPOs or related staff performing similar duties.

Number of large enterprises involved	40,000
% Rate of DPO designation	10%
DPO required	4,000
Total labour cost	€320 million (per annum)

This table assumes that 90 per cent of large enterprises already have staff performing comparable duties. For 10 per cent of enterprises requiring DPOs, the total labour cost would be €320 million (per annum). However, it would be reasonable to assume that, given the size

of these enterprises, some of this cost would be reduced by re-training and re-skilling existing employees. It is impossible, however, to determine this with any degree of certainty.

Similar considerations apply in the case of enterprises processing personal data falling under categories 1-6 above, as it would be impossible to determine the number of enterprises that process those types of data reliable certainty. Some estimates based on simplifying assumptions are however made below.

In the following tables, it is assumed that

- SMEs and micro-sized enterprises will either train and certify existing staff in performing routine data protection tasks, or recruit external contractors for that purpose;
- Only 50% of SMEs and micro enterprises will be data controllers;
- External contractors charge similar rates to legal validation rates, which have been determined from stakeholder feedback to be €250 per hour;
- Checking compliance in processing operations which are likely to present specific risks will take four hours on average for all enterprises.

Number of enterprises by size	Micro: 9,020,000	Small: 675,000	Medium: 105,000	Totals
% of data controllers	0.001	0.001	0.001	
Number of data controllers	9,020	675	105	9800
Risky processing operations, annual number of times	1	1	1	3
External contractor hours required	4	4	4	12
Total charges	€1,000	€1000	€1000	€3,000
Total costs for data controllers	€9,020,000	€675,000	€105,000	€9,800,000

This table illustrates that if 0.001% of small and medium-sized enterprises who are data controllers require validation in terms of processing risky data, the total cost for each data controller would be €1,000 with a total cost across the EU of €9,800,000 (per annum).

In examining these figures, it is arguable that the costs are broadly in line with other external costs facing small and micro-sized enterprises such as accountancy or IT related fees.

Data Protection Impact Assessments

○ Background

The obligation for data controllers to carry out a DPIA when processing operations are likely to present specific risks to the rights and freedoms of data subjects will entail some additional compliance costs (in terms of conducting the DPIA) and administrative burden (in terms of providing the information to public authorities about the DPIA).

DPIAs, however, have the potential to simplify data protection processes for data controllers in the medium- to long-term by ensuring effective compliance with data protection rules. Recent experience in DPIAs in several Member States and internationally has shown that this

procedure has beneficial effects in terms of rationalising and streamlining processing operations, and closes potential gaps in compliance and security.

A DPIA can help in identifying and managing data protection risks, avoiding unnecessary costs (in terms of problems being discovered at a later stage), avoiding inadequate data-processing solutions, improving the security of personal data and most importantly for an economic operator, avoiding the loss of trust and reputation.

While labour costs for some categories of data controllers might not increase due to employees with relevant skills and responsibilities already being in place, with regard to DPIAs, it can be assumed that a broader range of stakeholders will incur resource costs. While in some Member States, such as the UK, the use of Privacy Impact Assessments (PIAs) in government departments and agencies is growing, most Member States and the vast majority of data controllers have yet to use PIAs or DPIAs. Estimating potential costs for DPIAs is dependent on a number of contextual factors.

In theory, if a new project, technology, service, product or any scheme involves the collection and/or processing of personal data, a DPIA (or, better still, a PIA) would ideally be carried out. The scale and rigour of the DPIA will depend on how an organisation perceives the risks and the seriousness with which it tackles those risks. If the risks are regarded as minimal or negligible, then a small-scale DPIA may be conducted. If the organisation perceives significant risks, then it would be advisable to opt for a full-scale DPIA, one that engages stakeholders, with the aim of identifying all possible risks, assessing those risks and devising strategies to avoid or mitigate those risks.

The reporting costs of a DPIA would be the least costly part of a DPIA – the real costs will be in determining whether a DPIA should be conducted, gathering information about the project, deciding whether to engage stakeholders (internal and/or external to the organisation), identifying the risks, assessing the risks, identifying options for avoiding or mitigating the risks and only then preparing a DPIA report, making recommendations, following up on those recommendations to ensure they are actually implemented. There may be additional costs if an external assessor is brought in to conduct the DPIA. Engaging stakeholders could take several forms – e.g. an online consultation, briefing meetings, working groups, face-to-face interviews, etc. Even if a DPIA is conducted without resorting to external stakeholders, usually there will be several internal stakeholders involved, e.g. legal staff, project staff, operational staff, procurement staff, perhaps HR staff, the public relations department, risk managers, internal audit staff, etc. The amount of time consumed by a DPIA (or PIA) would depend on how serious the privacy (or data protection) risks are estimated to be, but it could escalate considerably.

○ ***Benefits of conducting a DPIA***

Several benefits can be identified for conducting a DPIA¹⁵⁸:

- A company (or government department) that undertakes a PIA with good intent, with a genuine interest in engaging stakeholders, including the public, has an opportunity to earn trust and good will from individuals-consumers. Businesses able to sustain a high

¹⁵⁸ The benefits listed here have been extracted from Wright, David, and Paul de Hert, “Introduction to privacy impact assessment”, Chapter 1, in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2011 [forthcoming]. The book discusses PIA, rather than a more narrowly scoped DPIA, but the benefits of a DPIA will be broadly the same.

level of trust and confidence can differentiate themselves from their rivals and thereby gain a competitive advantage.

- If the project does raise difficult issues with regard to data protection, ideas from stakeholders may be particularly welcome. Even if stakeholders do not manage to generate some new considerations, the organisation at least has an opportunity of gaining stakeholders' understanding and respect.
- Transparency in the process may also be a way of avoiding liabilities downstream. If the organisation is able to demonstrate that it did engage and consult with a wide range of stakeholders, was forthcoming with information, considered different points of view, it will be more difficult for some stakeholders to claim subsequently that the organisation was negligent in its undertaking. By being open and transparent from the outset, the organisation can minimise the risk of negative media attention.
- The New Zealand PIA Handbook describes a privacy impact assessment as an “early warning system”. The PIA 'radar screen' can enable an organisation to spot a privacy problem and take effective counter-measures before that problem strikes the business as a privacy crisis. It goes on to say that the PIA process can help the organisation by providing credible information upon which business decisions can be based and by enabling organisations to identify and deal with their own problems internally and proactively rather than awaiting customer complaints, external intervention or a bad press.
- PIA is a form of risk assessment, an integral part of risk management. It encourages cost-effective solutions, since it is more cost-effective and efficient to build “privacy by design” into projects, policies, technologies and other such initiatives at the design phase than attempt a more costly retrofit after a technology is deployed or a policy promulgated. A PIA creates an opportunity for organisations to anticipate and address the likely impacts of new initiatives, to foresee problems and identify what needs to be done to design in features that minimise any impact on privacy and/or to find less privacy-intrusive alternatives.
- A PIA should also be regarded as a learning experience, for both the organisation that undertakes the PIA as well as the stakeholders who are engaged in the process. An open PIA process helps the public understand what information the organisation is collecting, why the information is being collected, how the information will be used and shared, how the information may be accessed, and how it will be securely stored. The PIA's educational role is a way of demonstrating that the organisation has critically analysed how the project will deal with personal data. It might be the case that certain identified risks on privacy cannot be mitigated and/or have to be accepted (residual risks); even so, the PIA report, as the result of a clear and systematic process, is something to which interested parties can refer and be informed of the reasons why some assumptions were made and decisions taken. Thus, a PIA promotes a more fully informed decision-making process.

- *Expected economic impacts and case studies*

As a one-off cost which might be significant, some organisations, especially smaller ones, might view the obligation to conduct a DPIA with concern. However, privacy impact assessments are a growing component of some organisations' strategic thinking and risk planning in relation to the development of new products and services. Even without a

provision about DPIA in the new data protection framework, this trend will continue. The recently approved RFID PIA Framework provides evidence of this.

The first example below illustrates the indicative estimated costs of a small-scale DPIA:

Example 1: Small scale DPIA DataStore: Commercial and innovative uses of sensitive data

As part of the development of its marketing operations, DataStore has purchased behavioural advertising software program from a non-EU vendor. The system integrates with DataStore’s consumer databases and those of other online service providers to target DataStore advertising at individuals who visit the DataStore website. Customers will be sent an initial sign-up e-mail explaining the data processing procedures and asking for consent.

After consulting with relevant regulatory authorities, DataStore recognises that it needs to conduct a DPIA. The DPIA includes a reporting obligation to consumers and to the relevant regulatory authority.

DPIA components	Costs in euros	Totals in euros
Labour	€450 x 20 days	€9,000
IT	€1,000	€1,000
Stakeholder engagement	€1,500	€1,500
Auditing	€2,500	€2,500
Total		€14,000

The example above focuses on a small number of impacted data subjects utilising a new product offering in one Member State, involving the automatic processing of personal data. The assumptions made in this example are as follows:

1. The DPIA takes 20 days to complete at a rate of €450 per day.¹⁵⁹
2. The data controller conducts a limited exercise with stakeholders – in this example, one focus group (€1,000) and an online consultation exercise (€500).
3. There are IT-related costs of €1,000 to analyse the feedback and data generated during the course of the DPIA. This also includes any costs associated with disseminating the results of the DPIA.
4. 10 hours of legal validation are needed to audit the results of the DPIA prior to any reporting obligations or notifications.

The second example below focuses on a medium-scale DPIA:

¹⁵⁹ This labour rate is the EU figure for external consultations. Conducting a DPIA is assumed to be a comparable exercise in terms of labour expertise, like other consultation and research exercises. One can expect some divergences in costs in Member States.

Example 2: LocNav: Location based data and services

LocNav is a small regional operator offering satellite navigation services in a number of member states. It plans to implement product and service offerings with local businesses as part of its SatNav feature set. The service will advertise particular retail and other amenities for users of the system if asked to do so in planning a trip by data subjects.

It decides to carry out a DPIA to assess any potential risks to privacy and to assess the best way of maintaining compliance with data protection regulations.

DPIA components	Costs in euros	Totals in euros
Labour	€450 x 40 days	18,000
IT	€1,500	1,500
Stakeholder engagement	€10,000	10,000
Auditing	€2,500	5,000
Total		€34,500

The assumptions made in this example are as follows:

1. The DPIA takes 40 days to complete at a rate of €450 per day.¹⁶⁰
2. The data controller engages stakeholders via a series of eight focus groups (€8,000) and an extended online consultation exercise (€2,000).
3. There are IT-related costs of €1,500 to analyse feedback and data generated during the course of the DPIA. This also includes any costs associated with disseminating the results of the DPIA.
4. 10 hours of legal validation are needed to audit the results of the DPIA prior to any reporting obligations or notification.

The third example below illustrates a large-scale DPIA.

Example 3: Security and biometrics

In compliance with national legislation, a law enforcement data controller has implemented a biometric recognition system utilising airport-based CCTV systems which identify wanted suspects and suspicious behaviour in public spaces.

After consulting with the relevant national data protection authority, the data controller agreed that a DPIA should be carried out. In reporting the results of the DPIA, the DPO agreed to make the results public via governmental websites.

¹⁶⁰ As stated above, this labour rate is the EU figure for external consultations.

DPIA components	Costs in euros	Totals in euros
Labour	€450 x 60 days x 5 Experts	€135,000
IT	€1,500	€1,500
Stakeholder engagement	€10,000	€10,000
Auditing	€2,500	€2,500
Total		€149,000 ¹⁶¹

The assumptions made in this example are as follows:

1. The DPIA takes 60 days to complete and involves five experts at a rate of €450.¹⁶²
2. The data controller engages stakeholders via eight focus groups (at a cost of €8,000) and an extended online consultation (€2,000).
3. There are IT-related costs of €1,500 to analyse feedback and data generated during the course of the DPIA. This also includes any costs associated with disseminating the results of the DPIA.
4. 10 hours of legal validation are needed to audit the results of the DPIA prior to any reporting obligations or notifications.

Estimating the administrative costs associated with DPIAs is a difficult task as the nature of DPIAs in and of themselves will be very context-specific to the size of enterprise needing to undertake one and the specific nature of the project or technology or service or other scheme for which the DPIA is to be conducted. Likewise, the main bulk of costs associated with a DPIA will arguably not be linked with the reporting obligations of proposed changes; rather the main body of costs will be in the consultation and identifying, assessing and mitigating risks as well as the actual work of conducting the DPIA itself.

¹⁶¹ This figure also corresponds to stakeholder feedback for a large multi-national as to expected costs in conducting a privacy impact assessment.

¹⁶² This labour rate is the EU figure for external consultations.

ANNEX 7

ANALYSIS OF THE IMPACTS OF POLICY OPTIONS ON FUNDAMENTAL RIGHTS

1. POLICY OPTION 1: SOFT ACTION

This option would have positive impacts for the *protection of personal data and privacy* by clarifying and promoting the conditions for exercising the existing data subject's rights:

- interpretative communications and explicit references to the transparency and data minimisation principles would increase legal certainty also in relation to data subjects' rights ;
- non-legislative measures would enhance the effectiveness of individuals' rights, in particular by awareness-raising and promoting Privacy Enhancing Technologies and voluntary privacy certification schemes, which would support the application of data protection principles.

However this positive impact will remain limited, as it aims to make the application of the existing data subjects' rights more effective, but without adding substantial changes as regards these rights and their enforcement.

This option will also have a positive impact in relation to the *rights of the child* as clearer information policy and promotion of awareness-raising will contribute to the protection of children.

2. POLICY OPTION 2: MODERNISED LEGAL FRAMEWORK

This option has a very positive impact on the *protection of personal data* in all its dimensions. In particular the clarification of the role and conditions of consent will enhance the data subjects' control over their data. Data subjects' rights would be significantly strengthened by a detailed set of rules on the data subject rights, which comprises in particular additional information obligations for controllers towards the data subject, as a general precondition for exercising the rights in relation to data protection. Specific rights such as the right for deletion will be strengthened and clarified ("right to be forgotten"). Rules on the modalities will facilitate the data subject's exercising their rights. The specific safeguards on the protection of 'sensitive' personal data will be extended to genetic data.

A range of further new and clarified elements would reinforce the effectiveness of the right to protection of personal data: reducing the fragmentation and increasing legal certainty by more detailed rules in the legal instrument and implementing acts and strengthened cooperation between Data Protection Authorities would considerably help to ensure the same level of data protection and the consistent implementation of the right to data protection in all MS and towards non EU-controllers and the effectiveness of enforcement.

The right to *respect for private life* would be equally strengthened by the measures to enhance the protection of individuals' personal data, but also, in addition, as regards the clarification of the exemption of purely private activities from the application of the data protection rules.

The clarification of the rules on 'sensitive' data and its extension to genetic data would also enhance *non-discrimination*.

The clarification of the application of rules for children will have a further positive impact on the *rights of the child*.

The relation of data protection rules to the *freedom of expression and information* will be clarified for the media, but also for private persons, who (e.g. as bloggers) make personal data of other accessible for an indefinite number of individuals.

As regards the *freedom to conduct a business* there would be, on the one hand, positive impacts by reducing fragmentation, enhancing legal certainty and simplification (such as by reducing the notification requirement). - On the other hand; this option contains also elements which could impact the *freedom to conduct a business* negatively. New specific requirements and uniform rules (e.g. introduction of Data Protection Impact Assessments, reinforced data subject rights, particularly when using Internet) could limit to a certain extent freedom to conduct business. However, such limitation does not seem disproportionate, taking account the positive impacts. This is in particular the case for the appointment of Data Protection Officers, which will be entrusted with tasks which would otherwise be carried out by other means, in order to comply with the data protection rules.

The protection of *intellectual property rights* is not impacted by reinforced protection of data subject rights.

This option would have also a positive impact on *health care*, as more uniform rules will be established for the exceptions to the processing of sensitive data, in particular those concerning health data.

The *right to an effective remedy* will be reinforced by providing access to the courts not only to the individual or controller or processor concerned, but also by providing the right for associations to bring an action before the court on behalf of individuals. Also the right of DPAs to engage in legal proceedings would be clarified.

3. POLICY OPTION 3: DETAILED LEGAL RULES AT EU LEVEL

As regards *the protection of personal data and privacy* this option would have a very high positive impact. On top of the very positive impact of the measures provided by Policy Option 2, the data subjects' rights and legal certainty would be further strengthened by detailed harmonisation in all policy fields.

On *freedom to conduct a business*, this option would have a similar impact as Policy Option 2.

In relation to *health care*, there would be an increased positive impact as there would be more detailed harmonised rules on data protection in the health and medical sector.

As regards *freedom of expression* and the *protection of Intellectual property rights* there would be no additional measures, meaning that the impact would be the same impact as in Policy Option 2. There would be a higher positive impact on *the right to an effective remedy and to a fair trial* thanks to the introduction of collective actions in this area.

ANNEX 8

CONSULTATION OF SMEs

INTRODUCTION

SME panel consultations are regularly conducted through the Enterprise Europe Network, which is managed by DG Enterprise and Industry. SMEs in EU Member States are contacted by the regional associations that constitute the Enterprise Europe Network. Participation in the consultations is voluntary.

In the context of this impact assessment, the SME panel was utilised in order to consult SMEs on the data protection obligations in the baseline scenario. 383 responses were submitted to the consultation.

SUMMARY OF MAIN FINDINGS

The main findings of the SME consultation are the following:

2.1. Notifications to DPAs

Nearly one third of the participants (29.2%) stated that they notify processing of personal data to DPAs. Another third of respondents (33.2%) stated that their data processing does not need to be notified. The remainder either stated that they do not process any personal data (21.7%) or responded "I don't know / not applicable" (14.4%).

Generally, SMEs responded that they do not find these notifications particularly difficult, but many find them bureaucratic (30%), even if they do not notify themselves.

Regarding the financial impact of these declarations, about 30% of those providing an estimate of costs considered them to be higher than €500, while about 40% estimated them at less than €100 and 22% between €100 and €300. However, given that 21.5% of consulted stakeholders did not provide any estimate and most respondents either did not answer this question or chose "I don't know / not applicable", these financial estimates concern only a very limited subset of the panel.

2.2. Privacy Policies on SME Websites

A high percentage of respondents (42.8%) indicated that their privacy policy does not appear on their website. Slightly fewer respondents (36.8%) stated that their website does include a privacy policy.

2.3. Data Protection Officers

Almost half of respondents have some type of Data Protection Officer, although only few (6%) stated that they employ a person to deal with data protection issues full-time, whereas most of these respondents (40%) stated that someone does it alongside other activities.

A smaller share of respondents (38.1%) stated that there is no person formally assigned in their SME to deal with data protection issues and the remainder responded "I don't know / not applicable".

2.4. Information to data subjects and its financial impacts

Nearly half (48.6%) of the SMEs have been providing information to data subjects, as required by data protection laws, but only 27.4% of responding SMEs always provide this

information. More than 21% of respondents stated that they never provide such information and 25% responded "I don't know / not applicable".

The financial impact of information to data subjects appears to be relatively low, since 16.2% of respondents indicated costs of less than €100 and only about 12% of the respondents indicated costs exceeding €100 (3.7% indicated costs exceeding €300 and another 3.7% indicated costs exceeding €500). The majority of respondents (70%) answered "I don't know / not applicable".

2.5. Access of data subjects to their personal data

The majority of SMEs consulted stated that they have never received requests from data subjects to access their data (53.8%). Only a minority declare having received such requests (about 19.3% rarely and 6.5% frequently).

Regarding the time needed for the SMEs to respond, only 19.1% are able to roughly quantify it, most of those (11.5% of total respondents) indicated that it requires less than 1 day of work.

Only very few stakeholders (2.6%) charge a fee for this access. These fees are generally between €10 and €50 with only one respondent (0.3%) charging more than €100.

54% of SMEs do not charge a fee for such requests and 32% answered "I don't know / not applicable".

2.6. SMEs and legal advice on data protection

Most of the consulted SMEs (54.3%) have never sought paid legal advice on data protection issues, whereas 20.4% responded that they have.

Only 16.5% of respondents were able to indicate the costs of obtaining these services. These appear to vary somewhat, with 3.7% of respondents indicating expenses of less than €200, 4.2% indicating expenses between €201 and €500, 3.9% indicating expenses between €501 and €700 and 4.7% indicating expenses of more than €701.

2.7. Data breaches

Most respondents (71.5%) have never experienced a data breach. Among the 7.1% of SMEs that state having experienced breaches, 1.6% related to data being lost, 2.1% stolen and 3.4% misused.

Among those SMEs that experienced breaches, roughly half (i.e. 3.9% of SMEs consulted) informed the individuals whose data were affected by breaches, whereas the other half did not. Regarding the cost of the notification to affected individuals, respondents indicated that the notification cost: less than €500 (for 1.6% of SMEs consulted), in the range €501-1000 (for 0.5%), in the range €1001-2000 (for 0.8%) and in the range €2001-5000 for only one single respondent (0.3%).

3. DETAILED RESULTS PER QUESTION

1. In most cases, the processing of personal data needs to be declared to the National Data Protection Authority. Have you ever declared the processing of personal data to your national Data Protection Authority (DPA)?

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
No, I don't process any personal data	83	(21.7%)
No, my processing does not need to be declared	127	(33.2%)
Yes, I declared processing to my DPA	112	(29.2%)
Don't know / Not applicable	55	(14.4%)
N/A	6	(1.6%)

2. If you answered yes in question 1, can you estimate the cost to your company of providing this information to your national Data Protection Authority?

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Less than €100	32	(8.4%)
€101 - €300	18	(4.7%)
€301 - €500	8	(2.1%)
More than €500	24	(6.3%)
Don't know / not applicable	145	(37.9%)
N/A	156	(40.7%)

3. Which description best reflects the declaration of data processing to national data protection authorities? [You may select more than one answer]

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Easy	43	(11.2%)
Difficult	37	(9.7%)
Bureaucratic	115	(30%)
Don't know / not applicable	141	(36.8%)
N/A	47	(12.3%)

4. Do you process personal data of individuals residing in Member States of the European Union (EU) other than your own, or of countries outside of the EU / European Economic Area (EEA)? [You may select more than one answer]

-multiple choices reply- (optional)

	Number of Respondents	% of Total Respondents
Yes, I do process personal data of individuals from Member States other than my own	92	(24%)
Yes, I do process personal data of individuals from countries outside the EU/EEA (such as the US or countries in Asia, Africa)	53	(13.8%)
No, I do not process personal data of individuals from outside my own Member State.	181	(47.3%)
Don't know / not applicable	94	(24.5%)

5. Have you experienced difficulties when needing to transfer personal data to other Member States in the European Union?

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Yes	19	(5%)
No	117	(30.5%)
Don't know / not applicable	202	(52.7%)
N/A	45	(11.7%)

6. Have you experienced difficulties when needing to transfer personal data to countries outside of the European Union?

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Yes	20	(5.2%)
No	93	(24.3%)
Don't know / not applicable	223	(58.2%)
N/A	47	(12.3%)

7. If your company has a website, does it include a page explaining your privacy policy?

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Yes	139	(36.3%)
No	164	(42.8%)
Don't know / not applicable	64	(16.7%)
N/A	16	(4.2%)

8. Is someone in your company formally assigned to deal with data protection issues?

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Yes, there is a full time position	23	(6%)
Yes, someone does it alongside his/her other activities	155	(40.5%)
No	146	(38.1%)
Don't know / not applicable	35	(9.1%)
N/A	24	(6.3%)

9. Data protection laws oblige data controllers to provide information to individuals on whom you hold personal data, known as 'data subjects', about the identity of the data controller, the purpose of the processing, whether it will be passed on to third parties and so forth. Have you ever provided this information to data subjects?

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Always	105	(27.4%)
Often	37	(9.7%)
Sometimes	44	(11.5%)
Never	80	(20.9%)
Don't know / not applicable	96	(25.1%)
N/A	21	(5.5%)

10. If yes in question 9, can you estimate how much it costs your company to provide this information to individuals every time you need to provide it? (Examples of such costs may include costs of legal advice, design and printing costs, clerical costs, administrative overheads etc).

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Less than €100	62	(16.2%)
€101 - €300	19	(5%)
€301 - €500	14	(3.7%)
More than €500	14	(3.7%)
Don't know / not applicable	144	(37.6%)
N/A	130	(33.9%)

11. Individuals are generally entitled to ask for access to their personal data you hold, for example in order to correct it, to delete it, or simply to obtain a copy. Have you already had such requests?

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Yes, frequently	25	(6.5%)
Yes, rarely	74	(19.3%)
No	206	(53.8%)
Don't know / not applicable	54	(14.1%)
N/A	24	(6.3%)

12. If yes in question 11, how long does responding to such requests usually take? [Average duration (in work days)]

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
More than 0,5 working day	44	(11.5%)
1 working day	13	(3.4%)
2 working days	10	(2.6%)
3 working days	6	(1.6%)
Don't know / not applicable	133	(34.7%)
N/A	177	(46.2%)

13. Do you charge a fee for processing such requests? -single choice reply- (optional)

	Number of Respondents	% of Total Respondents)
Yes	10	(2.6%)
No	207	(54%)
Don't know / not applicable	122	(31.9%)
N/A	44	(11.5%)

14. If yes in question 13, how much is the fee? -single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Less than €10	2	(0.5%)
€10 - €50	5	(1.3%)
€51 - €100	2	(0.5%)
More than €100	1	(0.3%)
Don't know / not applicable	138	(36%)
N/A	235	(61.4%)

15. Have you ever paid for legal advice on data protection issues, for example on preparing a privacy page on your website or data protection clauses for a contract?

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Yes	78	(20.4%)
No	208	(54.3%)
Don't know / not applicable	61	(15.9%)
N/A	36	(9.4%)

16. If yes in question 15, how much did this legal advice cost your company?

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Less than €200	14	(3.7%)
€201 - €500	16	(4.2%)
€501 - €700	15	(3.9%)
More than €700	18	(4.7%)
Don't know / not applicable	123	(32.1%)
N/A	197	(51.4%)

17. Have you had an incident involving personal data (e.g. personal data held by your company was lost, misplaced or misused during the incident)

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Yes, personal data was lost	6	(1.6%)
Yes, personal data was stolen	8	(2.1%)
Yes, personal data was misused	13	(3.4%)
No	274	(71.5%)
Don't know / not applicable	48	(12.5%)
N/A	34	(8.9%)

18. If yes in question 17, were you able to inform the individuals whose information was affected when the breach occurred?

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents)
Yes	15	(3.9%)
No	16	(4.2%)
Don't know / not applicable	126	(32.9%)
N/A	226	(59%)

19. If yes in question 18, can you estimate the total cost to your company of informing affected individuals about that incident?

-single choice reply- (optional)

	Number of Respondents	% of Total Respondents
Less than €500	6	(1.6%)
€501 - €1000	2	(0.5%)
€1001- €2000	3	(0.8%)
€2001- €5000	1	(0.3%)
€5001- €10000	0	(0%)
More than €10000	0	(0%)
Don't know / not applicable	129	(33.7%)
N/A	242	(63.2%)

ANNEX 9

CALCULATION OF ADMINISTRATIVE COSTS IN THE BASELINE SCENARIO AND PREFERRED OPTION

○ INTRODUCTION

In accordance with the European Commission Impact Assessment Guidelines (in particular Annex 10 on administrative burden), this impact assessment closely examined the administrative costs imposed by existing regulation and by the preferred policy option.

Data sources in this exercise included EUROSTAT figures, Eurobarometers, qualitative and quantitative data gathered through a series of public consultations with stakeholders, and desk research. The analysis of this annex is confined to the costs incurred by the private sector in order to comply with information obligations contained in the data protection rules¹⁶³. Other compliance costs imposed by existing legislation and the preferred option are beyond the scope of this analysis.

○ METHODOLOGY

All calculations are carried out using the Standard Cost Model (SCM). A number of methodological challenges were encountered in using the SCM in the context of data protection and adapting it to the particularities of the area. The most significant challenges and caveats are set out below, along with an explanation of the methodological steps undertaken:

- **All costs included in this calculation are considered to be administrative burdens** and not costs that would be incurred as a result of practices undertaken by an entity even in the absence of the legislation. For this reason the values in the column "Business as Usual Costs" are always zero.
- **Directive 95/46/EC** and the preferred option were thoroughly screened for information obligations on either enterprises or public authorities.
- The quantitative calculations cover only the private sector; the **public sector** is not included in the calculations as no reliable statistics are available regarding the number of data controllers in the public sector who must comply with the Directive in the baseline scenario, and subsequently with the obligations in the preferred option. **Framework Decision 2008/977/EC** has also been screened for information obligations that involve administrative burden on public authorities, but the involved costs were judged to be **negligible**, given the wide exemptions in this area as regards, for example, the duty of informing data subjects that their personal data is sent cross-border for processing by other public authorities.

¹⁶³ Annex 10 of the IA Guidelines defines administrative costs "as the costs incurred by enterprises, the voluntary sector, public authorities and citizens in meeting legal obligations to provide information on their action or production, either to public authorities or to private parties."

- Whenever **legal fees** are considered in the calculation an estimate of €250/hour was used, which represents a conservative average of the varying rates across Member States. This was confirmed by stakeholder feedback.
- Whenever **clerical work** is considered in the calculation, an estimate of the cost of a full-time employee as €50/hour was used.
- **Regulatory origin:** in the baseline scenario calculation, all information obligations have an EU regulatory origin, with the exception of the last row, "National Transpositions of Directive 95/46/EC". In the preferred option calculation, all information obligations have an EU regulatory origin.
- **Recurrence:** all cost calculations are made on an annual basis. Wherever the value in the "Frequency per year" column is less than 1, the figure refers to a multiannual recurrence. For instance, if the figure in the "Frequency" column is 0.2 the recurrence is on a 5-yearly basis.
- Concerning the **total number of data controllers** used in the calculation of administrative burden, in the absence of official statistics on the number of data controllers in the EU, the eventual estimate used in the SCM is based on EUROSTAT 2008 figures on the total number of enterprises in the EU. The table below sets out the reasoning and steps involved in obtaining the total number of data controllers used in the calculation:

Table 1: Number of enterprises and data controllers in the EU

Indicator	Ref. year	Source	Value
Number of enterprises in the EU (non-financial business economy): all can potentially be considered data controllers (processing personal data such as employee data, customer databases, etc)	2008	EUROSTAT 2008 ¹⁶⁴	21,003,900
Based on the data protection SME Panel (see Annex 9), particularly figures relating to the compliance of SMEs with the current data protection rules ¹⁶⁵ , it can be assumed that approximately 42% of the total number of companies can be <i>practically</i> considered as data controllers within the meaning of the Directive. <i>This is the approximate total number of enterprises/data controllers on which the administrative burden of the Directive is actually imposed.</i>	2010	Data Protection SME Panel	<u>8,821,638</u>

¹⁶⁴ EUROSTAT 2008, *Key figures on European business with a special feature on SMEs*, Available at http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-ET-11-001/EN/KS-ET-11-001-EN.PDF

¹⁶⁵ SME Panel on data protection, Questions 7 (36% compliance) and 9 (48% compliance).

- Not all data controllers in the EU are affected by the problem of **legal fragmentation**. The data controllers affected would be those that process personal data of individuals from another Member State, **and** also have an establishment in that Member State, within the meaning of Article 4.1 (a) of the Directive, which allows for a "cumulative" and simultaneous application of different national laws to a same data controller established in several Member States. This means that such a controller will have to comply with the different national laws, obligations and varied requirements that apply for each of its establishments. It is important to note that the notion of "establishment", as confirmed by the opinion of the Article 29 Working Party on the issue, has generally been interpreted broadly by DPAs. In practice even a legal representative, a one-man office or a simple agent in a Member State are often considered as an "establishment", and thus lead to the application of the national laws of the Member States concerned.
- In order to obtain the **number of entities affected by legal fragmentation**, in the absence of official statistics, the proxy of *number of enterprises involved in cross-border trade* was used. These figures were obtained from the 2008¹⁶⁶ and 2010¹⁶⁷ Eurobarometers on consumer protection, where 21% and 22% were observed respectively (hence the more conservative figure of 21% was used). The reason for choosing this proxy is that an enterprise conducting business cross-border in another Member State, provided that it is also *established* in that Member State (within the meaning of Article 4.1 of the Directive), will be subject to the data protection law of that Member State. This would in turn entail significant additional costs in terms of legal adaptation and ensuring compliance with the data protection laws of that Member State.

Table 2: Methodology for data controllers affected by legal fragmentation

Indicator	Ref. year	Source	Value
Number of data controllers in the EU	2010	Data Protection SME Panel	8,821,638
No. of B2C service/retail companies selling to final consumers in a country different to their own (21%).	2008, 2010	Flash Eurobarometers 224 and 300	21%
Total number of data controllers engaged in cross-border trade	2008, 2011	2008 EUROSTAT figures on enterprises in the EU, Flash EB 300.	1,852,544
Assuming that only 50% of service /retail companies selling to final consumers in a Member State different to their own are also established in those Member States according to Article 4.1(a) of the Directive (e.g. by having a branch, a legal representative, a commercial agent etc in those Member States)			<u>926,272</u>

- The figure of 926,272 in the table above is obtained by multiplying the total number of data controllers in the EU (8,821,638), by the percentage of B2C companies engaged in cross-border trade (21%). It is assumed that the cross-border indicator of 21% applies also in the case of B2B cross-border trade. The resulting figure of 1,852,544 is further subtracted by 50% in the last row of the table to account for those data controllers which

¹⁶⁶ Flash Eurobarometer 224 – Business attitudes towards cross-border sales and consumer protection, available at http://ec.europa.eu/consumers/strategy/docs/fl224%20eurobar_cbs_summary.pdf (survey of managers of companies over 10 employees). This figure is extrapolated to companies of less than 10 employees.

¹⁶⁷ Flash Eurobarometer 300 - Retailers' attitudes towards cross-border trade and consumer protection, available at http://ec.europa.eu/consumers/strategy/docs/retailers_eurobarometer_2011_en.pdf

may not actually be established in other Member States, according to Article 4.1(a) of the Directive.

- In the 2010 Eurobarometer 21% of retailers said they also sold to consumers in other EU countries. More precisely, 2% of retailers reported selling products and services in just one additional EU country, 6% mentioned two or three other EU countries and the largest proportion – 13% – was engaged in cross-border sales in at least four other EU countries.

Table 3: Number of companies/data controllers active cross border

Total number of data controllers established and processing data cross border	926,272	
% data controllers processing data in one additional MS (2010 EB)	2%	88,217
% data controllers processing data in two or three additional MS (2010 EB)	6%	264,649
% data controllers processing data in at least four additional MS (2010 EB)	13%	573,407

- The figures from Table 3 are used in rows 5, 6, 7 of the administrative burden calculation spreadsheet.

3. DETAILED EXPLANATION OF ADMINISTRATIVE BURDEN CALCULATION

(a) *Baseline Scenario*

- (i) **Cost of information obligations:** Line 1 refers to the obligation on data controllers to provide information to data subjects according to Articles 10 and 11 of Directive 95/46/EC. It is estimated that 4 hours of legal validation work are required. It is further estimated that a clerical full-time employee will need to work for two hours to prepare this material. The costs of reproducing the information material is assumed to be zero. It is assumed that this is a cost which recurs on a 5-yearly basis, in order to account for technological lifecycles, which would require adaptations in the information provided.
- (ii) **Cost of providing information to data subjects about access rights:** Line 2 refers to the obligation on data controllers to inform data subjects on whether their personal data are being processed, which data and which categories of data are being processed, the purposes of the processing, how they are being processed (manually or automatically), the right to request the rectification, erasure or blocking of data being processed, and to notify any third parties of any changes to the personal data requested by the data subject. It is assumed that this task requires two hours of legal validation (€500) and three hours of clerical work (€150), and that it is a cost which recurs on a 5-yearly basis, in order to account for technological lifecycles, which would require adaptations in the information provided.
- (iii) **Cost of Notifications of processing activities by data controllers** to national data protection authorities: based on figures provided by national DPAs in their 2009 Annual Reports, the total number of new notifications in the EU in 2009 were 552,840. This figure was rounded up to 650.000 to account for 5 Member States that

did not submit their statistics (DE, ES, PT, HU and LV). From stakeholder feedback submitted in public consultations, the cost of each new notification is estimated at approximately €200 per notification¹⁶⁸, comprising 4 hours work by a full-time clerical employee. This figure would include updates of existing notifications as the means of processing may change over time. As the figure of 650.000 refers to *new notifications per year*, the number in the Frequency column is 1.

- (iv) **Prior Checking:** This refers to the cost of notifying public authorities about processing which might present specific risks to the rights and freedoms of individuals (Article 20 of the Directive). This is estimated to involve 2 hours of legal validation (€ 500) and 4 hours of clerical work (€200). There were approximately 15.000 prior checks reported to the Commission for 2009. This figure was rounded up to 16.000 to account for those Member States that did not report statistics on this.
- (v) **Baseline costs of legal fragmentation in the internal market / national transpositions of Directive 95/46/EC:** the calculation of the costs of legal fragmentation in terms of administrative burden is based on the following elements:
- 10 hours of legal validation work to adapt the business model of the data controller to the data protection requirements of the additional Member States he is established in (€2,500)
 - €2,000 for translation costs (e.g. on information materials for data subjects, privacy policies, etc)
 - 10 hours of clerical work (€500)
 - It is assumed that this is a cost which recurs on a 5-yearly basis in order to account for technological lifecycles, which would require legal adaptations to ensure legal compliance.

(b) Preferred Option

- (i) **Introduction of an explicit principle of transparency:** Line 1 refers to the introduction of a general principle of transparency on data controllers, which will practically translate into providing clear and intelligible information to data subjects. The obligation is estimated to involve two hours of clerical work for a full time employee. This will be a one-off cost of adapting to the new requirements of the data protection rules on transparency.
- (ii) **Extending some obligations applicable to data controllers to data processors:** it is assumed that a big majority of information obligations relating to data processors will be dealt with by data controllers upstream. Some obligations may be incurred by data processors (particularly as regards Line 3 – obligation to demonstrate compliance), but the number of processors affected is very difficult to estimate with any degree of certainty.
- (iii) **Abolish the existing generalised system of notifications to DPAs:** see Line 3 under the Baseline Scenario calculation.

¹⁶⁸ This estimate is based on information received from the DPAs in NL and LU. For example, in Netherlands it takes about half a day to fulfil the notification requirement. In Luxembourg the company needs to complete 3-4 forms and the estimated cost for each file is €100. The notification form used in the UK fits within these estimates, and it can be extrapolated that the situation is similar in most of the Member States.

- (iv) **Introduction of a general obligation for data controllers to demonstrate compliance with data protection law:** Line 4 estimates the cost of *providing information about compliance*, involving 4 hours of clerical work by a full time employee to gather and prepare all the relevant information. Such information may include disclosures about the appointment of DPOs and the conducting of DPIAs. As this change includes among other the appointment of specially trained personnel and the conduct of risk assessments through the DPIA, is assumed that this action would need to be performed every 3 years, in order to account for technological lifecycles, which would require adaptations in the information provided.
- (v) **Data breach notifications:** Line 5 estimates the cost of data breach notifications; it is estimated that currently 3,000 data breach notifications take place in the EU for the telecoms sector, at a cost of 20,000 each (based on 319 data protection breaches reported to the UK DPA in 2008/2009 and extrapolated for the EU¹⁶⁹; figure of costs based on stakeholder feedback and desk research). If notification is extended to all sectors, it is estimated that an extra 1,000 breach notifications would occur. The additional cost of notifying about them would therefore be in the order of 20 million per annum.
- (vi) **Eliminating the costs of legal fragmentation:** Line 6 mirrors line 4 of the baseline scenario, but with a negative prefix as the estimated *annual* costs will be eliminated.

4. CONCLUSION

The calculations in this annex estimate administrative burdens to amount to:

- **€5.257.752.500 per annum in the baseline scenario, of which approximately €2.911.143.000 is attributable to legal fragmentation.**
- **€1.556.749.132 in savings per annum in the preferred option, vis-à-vis the baseline scenario (net change).**

¹⁶⁹ Based on 319 data protection breaches reported to the UK DPA in 2008/2009 and extrapolated for the EU; figure of costs based on stakeholder feedback and desk research.

ANNEX 10

IMPACTS OF THE PREFERRED OPTION ON COMPETITIVENESS

8. EXPECTED IMPACTS OF THE PREFERRED POLICY OPTION ON THE COMPETITIVENESS OF THE EU ECONOMY

This annex provides additional analysis of the expected impacts of the preferred policy option on the competitiveness of the European economy.

The likely impacts are evaluated in terms of three dimensions of competitiveness:

- **Cost competitiveness:** the cost of doing business, which includes the costs of factors of production (labour, capital and energy);
- **Capacity to innovate:** the capacity of the business to produce more and/or better quality products and services that meet better customers' preferences
- **International competitiveness:** the above two aspects could also be assessed in an international comparative perspective, so that the likely impact of the policy proposal on comparative advantages on the world markets is taken into account.

As a horizontal initiative, the data protection reform has impacts on most industries. The personal data of natural persons is potentially processed in all sectors of the economy. The reform of European data protection rules will therefore introduce changes that cut across industrial sectors, and have a global impact on the economy of the EU.

The envisaged approach of increasing harmonisation at EU level will have a significant impact on business and enhance the attractiveness of Europe as location to do business, at the same time as strengthening the EU in its global promotion of high data protection standards. In fact, while the reform puts individuals in a better position to exercise their data protection rights, it will also allow for significant cost reductions for businesses through more harmonisation.

The current fragmentation of the legal framework gives rise to administrative burden costing EU businesses close to €3 billion per year. This cost could be removed and the resources made available could potentially be used by businesses to enhance their investment strategies, both within the EU and beyond. Thus, thanks to the reduced fragmentation of the regulatory environment, the EU will have a more predictable business environment in data protection, with a set of rules encouraging more consumer confidence and a better-functioning internal market. A multinational company operating in several Member States will no longer be subject to different requirements and the resulting costs and legal uncertainty.

9. COST AND PRICE COMPETITIVENESS

9.1. Cost of inputs

The costs of doing cross-border business in the internal market will be reduced considerably by the clarification of the rules on applicable law, so that a data controller established or using equipment in more than one Member State will be subject to one single law only. As a result of the reform, businesses will have to comply with one set of common, harmonised rules for the processing of personal data and ensure that personal data flows without obstacles throughout the EU.

The data protection reform will create a level playing field for data controllers and reduce the administrative burden linked to notifications to Data Protection Authorities. Multinational companies with activities in more than one EU Member State will reap significant benefits from having to contact only one, single Data Protection Authority who will be responsible for their supervision, thus improving coherence and compliance and reducing costs. It will also reduce barriers to entry for potential new entrants, making the internal market more attractive and allowing them to fully exploit its potential.

The objective of enhancing the internal market dimension of data protection is likely to have positive impacts on business cost efficiency, given that it proposes to:

- establish a "one-stop-shop" for data controllers in the EU ensuring consistent enforcement of data protection rules,
- rationalise the current governance system to help ensure a more consistent enforcement,
- drastically cut red tape: remove unnecessary notification obligations for data controllers,
- simplify requirements for international data transfers.

Given these changes, the reform is expected to be positively received by economic operators, as it will reduce their overall compliance costs, particularly those linked to the currently fragmented rules and the data protection-related administrative burden.

Taking account of the concerns of industry regarding the administrative and financial costs of implementing some of the proposed changes, and in particular to avoid the possibility of imposing disproportionate burdens on small companies, measures with a potential cost impact such as the appointment of Data Protection Officers and the conduct of data protection impact assessments, have limitations and thresholds included in the relevant legal obligations, thus considerably limiting the cost impacts on SMEs.

The reform is also likely to have a positive impact on consumer confidence in online environments, so that increased volume of transactions of goods and services through online channels can be expected. In addition to the providers of online services who benefit directly, this has the potential to benefit also the large supplier base which provides goods for online transactions, as well as sectors involved in the completion of online transactions, e.g. courier and postal services delivering the goods ordered online and related businesses.

9.2. Cost of labour

No material changes of data protection rules relating to employment relationships are proposed. Clarification and harmonisation of general data protection concepts will remove divergences and reduce costs caused by fragmentation.

9.3. Other compliance costs

The appointment of data protection officers will, for those organisations to which the obligation applies, impose additional costs to the extent that a comparable function does not already exist internally or in the form of an external consultancy contract. Data Protection Impact Assessments will also impose costs depending on the frequency and the level of scrutiny required.

On the one hand, thresholds and limitations ensure that any additional costs remain proportionate to the volume of operations. On the other hand, both measures contribute considerably to increased compliance of the organisation, which can in the long term protect

it from expensive complaint handling, administrative investigation or litigation. This applies also to an obligation to demonstrate compliance by documenting internal policies and procedures. Furthermore, for data controllers established in more than one Member State, these additional compliance costs would be offset by the reduction of fragmentation (*see also Annex 6*).

10. CAPACITY TO INNOVATE

10.1. Capacity to produce and bring R&D to the market

The current inconsistent implementation of EU data protection laws impacts the uptake of online services and new technologies in general. Individuals are affected because of a lack of trust in the digital environment and fears about possible misuse of their data. This creates opportunity costs for economic operators and public authorities and slows down innovation.

Strong growth of the internet economy, widespread use of new mobile devices and the expansion of e-commerce and other web-based services could bring sizable economic benefits, and provide a strong platform for companies able to develop new products and services and to bring them to market. The EU has supported research and development in privacy friendly and privacy enhancing technologies, as well as in secure tools. Market acceptance of these technologies and tools will improve considerably when they are integrated into systems offered to a market of 500 million potential customers.

10.2. Capacity for product innovation

Clear and harmonised data protection rules can become a trigger for innovation. For example, privacy enhancing technologies or privacy by design and data protection consulting are sectors which could benefit from an environment where increased data protection safeguards are the norm. European industry could become world leaders in privacy enhancing technologies or privacy by design solutions, drawing business, jobs and capital to the European Union. Privacy enhancing tools for data transfer and aggregation, as well as cloud computing will generate new business opportunities.

10.3. Capacity for process innovation (including distribution, marketing and after-sales services)

Clarification and harmonisation of data protection rules across the EU offers a larger, more streamlined and more open market for investment and increases incentives for innovation.

11. INTERNATIONAL COMPETITIVENESS

11.1. Competition in internal market

Clarification of data protection concepts and principles, more harmonisation of data protection law, clarification of applicable law and improved consistency of enforcement all contribute to creating a level playing field in the EU as far as data protection is concerned. They will remove incentives for forum shopping and the distortion of competition by diverse interpretation of existing principles. This will improve competition in the internal market and increase the resulting benefits in terms of subsequent downward pressure on prices and more innovative products and services.

11.2. Competition in external markets

The fact that the EU is reforming its data protection rules to enhance individual rights can be perceived by many businesses as a competitive advantage, providing a business environment where the legitimate and safe processing of personal data is rewarded with the trust of more consumers.

The change in rules, making the European internal market more effective and creating a more predictable regulatory environment is in turn expected to make Europe become a more attractive place for doing business, as the rules will be less heavy and more streamlined.

The main elements in the preferred policy option contributing to this effect are the:

- Clarification of applicable law, ensuring that only one law applies,
- Simplification of the conditions and procedures for third country data transfers, including for groups of companies,
- General reduction of red tape and fragmentation
- Consistent and effective enforcement.

EU based providers will be able to offer a service with higher quality in terms of data protection and security at competitive prices at a global scale.

11.3. Summary

11.3.1. Impact on competitiveness

	Data Processors / controllers	
Cost and price competitiveness	Positive	
Cost of inputs	Strong reduction of compliance costs. An estimated €2.2 billion in the administrative burden of legal fragmentation will be virtually eliminated by the increased harmonisation.	
Other compliance costs (e.g. reporting obligations)	DPOs and DPIAs, as well as a general assessment of compliance, improve data protection compliance and reduce risk of cost for non-compliance for complaint-handling, administrative investigations or litigation and negative effects for brand and customer base.	Obligation (DPOs may in businesses n function. Int protection in cost to a lim Introducing demonstrate law is estima administrativ
Price of outputs	Improved consumer confidence in on-line trading environment expected to have positive impact on business ability to trade across borders and in competition. Level playing field in single market creates economy-of-scale benefits	
Capacity to innovate	Positive	
Capacity to produce and bring R&D to the market	Improved by higher consumer confidence in providing data. Application of privacy by design principle and increased use of PETs enable development of new products and services using privacy as a competitive advantage.	
Capacity for product innovation		
Capacity for process innovation (including distribution, marketing and after-sales services)	Clarification and harmonisation of data protection rules across EU offers larger market for new developments and increases incentive for innovation	
International competitiveness	Positive	
Market shares internal market	Increased harmonisation will create a more level playing field for businesses and foster their intra-EU and international competitiveness.	

Market shares external markets	Strong data protection can build consumer confidence and strengthen the potential of the market. Simplification of procedures for data transfers to third countries makes international cooperation easier and reduces costs.	
--------------------------------	---	--