COUNCIL OF THE EUROPEAN UNION

Brussels, 27 January 2012

5833/12 ADD 1

Interinstitutional File: 2012/0010 (COD)

DATAPROTECT 6
JAI 41
DAPIX 9
FREMP 8
COMIX 59
CODEC 217

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	27 January 2012
to:	Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.:	SEC(2012) 72 final
Subject:	Commission staff working paper Impact Assessment accompanying the document Regulation on the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

Delegations will find attached Commission document SEC(2012) 72 final.

Encl.: SEC(2012) 72 final

EUROPEAN COMMISSION

Brussels, 25.1.2012
SEC(2012) 72 final

COMMISSION STAFF WORKING PAPER

Impact Assessment

Accompanying the document

Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
and
Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

{COM(2012) 10 final}
{COM(2012) 11 final}
{SEC(2012) 73 final}

COMMISSION STAFF WORKING PAPER

Impact Assessment

Accompanying the document

Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
and
Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

Disclaimer

This impact assessment report commits only the Commission's services involved in its preparation and the text is prepared as a basis for comment and does not prejudge the final form of any decision to be taken by the Commission.

Article 29 Working Party (WP 29): Data Protection Working Party established by Article 29 of Directive 95/46/EC. It provides the European Commission with independent advice on data protection matters and supports the development of harmonised policies for data protection in the EU Member States.

Binding corporate rules (BCR): Codes of practice based on European data protection standards, approved by at least one Data Protection Authority, which multinational organisations draw up and follow voluntarily to ensure adequate safeguards for transfers or categories of transfers of personal data between companies that are part of a same corporate group and that are bound by these corporate rules.

Controller* **or Data controller:** Natural or legal person, public authority, organisation, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Data Protection Authority (DPA)*: National supervisory authority, acting with complete independence, responsible for monitoring the application of data protection rules at national level (e.g. handling complaints from individuals, carrying out investigations and inspections of data controllers' activities, engage in legal proceedings against violations of data protection rules).

Data Protection Impact Assessment (DPIA): A process whereby a conscious and systematic effort is made to assess privacy risks to individuals in the collection, use and disclosure of their personal data. DPIAs help identify privacy risks, foresee problems and bring forward solutions.

Data Protection Officer (DPO): A person responsible within a data controller or a data processor to supervise and monitor in an independent manner the internal application and the respect of data protection rules. The DPO can be either an internal employee or an external consultant.

Data subject: An identified or identifiable person to whom the "personal data" relate.

Personal data* **(sometimes simply referred to as "data"):** Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Personal data breach**: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Union.

Processing of personal data*: Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such

---

* Based on the definitions in Article 2 of Directive 95/46/EC.

** Based on the definition in Article 2(i) of Directive 2002/58/EC (as amended by Directive 2009/136/EC).

as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Processor* **or Data processor:** The processor is the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Sensitive data: Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, data concerning health or sex life, and data relating to offences, criminal convictions or security measures.

TABLE OF CONTENTS

LIST OF ANNEXES

1. INTRODUCTION

The centrepiece of EU legislation on data protection, Directive 95/46/EC[1] (hereinafter "the Directive"), was adopted in 1995 with two objectives in mind: to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States. It was complemented by several instruments providing specific data protection rules in the area of police and judicial cooperation in criminal matters[2] (ex third pillar), including Framework Decision 2008/977/JHA (hereinafter "the Framework Decision")[3].

Rapid technological and business developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life.

Building trust in the online environment is key to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services, including public e-government services. If not addressed, this lack of confidence will continue to slow down the development of innovative uses of new technologies, to act as an obstacle to economic growth and to block the public sector from reaping the potential benefits of digitisation of its services, e.g. in more efficient and less resource intensive provisions of services. This is why data protection plays a central role in the *Digital Agenda for Europe*[4], and more generally in the *Europe 2020 Strategy*[5].

The Lisbon Treaty defines the right to data protection as a principle of the EU and introduces a specific legal basis for the adoption of rules on the protection of personal data[6] that also applies to police and judicial cooperation in criminal matters. Article 8 of the EU's Charter of Fundamental Rights (CFR) enshrines data protection as a fundamental right.

The European Council invited the Commission to evaluate the functioning of EU instruments on data protection and to present, where necessary, further legislative and non-legislative initiatives[7]. In its resolution on the Stockholm Programme, the European Parliament[8] welcomed a comprehensive data protection scheme in the EU and called for the revision of the Framework Decision among other measures.

The Commission's broad public consultations and extensive stakeholder dialogues have confirmed that there is general agreement that the current framework remains sound as far as its objectives and principles are concerned. However, it has not prevented fragmentation in the way data protection is implemented across the Union, which causes legal uncertainty and a widespread public perception that there are significant privacy risks associated notably with online activity[9].

---

1 OJ L 281/95, p.31. The Directive builds upon and develops the principles enshrined in the 1981 Council of Europe Convention No 108 for the protection of Individuals with regard to Automatic Processing of Data.

2 See the full list in Annex 3.

3 OJ L 350, 30.12.2008, p. 60

4 COM(2010)245 final.

5 COM(2010)2020 final.

6 Article 16 of the Treaty on the Functioning of the European Union.

7 In the Stockholm Programme - OJ C115, 4 May 2010.

8 See the Resolution of the European Parliament on the Stockholm Programme adopted 25 November 2009.

9 Special Eurobarometer (EB) 359, *Data Protection and Electronic Identity in the EU* (2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf ("*EB 2011" in future references*).

This is why it is time to ***build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities.***

The Commission highlighted the policy objectives of this reform in its Communication on a comprehensive approach on personal data protection in the European Union adopted on 4 November 2010[10]. It is now translating these policy objectives into concrete reform proposals.

This impact assessment focuses on the review of the Directive and the Framework Decision. The Commission will assess the need to adapt other legal instruments to the new general framework at a later stage[11].

2. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

2.1. Identification

Title: Impact assessment on the reform of the data protection regulatory framework
Lead DG: Justice
Agenda planning number: AP 2010/279, CWP 2011 Annex 1

2.2. Organisation and timing

The evaluation and impact assessment process for the review of the personal data protection regulatory framework started with a general public consultation phase in May 2009. Evaluations of the Directive and of the Framework Decision were carried out by the Commission services in 2010 and 2011 (*see below § 3.1 and annexes 2 and 3*). Two external studies[12] supported the evaluation and impact assessment. A specific report by the Commission evaluates the implementation of the Framework Decision by Member States.[13]

The inter-service impact assessment steering group was convened for the first time on 3 March 2010 and met again on 27 May 2010, 9 March 2011 and 14 July 2011. The following Commission services were invited to participate in the steering group: the Secretariat-General, the Legal Service, DG AGRI, DG AIDCO, DG COMM, DG COMP, DG EMPL, DG ENER, DG ESTAT, DG HOME, DG INFSO, DG JRC, DG MARKT, DG MOVE, DG OLAF, DG RTD, DG SANCO, DG TAXUD, DG TRADE and the EEAS.

2.3. Consultation of the IAB

Following the IAB opinion, the following changes were made to the present report:

---

10 COM(2010)609. The Commission's general approach was welcomed and the priorities set out in the Communication were largely supported by the European Parliament, the Council and the Economic and Social Committee. The European Parliament adopted an own initiative report (Report on a comprehensive approach on personal data protection in the European Union, (2011/2025(INI)). The Council issued Conclusions on the Commission Communication (0371st JUSTICE and HOME AFFAIRS Council meeting, 24 and 25 February 2011). The EESC adopted an opinion[10] (Report on a comprehensive approach on personal data protection in the European Union, (2011/2025(INI)).

11 See point 3 of the Communication COM(2010)609, p. 18.

12 The studies were carried out, respectively, by GHK consulting and Trilateral Research. The first study was more comprehensive (from March 2010 to January 2011) while the second (May/June 2011) focused on the economic and social impacts of key measures.

13 The implementation deadline of the Framework Decision was 27 November 2010. The implementation report is presented together with the reform proposals.

- The objectives of the current legal framework (to what extent they were achieved, to what extent they were not), as well as the objectives of the current reform, were clarified;
- More evidence and additional explanations/clarification were added to the problems' definition section;
- A section on proportionality was added;
- All calculations and estimations related to administrative burden in the baseline scenario and in the preferred option have been entirely reviewed and revised (*including Annex 9 on administrative burden calculations*), and the relation between the costs of notifications and the overall fragmentation costs has been clarified;
- Impacts on SMEs, particularly of DPOs and DPIAs have been better specified;
- The analysis of impacts (especially economic ones, on competitiveness) has been improved;
- The description of the options has been revised and clarified;
- A table comparing the different options was added, as well as on the preferred option;
- A new annex (n° 10) on competitiveness proofing of the preferred option was added.

2.4. Consultation and expertise

The evaluation included a broad-based consultation process, which lasted for more than two years and included two phases of public consultation.

The first general public consultation was launched in May 2009 with a conference on personal data protection. The replies to the consultation and the summary of the results are available at: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. A second public consultation was launched following the adoption of the Commission's Communication of 4 November 2010[14]. A summary of the responses is included in annex 4.

Targeted consultations were also conducted with key stakeholders; specific events were organised on 29 June 2010 with Member State authorities and on 1 July 2010 with private stakeholders, including private companies, as well as privacy and consumers' organisations.

In November 2010, Vice-President Reding organised a roundtable on the data protection reform and on 28 January 2011 (Data Protection Day), the European Commission and the Council of Europe co-organised a High-Level Conference to discuss issues related to the reform of the EU legal framework as well as to the need for common data protection standards worldwide (http://www.data-protection-day.net/init.xhtml?event=36). Two Conferences on data protection were hosted by the Hungarian and Polish Presidencies of the Council on 16-17 June 2011 and on 21 September 2011 respectively.

[14] http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm

Dedicated workshops and seminars on specific issues were held throughout 2011. On 24 January ENISA (the European Network and Information Security Agency, dealing with security issues related to communication networks and information systems) organised a workshop on data breach notifications in Europe[15]. On 2 February the Commission convened a workshop with Member States' authorities to discuss the implementation of the Framework Decision and, more generally, data protection issues in the area of police cooperation and judicial cooperation in criminal matters. On 21-22 February the Fundamental Rights Agency held a stakeholder consultation meeting on "Data Protection and Privacy". A discussion on key issues of the reform was held on 13 July 2011 with national Data Protection Authorities.

EU citizens were consulted through a Eurobarometer survey held in November-December 2010[16].

The "Article 29 Working Party" (WP29)[17] provided several opinions and useful input to the Commission[18]. The EDPS also issued a comprehensive opinion on the issues raised in the Commission's November 2010 Communication[19].

A large majority of stakeholders agreed that the general principles remain valid but that there is a need to adapt the current framework in order to ***better respond to challenges posed by the rapid development of new technologies (particularly online) and increasing globalisation,*** while maintaining the technological neutrality of the Directive. Private sector data controllers in particular have underlined the need to ***increase harmonisation*** within the EU and to better apply the existing data protection principles in practice. Furthermore, they consider that the **complexity of the rules on international transfers** of personal data constitutes an impediment to their operations as they regularly need to transfer personal data from the EU to other parts of the world.

3. PROBLEM DEFINITION

3.1. Evaluation of the EU data protection framework

The main and overarching objective of the current legal framework on data protection is to ensure a **high level of data protection** for all individuals in the EU.

The Directive also aims at achieving an **equivalent level of data protection** in all Member States in order to ensure the **free flow of information within the internal market**.

In the police and criminal justice area, a specific aim – enshrined in the Framework Decision – is to **enhance mutual trust** and thus **support the exchange of personal data** between police and judicial authorities.

All these objectives, which remain entirely **valid** today, have only been **partially achieved** under the current legal framework.

---

15 See http://www.enisa.europa.eu/act/it/data-breach-notification/.

16 Cit. footnote 9.

17 WP29 was set up in 1996 (by Article 29 of the Directive) with advisory status and composed of representatives of national Data Protection Supervisory Authorities (DPAs), the European Data Protection Supervisor (EDPS) and the Commission. For more information on its activities see http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

18 See in particular the following opinions: on the "Future of Privacy" (n° /2009, WP168); on the Concepts of "Controller" and Processor" (n° 1/2010, WP169); on Online Behavioural Advertising (n°2/2010, WP 171); on the Principle of Accountability (n° 3/2010, WP 173); on Applicable Law (n° 8/2010, WP 179); and on consent (n° 15/2011, WP 187). Upon the Commission's request, it adopted also the three following Advice Papers: on Notifications, on Sensitive Data and on Article 28(6) of the Data Protection Directive. They can all be retrieved at: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm.

19 Available on the EDPS website: http://www.edps.europa.eu/EDPSWEB/.

As to the first objective, the Directive contains principles that are still sound and guarantee a high level of protection. However, there are today **new challenges to the protection of personal data** that could not be foreseen 16 years ago, when the Directive was adopted, linked to technological developments and globalisation. In particular, the development of the internet has greatly facilitated and increased the scale of data collecting and sharing, across geographical and virtual borders. The result is that personal data today may be processed more easily and on an unprecedented scale by both private companies and public authorities, which increases the risks for individuals' rights and challenges their capacity of keeping control over their own data (*see Section 3.3., Problem 2 below*). Moreover, there are wide divergences in the way Member States have transposed and enforced the Directive, so that in reality the protection of personal data across the EU **cannot be considered as equivalent today.**

Differences in national transposition and enforcement have also limited the achievement of the "internal market objective" of the Directive, as highlighted already in the 2003 and 2007 implementation reports[20]. Although there is no evidence that any Member State has ever blocked the flow of personal data to or from another Member State, these differences in approach have led to costly legal fragmentation and uncertainty with negative consequences for businesses, individuals and the public sector (*see Section 3.2., Problem 1 below*).

The application of the EU data protection *acquis* in the area of ***police cooperation and judicial cooperation in criminal matters***, in particular the Framework Decision, resulted in gaps and inconsistencies, which have affected both the level of protection for individuals and the mutual trust and cooperation between police and judicial authorities (*see Section 3.4., Problem 3 below).*

3.2. PROBLEM 1 – Barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement

3.2.1. Description of the problem

The current divergences in the implementation, interpretation and enforcement of the Directive by Member States ***hamper the functioning of the internal market and cooperation between public authorities in relation to EU policies.*** This goes against the fundamental objective of the Directive of facilitating the free flow of personal data in the internal market. These divergences raise the compliance costs related to data processing and transfer operations between Member States, without any corresponding benefit in terms of data protection, and may discourage some economically or socially beneficial activities which would require cross-border transfers of data within the EU. It is estimated that the fragmentation of the legal framework gives rise to administrative burden costing EU firms close to € 3 billion per year.

The rapid development of new technologies and globalisation further exacerbates this problem. A comparative study on different approaches to new privacy challenges for the European Commission[21] found that

> *"We have seen dramatic technological change since the European Commission first proposed the Data Protection Directive in 1990. The Internet has moved out of the*

[20] See, respectively, COM(2003)265 final and COM (2007)87 final.

[21] http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

university lab into 56% of European homes and 95% of OECD businesses. Computer processing power has continued to follow Moore's Law, with transistor density doubling every 18-24 months – around one thousand-fold in the last two decades. Computer storage capacity and communications bandwidth have both been increasing even more quickly, doubling every 12 months and hence a thousand-fold each decade. These exponential increases have radically increased the ability of organisations to collect, store and process personal data. The physical environment is now saturated with sensors such as CCTV cameras and mobile phones, with biometric and electronic identifiers used to link data to individuals. In the digital world almost every communication and Web page access leaves behind detailed footprints. The Internet and mobile information appliances allow large quantities of personal data to be trivially moved between jurisdictions. Data mining tools attempt to find patterns in large collections of personal data, both to identify individuals "of interest" and to attempt to predict their interests and preferences. New multinational companies have sprung up around these technologies to service a global customer base, with smaller enterprises outsourcing employee and customer data processing to developing world companies."

There are hardly any business transactions today which are not supported by information technology. Online transactions produce a trail of personal data by their very nature. With the introduction of loyalty cards and other systems, even day-to-day retail operations in normal supermarkets now leave a trail of personal data. Most travelling and leisure activities and service contracts have become unthinkable without the processing of personal data at a large scale. While for some traditional services, e.g. payment cards, the revenue from the collection and use of data has become more important than that from the actual consumer service, new business models have emerged that rely exclusively on this revenue source for their financing and profit, e.g. some search engines and social networking services monetizing their data through targeted advertising.

Where these services are provided online, they are generally accessible regardless of the geographic location of user and service provider, and the operation of the service includes the transfer of personal data across borders. Large enterprises can afford the necessary legal expertise to ensure compliance with all relevant legislations and/or the technical efforts to ensure that their offering is adapted for each jurisdiction to the local requirements. Small and medium enterprises, on the contrary, do not have the resources for such expertise or adaptation and accordingly refrain from offering their services online altogether or choose to refuse servicing customers outside their national jurisdiction. While data protection legislation is not the only element contributing to these difficulties for businesses – others include intellectual property law, taxation and elements of civil law – it is one of the elements that need to be addressed in a comprehensive strategy to remove remaining obstacles in the digital single market, in line with the Commission's initiatives under the Stockholm Action Plan and the Digital Agenda for Europe.

a) Fragmentation and legal uncertainty

A first cause of the existing **fragmentation** of the legal framework on data protection is the fact that the Directive contains a number of provisions that are broadly formulated, and - sometimes intentionally - leave Member States significant room for manoeuvre in transposing them. For example, Article 5 of the Directive states that "Member States shall […] determine more precisely the conditions under which the processing of data is lawful". Furthermore, there is currently **no strong mechanism to ensure a harmonised interpretation** of the

Directive. The Commission's implementing powers are limited to the external dimension of the Directive (transfers of data to third countries). The opinions of the Article 29 Working Party on questions covering "the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures"[22] are not binding and are therefore not always followed in practice by DPAs.

As a consequence, key provisions and concepts have been interpreted and transposed in quite different ways by Member States, so that **the same processing is treated divergently across Member States and thus impacts cross-border processing activities by public authorities and businesses**. This concerns, for example, the following issues[23]:

- Consent:

Consent is currently defined in the Directive as "any freely given specific and informed indication", of the data subject's wishes to give his/her agreement to the processing of personal data relating to him or her[24] which must be "unambiguously given" in order to make the processing of personal data legitimate. National laws have transposed this concept quite differently and consequently national DPAs apply different interpretations of consent and of its modalities. In particular, the meaning of "unambiguously given" consent is interpreted in a variable manner: in some Member States, consent has to be given "expressly" and in some cases even in writing[25], while other Member States and DPAs also accept some forms of implied consent[26]. The consequence is that a valid consent in one Member State would not be legally valid in others, therefore creating uncertainty amongst data controllers operating in several Member States on whether a data processing is lawful or not.

- Sensitive data[27]:

"Sensitive data" are special categories of data (i.e., data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life) whose processing shall in principle be prohibited, unless certain conditions are fulfilled and safeguards provided.

Some Member States have specified and added categories to those included in the Directive, for example biometric data (e.g. the Czech Republic, Slovenia and Estonia) genetic data (Bulgaria, the Czech Republic, Estonia, Luxembourg and Portugal) or party membership (Poland). Some Member States have also included data from the judiciary, for example information about previous convictions or criminal behaviour (e.g. Cyprus, the Czech Republic, Estonia, Slovenia, Spain, the Netherlands and Poland). On the other hand, some national laws do not consider as sensitive data on ethnic origin, political opinions or philosophical beliefs. There is also a very varied implementation – due to the room for manoeuvre left by the Directive in this respect – of the exceptions from the general prohibition of processing 'sensitive data'. For example, in relation to the possibility of processing health-related data (an exception to the general prohibition), some Member States

---

22 Article 30, 1 a of the Directive.

23 See Annex 2 for a detailed analysis on divergences in the implementation of the Directive by Member States and for further examples.

24 Articles 2(h) and 7 (a) of the Directive.

25 Express/explicit consent is required under the national laws of Cyprus, Germany, Greece and Italy, In addition, under German law consent has to be given in writing (with exceptions); under Italian law, consent has to be "documented in writing" as a general principle.

26 See the Guidance – issued by UK Information Commissioner's Office (ICO) in 2002 - on the application of the Data Protection Act 1998 in relation to Use and disclosure of health data, retrievable at: http://www.ico.gov.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications.aspx#health.

27 See Article 8 of the Directive.

(e.g. Cyprus and Denmark) allow this only when data are processed by health professionals, whereas in the Czech Republic and in Slovakia processing of such data is possible also for health insurance purposes. Also in this case, different requirements across Member States entail legal uncertainty and costs for both private (e.g. companies operating in the health sector) and public data controllers (on this aspect, see Section 3.2.2 b).

- ***Notification:***

Currently data controllers have the obligation to notify their processing operations to national DPAs, unless there are grounds for being exempted[28]. A large discretion is left to Member States in deciding possible exemptions to such obligation (and any other form of simplification), so that the same data processing activity could involve an obligation to notify the DPA in some Member States and not in others. For example, some Member States have made extensive use of the possibility for exemptions from the notification requirement by increasing the accountability of the data controller - in particular through the appointment of a Data Protection Officer (DPO)[29] – while others make very limited exemptions. Moreover, several DPAs charge for notifications, whereas others do not (the charge for a single notification ranges from about €23 to €599 and may depend on whether a data controller is a natural or legal person, public or private sector etc)[30].

All of this imposes costs and cumbersome procedures on business, without delivering any clear corresponding benefit in terms of data protection. All economic stakeholders have confirmed in the course of the public consultation that the current notification regime is unnecessarily bureaucratic and costly. DPAs themselves agree on the need to revise and simplify the current system[31].

This problem is made more acute by the current regime on **applicable law** as established by the Directive[32], 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 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[33], has generally been interpreted broadly by DPAs. In practice even an attorney office, 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.

This means that the **fragmentation** – and the costs linked to that (see Section 3.2.2 below) - caused by diverging national requirements combined with the simultaneous application of national laws affects not only large enterprises with physical establishment/branches in Member States but most of the companies carrying out cross-border activities.

Example 1 below helps to show how these costs arise.

---

28 See Articles 18 and 19 of the Directive.

29 DPOs exist today in several Member States (Germany, Sweden, the Netherlands, Luxembourg, Slovakia, Estonia and Hungary), with variable status and competences. Their appointment is optional in most Member States, except in Germany - where this is a compulsory obligation for public data controllers and for private controllers permanently employing at least 10 persons in the automated processing of personal data or when the processing is subject to prior checking - + Hungary and Slovakia?.

30 See WP29 Advice Paper on notifications, cit. footnote 18.

31 Ibidem.

32 See Article 4(1) of the Directive.

33 See WP29 opinion on applicable law: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf

Example 1 [34]: Legal complexity and cost of notifications for a data controller processing personal data in 15 Member States

A chain of shops has its head office in Member State X and franchised shops in 14 other Member States. Data relating to clients are collected in every shop, but are transferred to the head office in Member State X where some activities related to the processing of data take place (e.g. targeted advertising). The data protection law of Member State X would therefore be applicable to the processing activities carried out by the head office. However, the individual shops remain responsible for processing of their customers' personal data, which take place in the context of the shops' activities (for example, the collection of customers' personal data). To the extent that processing is carried out in the context of each shop's activities, it is subject to the law of the Member State where that shop is established. This means that each shop must notify its personal data processing operations to the national DPA according to the data protection law of the Member State where the shop is established, if notification is required by that law. The head office in Member State X and the individual shops in the other Member States could therefore be faced with the following scenario regarding notifications:

- Five Member States exempt all data controllers from notification requirements except in cases of sensitive data processing; hence the shops established in those five Member States do not have to notify their data processing operations.

- Member State X and four additional Member States A, B, C and D oblige all data controllers to notify processing operations and charge a fee of €300. The head office and the shops established in those five Member States have to notify the Data Protection Authority (DPA) in the Member State where they are established.

- Three Member States E, F and G exempt data controllers from notifications *only if* they have appointed a Data Protection Officer (DPO). If not, they have to notify and pay a charge of €150. The shops in these Member States have not appointed a DPO and therefore they have to notify their operations.

- Member State H obliges data controllers to notify processing only when processing is done through automated means and charges a fee of €500. The shop has to notify.

- Member State I obliges all data controllers to notify and charges a fee of €25.

In all cases where the shops have to notify the data processing operations in accordance with national data protection rules, the head office of the company has to consult a local lawyer to ensure legal compliance. Taking an average legal cost across the EU of €250/hour and assuming four hours of legal work per Member State, excluding the Member States that do not oblige data controllers to notify processing, the company would incur a cost of €10,000 in order to obtain legal advice. Including the notification fees for the processing activities in Member States X and A-I, the total costs of the notification requirement would be €12,475.

The **overall cost of notifications** – only in terms of administrative burden - is of approximately **€130 million per year** (see Annex 9 for details). In addition to the administrative burden, other direct and indirect costs of the requirement and its fragmentation have to be taken into account. This includes, inter alia, ***direct fees for notifications*** collected by some data protection authorities.

Notifications are, however, only **one procedural element illustrating the effect of fragmentation with particular clarity, but by far not the most important one in terms of**

[34] Based on the example in WP29 Opinion on Applicable Law, p.15.

its economic effect. A more detailed estimation of the overall effects of fragmentation is provided in Annex 9.

Fragmentation also negatively affects efficiency and effectiveness of **public authorities** as explained under Section 3.2.2 b) below.

- Transfers to third countries

Divergent approaches in the transposition of the Directive also apply to the provisions on **transfers to third countries**, which are additionally challenged by the increasingly globalised nature of data flows (i.e. the fact that personal data are being transferred across a large number of virtual and geographical borders, such as in the framework of "cloud computing").

This is illustrated by the following:

a) Adequacy:

One of the criteria for transferring personal data to a third country is that the latter provides for an ***'adequate' level of protection*** in relation to the data being transferred[35]. Currently, the decision on such adequate level of protection of a third country may be taken either by the Commission – in which case all Member States are bound by it - or by Member States themselves. In the latter case, some Member States allow the data controller itself to conduct the adequacy check (e.g. the UK), while others reserve it for national authorities, in particular the DPAs (e.g. France). This leads to a situation whereby transfers towards a certain third country may be considered lawful (as the level of data protection is considered to be adequate) in a Member State but not in others, and thus creates legal uncertainty for data controllers operating in more than one Member State that want to transfer data lawfully to a third country.

b) "Standard contractual clauses":

These are standard data protection clauses, established by Commission Decisions, to be included in contracts that allow data transfers from a data controller established in the EU to data controllers and processors in third countries[36]. Although Member States are under the obligation to recognise the standard contractual clauses approved by the Commission as fulfilling the requirements laid down by the Directive for the transfer of data to a third country - and can thus not refuse the transfer - some of them still require their national DPAs to review them and give their prior authorisation to the transfer. In such cases, data controllers are subject to unnecessary and varied requirements/authorisations, in spite of the establishment of model clauses aimed at facilitating the transfers while ensuring the necessary guarantees in terms of protection.

c) "*Binding Corporate Rules" (BCRs):*

"Binding Corporate Rules" (BCRs) are internal rules followed by a multinational corporation for transfers of personal data between the groups of companies belonging to the same multinational corporation, approved by one (or more) DPAs. BCRs have been developed as a matter of practice by DPAs and by the WP29[37] on the basis of an extensive interpretation of Article 25(2) of the Directive, in order to facilitate data transfers within multinationals operating worldwide. In such cases, if the transfers had to be regulated via contractual clauses (standard or not), this would require the conclusion of a myriad of contracts between the

---

35 See Article 25 of the Directive.

36 See http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm#h2-3.

37 WP29 adopted several opinions on BCRs available at: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm#data_transfers.

different entities of the group, which would have to follow the requirements provided for under the different national laws applicable. This type of situation can be avoided via the use of BCRs, which are therefore recognised as a useful tool by economic stakeholders, particularly by companies operating across several Member States and third countries. There are, however, some shortcomings that currently discourage companies from using them[38], such as:

- not all Member States and DPAs recognise the decisions taken by other DPAs and impose additional national requirements. The so-called "mutual recognition procedure" – whereby BCRs are reviewed and approved only by the "lead DPA", assisted by two other concerned DPAs[39] - is currently accepted only by 17 Member States plus the 3 EEA countries;

- the length of the current procedure for recognising/approving BCRs: six months as an average, but up to two years in complex cases and even longer when several authorisations are required according to national law;

- BCRs are currently limited to data controllers and do not cover data processors[40];

- the uncertainty about the possibility of applying BCRs to "groups of companies", because there is no clear definition of what this would cover.

According to feedback from stakeholders, particularly large enterprises, the above situation is an obstacle to business operations and reduces the attractiveness of the EU as a business location, as companies regularly need to transfer personal data from EU Member States to other world regions.

b) Inconsistent enforcement of data protection rules across the EU

In the 2003 implementation report of the Directive, the Commission considered enforcement as one of the problematic issues – mainly due to the limited resources of DPAs and to their non-prioritisation of enforcement tasks - stressing that "more vigorous and effective enforcement" was needed to improve compliance with the legislation. "Closer cooperation among the supervisory authorities" was also seen as a means – as an alternative to the revision of the Directive – to remedy the divergences between Member States' laws.

However, as confirmed by a comprehensive report issued recently by the Fundamental Rights Agency[41], the situation has not really improved since then.

– **Limited resources available to DPAs**

First of all, there are still important **variations in the level of funding** of data protection authorities and the resources available to them. Some DPAs are still under-resourced[42] and have thus difficulties in handling all complaints they receive, in carrying out enforcement actions and in cooperating effectively with other DPAs[43].

---

38 Based on information provided by 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. 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.

39 For the criteria currently used to determine the "lead DPA" see Working Document WP107 of WP29.

40 More specifically, BCRs can be used currently for transfers of personal data that is originally processed by the company as controller withint he same corporate group (such as data related to customers, employees) and not allowing the use of BCRs for data originally processed in the group as processor (such as processing made in the context of outsourcing services).

41 See the 2010 study on *Data Protection in the European Union: the role of National Data Protection Authorities*, available at http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf . See also Annex 2 for more details.

42 This is the case, for instance, in Austria, Romania and Slovakia.

43 A letter was also sent to the Commission in July 2011 by the Chair of WP29 highlighting the financial difficulties of certain DPAs, which would limit their participation in WP29 meetings.

– **Different powers of national DPAs**

Secondly, in some Member States the "effective powers of intervention" of DPAs as required by the Directive[44] are limited: for example, not all DPAs have the power to stop processing (e.g. BE), order the destruction or erasure of data (e.g., BE, DE, SE), access data banks and filing systems (e.g. UK) or to refer/bring the case before the judicial authorities (e.g., EE). Equally, not all DPAs have the power to impose fines on data controllers (e.g. BE, DK, LT, HU, AT, PL, SE); when fines are foreseen, their amount also varies considerably (see Annex 2 for details). In some cases, DPAs may only negotiate amicable solutions with those having violated the law or to refer them to courts (e.g., BE). Finally, some DPAs appear not to act with "complete independence" as required by Article 28(1) of the Directive and interpreted by the Court of Justice[45]. This means that the effective level of data protection varies across the EU, with the consequence that EU citizens' fundamental rights – the right to privacy, for example – may in practice differ from one Member State to the next.

– **Lack of effective cooperation between DPAs and absence of regulatory powers for the European Commission**

The Directive establishes a general duty of mutual cooperation and information exchange between national supervisory authorities[46]. However, as highlighted by DPAs themselves, practical cooperation between national supervisory authorities in cross-border cases can and should be improved[47].

Moreover, existing non-binding mechanisms and structures to ensure DPAs cooperation and to contribute to the "uniform application" of national laws on data protection – the Article 29 Working Party (WP29), in particular - are deficient in this regard[48]. While the WP29, and advisory body to the Commission[49], regularly adopts opinion on the interpretation of different provisions of the Directive to help uniform application, these are not binding and are not always followed by DPAs[50].

In addition, the fact that the Commission also ensures the secretariat of the WP29[51] 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. For example, while the Directive states that WP29 "[shall] act independently", some of its opinions - largely publicised in the press – have been perceived by some stakeholders as being "the Commission's view (or interpretation)" of a certain matter related to the Directive[52]. This misperception can be particularly problematic in cases where the opinions openly criticise EU policies[53]. On the other side, WP29 tends to consider that its independence can be undermined by the fact that the Commission provide for its secretariat and determine the available resources.

---

44 See Article 28(3), second indent.

45 The Commission has launched infringement procedures to address this issue: see in particular the recent judgement by the European Court of Justice (ECJ) in Case-C-518/07, Commission and EDPS vs. Germany. An infringement procedure on the same ground was launched against Austria in 2010; the situation in other Member States is currently being examined.

46 See Article 28(6).

47 See their Advice Paper on Article 28(6), cit., footnote 18.

48 The result of a survey carried out by the Commission with Member States showed that few of them have in one or two occasions modified their law following an opinion of the WP29 (see annex 2 for more details).

49 Its members are national DPAS, the EDPS and the Commission (the latter without voting rights).

50 The result of a survey carried out by the Commission with Member States showed that few of them have in one or two occasions modified their law following an opinion of the WP29 (see annex 2 for more details).

51 WP29 website is also hosted on the Europa server http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

52 See for example the – quite controversial - opinion on behavioural advertising (Opinion 2/2010): http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf.,

53 See for example WP29 Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_en.pdf.

The result of the above is that the existing governance system often leads to divergent decisions of DPAs *vis-à-vis* the same data controller for the same data processing, i.e. there is currently no "one-stop shop" for data controllers. This adds further to the uncertainty and costs faced by companies. No 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 and are subject to different national laws as well as to the "jurisdiction" of different DPAs.

This clearly does not help addressing, and on the contrary exacerbates, the problem of legal fragmentation at EU level and prevents an effective and consistent handling of cases where the right to data protection is affected on a European – if not global – scale.

Example 2 below illustrates the ***difficulties in ensuring a common and consistent European approach in enforcing the rules*** *vis-à-vis* data controllers affecting personal data across the EU and highlights the limits of the current enforcement model, as well as the lack of satisfactory cooperation between national DPAs.

Example 2: Different approaches towards online mapping services

A multinational company with several establishments in EU Member States has recently deployed an online navigation and mapping system across Europe. This system collects images of all private and public buildings, and may also take pictures of individuals.

The data protection safeguards applied to this service and thus the requirements imposed upon data controllers vary substantially from one Member State to another. Depending on the Member States and on their implementation of the notification requirements into national law, a notification may or may not be required for this system. In one Member State, the deployment of this service led to a major public and political outcry, and some aspects of it were considered to be unlawful. This concerned, for example, the inclusion of un-blurred pictures of persons entirely unaware that they were being photographed. The company then offered additional guarantees and safeguards to the individuals residing in that Member State after negotiation with the competent DPA. However the company refused to commit to offer the same additional guarantees to individuals in other Member States facing similar problems. Whereas in some Member States the company was sanctioned, in other Member States the DPAs considered that such a navigation or mapping system was in line with data protection requirements. The WP29 attempted, unsuccessfully, to coordinate the different DPAs positions so as to have a common EU approach and ensure a consistent enforcement of the rules *vis-à-vis* data controllers and individuals.

3.2.2. Who is affected and to what extent?

a) Economic operators

As the Directive leads to the simultaneous application of national laws where the controller is established in several Member States*, **data controllers operating across borders need to spend time and money*** (for legal advice, to prepare the required forms/documents etc) to comply ***with different, and sometimes contradictory, obligations***, such as the different requirements for notifications of data processing to DPAs. According to stakeholders' feedback, the data controller has to bear an ***administrative burden*** estimated to correspond to around ***€200 per (new) notification to the DPA***, without including the notification fees charged by the DPA itself. This leads to an overall administrative burden of **€ 130 million per year** due to notifications requirements (see Annex 9 for details). In addition to the administrative burden, other direct and indirect costs of the requirement and its fragmentation have to be taken into account. This includes, inter alia, ***direct fees for notifications*** collected by some data protection authorities.

As highlighted above, notifications are only **one procedural element illustrating the effect of fragmentation with particular clarity, but by far not the most important one in terms of its economic effect**. A more detailed estimation of the overall effects of fragmentation is provided in Annex 9.

The administrative burden resulting from the fragmentation within the EU internal market is estimated at about € 2.9 billion per annum[54], accounting for about half of the overall administrative burden linked to the Directive (i.e. about € 5,3 billion). These estimates are based on the Standard Cost Model and do not take account of compliance costs other than "administrative burden" (for example, to adapt to variable security requirements in different Member States). These additional compliance costs are, however, difficult to quantify given the variety of requirements across Member States.

To give an idea of overall compliance costs born by large and very large companies, a recent study - concerning companies based both inside and outside Europe[55] - estimates that each of these large multinational companies spends as an average €2.5 million per year on overall compliance with various data protection obligations (including administrative burden and other costs). A large part of these compliance costs are due to the fragmentation of national data protection rules - within the EU and beyond - and also cover compliance obligations non-data protection related. The same study concludes that the cost of non-compliance for such companies is much higher[56].

However, fragmentation is not only a problem for large, multinational enterprises. On the contrary, the complex situation on the ground deriving from diverging and sometimes conflicting data protection requirements at national level also constitutes a disincentive for all enterprises operating in the internal market from expanding their operations cross-border or establishing in more than one Member State. This problem thus concerns all EU businesses, including micro-enterprises and SMEs: this complexity leads to significant costs in terms of legal fees if they consider expanding their operations cross-border, and often acts as a disincentive from so doing. The outcome is that they do not reap the advantages of the internal market, with subsequent impacts on the EU economy, competition within the EU, and competitiveness in general.

b) Public authorities

Differences between Member States in implementing and interpreting the Directive also create difficulties for public authorities. It is difficult to estimate the costs, including the administrative burden, born by public authorities. Moreover, given the nature of their activities – generally addressed, in most cases, to individuals residing in the Member State of origin - they are likely to be only marginally affected by fragmentation.

However, fragmentation is relevant to the extent that it affects cooperation between national authorities aiming at attaining common EU objectives, for example in the area of public health[57].

---

54 This figure does not include the administrative burden for companies established outside the EU to which – due to the current criteria on applicable law– different EU national laws would also apply.

55 "The True Cost of Compliance – A Benchmark Study of Multinational Organisations" – Research Report, Independently Conducted by Ponemon Institute LCC, January 2011. 91% of the study sample concerns companies with over 1000 employees based in the EU, in North America and other world regions. (http://www.tripwire.com/ponemon-cost-of-compliance/pressKit/True_Cost_of_Compliance_Report.pdf).

56 This is estimated to be approximately €6,5 million, including costs linked to business disruption, reduced productivity, fees, penalties and other legal and non-legal settlement costs.

57 See Articles 168, 114 TFEU and Article 35 of the EU Charter of Fundamental Rights.

One way of ensuring health protection is to produce information on health indicators and trends at EU level to compare national public health between Member States, identify health problems common to Member States and trace their causes, inform EU policy on health and take decisions based on evidence. Health data are considered sensitive under the Directive. Their processing for monitoring public health is only allowed in specific situations, in particular where consent is given by data subjects or for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services or where Member States deem processing necessary due to substantial public interest. Since the Directive does not harmonise the rules for the processing of data specifically for public health purposes, Member States' practices vary greatly. As illustrated in the examples below, this lack of harmonisation and divergent national implementation affects cooperation between national authorities aiming at attaining common EU objectives.

Example 3: Divergent practices as a barrier to EU public health cooperation

Two examples of difficulties in pursuing public health policies due to divergences in data protection requirements are ***cancer registries*** and ***contact tracing***. In the first case, some Member States require the "prior informed consent" of individuals regarding the reporting of cancer incidence and mortality data, whereas other Member States have different requirements. The consequence of these differences is that cancer registries cannot operate in some Member States, or in some cases, the registries even collapse, and the reporting and comparison of cancer incidence across the EU is not sufficiently reliable.

In the second case, the collection of data on communicable diseases for contact tracing from entities concerned by travel activities for public health purposes, is not effectively conducted within the EU because some Member States have established diverging conditions for the processing of such data. This problem was particularly acute, for instance, during the H1N1 flu pandemic.

c) Individuals

Legal uncertainty and complexity have a chilling effect of on the preparedness of businesses, in particular SMEs, to offer their services across borders or online at all. This reduces the choice of offerings for consumers and the competition in the market. The potential benefits of the online single market are only available to a limited extent. At the same time, legal uncertainty also affects directly the willingness of consumers to make use of online services and in particular cross border services. Concerns about privacy and data protection are one of the factors that act as obstacles to the full development of the online single market.

3.3. PROBLEM 2 – Difficulties for individuals to stay in control of their personal data

3.3.1. Description of the problem

Individuals enjoy different data protection rights, due to fragmentation and inconsistent implementation and enforcement in different Member States. Furthermore, individuals are often neither aware nor in control of what happens to their personal data and therefore fail to exercise their rights effectively.

Globalisation and technological developments, particularly the fact that personal data are nowadays being transferred across an increasing number of virtual and geographical borders in the online economy, including through ***"cloud computing",*** further challenge the control individuals may keep over their own data.

a) Insufficient awareness, loss of control and trust, particularly in the online environment

In the ***online environment***, it is increasingly difficult for individuals to be aware of the processing of the data related to them and the risks linked to such processing, to maintain control over their own data and, ultimately, to assert their rights *vis-à-vis* data controllers.

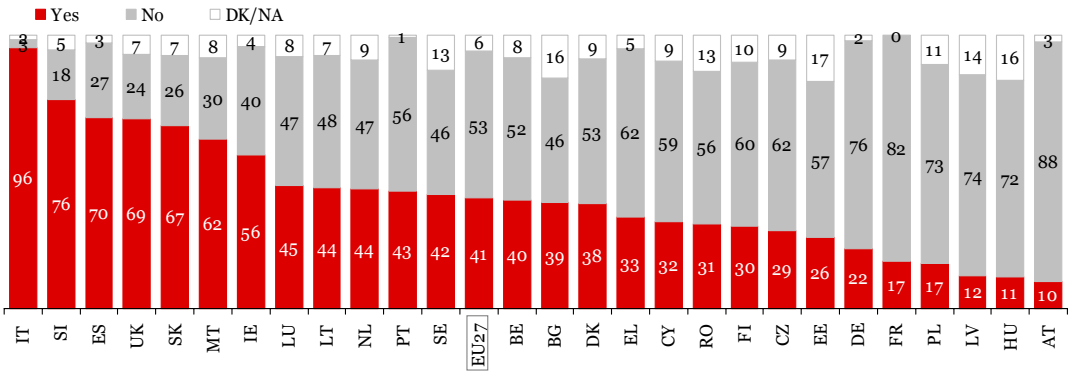
Two thirds of European citizens feel that the disclosure of personal data is a major concern for them and six in ten citizens consider that nowadays there is no alternative to disclosing personal data in order to obtain products and services[58]. Three quarters of citizens feel that they have either no or only partial control of their personal data on social networking sites[59].

– **Insufficient awareness and underestimation of privacy risks**

In order to be in control, individuals ***need to be aware*** by whom, on what grounds, from where, for what purposes, and for how long their personal data are being processed and what their rights are in relation to the processing. Currently, the duty to inform the data subject does not cover each of these elements; and even when sufficient information is available, it is often not understandable for the individual[60].

A 2008 survey[61] revealed that on average in the EU only 41% of data controllers maintain and update privacy policy notices. This percentage is even lower for SMEs[62].

Maintaining and updating privacy policy notices



Q13a. Does your company maintain and update privacy policy notices?
%, Base: all respondents, by country

When they are provided, ***online privacy policy notices ("Privacy Statements")*** are often overly complex, making use of technical and legal terminology. This complexity is reflected in the responses to a 2011 Eurobarometer survey: close to six in ten internet users claim they read privacy policies (58%), but only a third say that they read them and understand them (34%); a quarter say that they read them but do not fully understand them (24%). A quarter

58 EB 2011.

59 EB 2011.

60 For example, individuals do not always realise that "free" online services generate processing of their personal data.

61 Flash Eurobarometer 226 *Data Protection in the European Union – Data Controllers' Perceptions* (2008), p.34. Available at http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf ("EB 2008" in future references).

62 The consultation of SMEs (see Annex 8) showed that only 36.3% of respondents have a privacy policy on their company's website. Furthermore, 48.6% of SMEs state that they have been providing information to data subjects, as required by data protection laws, but only 27.4% of them state that they always provide this information. More than 21% of respondents state that they *never* provide such information to data subjects.

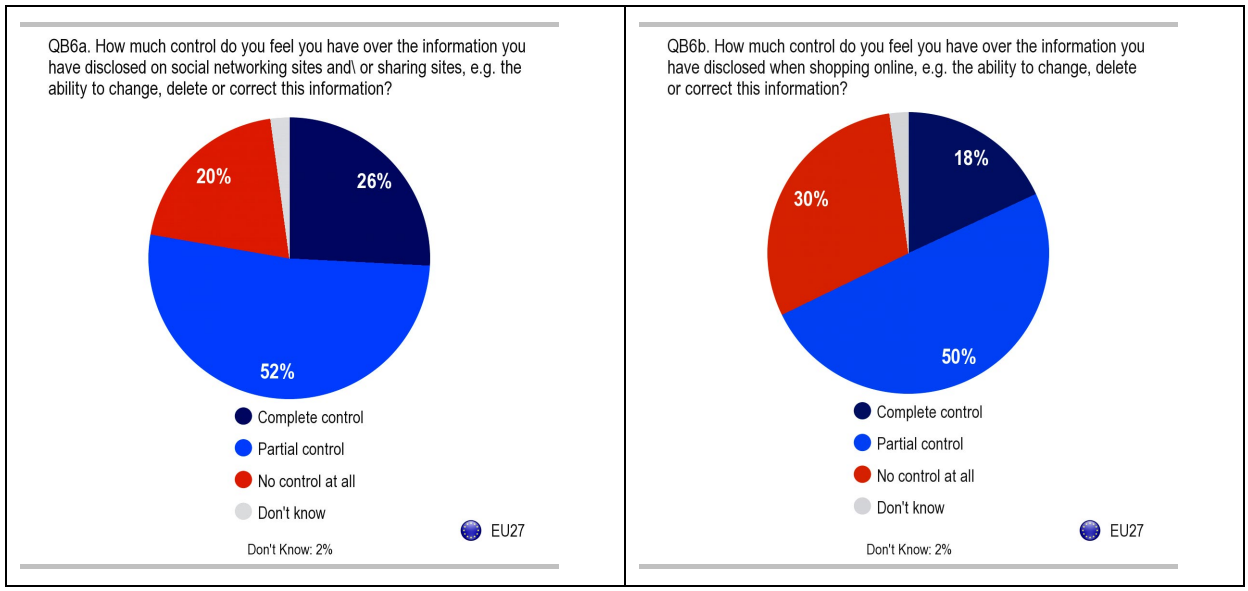
say they do not read them (25%), one in twenty say they do not know where to find them (5%) and almost one in ten ignore privacy statements (8%).[63]

The lack of readily available and easily understandable information makes it difficult for individuals to become aware of the ***risks*** linked to the use of their personal data and take the necessary measures to ensure their own protection. For instance, almost half of the respondents to a recent Eurobarometer do not feel sufficiently informed on social networking and file sharing sites[64].

This is particularly relevant with respect to ***children***, who tend to underestimate the risks and consequences of making their personal data available online. A recent survey funded under the Safer Internet programme[65] shows that 38% of children aged between 9 and 12 and 77% of 13-16 year olds have a profile on a social network site (SNS)[66] even though the privacy policies of most social networking sites prohibit this. A quarter of 9-12 year olds have their profile as 'public', displaying in some cases private information such as their address and/or phone number to all other users.

– **Loss of control and trust**

As confirmed by a recent Eurobarometer survey[67], profiling, data mining, and technological developments that ease the exchangeability of personal data make it even more important for individuals to be in control of their personal data. The graph below shows the extent to which individuals feel in control of their personal data online.



In a recent Eurobarometer survey, 75% of respondents that owned an account on a social networking site and 80% of online shoppers consider that they have no or only partial control over their personal data. 70% of them are concerned that economic operators processing their personal data may use it for a different purpose than the one they were collected for[68].

63 Ibidem.
64 EB 2011.
65 See for details on the programme: http://ec.europa.eu/information_society/activities/sip/index_en.htm.
66 For details see: http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/ShortSNS.pdf.
67 EB 2011.
68 Ibidem.

In relation to ***profiling***, the Directive grants individuals the right not to be subject to a decision which is based solely on automated processing of data intended to evaluate personal aspects of the data subject. This safeguard only applies to decisions based "solely" on automated processing so that there is a risk that it is easily circumvented by including a merely formal human intervention in the decision process which has no influence on its outcome. Examples for such procedures include the conditions of a telephone service or insurance contract, where conditions and tariffs are adjusted on the basis of a scoring of the potential customers on the basis of general and individual data related to him or her. While the decision to make a specific offer is formally with the sales staff, this person's decision is defined by the outcome of an automated system so that he or she effectively has no margin of decision to deviate from that suggestion. In the specific case of ***behavioural advertising***[69], 54% of Europeans feel uncomfortable with practices which involve online profiling and a large majority of them (74%) would like to be given the opportunity to give (or refuse) their specific consent before the collection and processing of their personal data[70].

With current technologies it is possible to collect and process personal data anywhere, at any time and in many different forms. For instance, mobile devices can nowadays easily obtain information about the ***geographical location*** of individuals in real time by many different technological means[71]. Services based on location information are considered one of the most dynamic areas for innovation. Location based services can provide considerable benefits to individuals, from improved real-time routing algorithms which consider traffic density and congestions and provide faster and more fuel-efficient routes than static systems, over faster dispatching of emergency services based on accurate real-time location information, to advertising services in the immediate vicinity of the requesting individual. The possibilities for using location information as parameters in services such as search, social networking or other web 2.0 services are still being explored. On the other hand, location information ***may be retained to create motion profiles of individuals*** containing information about their each and every move at a level of detail and for a period far beyond what individuals would remember themselves. Divergent application of data protection rules would not only hamper the development of useful services, but would also reduce citizens' willingness to use existing services when they fear becoming subject of constant monitoring of their lives.

When using online services, individuals are associated with ***technical (online) identifiers*** provided by their devices, applications, tools and protocols[72] and leave traces of their activity at each server they communicate with. This interaction log and other information received by the servers, e.g. time and contact of interaction, location data etc, can build a very detailed trace of an individual's online activity. Even without a name or other traditional identifying attribute, it is often possible to effectively identify the individual to whom the data relates. However, legal practice in Member States differs as to the assessment of identifiability of such online data collections (and hence whether to consider such data as personal data) and thereby leaves individuals with uncertainty and effective impossibility to assert their rights regarding the fastest growing and most comprehensive collections of data about their

---

69 This is a technique used by online publishers and advertisers to increase the effectiveness of their campaigns. Behavioural targeting uses information collected on an individual's web-browsing behaviour, such as the pages they have visited or the searches they have made, to select which advertisements to display to that individual. This allows site owners or ad networks to display advertising content which is considered to be more relevant to the interests of the individual viewing the page. On the theory that properly targeted ads will generate more consumer interest, the web site publisher and advertising agency may charge a higher price for these advertisements than for random advertising or ads based on the context of a site.

70 EB 2011. See also WP29 Opinion 2/2010 on Online Behavioural Advertising, as well as Opinion 15/2011 on consent , both available at: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_search_en.htm.

71 E.g. by using satellite navigation data, WLAN broadcast information and maps of communication network antenna information.

72 Such as IP or MAC addresses, cookie identifiers, IMEIs and others.

behaviour. While some Member States recognise the sensitivity of such data and provide for clear rules on the use and retention of usage data, others do not provide for legal provisions addressing this issue, leaving the application of data protection principles to decision on a case by case basis.

The fact that important data controllers operating in the digital/online market are **established outside the EU** makes it even more challenging for individuals to keep control over their own data in such cases and to effectively exercise their rights. The practical application of the criteria provided by the Directive on whether and when EU laws are applicable to processing of personal data by controllers established outside the EU/EEA is currently subject of considerable discussion. Member States apply different interpretations regarding the "use of equipment" on the territory of Member States[73]. Other relevant issues of interpretations concern the identification of the actual data controller and the distinction between controllers and processors. Moreover, even in cases where the applicability of EU legislation is established, enforcement of data protection laws and administrative measures and decisions remains problematic. Even when parts of the equipment used for processing are located within the EU, EU based authorities usually have no means to enforce decisions or sanctions on entities whose main establishment is outside the territory of their jurisdiction. They may also meet difficulties to enforce the basic requirement for the establishment of an EU representative by data controllers not established in the EU but subject to EU legislation. In particular in cases where services are clearly customized to address citizens of a specific EU Member State, by using the county's languages and adapting to its cultural preferences and obtaining revenue from advertising local brands, products and services, it is usually not even possible for the citizen to recognize that by using such services they are entrusting their personal data to a data controller which may not effectively be subject to the adequate data protection legislation.

Where personal data is collected by an entity established in the EU which is part of an international group or acts on behalf of a main service provider outside the EU, provision of services is often based on the transfer of most or all personal data collected to processing facilities outside the EU. In principle, such transfers to third countries are subject to conditions which shall ensure that appropriate data protection safeguards are observed by the receiving entity in a third country. From an individual's perspective, it is important to know whether the controller – e.g. as a provider of a service on the web – complies with the conditions and legal requirements, and how to obtain support in case of a suspected breach of the rules.

– **Data breaches**

The increased number of ***data breaches*** of large companies' customer databases is an additional factor undermining individuals' trust and confidence. As shown by the example below, these security failures may lead to harmful consequences for individuals, ranging from undesired spam to identity theft[74]. In the context of the SME consultation, in relation to data breaches, 7.1% of respondents have recently experienced a breach (of which 55% actually informed the individuals whose data were affected by breaches) and indicated a cost of less than €500 for the notification (see Annex 8 for details).

Example 4: Recent data breach case putting data subjects' personal data at risk

[73] See WP29 opinion on applicable law on this matter, cit. footnoie 18, pp. 18-25

[74] Interesting figures on recent data breaches and losses can be found at: http://datalossdb.org (*data not verified*).

One recent prominent case of data breach was that of a gaming service, in which according to media reports tens of million user accounts were compromised by hackers, including users' names, addresses and possibly credit card data. A further problem in this case was the fact that the data controller delayed the notification of the breach to data subjects by one week after the breach in the security of the network had been discovered. This attracted additional criticism by users, and prompted questions on whether there needed to be explicit deadlines within which a data controller must notify a data breach to data subjects and supervisory authorities.

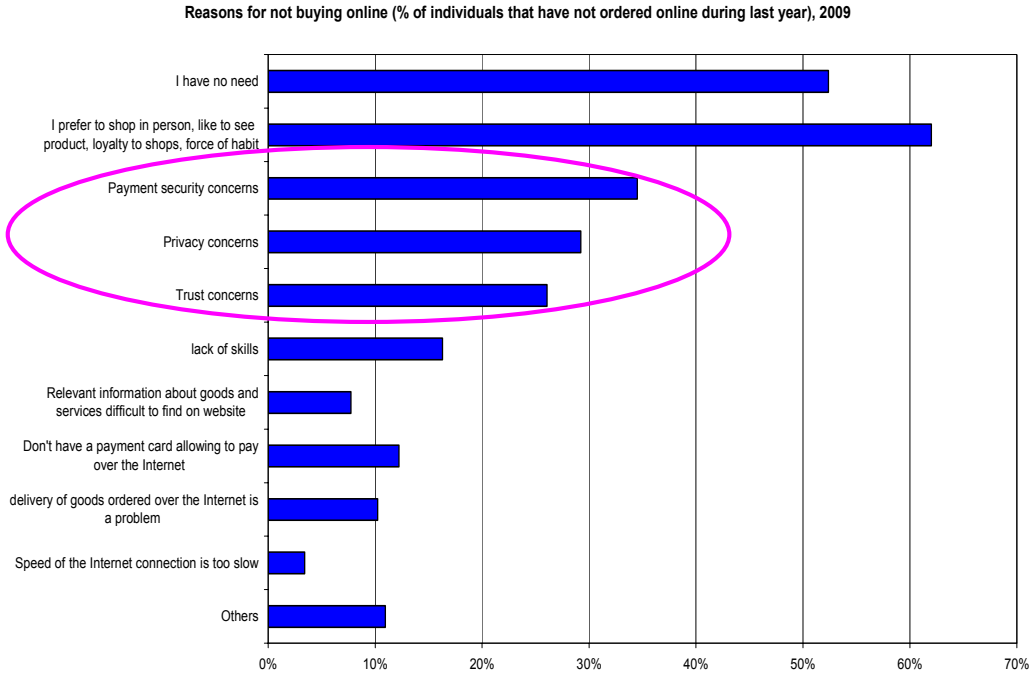
Individuals react on the increase of data breaches with raising concern. The percentage of individuals that would want to be informed when their personal data is lost, stolen or altered in any way is constantly increasing and has reached the level of 88% EU wide[75]**.** At present, EU wide harmonised rules on the notification for data breaches exist only for the electronic communications sector, which are still being implemented by many Member States following the 2009 Telecom Reform. For other sectors, some Member States have implemented rules at national level through different legal instruments (laws, regulations, guidance by the DPA, but no harmonised rules have been established so far. Increasing pressure to establish such rules could move national legislators to adopting national legislation on breach notifications. This could create the risk of increased divergence between Member States on this aspect.

– **Fragmentation**

Individuals' confidence and trust is already weakened by the ***fragmentation, legal uncertainty and inconsistent enforcement*** of data protection rules across Member States. The same individual, travelling to another Member State or shopping cross-border on the internet, would see his/her ***rights, and the way of exercising them, vary significantly*** depending on the applicable national legislation. Thus, individuals, even if they are aware of the data protection provided by their own Member States, often do not know how to exercise their data protection rights when their personal data are processed across several Member States. This is an additional factor ***reducing their readiness to shop for goods and services from other Member States.***

According to the Digital Agenda for Europe, a lack of trust in the online environment is hampering the development of Europe's online economy. A recent Eurostat survey shows that privacy and trust concerns are amongst the top reasons preventing people from buying online[76]. Among people who did not order online in 2009, the top reasons were: payment security concerns, privacy concerns, and trust concerns.

[75] Special Eurobarometer 362 E-Communications Household Survey,
[76] See Digital Agenda for Europe, p.12.



.

Source: Eurostat Community Survey on ICT Usage by Households and by Individuals 2009

b) Difficulties in exercising data protection rights

The Directive provides for a set of rights for individuals, such as the right to access, rectify, block and delete their own data, as well as the right to receive information for what purposes and by whom their data are processed. The Directive also provides judicial remedies as well as the right to receive compensation for damage suffered. These rights are, however, expressed in general terms and the way they can actually be exercised is not clearly specified.

– **Difficulties to access one's own data**

Access to personal data is a significant matter[77]: as evidenced by a 2008 survey of data controllers, 46% of data controllers surveyed indicated that their company had received requests for access to personal data in the preceding year[78].

However, individuals can access their own data more easily in some Member States than in others. In some Member States, data controllers are allowed to demand a fee to access their data, while in others it is free of charge[79]. Some Member States impose a deadline on data controllers to respond to access requests, while others do not. The Commission has received several complaints from individuals that asked data controllers for access to the data stored about them and received no or unsatisfactory responses. Complaints to their national data protection authorities did not lead to effective remedies, as these authorities declared themselves not competent or incapable of following up in some cases. All these observations contribute to individuals' perception that their rights are not effectively guaranteed by the current implementation of the framework across the Member States.

– **Difficulties to have one's own data deleted – the "right to be forgotten"**

---

77 Access to personal data is part of the fundamental right to data protection as enshrined in the charter of fundamental rights.

78 EB 2008.

79 EB 2011.

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 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 environment[80].

While the Directive already requires that data is not kept in a form which permits identification of data subjects for any longer than necessary for the purposes for which the data were originally collected or for compatible purposes for which they are further processed, in practice this is often not implemented properly. For an individual, it is very difficult to assess the data preservation policies of a data controller. In any case, if the processing of personal data is based only on the consent of the data subjects, there is generally no justification for keeping this data after the data subjects have withdrawn their consent and requested deletion of the data. Faced with different interpretations and practices in different Member States, both individuals and data controller need more clarity on the rules on the deletion of data.

– **Difficulties to withdraw and transfer personal data from an application or service – "data portability"**

There is also no explicit right for the individual ***to extract his/her own personal data*** (e.g. his/her photos or a list of friends) from an application or service in a format that may be processed further, so that the individual may transfer data to another application or service. With increasing use of certain online service, the amount of personal data collected in this service becomes an obstacle for changing services, even if better, cheaper or more privacy friendly services become available. This could mean the loss of contact information, calendar history, interpersonal communications exchanges and other kinds of personally or socially relevant data which is very difficult to recreate or restore. Even where possible, re-entering the data manually into another service can be a major effort. This situation effectively creates a lock-in with the specific service for the user and makes it effectively very costly or even impossible to change provider and benefit from better services available on the market. Portability is a key factor for effective competition, as evidenced in other market sectors, e.g. number portability in the telecom sector.

– **Difficulties to access effective remedies**

As regards ***administrative and judicial remedies and compensation***, individuals are in most cases not aware of the possibility to lodge a complaint to a DPA: 63% of respondents to a recent Eurobarometer have never heard of any public authority responsible for the protection of personal data[81].

Therefore, in many Member States judicial remedies, while available, are very rarely pursued in practice. This is also related to a general reluctance to bring an action to court against large global companies in particular, when costs for legal action are disproportionate compared to the potential compensation that could be obtained.

Whereas the Directive provides the possibility that associations representing a data subject may lodge claims to the DPA, there is not a right to be represented by an association in a court case, which might otherwise give an incentive and limit the financial risk of going to court in relation to an infringement of data protection rules.

---

80 http://www.guardian.co.uk/technology/2011/oct/20/facebook-fine-holding-data-deleted

81 EB 2011.

3.3.2. Who is affected and to what extent?

The difficulties in exercising data protection rights potentially affect every individual in the EU, given the rapid growth of digital information on individuals as a result of evolving information and communication technologies. Processing of personal data is part of everybody's daily life: every transaction is likely to create a digital record, e.g. opening a bank account, shopping on line (on average, about 40% of individuals in the EU currently use the internet to purchase goods and services[82]), requesting a shop's loyalty card, buying a book or uploading photos on the internet.

a) Individuals

Individuals, including children, are potentially exposed to different types of harm. This includes reputational or even physical harm (caused e.g. by the publication of health-related data on a public blog without the concerned person's consent or harassment caused e.g. by unsolicited advertising) and also financial harm particularly by identity theft, the total cost of which at EU level is estimated at around €700 million per year[83]. In particular for young people, the disclosure of personal data can cause immense social and mental harm. The media have given much attention to several recent cases where sensitive personal information was published and led to bullying and harassment or serious humiliation so that the victim was driven into suicide. Personal data breaches are also becoming more common and more severe. A 2010 study[84] in the UK indicates that, out of 622 UK-based IT and business managers, analysts, and executives from 15 industry sectors, 71% reported at least one incident of data breach in their respective organisations. The same study reports that while the average organisational cost of a data breach decreased by nearly 3% – from £1.73 million in the 2008 annual study to £1.68 million in 2009 – the average cost per compromised personal data-set rose by £4 (7%), from £60 to £64 (approximately €74[85]).

Based on information from 20 Member States, there were 54,640 complaints concerning (potentially) unlawful processing of personal data or breaches of data protection rights in the EU in 2009[86]. Half of the total number of requests and complaints received by the Commission in 2010 in relation to fundamental rights and freedoms concern data protection[87]. Many individuals may have experienced detriment, but either resolved the issue with the data controller or did not pursue the complaint. Those that pursue a complaint are likely to have experienced significant harm. Over a third (39%) of all potential EU users of the internet may not be fully benefitting because of concerns over safety and data protection[88]. Individuals limit their use of new technologies, particularly the internet and online services, because of lack of trust in the digital environment and fears about possible misuse of their personal data. Those not benefitting from ICT because of fears over data protection lose out in terms of price benefits online and in time taken to access goods and services.

---

82 See the Digital Agenda Scoreboard 2011, available at http://ec.europa.eu/information_society/digital-agenda/scoreboard/docs/scoreboard.pdf, p.12-17.

83 This figure is based on data concerning identity thefts in the UK (see the study by the Information Commissioner's Office *The Privacy Dividend: the business case for investing in proactive privacy protection*, 2010: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_dividend.pdf) and which have been weighted taking into account the lower frequency of identity thefts in other EU countries (e.g., France, Spain, Germany) compared to the UK.

84 Ponemon Institute LLC, Symantec, *2010 Annual Study: UK Encryption Trends.*

85 Based on March 2011 exchange rates.

86 Information gathered via a survey by GHK consulting in the framework of their study.

87 Cf. Commission 2010 Report on the Application of the EU Charter of Fundamental Rights, p. 31; http://ec.europa.eu/justice/policies/rights/docs/report_EU_charter_FR_2010_en.pdf

88 Flash Eurobarometer N° 250 (2008) - Confidence in the Information Society.

Privacy and the protection of personal data are fundamental rights enshrined in the Charter of Fundamental Rights of the European Union. They play a key role for the exercise of fundamental rights in a broader sense. Many of the fundamental freedoms can only be fully exercised if the individual is reassured that it is not subject of permanent surveillance and observation by authorities and other powerful organisations. Freedom of thought, freedom of expression, freedom of assembly and association, but also the freedom to conduct a business will not be exercised fully by all citizens in an environment where the individual feels that each of her or his moves, acts, expressions and transaction is subject to scrutiny by others trying to control him or her. Exercise of these freedoms is crucial to maintain all fundamental rights.

In a free and democratic society, the individual must have reassurance that fundamental rights are respected. Measures to protect individuals with regard to the processing of personal data must be effective, credible and easily accessible for the individual. Information about risks to privacy must be made accessible and the conditions of the processing of personal data must be transparent and understandable.

In today's digitised society, communication and interaction rely on digital media and communications channels. Web 2.0 tools, including social media, play an increasingly important role for social interaction and exchange. Not being able to use these media effectively restricts the exercise of fundamental rights in the social reality. Where the individual suspects that his or her interactions in this space are subject of surveillance, collection and analysis by authorities, service operators or others, it looses partly the possibility of exercising some fundamental rights. This chilling effect can already be caused by the perception of surveillance, which may or may not exist. The lack of transparency of processing and of accessible means to effectively enforce data protection rules is therefore directly affecting individuals' fundamental rights.

The same effect is also true with regard to the economic aspects of citizens' life. Be it consumers who are subject to profiling and classification, or employees or job candidates subject to extensive research and analysis of their online activities, the economic possibilities of individuals are reduced towards the organisations having access to extensive data collections about them. The individual's negotiation position is severely affected by the imbalance of information and the possibility of the other side to use detailed knowledge of the situation and needs, e.g. when offering a loan or an employment contract with less advantageous conditions for the consumer or employee.

Lack of transparency of data processing, lack of credible enforcement and the absence of effective remedies and sanctions for violations of the principles contribute to creating a climate in which the individuals do not rely on exercising their fundamental freedoms and economic rights fully, even when some concerns regarding data collection and surveillance may be exaggerated over the reality. Doubts about the actual degree of protection have a chilling effect on democracy and also on the economic activity in the market.

b) Economic operators

Many economic activities are linked to the processing of personal data. The current inconsistent application of EU laws impacts the ***take-up of online and audiovisual media services.*** Individuals limit their use of new technologies because of a lack of trust in the digital environment and fears about possible misuse of their data. This creates 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 tremendous economic benefits.

c) Public authorities

Public authorities have undertaken considerable investments in making public services accessible online. This dematerialisation can create considerable benefits in terms of efficiency, quality of services and reduction of resources required for the provision of services. When citizens can enter their requests for certain public service directly into online systems, they enjoy a better service then when they would have to go to the authority physically or to communicate in writing, while the authority at the same time saves resources for servicing physical visitors or processing paper mail and for entering data into their systems.

The potential benefits require citizens' willingness to make use of online offerings. Lack of confidence and trust in the services, fear or potential misuse of data collected will make many potential users refrain from using these services. With growing concern about privacy in the online world, this section of the population may grow further. This development reduces the value of the investments in public online services and their positive effects for the public budget, when the more traditional and more expensive ways of offering public services have to be maintained.

3.4. PROBLEM 3 – Gaps and inconsistencies in the protection of personal data in the field of police and judicial cooperation in criminal matters

3.4.1. Description of the problem[89]

The scope of the Directive, based on an internal market legal basis, specifically excluded police and judicial cooperation in criminal matters. The Framework Decision adopted in 2008 to regulate data processing in the area of police cooperation and judicial cooperation in criminal matters reflects the specificities of the pre-Lisbon "pillar" structure of the EU[90] and is characterised by **a limited scope and various other gaps,** often leading to legal uncertainty for individuals and law enforcement authorities, as well as to practical difficulties of implementation. Moreover, while the Framework Decision contains general data protection principles (e.g., on lawfulness of data processing, right to access, rectify and delete one's own personal data), it provides at the same time for wide possibilities of derogating to them at national level, thereby not harmonising them. This does not only risk emptying such principles of their very purpose – and thus negatively affecting the fundamental right of individuals to the protection of their personal data in this area - but also hinders the smooth exchange of personal data between relevant national authorities. This situation is aggravated by the uncertain relation between the Framework Decision and existing "former third pillar" instruments with specific data protection rules, which adds to the complexity of the legal framework at EU level and increases the legal uncertainty for both individuals and law enforcement authorities.

a) Limited scope of application of the Framework Decision

The Framework Decision is limited in scope in that it does not cover data processing by police and judicial authorities at ***domestic (purely national) level,*** since its scope is limited to cross-border processing activities (i.e. personal data that "are or have been transmitted or made available" between Member States or between a Member State and Union authorities or

---

89 See Annex 3 for further details.

90 This also entails no powers for the Commission to launch infringement procedures against Member States and limited powers for the ECJ for a transitional period of 5 years from the entry into force of the Lisbon Treaty (i.e. until 1st December 2014). See Article 10 of Protocol No 36 on transitional provisions annexed to the treaties.

bodies[91]). This is problematic both in legal and in practical terms. Legally, the newly established Article 16 TFEU covers all areas "which fall under the scope of Union law" - thus including police cooperation and judicial cooperation in criminal matters[92]. Hence, both 'purely domestic' and 'cross-border' activities are covered. Given that the Framework Decision only covers cross-border processing activities of police and judicial authorities in criminal matters, the legislator has now the duty to extend its scope in order to fill this gap, which causes several problems[93].

First of all, as confirmed by several Member States' experts during the workshop organised on 2 February 2011 on the implementation of the Framework Decision and in the replies to the Commission's questionnaire related to the implementation of the Framework Decision[94], 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. Plus, *a priori*, any purely domestically processed data may be subject to cross-border transmission. This somehow "artificial" distinction thus complicates the actual implementation and application of the Framework Decision: law enforcement authorities are burdened by unmanageable distinctions between domestic data and data transmitted or available for transmission. Criminal files are in quite a number of cases composed of data originating from different authorities. The consequence of the limited scope is that parts of such files — the parts containing data originating from authorities in other Member States — are protected under the Framework Decision whereas other parts are not protected, or at least not under the same regime. In addition, the legal certainty for individuals can be harmed since data originating from third countries, but not exchanged between Member States are not covered by the Framework Decision. The processing of those data entails specific risks to the data subject should there be, for instance, no legal obligation in a Member State to examine the accuracy of those data.

Secondly, good co-operation between Member States requires there to be mutual trust between Member States, as a condition for a successful exchange of information. If common standards are applied to the processing of data this will facilitate cooperation and mutual exchange of information between Member States' law enforcement authorities.

Finally, this distinction exists neither in the Directive nor in the relevant Council of Europe instruments[95].

b) Low level of harmonisation of the Framework Decision

The Framework Decision provides for a ***very minimum level of harmonisation*** and leaves a very large room for manoeuvre to Member States in terms of its implementation into national law, for example in relation to the ***right of access*** of individuals to personal data related to them (Article 17) or to the exceptions to the ***purpose limitation principle*** (Articles 3 and 11). Provisions on ***information*** to be given to data subjects are very general (Article 16) and

---

91 Including information systems established on the basis of Title VI of the previous Treaty (TEU).

92 Specific rules for processing by Member States in the area of Common Foreign and Security Policy shall be laid down by a Council Decision based on Article 39 TEU.

93 Article 16 states that "The European Parliament and the Council […] shall lay down the rules relating to the protection of individuals with regard to the protection of individuals with regard to the processing of personal data […]" (*emphasis added*).

94 See the Implementation Report of the Framework decision (COM…)

95 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.: 108), ('Convention 108') and its Additional Protocol (ETS No.: 181), as well as Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector.

basically refer to national laws, and therefore implemented variably. Moreover, the Framework Decisions allows national laws to impose higher safeguards than those established in there for any issue covered (Article 1(2)). In certain cases, specific national processing restrictions in place in one Member State have to be met by the other Member States (Article 12). Therefore, exchanges of information still remain subject to very different national 'rules of origin' and varying standards that affect efficiency in law enforcement cooperation. As a consequence, police authorities may have to apply heterogeneous legal requirements to processing systems containing data originating from different Member States depending on various factors, such as whether personal data have been collected domestically or not, whether each of the transmitting bodies has given its consent for the envisaged purpose, whether further processing restrictions requested by each of the transmitting bodies exist etc.

Also rules on ***international transfers*** (Article 13) leave a large room of discretion to Member States in assessing the "adequacy" of a third country for the purposes of transferring personal data to prevent, investigate, detect or prosecute criminal offences or the execution of criminal penalties. This creates legal uncertainty and affects practical implementation, as pointed our by some Member States in their reply to the questionnaire on the Implementation of the Framework Decision, calling for more uniform rules in this area[96]. The absence of a sufficiently harmonised system for the exchange of personal data with third countries also harms the trust between the authorities of the Member States, since an authority might be less willing to share information with an authority in another Member State if this Member State could also share this information with authorities of third countries in the absence of clear safeguards. It also enables "forum shopping" by authorities of third countries: those authorities could ask for information in the Member State with is considered to have the lowest legal requirements for transfers.

Additionally, the Framework Decision does not contain any mechanism – no implementing powers for the Commission, no advisory group similar to the "Article 29" Working Party - fostering a common approach in its implementation or supporting common interpretation of its provisions. The Commission has currently no infringement powers in cases of non- or incorrect transposition of the Framework Decision, and the Court of Justice has limited powers as well for a transitional 5-year period from the entry into force of the Lisbon Treaty[97].

c) Additional gaps and shortcomings of the Framework Decision

The Framework Decision also fails to address issues that are particularly important in the framework of data processing by police cooperation and other law enforcement authorities.

First of all, there are no specific provisions in the Framework Decision regulating the ***processing of genetic data*** for the purposes of a criminal investigation or a judicial procedure. As pointed out very clearly by the European Court of Human Rights[98], this is an area were clear rules are essential to regulate the scope and application of measures by law enforcement authorities. The Court ruled that protection afforded by Article 8 of the European Convention

---

96 See the Annex to the Implementation Report of the Framework decision (COM…), Table 6.

97 See footnote 91.

98 S. and Marper v. the United Kingdom, judgment of 4 December 2008, applications nos. 30562/04 and 30566/04, which showed the importance of adequately protecting such data particularly in relation to use by police authorities. The Court ruled, in particular, 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.

on Human Rights would otherwise be unacceptably weakened by the use of modern scientific techniques (such as DNA testing) in the criminal justice system without a careful balancing between the potential benefits of the extensive use of such techniques against important private-life interests.

Other relevant issues not covered by the Framework Decision, which are included in some other "former third pillar" instruments as well as in Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, are the following:

– 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 receive.

d) Unclear relation between the Framework Decision and other "former third pillar" instruments

In addition to the above problems linked to the limited scope and other gaps of the Framework Decision, the relation between its provisions and specific data protection rules contained in other "former third pillar" legal acts[99] – adopted prior to the Framework Decision - is not entirely clear. In principle, the Framework Decision leaves unaffected most of the acts previously adopted containing specific data protection provisions, in particular where such provisions constitute "a complete and coherent set of rules"[100]. In other cases, however, the Framework Decision is only partially applicable, i.e. it does not apply where the provisions of these (former third pillar) acts impose conditions upon the receiving Member States that are "more restrictive" than those in the Framework Decision[101]. These rules setting the relation between the Framework Decision and data protection provisions contained in other acts in the area of police and judicial cooperation in criminal matters are unclear and leave a large room for interpretation on a case-by-case basis as to which rules shall apply to a concrete situation.

The result is a fragmented environment creating legal uncertainty for both the concerned individuals and law enforcement authorities. As a consequence, law enforcement agencies may be reluctant to share information for enforcement purposes due to concerns about the legal consequences[102]. This negatively affects the effectiveness of cross-border cooperation in this area.

---

99 See Annex 3 for the list of such acts.

100 See Article 28 and recital 39. Some of these instruments are specifically mentioned (e.g. the acts regulating the functioning of Europol, Eurojust, the Schengen Information System and the Customs Information System) but the list is not exhaustive.;

101 See recital 40.

102 This is confirmed by a (non-public) study carried out by the International Centre for Migration Policy Development ("Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments", September

Example 5 – Difficulties for police authorities created by a variable and complex legal environment

A police authority in one Member State (country A) is dealing with an investigation related to cross-border trafficking of human beings. The nature of the case implies that information, including personal data of suspects, is required from two other Member States (country B and country C).

When processing the data related to the above investigation, the police authorities in country A have to apply different data protection rules for different aspects of the file related to the investigation, depending on whether the data come from their own Member State or have been received from country B or C. This means that, for example, different rules may apply to the further transmission of data related to the investigation – which may not be easily separated/distinguished depending on their origin - to other non-police authorities (i.e., immigration or asylum authorities) or in relation to the information that can be provided to the individuals concerned.

3.4.2. Who is affected and to what extent?

The complex and fragmented legal environment in the area of police cooperation and judicial cooperation in criminal matters is highly problematic as it creates uncertainties about the rules applicable and hence affects individuals, public authorities and private data controllers, in the following way:

– ***Individuals*** are unlikely to know which rules apply to the processing of personal data by the police and other law enforcement authorities and thus what their rights are in this context. They also enjoy different rights depending on which Member State or public authority is processing their data.

– The differences in Member States' data protection standards in this area, as well as the uncertainties about the rules to be applied to a specific situation, ***affect the smooth cooperation between Member States' police and judicial authorities.*** The fact that different, sometimes conflicting rules, may apply to personal data related to a same investigation – depending on the origin of the data and/or on which specific instruments apply - adds a layer of complexity to the work of police and other competent authorities in Member States, particularly in the case of cross-border matters.

– ***Private companies*** operating in different Member States are affected by the absence of common and uniform rules at EU level on issues such as further processing by law enforcement authorities of data held by them.

3.5. The drivers behind the identified problems

The ***main drivers behind the three problems are the shortcomings of the existing legal framework and of the current governance system in the area of data protection.***

As regards the ***Directive,*** the analysis of the problems showed that, while most of its key principles remain sound, several of its provisions are not sufficiently clear, are sometimes difficult to apply to new situations and developments and often leave an excessively large margin of manoeuvre to Member States in their national implementation. This leads to important variations and divergences across the EU. Enforcement of the Directive is not always satisfactory and, above all, is inconsistent across Member States.

2010). The study finds that one of the main legal problems in cross-border information exchange derive from the differences in national legislation in member States, in particular differences in privacy and data protection always (or the different definitions of what constitutes a crime).

This has precluded the desired level of harmonisation within the internal market, created legal uncertainty and unnecessary costs for business (Problem 1) and made it difficult for individuals to exercise their rights effectively (Problem 2).

Protection of personal data in the area of police co-operation and judicial co-operation in criminal matters is characterised by a lower level of harmonisation (limited scope, wide derogations, insufficient safeguards) and a fragmented landscape, leading to legal uncertainty (Problem 3). Enforcement is even more problematic in this area given the peculiarities of the "former third pillar *acquis*" in terms of (limited) powers of the Commission and of the ECJ.

Globalisation and technological developments have contributed to and exacerbated all three problems, by greatly facilitating and encouraging the exchanges and flows of personal data worldwide in all areas and sectors, including law enforcement, with the development of new applications and services and the availability of increasingly sophisticated tools.

3.6. Baseline scenario: How would the problem evolve?

Globalisation and technological developments, which are the common drivers of the problems are expected to pose ever-increasing challenges to the fundamental right to data protection. The extent and the seriousness of existing problems are therefore also expected to increase. Without further regulatory intervention, it is anticipated that under the baseline scenario the problems in the current situation would evolve as follows:

3.6.1. Fragmentation, legal uncertainty and inconsistent enforcement

Member States are likely to continue to implement and enforce the Directive in a diverging way. Data protection issues with a cross-border dimension are likely to remain without a consistent response.

The numbers of businesses operating in more than one Member State and of public authorities exchanging data with other Member States' authorities are expected to continue to rise (due in particular to further EU integration and globalisation, involving for instance e-government applications and the increasing ease of exchanging personal data[103]). Given that the largest part of the administrative and compliance costs originates from cross-border processing, the costs for companies (particularly large companies) and public authorities are likely to increase further.

The ***total administrative burden*** imposed by the Directive in the ***baseline scenario*** is estimated to amount to about ***€5,3 billion per annum***. The costs of legal fragmentation in the baseline scenario (expressed solely in terms of administrative burden) for economic operators processing personal data in more than one Member State, are estimated to amount to approximately ***€2.9 billion per annum*** (*see Annex 9 for details*).

As regards enforcement, experience has shown that the progressive increase in cross-border transfers and of data controllers operating across several Member States did not lead, by itself, to increased cooperation between Data Protection Authorities. The legal uncertainty caused by inconsistent – and sometimes contradictory – decisions taken by DPAs will therefore increase, as will related costs. As a result, the credibility of the EU data protection framework will gradually decline.

---

[103] This is one of the key targets of the Digital Agenda for Europe. For more see Digital Agenda Scoreboard 2011, available at http://ec.europa.eu/information_society/digital-agenda/scoreboard/docs/scoreboard.pdf, p.16-17.

3.6.2. Difficulties for individuals in exercising their data protection rights effectively

There is a strong likelihood that the current difficulties in maintaining control over one's own data and in effectively exercising data protection rights will increase, given the large and growing volume of personal data collected and the ease with which it can be processed and communicated thanks to new technologies.

Individuals are likely to encounter increasing problems with the protection of their personal data, or refrain from fully using the internet as a medium for communication and commercial transactions. The 75% of individuals currently not feeling in complete control of their personal data on social networking sites (and 80% when shopping online) is not likely to decrease without regulatory intervention which can support the confidence of individuals. Such a development could counteract the key performance target of the Digital Agenda for Europe for 50 % of the population to buy online by 2015.[104]

Individuals are also likely to face increasing difficulties in knowing what their data protection rights are when their data are processed by companies or public authorities involved in cross border data processing, in particular with the development of cloud computing. They would increasingly be unable to foresee the scope of their data protection rights in order to adapt their behaviour.

3.6.3. Inconsistencies and gaps in the protection of personal data in the field of police and judicial cooperation in criminal matters and inconsistency of the rules

The Commission and the Court of Justice will eventually become competent as regards the implementation and the application of the Framework Decision after the expiry of the five-year transition period provided by the Lisbon Treaty. Thus, the "lisbonisation" of the Framework Decision will be a matter of fact as of 1st December 2014 even in the absence of an intervention from the legislator.

However, the problems and difficulties linked to the limited scope and other gaps of the Framework Decision will become more acute in the current context of growing intra-EU and international cooperation and data exchange as showed by the increasing number of exchanges of personal data for these purposes, at EU or Member State's level. Also the current fragmentation will be maintained.

3.7. SUBSIDIARITY AND PROPORTIONALITY

3.7.1. Subsidiarity

The need for EU level legislation on the protection of personal data and the free flow of such data within the Union was already recognized by the European legislator with the adoption of the Directive. As explained in the previous sections, while the Directive has indeed contributed to addressing the problems observed at the time, such problems have become more important and widespread due to the recent technical and economic developments. Therefore, the need for an EU level instrument further harmonising the protection of personal data is even more urgent today than when the Directive was adopted.

In light of the problems outlined above, the analysis of subsidiarity indicates the necessity of EU-level action on the following grounds:

---

[104] Ibidem, p.12.

– The right to the protection of personal data is enshrined in Article 8 of the Charter of Fundamental Rights. Article 16 TFEU is the legal basis for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data;

– Personal data can be transferred across national boundaries, both EU-internal borders and to third countries, at rapidly increasing rates. In addition, there are practical challenges to enforcing data protection legislation and a need for cooperation between Member States and their authorities, which need to be organised at EU level to ensure the necessary coherence and level of protection within the Union. The EU is also best placed to ensure effectively and consistently the same level of protection for individuals when their personal data are transferred to third countries;

– Member States cannot alone reduce the problems in the current situation. This is particularly the case for those problems that arise from the fragmentation in national legislations implementing the EU data protection regulatory framework. Thus, there is a strong rationale for the legal framework for data protection being at the EU level. There is a particular need to establish a harmonised and coherent framework allowing for a smooth transfer of personal data across borders within the EU while ensuring effective protection to all individuals across the EU;

– Whilst it would be possible for Member States to enact policies which ensure that this right is not breached, this would not be achieved in a uniform way in the absence of common EU rules and would create restrictions on cross-border flows of personal data to other Member States that do not meet the same data protection standards;

– The EU legislative actions proposed are likely to be more effective than similar actions at the level of Member States because of the nature and scale of the problems, which are not confined to the level of one or several Member States.

3.7.2. Proportionality

One of the aims of the reform is to reduce the current legal fragmentation and all the problems linked to that (*see Section 3.2.1 above*), in particular by further harmonising Member States' substantive laws and by setting up governance mechanisms to make enforcement more effective and more consistent across the EU.

The envisaged actions are proportionate as they are within the scope of the Union competences as defined by the Treaties and are necessary to ensure uniformity of application of EU legislation, ensuring effective and equal protection of individuals' fundamental rights. Action at EU level is essential to continue ensuring credibility and a high level of data protection in a globalized world, while maintaining the free flow of data. The proper functioning of the internal market requires that the provisions ensure a level playing field for economic operators.

The current initiative builds on the current Directive and intends to cover the existing gaps by making the implementation of existing principles by Member States more effective and their application more cost efficient. To this end, the reform intends to strengthen the coordination powers and reinforce the role of the advisory body composed of the Data protection

authorities of the EU, currently the Article 29 Working Party. The powers of the existing data protection authorities should also be more harmonised to ensure a better and more consistent enforcement. The Commission also intends to facilitate certain procedures and instruments relating to the relation between the Union and third countries, such as Binding Corporate Rules, which are an existing co-regulation mechanism, where no comprehensive mutual recognition system at EU level was ensured.

Where possible, the reform leaves space to actors to implement appropriate measures to achieve the purpose of the instruments, e.g. by strengthening accountability and responsibility of data controllers and processors for assessing and mitigating data protection risks and by cutting unnecessary administrative burden, with the objective of reinforcing the proportionality of the data protection framework.

Compared to the existing legislation, the Commission aim is to propose a stronger and more prescriptive approach in the area of data protection. This approach is justified by the observations of the practical operation of the current system and the problems described in the present impact assessment. Where the current Directive deliberately and explicitly leaves margin to Member States for interpretation, this has led to widely diverging interpretation and practices. This is also true to a large extent for those cases where the Directive fails to provide for clear rules or where it is silent. In an environment where processing of personal data was predominantly at national level and transfer across borders was still limited, such differences could be tolerated, even though with some limiting effects. As in the meantime the internal market has become more important and effective, in particular due to the increased provision of services online, for which cross border operation is possible without any extra efforts or costs, the divergences have become such an important obstacle that stronger measures at EU level are required. The Commission's proposal observes the need to balance by providing for stronger measures only in those areas of Union competence where the protection of fundamental rights and the Single Market require stronger harmonisation and by leaving margin to Member States in all areas where culture, tradition or the national constitutional system require this, e.g. :

- the area of police cooperation and judicial cooperation in criminal matters. While general data protection rules will as a matter of principle be applicable to this area as well, some flexibility will be left to Member States in defining the limitations and exceptions;

- the relation between data protection and freedom of expression, which is very much linked to cultural and social traditions in Member States.

3.8. Relation with fundamental rights

The right to protection of personal data is established by Article 8 of the Charter and Article 16 TFEU, based on Directive 95/46/EC as well in Article 8 of the ECHR and in the Council of Europe 108 Convention. As clarified by the ECJ (judgment of 9.11.2010 in cases C-92/09 and 93/09, Schecke), the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society[105].

Data protection is closely linked to ***respect for private and family life*** protected by Article 7 of the Charter. This is reflected by Article 1(1) of Directive 95/46/EC which provides that,

[105] In line with Article 52(1) of the Charter, limitations may be imposed on the exercise of the right to data protection as long as the limitations are provided for by law, respect the essence of the right and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to privacy with respect of the processing of personal data. Other potentially affected fundamental rights are the following:

- **Freedom of expression** (Article 11 of the Charter);
- **Freedom to conduct a business** in accordance with Union law and national laws and practices (Article 16);
- The **right to property** and in particular the **protection of intellectual property**(Article 17(2);
- The **prohibition of any discrimination** amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21);
- The **rights of the child** (Article 24);
- A high level of **human health protection** in the definition and implementation of all the Union's policies and activities (Article 35 of the Charter);
- The **right to an effective remedy before *a tribunal (***Article 47 of the Charter*).*

The impact of the measures proposed in the framework of the data protection reform on these rights is examined in Section 6 and in Annex 7.

4. POLICY OBJECTIVES

The current reform aims at, first of all, **completing the achievement of the original objectives**, taking account of **new developments and challenges** arising today, i.e.:

1. ***Enhancing the internal market dimension*** of data protection;
2. ***Increasing the effectiveness of the fundamental right to data protection*** .

In addition, the entry into force of the Lisbon Treaty - and in particular the introduction of a new legal basis (Article 16 TFEU) - offers the opportunity to achieve a **new objective**, i.e.:

3. E*stablishing a* ***comprehensive EU data protection framework and enhancing the coherence and consistency of EU data protection rules, including in the field of police cooperation and judicial cooperation in criminal matters*** .

In order to enhance the ***internal market*** dimension of data protection (objective 1), the Commission strives to achieve the specific objectives of:

- **Harmonising and clarifying EU data protection rules and procedures to create a level playing field.**

  Diverging national interpretations of concepts, principles and procedures under EU data protection rules shall be prevented. Key elements of the legal provisions shall be clearly and completely defined at EU level, leaving margin for interpretation to Member States only where this is necessary in order to properly respect national legal, social, cultural and administrative traditions and systems to the extent that these differences do not undermine the functioning of the internal market. This shall also ensure that data controllers enjoy legal certainty on the obligations they are subject to, on the basis of EU wide provisions. At the same time, flexibility and adaptability of the framework to technical, economical and societal development must be ensured at EU level. Rather than leaving a wide margin of interpretation to Member States, additional clarification and precision of the rules and procedures shall

be added to the framework at EU level through a faster and more lightweight procedure than a full legislative procedure. The Union's position in the global economy shall be strengthened by simplifying and clarifying the conditions for the transfer of personal data to third countries.

- **Ensuring consistent enforcement of data protection rules.**

  Further to increasing harmonisation of the legal provisions as such, their practical application and enforcement should also be more consistent. To this effect, data controllers shall have a single authority as the unique contact point for supervision and enforcement cases throughout the entire EU, which shall act on the basis of appropriate and effective coordination ensuring consistency of the principles applied by all authorities. Authorities' powers shall be equivalent and adequate throughout the Union and they shall be equipped with adequate resources.

- **Cutting red tape.**

  While harmonisation and consistent enforcement will already contribute to drastically reducing duplication of administrative burden needed for compliance with diverging procedures and interpretations, the reform shall ensure that only such information and notification obligations are maintained that have a positive effect on the protection of personal. Procedures for data transfers to third countries shall be clear, simple and effective in ensuring data protection.

In order to increase the ***effectiveness of data protection rights*** (objective 2), the Commission strives to achieve the specific objectives of

- **Ensuring that individuals are in control of their personal data and trust the digital environment,**

  Individuals must enjoy effective transparency about the conditions of the processing so that they can make a meaningful decision whether or not to agree to it. The individual should be aware when they are deemed to giving their consent to data processing. They should also be reassured that they will be informed about any breaches of the security of their personal data. The execution of individuals' rights should be easy and their extent should be clear, e.g. regarding access to their own data and its withdrawal and transfer form one data controller to another or its deletion, as well as the data controller's obligation to minimise the processing of personal data. Another element for the creation of trust and confidence is clarity about available remedies in cases of breaches and appropriate sanctions. In cases concerning many persons, it should not be up to each data subject to pursue legal redress individually, but it should be possible to handle cases through associations, reducing effort for data controllers, individuals and the supervisory and judicial system.

- **Ensuring that individuals remain protected including when their data are processed abroad**

  Individuals should have confidence that they enjoy data protection rights whenever they buy goods or use services (including information society services) that are offered to them from outside the EU or when their behaviour

is monitored (for example, when people are tracked on the internet with data processing techniques applying a 'profile' to them, particularly to take decisions concerning them based on their preferences, behaviour or attitudes).

- **Reinforcing the accountability of those processing personal data.**

  Individuals can gain more confidence in data protection when they can rely on data controllers' interest in actually ensuring appropriate safeguards rather than only being formally compliant with the letter of the law. Data controllers should be incentivised to take this approach by increasing their responsibility and accountability for the measures they take. By this, they should be encouraged to apply the principle of privacy by design or to perform privacy impact assessments.

In order to increase the ***coherence of the data protection framework*** across all areas of Union competence (objective 3), the Commission strives to achieve the specific objectives of

- **Ensuring that individuals' data protection rights are fully guaranteed in this area** and
- **Enhancing trust and facilitating police co-operation and judicial co-operation in criminal matters**.

  It should be clear that the principles of data protection apply also to this area, including also to domestic processing in the police and judicial area. This will include seamless integration into the competences of the Court of Justice of the EU and of the Commission, as well as an increased role for data protection authorities and their coordination body (currently the Article 29 Working Party).

  This will ***enhance the coherence and consistency of the EU data protection framework***, in particular by revising the current rules on data protection in the area of police cooperation and judicial cooperation in criminal matters. It will also contribute to the fulfilment of the original objectives of the Framework Decision, i.e. the need to ensure a high level of protection to individuals, on the one hand, and to enhance mutual trust and facilitate the exchange of information between police and judicial authorities, on the other hand.

Table 1 below sets out the specific and operational objectives.

Table 1: Policy Objectives

General objectives	Specific objectives	Operational objectives
1. To enhance the internal market dimension of data protection	**To harmonise and clarify EU data protection rules and procedures to create a level playing field**	– To ensure that the data protection framework can be applied in a uniform way throughout the EU and reduce the current legal fragmentation – To allow flexibility to adjust to rapid technological development, while maintaining technological neutrality – To ensure legal certainty for data controllers – To address globalisation and simplify and clarify the conditions for international transfers
	To ensure consistent enforcement of data protection rules	– To establish a "one-stop-shop" for data controllers in the EU – To ensure stronger powers and adequate levels of resources (to DPAs) for enforcement and control – To develop binding cooperation procedures and effective mutual assistance between DPAs – To rationalise the current governance system to help ensuring a more consistent enforcement
	To cut red tape	– To reduce/remove unnecessary formalities, such as notification obligations for data controllers (except for risky processing) – To simplify formalities for international transfers
2. To increase the effectiveness of the fundamental right to data protection	**To ensure that individuals are in control of their personal data and trust the digital environment**	– To increase transparency of data processing vis-à-vis individuals including in case of data breaches – To strengthen and expand individuals' rights (access, rectification, deletion ("right to be forgotten"), withdrawal ("data portability"), data minimisation, meaningful consent) – To provide for more effective remedies and sanctions – To empower associations to act on behalf of data subjects
	To ensure that individuals remain protected including when their data are processed abroad	– To clarify the scope of application of EU law to foreign data controllers To provide for benchmarks for assessing the protection afforded by third countries to EU data
	To reinforce the accountability of those processing personal data	– To provide accountability mechanisms for data controllers (Data protection by design, data protection impact assessment for risky processing etc.)
3. To establish a comprehensive EU data protection framework and enhance the coherence and consistency of EU data protection rules, including in the field of police cooperation and judicial cooperation in criminal matters	**To ensure that individuals' data protection rights are guaranteed in this area** **To enhance trust and facilitate police co-operation and judicial co-operation in criminal matters**	– To apply general data protection principles to police cooperation and judicial cooperation in criminal matters – To address the specificities of data protection in these fields – To reduce shortcomings and inconsistencies in particular by covering domestic processing activities – To ensure the competence of the Court of Justice and the Commission – To expand the advisory role of the Working Party 29

Compliance with horizontal EU policies

The above objectives are in compliance with and complement the horizontal policies of the EU. In particular:

– *the Europe 2020 Strategy and the Single Market Act*[106], as they help deepening the internal market by streamlining rules and further harmonising them where needed, thereby boosting EU business competitiveness;

– *the Digital Agenda for Europe*[107], since they contribute to the development of a digital single market and aim to increase individuals' digital confidence;

– *the Action Plan for Implementing the Stockholm Programme*, as they "strengthen the EU's stance in protecting the personal data of the individual in the context of all EU policies" and in the context of international relations;

– *the general EU Better Regulation policy*[108], as they aim at simplifying the regulatory environment, streamlining existing obligations and procedures and reducing administrative burden (see also § 7.4 below);

– *the Small Business Act* for Europe[109], as it provides a comprehensive SME policy framework, promotes entrepreneurship and anchors the "Think Small First" principle in law and policy making to strengthen SMEs' competiveness.

5. POLICY OPTIONS

A number of possible measures have been identified to address each of the three problems and to achieve the objectives defined in Section 4. Measures differ in the extent of EU intervention, and in particular in the strength of the regulatory approach, ranging from interpretative guidance and codification of best practices, to further and detailed harmonisation of rules and centralised enforcement. By grouping measures according to their strength, three options have been identified, each of which represents a comprehensive approach aiming at achieving the identified policy objectives.

- **Option 1** would mostly rely on clarifying the interpretation and application of the existing rules via 'soft law' and provide for a limited legislative intervention aimed at codifying existing best practices and clarifying some specific concepts. Due to the nature of problem 3, i.e. improving data protection rules in the area of police and justice, this approach would not be suitable to address it; therefore, option 1 does not contain measures related to this problem.

- Most of the measures composing **option 2** require legislative amendments, although the non-regulatory measures under policy option 1 could be combined with or added to the measures under this option. This concerns in particular actions on awareness raising and promotion of PETs. This option contains measures addressing all three problem areas.

---

106 COM(2011)206 final.
107 COM(2010)245 final.
108 See http://ec.europa.eu/governance/better_regulation/index_en.htm.
109 COM(2008)394 final; cf. on the review of the "Small Business Act" COM(2011)78 final.

- Policy **option 3** would also be based on an essentially legislative approach and include most of the measures considered under option 2. It would, however, go farther and provide for more detailed and prescriptive rules, also regulating and harmonising specific sectors. It would also apply a 'centralised' approach in relation to enforcement by establishing a European agency. As regards the former "third pillar", this option would also be the most far-reaching as it would foresee the amendment of all "third pillar" instruments in order to align them entirely with the new data protection rules. This option contains measures addressing all three problem areas.

The options are described in more detail below. For the status quo option see the description of the baseline scenario under Section 3.6.

5.1. Options to address Problem 1: Barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement

5.1.1. Addressing fragmentation and legal uncertainty

Option 1: Interpretation, technical support tools and encouragement of self-regulation.

Under this option, the Commission would make extensive use of soft policy instruments and provide technological support to Member State authorities in order to improve the regulatory environment in the internal market, and propose only very limited legislative amendments targeted at specific issues that cannot be addressed effectively in any other way.

This option would include in particular:

- Creating a single ***EU-wide IT system (central platform) for notifying processing***, based on a common format and procedures agreed by national DPAs, would be set up. Data controllers would submit only one form electronically and mark the countries they need to notify (as proposed by the WP29 in its Advice paper on the matter). Requirements, exceptions and derogations (currently allowed for by the Directive) would however not be harmonised, which means that further information would have to be provided if required by national law(s).
- Increased ***use of interpretative Communications*** by the Commission to provide more detailed guidance to Member States, public authorities and businesses on the application of Union law, and on the interpretation of certain concepts defined in the Directive to favour a more uniform interpretation of the current rule. These would *in primis* cover issues and notions whose diverging interpretation has led to quite different implementation and practices by Member States (e.g. definition of personal data, provisions on applicable law).
- The lack of harmonisation would further be addressed by the encouragement *of* ***EU-wide self-regulation initiatives building on the existing data protection acquis ("co-regulation"),*** e.g. on on-line advertising, medical research, e-health, network and information security. The Commission would support this process by providing support and advice, building on its own experience with these types of instruments with the aim of ensuring that the critical success factors (e.g. participation of all relevant stakeholder groups, transparency of the process, feedback and measurement, monitoring and enforcement)[110] are properly taken into account. Use of the existing mechanisms for

[110] http://ec.europa.eu/dgs/health_consumer/self_regulation/

formal recognition by national supervisory authorities and the Article 29 Working Party would be encouraged.

- Limited legislative amendments to ***clarify the key criteria for adequacy of data protection in third countries***, and to create an ***explicit legal basis for Binding Corporate Rules (BCRs)***, in order to facilitate secure international transfers of personal data.

Option 2: Legislative amendments addressing gaps in current harmonisation that cause harmful fragmentation

Under this option, the Commission would present legislative proposals aimed at solving specific problems caused by divergent approaches in Member States. These legislative proposals would concern in particular:

- ***Simplified basic registration system:*** this would replace the current system of notifications by data controllers to DPAs with a simpler system of basic registration with DPAs (i.e. this registration would include the identity of the data controller, the contact details, an indication of the nature of the business; and an indication of the processing, and/or personal data held).

- Ensure that ***data controllers are always subject to one single law***. Two sub-options are possible:

  a) If the new instrument is a Directive, - the provisions on applicable law would be clarified in the following way:

  - for data controllers based in the EU, the ***sole criterion determining the applicable law would be the main establishment*** of the data controller, defined as the place of its establishment in the EU where the main decisions as to the purposes, conditions and means of the processing of personal data are taken and as the place where the main processing activities take place when no decision are taken in the EU;

  - ***For data controllers based outside the EU***, the offering of goods and services (including information society services) to individuals in the EU, or the monitoring of EU individuals would become the main criteria to determine the applicable law.

  b) If the new instrument is a Regulation, the latter would be the law applicable throughout the EU. The Regulation would also be applicable to data controllers outside the EU if they offer goods and services (including information society services) to data subjects in the EU or monitor their behaviour.

- Ensure that ***one single DPA*** – the one of the Member State of main establishment - is responsible *vis-à-vis* a given data controller, thus establishing *a* ***"one-stop shop"*** for data controllers. The decisions taken by the responsible DPA would have to be ***recognised and enforced in the other Member States*** concerned. It would, however, always be ensured that an individual retains the possibility of addressing himself/herself to the DPA of his/her Member State of residence, as well as – where appropriate – to the courts in the country of residence for proceedings against the controller or processor.

- ***Increased harmonisation of the substantive rules at EU level*** - either by a directly applicable Regulation or by a "maximum harmonisation" Directive – by establishing

more prescriptive and more precise rules, thus reducing the margin for manoeuvre currently left by the Directive to the Member States.

- Giving the Commission the competence to adopt ***implementing acts or delegated* acts** where there is a need for uniform implementation of specific provisions, or when there is a need to supplement or amend specific non-essential data protection provisions. This would allow the Commission to adopt detailed and specific rules covering certain aspects/sectors where the need may arise (e.g. application of security measures in various situations, application of data breach notification in specific circumstances, further specifying the conditions for data protection officers), while taking into consideration, wherever necessary, the relative position of micro, small and medium enterprises and the regulatory burden they incur in application of the "think small first principle".

- ***Simplifying rules and procedures for transfers of personal data to third countries*** by giving the Commission exclusive competence for adequacy decisions, extending the scope of BCRs to include data processors and introducing a clear definition of "groups of companies". Moreover, prior authorisations by DPAs will be deleted in the large majority of cases.

- Going **a step further in co-regulation**, by providing for the possibility for the Commission to give general validity within the Union, via implementing measures, to Codes of Conduct submitted by associations and other bodies representing categories of controllers in several Member States.

Option 3: Detailed harmonisation in all policy fields

This option would include all elements of option 2 (except the basic registration system) and include much more detailed EU legislation. The following additional measures would be added:

- ***Abolishing the general obligation to notify data processing operations***, currently foreseen by Article 18 of the Directive (and there would be no basic registration either. However, prior authorisation by the competent DPA would be maintained in cases of data processing likely to present specific risks to the rights and freedoms of data subjects.

- Developing ***an EU-wide certification scheme*** for data protection compliance for **EU and third country controllers and processors**, to be certified as complying with EU data protection rules. Such scheme could be based on appropriate standardisation by recognized standardisation organisations and should be supported by adequate monitoring, complaint processing and compliance mechanisms.

  Establishing ***detailed and further harmonised rules*** for specific sectors and circumstances (health and medical sector, employment relationships), based on relevant Council of Europe recommendations. In particular:

  – ***Employment*** relationships - key measures:

    a) ***Proportionality and legitimacy requirements*** mentioned in Articles 6 and 7 of Directive 95/46/EC would be regulated in details for employment relationships.

b) the processing of data concerning health and ***the processing of drug and alcohol testing data by the employer shall in principle be prohibited***, subject to limited exceptions;

– ***Health/medical sector*** - key measures:

c) personal data shall in principle only be obtained from the data subject (with very limited exceptions);

d) persons subjected to genetic analysis should be informed of unexpected findings under specific conditions.

5.1.2. Addressing inconsistent enforcement

Option 1: Interpretation, technical support tools and encouragement of co-operation

Under this option, the Commission would use soft policy instruments to improve the cooperation and coordination between Member State authorities and encourage more consistent application of EU legislation. This option would include in particular:

- The Commission would adopt ***interpretative Communications*** in order to clarify and specify in detail the content of investigative and intervention powers of DPAs, so as to encourage a more uniform practice at national level. The notion of ***independence of DPAs*** would be further clarified in the light of Article 8 of the Charter and recent ECJ case-law.

- ***Cooperation between DPAs*** would be improved by:

  – Extending the role of WP29 to include the competence to ***provide advice to DPAs and elaborate best practices*** on the application of EU data protection rules;

  – Providing them with practical tools, namely ***IT tools***, to better exchange information (e.g. on complaints received, on investigations being carried out);

  – Funding from the EU budget would be made available in order to promote and encourage ***common training and the exchange of officials*** between DPAs.

Option 2: Reinforcement and harmonisation of DPA powers and strengthened co-operation between DPAs

The shortcomings identified would be directly addressed by specific legislative changes, namely:

- ***Reinforcing DPAs and harmonising their tasks and powers*** and obliging Member States through the EU legal instrument to provide adequate resources. This would include, in particular:

  – Further ***strengthening their independence*** and ***further harmonising DPAs' tasks and powers*** to enable them to carry out investigations, take binding decisions and impose effective and dissuasive sanctions;

  – Establishing a legal basis detailing the obligations for ***co-operation and mutual assistance*** between DPAs, including the obligation for a DPA to carry out

investigations and inspections upon request of other DPAs.

- ***Harmonising data protection offences*** subject to administrative sanctions as well as the ***level of sanctions***. Supervisory authorities should be empowered to respond to specifically listed data protection violations by way of administrative sanctions; the offences which are to be subject to such sanctions would be harmonised at EU level.

- ***Replacing the current WP29 by a European Data Protection Board***, with a strengthened role and tasks, in particular in order to ensure a more consistent enforcement (see below).

- Setting up a ***consistency mechanism*** at EU level which will ensure that decisions taken by a DPA with a wider European impact take full account of the views of other concerned DPAs. This system would foresee a ***role for the Commission and for the European Data Protection Board***, in order to ensure consistency and compliance with EU rules. More specifically:

  – The Commission and the European Data Protection Board would be informed about national DPA draft measures in cases where such decisions would have a "European impact". The Board would have the opportunity to issue an opinion on the matter, to be taken into account by the concerned DPA. The Commission would also be able to adopt an Opinion on the draft DPA Decision and, as a last resort, a reasoned Decision requesting the concerned DPA to suspend the adoption of its draft measure, where required to ensure full compliance with Union law.

  – This suspension could last up to 12 months, during which the Commission may decide to adopt implementing measures to ensure the correct and consistent application of EU rules.

- Ensuring the independence and effectiveness of the new European Data Protection Board by establishing the EDPS as responsible for providing the Board secretariat (instead of the Commission).

Option 3: Centralised enforcement and EU-wide harmonised sanctions

Option 3 would foresee the establishment of a centralised EU-level enforcement structure ensuring the functioning of personal data protection in the internal market by:

- Establishing ***a central EU Data Protection Authority*** (i.e. a new EU regulatory agency) responsible for the supervision of all data processing with an internal market dimension, which could also take binding decisions *vis-à-vis* data controllers.

- Defining ***harmonised EU-wide criminal sanctions*** for breaches of data protection rules.

5.2. Options to address Problem 2: Difficulties for individuals in exercising their data protection rights effectively

5.2.1. Addressing individuals' insufficient awareness and loss of control and trust

Option 1: Interpretation, information and encouragement of self-regulation

The Commission would focus on using soft policy instruments to improve the practical implementation of existing rules by data controllers and the awareness of individuals, and make limited legislative proposals clarifying some existing concepts of the Directive. This would include in particular:

- ***Awareness-raising activities for individuals***, particularly children. In terms of enhancing the ***effectiveness*** of individuals' rights, the focus under this policy option would be on non-regulatory measures namely ***awareness-***raising ***activities*** on data protection matters, particularly *vis-à-vis* children, namely by increasing EU funding for such activities.

- ***Promoting privacy-friendly default options***, greater uptake of ***Privacy Enhancing Technologies (PETs)*** and encouraging ***privacy certification scheme/privacy seals***, research activities including on behavioural economics to help design privacy-friendly applications. This would be achieved by increasing the ***EU financing for studies and research*** in the above areas.

- The only ***regulatory measures*** under this option addressing this problem would be the introduction of ***explicit references to the principles of transparency and data minimisation*** in the relevant instruments, aiming at clarifying existing principles in the current legislation.

Option 2: Legislative amendments to reinforce responsibility of data controllers and processors

This option focuses on targeted legislative amendments directly addressing specific issues for which the need for regulatory clarification and increased precision has been established. It also includes the measures from option 1 introducing transparency and data minimisation as explicit data protection principles:

- Further ***clarifying the concept of personal data*** by better specifying what identified or identifiable natural person means, using wording from current recital 26 of the Directive and including an explicit reference to online identifiers.

- ***Clarifying the rules on consent***, in particular by specifying that – where consent is the legal ground for data processing – it should be given **explicitly** (i.e. by either a statement or a 'clear affirmative action' by the data subject) and that the data controller should be able to demonstrate it. Moreover, the data subject should be able to withdraw his/her consent at any time. Furthermore, the context of the consent should allow a genuine and free choice and in particular it should be excluded as a ground for lawful processing in case of significant imbalance between data controller and data subject (e.g., in the framework of an employment relationship).

- Including ***genetic data*** into the category of "sensitive data" (i.e., data whose processing is prohibited as a rule, with exceptions and derogations) and better framing the exceptions to the processing of sensitive data, particularly health data.

- Provide for specific rules regarding the application of data protection rules to ***children's data***, e.g. concerning the information given to them and the data subject's right to request that data be erased or rectified ("right to be forgotten") and the prohibition of automated profiling for children. Specific rules on ***consent for children below 13 years in the online environment*** – specifying that parental consent would always be required - would also help protecting a very vulnerable category of children because of their young age.

- Clarifying ***the rules applying to data processing by individuals for purely private purposes*** ("household exemption"). In this case, when the processing has no gainful interest and concerns a 'definite' number of individuals they would be totally exempted from data protection rules. .

- ***Strengthening data controllers' and processors' responsibility and accountability***, namely by:

  – providing ***for additional obligations for data controllers***, i.e. they will have to provide more mandatory ***information*** to individuals about the processing of their data, and in an intelligible form, using clear and plain language, in particular for privacy statements. In addition to what is currently provided for by the Directive, data subjects would have to be better informed about the processing operations, e.g. clearly indicating the period for the storage of the data plus the contact details of the controller, of the controller's representative and of the DPO (if any), as well as about their own rights, including their right to address themselves to a supervisory authority, along with the authority's contact details;

  – Given the increasingly role played by data processors in today's environment, some of the obligations of the controller would also be extended to the processor, which are currently only bound to respect the instructions of the controller via contractual obligations. The same requirements should apply to ***data processors*** based in third countries that are processing EU data as laid down in a contract with the controller or prescribed by a legal act.

  – Introducing 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;

– Introducing ***Data Protection Impact Assessments (DPIAs***) with narrowly defined applicability criteria for processing operations likely to present specific risks to the rights and freedoms of data subjects.

– Introducing a "***Data protection by design"*** principle (i.e. the controller would be obliged to design the organisational structure, technology and procedures in a way that it meets the requirements of data protection);

Introducing a general obligation, extended to all sectors (currently this is only harmonised for the telecommunications sector and regulated by the e-Privacy Directive), to ***notify data breaches to DPAs and to individuals in cases of breaches likely to adversely affect them***. The controller will be obliged to notify the breach to DPAs **without undue delay and, where feasible, not later than 24 hours after having become aware of it. After notifying the DPA, the controller will also be obliged to inform individuals without undue delay about the breach.** The thresholds and criteria for notification to both Data Protection Authorities and concerned individuals would be defined in implementing measures to be adopted by the Commission.

Option 3: More detailed rules at EU level

This option includes all the measures from option 2, as well as the following further measures:

- In addition to the strengthened modalities of consent, under this option ***consent would become the "primary ground" for data processing***. This would thus introduce a hierarchy of legal grounds for processing personal data, of which consent would be the primary one and all the other existing ones would remain as residual grounds.

  Adding further categories to the list of sensitive data, namely:

  – data relating to ***children***;

  – ***biometric*** data;

  – and ***financial*** data, e.g. financial messaging data, credit histories and financial solvency (bad debtors lists) data contained in credit bureaux' "scoring" systems;

- Introducing ***harmonised EU-level criminal sanctions*** for breaches of data protection rules (see also problem 1) and would establish minimum rules with regard to the definition of criminal offences and sanctions in the area of personal data protection.

- Specifying ***detailed thresholds and criteria for notifying breaches to data subjects***, i.e., sectoral criteria, procedures and formats for notifying breaches to data subjects.

- ***Developing EU-wide certification schemes on data protection*** (see also problem 1).

5.2.2. Addressing the difficulty for individuals to exercise their data protection rights

Option 1: Interpretation and standardisation

The Commission would rely on soft policy measures and limited legislative amendments addressing the insufficient awareness and loss of control referred to in the previous section and in addition:

- Publish ***interpretative Communications regarding*** the ***interpretation and the modalities of exercising individuals' rights*** to data protection, e.g. clarifying that the right of access to one's own data should be exercised free of charge. Particular focus would be on data subjects' rights in the online environment.

- Mandate ***standardisation institutions*** to develop standards for technical and organisational measures improving the protection of personal data. These standards should address general issues, such as methodologies and procedures, assessment criteria and techniques, as well as specific technological and sectoral elements.

Option 2: Legislative amendments to clarify and strengthen individuals' rights and how they can be exercised

This option focuses on targeted legislative amendments addressing directly the need for regulatory clarification and precision, in particular:

- In order to enhance control by individuals over their own data, the existing provisions on ***modalities for access, rectification and deletion would be clarified and strengthened***. As regards the exercise of these rights, it would be provided that the controller's actions in response to the data subject's requests should be in principle free of charge and a deadline would be set for the data controller to respond to requests. The right of an individual to have its data deleted when it is no longer needed and that wrong data is rectified could be spelled out more clearly in the legal instrument, making their execution practicable.

- Introducing a right to ***data portability***, giving individuals the possibility to withdraw their personal data from a service provider and process them themselves or transfer them to another provider, without hindrance from the controller. Individuals should have the right and the practical possibility to obtain a copy of the data processed by a data controller on the basis of their consent, and where this is technically feasible and appropriate, to have their data transferred from one service provider to another one. The data should be provided in a format that allows further processing either by the individual itself.

- Strengthening the right of individuals to have their personal data deleted **("right to be forgotten"),** particularly in the online environment. As regards deletion of data, clarifications as to the ***duties*** of the data controller would be included in order to strengthen the right of the data subject to have his/her data deleted when there are no longer lawful grounds to retain them ***("right to be forgotten"***), also clarifying that the burden of proving the need for further conservation of the data lies with the data controller.

- ***Strengthening the provisions on judicial redress*** for data subjects, namely by making more explicit and clarifying the right for data protection authorities and associations aiming to promote the protection of personal data to bring action before courts on behalf of data subjects. This would, however, not amount to collective

redress and the associations would not be entitled to act on their own behalf, except in case of data breaches.

Option 3: EU level sectoral rules and redress mechanisms

This would include the measures from option 2, as well as:

- Specific provisions regulating in detail how to deal with ***online identifiers and geo-location data***.

- Introducing ***a right for collective redress*** regarding breaches of the protection of personal data. A general possibility for a collective legal action system in the area of protection of personal data (both injunctive and compensatory) would be introduced, allowing business and professional organisations and trade unions to represent individuals and bring actions before courts, by setting its basic procedural features including procedural guarantees for the parties and provide for the enforcement of judgements issued in other Member States.

5.3. Options to address Problem 3: Gaps and inconsistencies in the protection of personal data in the field of police and judicial cooperation in criminal matters

There is no Policy Option 1 to address this problem. For the area of the "former third pillar", only regulatory intervention can be effective, given the current gaps in data protection and the shortcoming of the legal instruments regulating this area. Therefore, a soft and interpretative approach is not considered as appropriate and only options 2 and 3 are elaborated.

Certain changes are not discretionary since they are the automatic consequence of the entry into force of the Lisbon Treaty and the abolition of the former "pillar" structure of the EU, namely:

- The "lisbonisation" of the Framework Decision, i.e. the fact of giving the ***Commission and the ECJ full powers*** to monitor the correct application of the *acquis* in this area by Member States. Based on Protocol (N°36) on transitional provisions annexed to the treaties[111], this will happen either when the "former third pillar" acts – including the Framework Decision – are amended or in any case five years after the entry into force of the Lisbon Treaty (i.e. on 1st December 2014)[112];

- The ***extension of the advisory powers of WP 29*** to this area.

5.3.1. Addressing gaps in the Framework Decision

Option 2: Extending the scope of data protection rules in this area

Under this option, the most important gaps of the Framework Decision would be addressed, in particular:

- **The extension of the scope** of the new legal instrument to cover ***domestic data processing****:* the scope of the data protection rules in this area would no longer be limited to cross-border data processing (transferring to or making available to

---

111 See Articles 9 and 10 of the Protocol.

112 See, in particular, Article 10, paragraphs 2 and 3.

competent authorities) – as it is currently the case – but would also cover domestic processing in line with Article 16 of the TFEU;

- ***The application of the general data protection principles to this area*****,** in order to ensure full compliance with Article 8 of the Charter of Fundamental Rights and with the relevant case-law of the ECtHR and the ECJ. This entails, namely:

- ***Stricter and more harmonised rules on purpose limitation***, i.e. on limiting processing of personal data to the purposes compatible with those of its initial collection, with limited derogations from this principle;

- ***More harmonised rules on international transfers*** by foreseeing that transfers in this area can take place only, as a general rule, where there is an ***adequacy decision*** by the Commission or where ***appropriate safeguards*** have been adduced by way of a ***legally binding instrument***. In the absence of the latter, transfer can also take place if the competent authorities have assessed all the circumstances surrounding the transfer operation and provided appropriate safeguards. Further derogations allow for transfers in exceptional circumstances such as: a) when the transfer is necessary to protect the vital interests of the data subject or another person or b) to safeguard legitimate interests of the data subject; and finally, c) when the transfer is essential for the prevention of an immediate and serious threat to public security (of a Member State or a third country).

- Provide for the obligation to appoint ***Data Protection Officers***.

- Provide for ***stricter and more harmonised obligations to adequately inform the data subjects about the processing of his/her data***, while providing for the necessary and proportionate ***limitations/exceptions*** to this principle (such as restricting or delaying the transmission of data), to take account of the specific nature of these fields (i.e. , to avoid obstructing official or legal inquiries, investigations or procedures; to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties; to protect public and national security; to protect the data subject or the rights and freedoms of others).

- Provide for **more harmonisation as to the criteria and conditions** on the ***right of access of data subject***- in line with Article 8 of the Charter – particularly in cases under national law where currently the data subject does not have direct access to personal data processed by police authorities and only has recourse to indirect access via the data protection supervisory authority. Possible limitations to this right would be the same as for the right to provide information (*see above*). However, in case of refusal of access (or restrictions), the reasons shall be provided in writing to the data subject.

- ***Add genetic data to the list of sensitive data*****,** in line with the case-law of the ECtHR[113].

[113] See footnote 98.

- The ***codification of selected principles*** based on the ***Council of Europe Recommendations and best practices*** regarding law enforcement and data protection, in particular on the distinction between personal data of different categories of data subjects (e.g. witnesses, suspects, convicted persons), as well as between personal data based on facts, on the one hand, and those based on personal assessment, on the other hand.

Option 3: More prescriptive and stringent rules

In addition to the measures included in option 2, this would also require Member States to:

- always ensure ***direct access*** to data subjects in this area;

- include ***biometric data*** amongst sensitive data;

- require the ***carrying out of a DPIA*** prior to the processing of data, in particular sensitive data, in large information systems.

5.3.2. Addressing fragmentation

Option 2: New instrument with strengthened and more harmonised rules

- The ***application of the general data protection principles to this area*** (*see above under § 5.3.1 for the specific measures*) would also contribute to **reduce the fragmentation and the legal uncertainty in this area**.

- ***Leave unaffected for the time being existing "former third pillar" instruments*** with specific data protection provisions, which would n remain "*lex specialis*". The Commission would prepare a report, after the entry into force of the new instrument, to assess the existence of any possible incompatibility and propose, where appropriate, specific amendments.

Option 3: Full integration of general principles in former third pillar instruments

This would include all elements of option 2 plus:

- The immediate ***amendment of all existing former "third pillar" instruments ,*** to the extent that they contain data protection provisions incompatible with the new proposed rules in order to fully align them. .

Table 2: Summary of Policy Options

	Sub-Problem	Specific Objectives	POLICY OPTION 1	POLICY OPTION 2	POLICY OPTION 3

	Sub-Problem	Specific Objectives	POLICY OPTION 1	POLICY OPTION 2	POLICY OPTION 3
ROBLEM 1: -Barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement ***General Objective: To enhance the internal market dimension of data protection***	Fragmentation and legal uncertainty	• **To harmonise and clarify EU data protection rules and procedures to create a level playing field** • **To cut red tape**	• Creating a single EU-wide IT system for notifying processing, based on a common format and procedures agreed by national DPAs; • Increased use of interpretative Communications by the Commission to provide more detailed guidance to Member States, public authorities and businesses on the application of Union law, and on the interpretation of certain concepts defined in the Directive; • Encouragement by the Commission to businesses and associations to engage more self-regulation and co-regulation for specific sectors or practices at EU-level, using the mechanisms provided for by the Directive; • Legislative amendments to clarify the key criteria for adequacy of data protection in third countries, and to create an explicit legal basis for Binding Corporate Rules (BCRs), in order to facilitate secure international transfers of personal data.	• Replacing the obligation to notify data processing operations by a simplified 'basic registration' system; • Simplifying the provisions on applicable law, to ensure that data controllers are always subject to the legislation of one Member State (or to the EU Regulation) only and supervision of only one supervisory authority; • Amending substantive rules to remove explicit margins for manoeuvre for Member States and increase clarity and precision of the rules in general (maximum harmonisation Directive or Regulation); • Strengthen mechanisms for co-Regulation • Giving the Commission the competence to adopt implementing or delegated acts where there is a need for uniform implementation of specific provisions, or when there is a need to supplement or amend specific non-essential data protection provisions. Simplifying rules and procedures for transfers of personal data to third countries by giving the Commission exclusive competence for adequacy decisions, extending the scope of BCRs to include data processors and introducing a clear definition of "groups of companies". Moreover, prior authorisations will be deleted in the large majority of cases.	Measures under Policy Option 2 (except basic registration) plus: • Abolishing notification of processing altogether (prior checks for cases of risky processing would be maintained); • Developing an EU-wide certification scheme for data protection compliance for EU and third country controllers and processors, to be certified as complying with EU data protection rules; • Establishing detailed and harmonised rules for specific sectors and circumstances (health and medical sector, employment relationships and scientific research)

	Sub-Problem	Specific Objectives	POLICY OPTION 1	POLICY OPTION 2	POLICY OPTION 3
	Inconsistent enforcement of data protection rules across the EU	**To ensure consistent enforcement of data protection rules**	• Interpretative Communications on the independence and the required investigative and intervention powers of DPAs; • Encouraging enhanced cooperation between DPAs, including by providing programmes for exchange of staff between DPAs and mutual training and best practice workshops and technical tools; • Extending the role of the WP29, to include the competence to provide advice to national DPAs and to elaborate 'best practices' through limited legislative changes.	• Reinforcing and harmonising DPA tasks and powers (including administrative sanctions) and obliging Member States through the EU legal instrument to ensure provide adequate resources; • Harmonising offences subject to administrative sanctions; • Providing for mutual recognition of DPAs' decisions and increased co-operation via a consistency mechanism and mutual assistance operated, under the supervision of the Commission, through a European Data Protection Board with a possibility for the Commission to intervene to ensure swift compliance with EU law (opinion and, as a last resort, decision to suspend the measure); • Ensuring the independence and effectiveness of the new European Data Protection Board by establishing the EDPS as providing its secretariat (instead of the Commission).	• Establishing a central EU Data Protection Authority (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; • Defining harmonised EU-wide criminal sanctions for breaches of data protection rules.

	Sub-Problem	Specific Objectives	POLICY OPTION 1	POLICY OPTION 2	POLICY OPTION 3
PROBLEM 2: Difficulties for individuals to stay in control of their personal data ***General Objective: To increase the effectiveness of the fundamental right to data protection***	Insufficient awareness, loss of control and trust, particularly in the online environment	**To ensure that individuals are in control of their personal data and trust the digital environment**	• Funding of awareness-raising activities for individuals, particularly children; • Encouraging greater uptake of Privacy Enhancing Technologies by business and voluntary privacy certification schemes/privacy seals; • Introducing explicit references to the transparency and data minimisation principles in the Directive	• Further clarifying the concept of personal data; • Clarifying the rules on consent (explicit; burden of proof on controller); • Including genetic data into the category of "sensitive data"; • Clarifying the application of rules including for children (e.g. in the context of the right to be forgotten, clearer information, prohibition of profiling, modalities for consent online); • Clarifying provisions relating to processing by individuals for private purposes ("household exemption"); • Strengthening data controllers' responsibility and accountability, including by extending data controllers' obligations to data processors and creating stronger transparency obligations for data controllers (e.g. giving individuals clear and intelligible information); • Introducing Data Protection Officers (DPOs) for public authorities, companies above 250 employees and companies performing risky processing; • Introducing Data Protection Impact Assessments (DPIAs) for processing operations likely to present specific risks,; • Introducing a "data protection by design" principle; • Introducing a general obligation to notify data breaches to DPA within 24 hours of becoming aware of it (wherever feasible) and, when likely to adversely affect them, individuals within without undue delay after the breach has been established.	Measures under Policy Option 2 plus: • Defining consent as a "primary ground" for data processing; • Adding further categories to the list of sensitive data (data related to children, biometric and financial data); • Introducing harmonised EU-level criminal sanctions for breaches of data protection rules (see also problem 1); • Specifying detailed thresholds and criteria for notifying breaches to data subjects; • EU-wide certification schemes on data protection (see also problem 1)

	Sub-Problem	Specific Objectives	POLICY OPTION 1	POLICY OPTION 2	POLICY OPTION 3
	Difficulties in exercising data protection rights	**To ensure that individuals remain protected including when their data are processed abroad**	• Publish interpretative Communications regarding individuals' rights, e.g. the right to access their own data, particularly in the online environment; • Mandate standardisation institutions to develop standards for technical and organisational measures improving the protection of personal data	• Strengthening and harmonising provisions on how individuals can exercise their rights of access and rectification to personal data (e.g. free of charge); • Introducing a right to data portability; • Strengthening the right of individuals to have their personal data deleted ("right to be forgotten"); • Strengthening the right of associations to bring action before courts on behalf of individuals; • Clarifying the conditions for the application of the balance of interest criterion as a legitimate ground for data processing.	• Specific provisions regulating online identifiers and geo-location data; • Introducing a right to collective redress regarding breaches of the protection of personal data.
PROBLEM 3: Gaps and inconsistencies in the protection of personal data in the field of police and judicial cooperation in ;is would happen to a lesser extent given the different legal nature of the two instruments and the need for	• Limited scope of application of the Framework Decision • Insufficient safeguards in the Framework Decision	**To ensure that individuals' data protection rights are respected in this area**		• Stricter rules on limiting data processing to the purposes compatible with those of its initial collection; • Providing minimum conditions for the right to information and the right of access for individuals; • Add genetic data to the category f sensitive data; • Obligation to appoint a DPO • Codifying selected principles based on the Council of Europe Recommendations and best practices regarding law enforcement and data protection (distinction to be made between different types of data)	All measures under Policy Option 2 plus: • Providing for the right of individuals to always have 'direct access' to their data. • Obligation to carry out a DPIA for risky processing in information systems

	Sub-Problem	Specific Objectives	POLICY OPTION 1	POLICY OPTION 2	POLICY OPTION 3
	• Low level of harmonisation of the Framework Decision • Unclear relation with other former third pillar instruments leading to legal uncertainty and fragmentation	**To enhance trust and facilitate police co-operation and judicial co-operation in criminal matters**		• Extended scope for the new legal instrument to cover domestic data processing; • Clearer and more uniform rules on international transfers • Leaving unaffected other existing "former third pillar" instruments	• Amending the relevant provisions of all existing third pillar instruments, to align them entirely with the new rules as laid down in the reformed general instrument.

6. ANALYSIS OF IMPACTS

Following the standardized impact assessment methodology of the European Commission, this section summarises the expected impacts of the three policy options addressing objectives 1 (to enhance the internal market dimension of data protection) and 2 (to increase the effectiveness of data protection rights) and the two policy options for addressing objective 3 (to ensure a comprehensive EU data protection framework including in the field of policies cooperation and judicial cooperation in criminal matters). For the first two policy objectives, each of the three options is assessed for its effectiveness regarding each of the two policy objectives, its economic and financial impacts, including on the Union budget where appropriate, social impacts and effect on fundamental rights. All measures are assessed for their effectiveness regarding both policy objectives, where appropriate. For the third policy objective, the two options are assessed for their effectiveness regarding the policy objective and their economic and social impacts. Specific environmental impacts could not be identified for any of the options. A detailed assessment of the impacts of each measure is included in **Annexes 5, 6, 7,** and **9**. **The analysis is the basis for the choice of the preferred option which is defined in section 7.** The impact on the ***simplification*** of the regulatory environment of the preferred option is summarized in section 7.4, given that the data protection reform is contributing to the Commission's Rolling Programme for simplification.

6.1. Policy objectives 1 and 2: Enhancing the internal market dimension of data protection and increasing the effectiveness of data protection rights

6.1.1. POLICY OPTION 1: Interpretation, technical support tools, encouragement of self-regulation and cooperation and standardisation

a) ***Effectiveness regarding Policy objective 1: Enhancing the internal market dimension***

As regards the objective of harmonisation and clarification of the EU data protection rules, ***interpretative Communications of the Commission*** regarding the ***key concepts*** defined in the Directive would not be binding for the Member States and could therefore have only limited impact on reducing legal uncertainty and resulting costs. The Commission would have to apply this tool with caution in order to avoid the risk that data controllers or data subjects relying on the Commission's interpretation face legal problems in Member States that do not comply with its interpretation in its national law.

More self-regulation at EU level could help provide some additional legal certainty for data controllers and enable easier operation of specific sectors of the Single Market, in particular when enhanced by elements of co-regulation, such as formal recognition of the supervisory authorities. The establishment of EU level self-regulation mechanisms could, however, only be achieved meaningfully and effectively with a clear and harmonised legal framework as its foundation.

More support for the ***use of PETs*** by data controllers, as well as ***increased standardisation*** of technical and organisational data protection tools and measures, would increase businesses' certainty about how to achieve compliance with legal obligations.

Legislative clarifications regarding the principles of transparency, data minimisation**,** adequacy and BCRs would increase harmonisation and legal certainty and contribute to more consistent enforcement of data protection obligations.

As regards the objective of ***consistent enforcement*** (independence and powers of supervisory authorities), ***Commission communications*** would not overcome Member States' reluctance to change their national rules in order to allow for more harmonisation and more independence and consistent powers of DPAs.

Enhanced coordinating tasks of the Article 29 WP, the provision of additional IT tools to facilitate sharing of information and cooperation between national authorities and EU programmes for common training and staff exchanges between DPAs would have a positive, though not major, impact on more consistent enforcement of the rules. However, this solution would have a limited impact on the problem of inconsistent enforcement as no binding mechanism would be in place to ensure actual cooperation and mutual assistance.

b) Effectiveness regarding policy objective 2: Reinforcing individuals' right to data protection

Soft policy measures, such as interpretative Communications (e.g. on aspects of exercising the right to access one's own data), awareness-raising activities and encouragement of more self-regulation could ***help improve individuals' awareness of their rights and better understand how to practically exercise their data protection rights***. They would however not be sufficient for individuals to ascertain their rights effectively in the absence of a strong underlying legal framework.

Data subjects' ability to exercise their rights would be slightly improved by introducing clarifications in the legal framework regarding ***transparency*** and the ***data minimisation*** principle. This would however only bring along limited improvement to individual's rights as it would not substantially improve rights of access, deletion etc, which are essential to enhance trust in the digital environment.

c) ***Economic and financial impacts***

The expected ***financial and economic impacts of this policy option are limited.***

For ***economic operators***, measures under this option would provide some additional legal clarity but would not substantially reduce the costs and burdens linked to the current fragmentation of the regulatory environment. Moreover, continuing divergences in national interpretations and practices would still undermine individuals' trust in cross-border transactions and therefore limit their use of the online environment.

This set of foreseen measures would give rise to some additional compliance costs for data controllers as introducing the principles of transparency and of data minimisation might require additional capabilities in processing data and controlling flows. These are however difficult to quantify as the current rules already contain, albeit less explicitly, such obligations, and many organisations have already implemented them in practice. Moreover, 'data minimisation' is a sound data management principle. Raising awareness of its importance could yield benefits to businesses by helping data controllers avoid data overflow and mitigate the risks caused by security breaches.

Budgetary impacts: the option would have an impact on the public authorities' both at EU and national level. It would include some additional compliance costs due to the establishment of the online platform for data controllers' notifications, the IT tool for exchanges of information between DPAs, and the programmes for best practice sharing and staff exchange between national supervisory authorities. The extended tasks for the WP 29 would lead to an increase

of the annual costs of its secretariat from the currently estimated costs of €1.7 million[114] by an approximate minimum of 30%, i.e. an additional €0.5 million per year for the EU budget.

EU funding would also be needed for awareness-raising activities to encourage the use of PETs and privacy certification schemes. In the period 2009-2010 the funding of projects under the Fundamental Rights programme, covering awareness-raising and other activities amounted to more than €800,000. A 25% increase could be envisaged to finance additional awareness raising projects and activities in the domain of data protection.

Simplification: a ***single platform for notification of processing operations*** to national supervisory authorities would reduce administrative overhead for data controllers as it would simplify the process. However, this measure would not remove the additional administrative burden created by diverging national rules that would still need to be complied with.

An amendment to the legal instrument ***streamlining and clarifying the adequacy criteria and procedures*** would accelerate the recognition process and have a positive impact on relations with third countries. Increasing the number of adequate countries would in turn reduce the current overheads for data controllers transferring data to third countries in the longer term. However, the costs linked to the current burdensome procedures related to transfers based on other grounds would not be reduced in the short term. Although providing a legal basis for Binding Corporate Rules would be a positive step to recognise and encourage the use of this tool as a means to facilitate transfers within corporate groups, this would not be sufficient to address the shortcomings that currently limit their use (i.e. limitation of their scope).

d) ***Social impacts and Fundamental Rights***

By improving the capacity of individuals to exercise their data protection rights more effectively, this option would have a limited positive social impact regarding fundamental rights.

e) ***Environmental impacts***

No impact.

6.1.2. POLICY OPTION 2: Legislative amendments addressing gaps in current harmonisation, clarifying and strengthening individuals' rights and reinforcing responsibility of data controllers and processors, reinforcement and harmonisation of DPA powers and strengthening of their cooperation

a) ***Effectiveness regarding policy objective 1: Enhancing the internal market dimension***

- Regulatory intervention improving harmonisation and clarification of EU data protection rules, including concepts such as personal data and consent, would significantly reduce legal uncertainty for private companies and public authorities. Consistency will be increased due to the reduced margin of interpretation and the implementing measures and/or delegated acts to be adopted by the Commission. These would be used in particular in cases where new technological or economic developments require a common approach to be adopted by authorities in all Member States. In recent years, a large number of such issues have arisen, where diverging approaches have been taken at national level and by the various DPAs. In contrast to the only instruments available for providing guidance at present - i.e. non-binding

[114] The current figures for the secretarial costs are based on two administrators and one assistant working full time on matters related to the WP29.

opinions of the Article 29 Working Party – delegated or implementing acts by the Commission would be legally binding and thus provide legal certainty to data controllers.

The increased harmonisation will be beneficial not only for large multinational enterprises operating in several Member States, but also for enterprises currently only operating in their domestic markets, including SMES, which are expected to welcome increased legal certainty and uniformity as a strong incentive to expand their operations cross-border.

Two ***sub-options*** are possible in this respect:

i) If the current Directive is replaced by a Regulation:

- a Regulation, being directly applicable upon Member States, would achieve a very high degree of harmonisation of the rules, without the need for transposition into different national laws. It would also eliminate the need for defining criteria for applicable law, as the Regulation would be the applicable law across Member States. This is the option favoured 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, this option would have a major 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.

The current ***cost of legal fragmentation***, only in terms of ***administrative burden***, is estimated to amount to ***almost € 3 billion*** (*see Annex 9 for details*). These costs are incurred by economic operators processing personal data in several Member States and to which the different national laws and requirements are applicable. Replacing the Directive by a Regulation would have the effect of cutting such costs and drastically simplifying the regulatory environment.

ii) If the current Directive is amended and made a "maximum harmonisation Directive":

A very detailed Directive, further harmonising the applicable rules and reducing the room for manoeuvre left to Member States, could also help ***substantially in cutting the costs and administrative burden in the baseline scenario due to fragmentation***. However, this would not eliminate the need for transposition by Member States and the differences in national transposition laws that this might entail. Moreover, there would always be the risk for "gold-plating" from Member States.

- ***Clarifying and simplifying the rules on applicable law*** - even more if the single applicable law will be the EU Regulation - and on the responsible DPA by establishing a "**one-stop shop"** for data protection supervision ***will strengthen the internal market,*** including by removing existing differences in administrative formalities *vis-à-vis* DPAs and simplifying the requirements. This will have a major positive impact on data controllers, which will not have to be subject to different requirements and DPAs practices for the same data processing operations involving several Member States.

- Replacing the general notification of data processing activities, while maintaining a simplified ***basic registration*** system (as well as prior checks for processing operations likely to present specific risks to rights and freedoms of data subjects), will relieve data controllers from a burdensome obligation currently implemented in a diverging manner. However, the basic registration would also entail additional administrative burden for data controllers in those Member States that already today largely exempt from the notification obligation.

- An EU-wide harmonised obligation to ***notify data breaches*** will ensure consistency and avoid the creation of diverging rules in the Member States. The definition of criteria and thresholds for notification is a key factor in determining the cost impact of data breach obligations on data controllers and requires an in-depth assessment and will thus be left to implementing measures. However, in order to avoid delayed notifications – particularly in cases where the breach is likely to have adverse consequences on the data subject – it is important that the notification both to the DPA (as a rule, wherever feasible, 24 hours from the point the controller becomes aware of the breach) and to the data subject is made without undue delay.

- Simplifying rules and procedures for transfers of personal data to third countries would have a positive impact on business as it would entail, in the large majority of cases, the elimination of the need for prior authorisations before transferring data to third countries. This is an important element to boost the international competitiveness of EU businesses (see also Annex 10).

- Strengthening data controllers' and data processors' responsibility by introducing obligations to establish ***Data Protection Officers*** in organisations of a certain size and nature and to perform ***Data Protection Impact Assessments*** (with appropriate thresholds – see below) and introducing the principle of ***data protection by design*** will also offer easier ways to ensure and demonstrate compliance for data controllers and increase their legal certainty.

- Consistency of enforcement will be fostered by reinforcing and harmonising DPAs' powers – including the power to impose dissuasive and effective administrative sanctions - and by the establishment of a strong co-operation and mutual assistance mechanism between DPAs for cases with an EU dimension. The newly established "***consistency mechanism"*** would ensure that a decision takes account of data subjects and data controller establishments in EU countries other than the one of its main establishment. Interventions by the Commission, based on the expert advice of the EU Data Protection Board would allow settling potential disputes. Increased competences of the Commission in particular through ***implementing measures and/or delegated acts*** would further strengthen harmonisation. Consistency of enforcement would also benefit from harmonising the offences subject to administrative sanctions. A ***streamlining of the advisory functions of the EDPS and of WP 29*** (that would become the EU Data Protection Board and whose secretariat would be provided by the EDPS) would further increase consistency in the internal market and simplify the EU-coordination on data protection issues without the need of creating a new EU Agency.

b) ***Effectiveness regarding policy objective 2: Reinforcing individuals' right to data protection***

Legislative amendments improving harmonisation and clarification of EU data protection rules – both those strengthening controllers' responsibility and accountability and those clarifying and improving existing rights – would contribute to significantly strengthening individuals' control over their own data and the actual exercise of their rights. This is particularly true for legal provisions **clarifying definitions** ("personal data") and key concepts such as the **modalities for valid consent**, the right to have one's own data deleted **("right to be forgotten")** or to withdraw and transfer it to other controllers **("data portability**"). This will reduce grey areas where the rights of individuals are sometimes not properly respected.

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.

Highly beneficial in terms of individuals' rights are also the provisions strengthening the protection of **children's data**. 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"). The specific rules on consent in the online environment for children below 13 years – for which parental authorisation is required – take inspiration for the age limit from the current US 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 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.

Strengthened rules on remedies and sanctions would also significantly contribute to enhance individuals' data protection rights.

Simplifications regarding applicable law to choose ***only one law and one single data protection authority for data controllers*** active in several Member States may bring individuals in a situation where they interact with data controllers not directly responding to their national supervisory authorities. However, individuals will always the possibility to address themselves to the DPA (and the courts, for actions against the controller or the processor) of their country of residence. Moreover, individuals' legal position will be strengthened through the possibility for ***associations to bring proceedings*** before the courts on their behalf.

On the basis of ***strengthened DPAs powers***, the improved cross-border enforcement cooperation (particularly via the consistency mechanism) and the streamlining of the advisory functions of WP29 and EDPS will enable individuals to exercise their rights throughout the EU in a more consistent way and will provide them with a stronger mechanism to assert their rights in the internal market effectively. Strengthened ***administrative sanctions*** available to DPAs against non-compliant data controllers will contribute to ensure that individuals' rights are actually respected and enforced.

Other ***administrative simplifications***, such as the reduction of processing notification obligations and procedural conditions for transfers to third countries will not directly affect individuals possibility to exercise their rights, where it is ensured that data controllers and processors ***responsibility and accountability*** is respected, and individuals have ***transparency*** about the processing of their data and receive fast and comprehensive ***information on breaches*** of personal data protection.

The introduction of ***DPIAs*** can contribute to improving transparency for individuals, as data controllers will be better informed about the risks connected to their data processing, and to the security of the processing of personal data, as data controllers and processors can better avoid privacy risks related to some types of processing and take mitigating measures for residual risks. This effect is further strengthened by application of the principles of ***privacy by design and data minimisation***. Where they exist, ***Data Protection Officers*** often serve as the contact point for individuals regarding privacy concerns and are in a position to provide clear and comprehensible information on data protection issues, both individually and in public communication.

c) ***Economic and financial impacts***

– **Business**

These measures would bring ***important economic benefits within the internal market*** and create a more level playing field for businesses and foster their intra-EU and international competitiveness (see Annex 10).

Data Protection Officers (DPOs)

The obligation for larger economic operators only (more than 250 employees) to designate DPOs is not expected to create disproportionate costs, as DPOs are already common in large and multinational companies whose business is linked with the processing of personal data. Compliance costs are expected to amount to € 320 million per annum for large companies in total (*see annex 6 for more details*). Such costs could even be reduced in the scenario whereby groups of companies would appoint a single DPO for the group. ***SMEs*** would be excluded from this obligation, except if their core activity consists of processing operations which require regular and systematic monitoring. This would mean focusing on those activities which, by their own nature entail significant data protection risks. For example, this would concern head-hunters companies engaged in profiling activities. In such cases, this burden would be justified by the nature of the processing and the particular risks, as well as the added value for data subjects' rights of having a dedicated officer in place. Moreover, ***SMEs*** involved in such processing activities are expected to resort to *ad hoc* legal consultants for DPO services – as opposed to hiring/designating full time employees – which would limit their costs[115].

All companies would have to keep in any case a register of data processing operations. This would be a minimum requirement and is part of the routine internal administration and management of the business and would not constitute, in itself, an additional burden. This would also have an impact on data processors given the increased role of data processors in processing activities (e.g. in cloud computing applications). The above thresholds/criteria would apply also in this case.

The requirement to designate a DPO in ***public authorities*** would entail a cost for Member States' public authorities other than DPAs. It is difficult to estimate such costs given that many public authorities already have DPOs or corresponding functions (this varies between Member States).

However, the fact that where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority, ensures that the financial burden imposed is not disproportionate and can be spread out between the administrative departments of a public authority in a cost-efficient way.

Data Protection Impact Assessments (DPIAs)

The cost of a DPIA inherently involves a case-by-case calculation, depending on the nature and scale of the exercise. However, this obligation would be foreseen only for those data processing presenting specific risks to the rights and freedoms of data subjects. The threshold

[115] In the context of the SME consultation (see Annex 8), approximately 47% of respondents either stated that there is nobody formally assigned in their company to deal with data protection issues, or responded "I don't know / not applicable". 6% stated that there is a full-time employee dealing with data protection issues, and approximately 40% that someone carries out these tasks alongside other activities.

criteria for the applicability of this provision would be narrowly and precisely defined to ensure that its scope would not be disproportionately wide. Therefore, like for DPOs, most ***SMEs*** will be exempted from this measure. Actual costs, for those companies subject to this obligation, will necessarily depend on a set of variable criteria, including the size of the organisation and how significant the data protection impacts of a new technology, service, product, or proposed policy are expected to be. Annex 6 includes three case studies of DPIAs, differentiated by size and magnitude. It is estimated that a small-scale DPIA would cost €14,000, a medium-scale DPIA would cost €34,500, and a large-scale DPIA would cost €149,000.

In terms of benefits to businesses, undertaking a DPIA can help to identify and manage data protection risks, improve the security of personal data, and avoid unnecessary costs (in terms of problems being discovered at a later stage and inadequate data processing solutions) and damage to trust and reputation.

The burden would also not be unreasonable for public authorities, as a DPIA would not be required where the assessment of the impact on privacy and data protection of a certain processing activity or system has already been carried out during the preparatory stage of the law on which such processing is based.

Including a general principle of ***Data Protection/Privacy by Design*** without specific obligations is not expected to create significant economic impacts, as it only strengthens existing obligations. The Commission would be given the power to adopt implementing measures setting specific obligations, which will be subject to a separate assessment.

Strengthening the criteria for making EU law applicable to data controllers/businesses based outside the EU – e.g. when offering goods and services to individuals within the EU, or when monitoring them – could have a negative impact on them to the extent that EU rules on data protection are more stringent than in their country of establishment and may in some cases go as far as discouraging them from doing business in the EU. This is however essential to ensure that protection of EU individuals' data is not circumvented by a mere "outsourcing" of data processing activities in countries not ensuring an adequate level protection.

Simplifying the rules for international transfers would, overall, have a positive impact on the international competitiveness of EU businesses. (see Annex 10)

– **Public authorities**

Strengthening ***DPAs'*** independence and powers, together with the obligation for Member States to provide them with sufficient resources, would entail ***additional costs for public authorities*** that are currently not equipped with appropriate powers and adequate resources. It is difficult to estimate such costs in detail, given the differences in the size, available resources and sources of funding, tasks and powers of national DPAs. Costs will be higher for those Member States whose DPAs are currently not equipped with the appropriate tasks, powers and resources to ensure a common level of data protection in the EU. On the other hand, additional resources could derive from the increase of the powers to impose sanctions for breaches of data protection rules.

The new cooperation and mutual assistance mechanism between DPAs to improve the effectiveness and consistency of enforcement would entail additional costs (including administrative burden) for national DPAs, as they would need 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;

– Have additional staff and mechanisms in place to investigate enforcement requests from DPAs in other Member States;
– Enforce the decisions taken by DPAs in other Member States as part of the "one-stop shop" system of supervision.

The additional tasks of the ***EDPS*** for providing the secretariat of the EU Data Protection Board replacing WP29 and in particular the involvement in the consistency mechanism are likely to require an increase of its current resources by an additional €3 million per annum on average for the first six years, including credits for additional human resources of 10 Full Time Equivalent (FTE).

– **Simplification**

The costs of current legal fragmentation for economic operators only in terms of administrative burden are estimated to amount to ***more than € 2.9 billion in total per annum.*** The expected ***net savings*** for economic operators would be around ***€ 2.3 billion per annum***, arising from the elimination of legal fragmentation and the simplification of notifications (basic registration). Clarifying the requirements for ***consent,*** as well as explicitly stating that the data controllers should be able to prove it (when required), will not entail significant additional costs, as the obligation to demonstrate that consent has been given, when the processing is based on it, exists already today. Thus, the purpose is not to introduce a (new) obligation for 'written consent' in all cases (a statement or clear "affirmative action" of the data subject would also be valid), but merely to clarify existing obligations in order to harmonise the current divergent practices across Member States and give legal certainty to data controllers, who would otherwise continue to face fragmentation. The streamlining of the advisory role of WP29 and EDPS simplifies significantly the advisory process and accelerates the provision of coordinated guidance.

d) ***Social impacts and Fundamental Rights***

These measures would give rise to significant positive ***social impacts***, including the strengthening of several individual ***fundamental rights***.

e) ***Environmental impacts***

No impacts.

6.1.3. POLICY OPTION 3: Detailed harmonisation and rules at EU level in all policy fields and sectors, centralised enforcement and EU wide harmonised sanctions and redress mechanisms.

a) ***Effectiveness regarding policy objective 1: Enhancing the internal market dimension***

Adding further detailed legal provisions, including and beyond the measures envisaged in option 2 – i.e. making consent as primary legal ground, adding additional categories of sensitive data, envisaging specific and detailed rules for the execution of individuals' rights and establishing detailed and harmonised rules on specific sectors, such as health and employment - would lead to a ***maximum reduction of divergences between Member States***. However, this would at the same time lead to an unbalanced situation, as there may be not enough flexibility for Member States to apply EU rules taking account of national specificities, which will make implementation difficult. As regards in particular issues without cross border impact, some flexibility is necessary for Member Sates allowing them to design solutions tailored to their specific issues.

The ***total abolition of notifications*** – while maintaining prior checks for risky processing - would greatly simplify the regulatory environment, reduce administrative burden and increase the consistency of enforcement. Having more harmonised rules would also contribute to pursuing public policies at EU level.

An ***EU-wide certification system*** for data controllers' compliance with their data protection obligations would provide them with full legal certainty in an *ex-ante* verification process.

Concerning the specification of detailed criteria and thresholds for notifying ***data breaches,*** US experience shows that the definition of such thresholds and criteria is a very complex and difficult exercise, and deserves an in-depth and specific assessment.

As regards consistent enforcement, the setting up of an ***EU Data Protection Agency*** (which would be a new EU Agency) would improve the consistency of enforcement and solve the inconsistencies for cases with a clear EU dimension. The EU Data Protection Agency would take over from national DPAs the responsibility for supervision of specific cross-border cases. However, regardless the economic implications of setting up such an agency (see below), this could lead to a situation where an EU agency would enjoy discretionary competences which could go too far under EU law[116]. ***EU harmonised criminal sanctions*** would further strengthen this effect but would raise opposition a the recourse to criminal sanctions in this area is very rare.

b) ***Effectiveness regarding policy objective 2: Reinforcing individuals' right to data protection***

Data subjects' rights, including the rights of children, would be further strengthened (compared to the impacts under policy options 2) by extending the definition of sensitive data to include data of children, and biometric and financial data and more precise rules for specific circumstances and sectors (e.g. location data and online identifiers). More detailed rules on the modalities of exercising individuals' rights would strengthen these.

Defining consent as a primary ground for data processing would not necessarily have a positive effect on individuals' rights as it may lead to numerous and eventually "artificial" expressions of consent (i.e. not really specific, freely given etc).

The definition of thresholds and procedurals elements of data breach notifications in the basic act instead of in implementing or delegated acts has no advantage for individuals.

The introduction of a right to collective redress could allow maximising rights by means of litigation.

A central Agency supervising the cross-border processing activities at EU level, a single contact point for individuals in many cases, would ease the exercise of their rights. However, national DPAs would remain competent for purely national situations.

Additional strengthening of individual rights would be expected from harmonising the level of **sanctions**, including **criminal** ones, at EU level for infringements of data protection rules. The latter element would lower the threshold for individuals to pursue their rights also through legal action when administrative procedures do not produce a satisfactory outcome.

An EU-wide certification scheme with clear and strictly applied criteria would provide individuals with a means to select data controllers for their transactions according to their

[116] See Case 9/56, Meroni & Co., Industrie Metallurgiche, SpA v. High Authority of the European Coal and Steel Community, 1958.

degree of compliance. A certification for third country controllers dealing directly with individuals would also have a positive effect.

c) ***Economic and financial impacts***

– **Economic operators**

Making a hierarchy between grounds for processing with consent as the primary ground would make the processing of personal data more difficult, cumbersome and costly for businesses. Expanding the categories of sensitive data to biometric, financial and children's data would also entail substantial costs as it would require data controllers to adapt their procedures and technical systems to more stringent rules concerning the processing of such data.

Specifying detailed ***criteria and thresholds for notifying data breaches*** would provide more legal certainty but is also likely to impose undue costs on data controllers.

As regards international transfers, the voluntary ***certificate/seal data controllers***' compliance with EU data protection rules would benefit EU competitiveness and facilitate data transfers between the EU and third countries.

– **Public authorities**

While the elimination of the general notification requirement will benefit controllers and processors (see below), it will have a negative impact on those DPAs for whom this currently represents an important – if not exclusive – source of financing, such as the Information Commissioner's Office (ICO) in the UK. It may also make it more difficult for certain DPAs to maintain an overview of data processing activities.

An EU-wide certification system would be a resource-intensive option.

The budgetary impacts of setting up a regulatory EU Data Protection Agency would be significant. For comparison, the overall 2011 budget for the EDPS amounts to € 7.6 million, the EU Fundamental Rights Agency's budget was € 20 million and that for the European Network and Information Security Agency was € 8.1 million. It is therefore expected that a regulatory agency for data protection would require a substantial annual budget in the range of € 7-15 million.

– **Simplification**

Abolishing notification or registration of data processing operations altogether would reduce costs and administrative burden for data controllers, amounting to € 130 million per annum only in terms of administrative burden plus the fee that may additionally be imposed..

d) ***Social impacts and Fundamental Rights***

The ***social/fundamental rights impact*** would be generally positive also under this option. Impacts would be similar as under option 2, but right to an effective remedy would be enhanced thanks to provisions on collective redress. Many of the more detailed measures do not create additional positive impacts.

It is expected that too detailed data protection legislation would not be easily accepted at national level as it would ***not leave enough flexibility for national social norms and cultural specificities*** (for instance in the employment sector, regarding surveillance of employees).

e) *Environmental impacts*

No impacts.

6.2. Objective 3: Enhancing the coherence of the EU data protection framework in the field of police and judicial cooperation in criminal matters

There is no Policy Option 1, as 'soft' action would not be appropriate to meet the objectives.

6.2.1. POLICY OPTION 2: Strengthened specific rules and new instrument with extended scope

a) *Effectiveness regarding the policy objective*

The extension of the scope of the general data protection instruments to cover the area of police and judicial cooperation in criminal matters would have a positive impact on the objective of enhancing the coherence of the EU data protection framework. It would also contribute to eliminating gaps in particular by extending the scope of data protection rules in this area to 'domestic' processing.

Individuals' rights would also be strengthened by setting minimum conditions for the ***right of access*** and providing stricter rules on ***purpose limitation***. The codification of some principles from the Council of Europe Recommendation on law enforcement, including on genetic data, will contribute to the fulfilment of the objective.

The establishment of a mechanism supporting common interpretations by extending the competences of the WP 29 and of the Commission in this area – as a consequence of the entry into force of the Lisbon Treaty- would further help to address inconsistencies and gaps.

b) *Economic and financial impacts*

Impacts would mainly concern the public sector. There is no indication that better coordination, harmonisation and clarity of rules would require any additional resources; rather the use of existing resources could become more efficient. The impact of new obligations, such as the appointment of a Data Protection Officer (DPO), would also be limited to the extent that the possibility is provided – as for public authorities in general - to appoint a single DPO for different areas, departments and offices (and not, for instance, one per each Police Office or Department).

c) *Social impacts and Fundamental Rights*

Clarification of provisions, reinforcement of individuals' rights and increased coordination would have a positive effect on individuals' fundamental rights, particularly on the right to data protection.

On the other hand, the fact that rules are tailored to the nature and needs of law enforcement activities – by providing for exceptions and limitations to individuals rights when, for example, this is necessary to avoid disrupting investigations, to protect public security and the rights and freedom of others etc – will avoid interfering with and disrupting the activities of police and judicial authorities in the performance of their public interest's tasks.

d) *Environmental impacts*

No impacts.

6.2.2. POLICY OPTION 3: Extended specific rules and full integration of general principles in former third pillar instruments

a) ***Effectiveness regarding the policy objective***

Explicit amendments of all instruments extending the general rules to the area of police and judicial cooperation in criminal matters, with limited derogations/specifications in line with the Charter, would have a very positive impact in terms of consistency and coherence of the rules in this area and of strengthening individuals' rights and would provide for a higher level of data protection.

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.

b) ***Economic and financial impacts***

As in option 1.

c) ***Social impacts and Fundamental Rights***

The positive social impact in terms of enhancement of individuals' data protection rights would be slightly stronger than under option 1. Measures under this option could, however, undermine the work of law enforcement authorities and affect their capacity to effectively prevent and combat crime.

d) ***Environmental impacts***

No impacts.

Table 3: Summary of economic impacts

Policy Option	Magnitude of Economic Impacts	Benefits	Costs
Policy Option 1	Limited	*Compliance costs* • Streamlining and clarifying the adequacy criteria and procedures would accelerate the recognition process and would facilitate data transfers to third countries. Increasing the number of adequate countries would in turn reduce the current overheads for data controllers transferring data to third countries in the longer term. *Administrative burden* • Simplification of Notifications: a single platform for data controllers' notification would accelerate the process (but no substantial reduction of administrative burden	*Compliance costs* • Continued divergences in national DP laws do not alleviate administrative burdens and disincentives cross-border trade (both for businesses and individuals) • Introduction of data minimisation principle • Costs flowing from online platform for data controllers' notifications, IT tool for exchanges of information between DPAs, best practice-sharing programmes, and staff exchange between national supervisory authorities • Extended tasks for WP29 would increase annual secretarial costs from €1.7 million by an approximate minimum of 30%, i.e. an additional €0.5 million per year for the EU budget. • Costs to the EU budget for awareness-raising activities (children, PETs uptake, certification, etc) *Administrative burden* • Introduction of transparency principle adds some administrative burden estimated at approximately €176 million per annum

Policy Option	Magnitude of Economic Impacts	Benefits	Costs
Policy Option 2	Extensive	*Compliance costs* • Increased harmonisation will create a more level playing field for businesses and foster their intra-EU and international competitiveness. • DPOs and DPIA increase data controllers' accountability, and will help identify and manage data protection risks, improve the security of personal data, avoid unnecessary costs and damage to trust and reputation. • Positive impacts on the international competitiveness of EU businesses through the simplification of rules for international transfers. *Administrative burden* • An estimated € 2.3 billion in the administrative burden of legal fragmentation will be virtually eliminated by the increased harmonisation. • Replacement of notifications by a basic registration system would reduce administrative burden linked to that of about 50% (€ 65 million, fees excluded).	*Compliance costs* • Obligation (where applicable) to appoint DPOs imposes some costs on business (estimated at €320 per annum for large businesses) • DPIAs (where applicable) impose costs on a case-by-case basis. It is estimated that a small-scale DPIA would cost €14,000, a medium-scale DPIA would cost €34,500, and a large-scale DPIA would cost €149,000. • Strengthening DPAs' independence and powers and resources, would entail additional costs for public authorities. It is difficult to estimate such costs in detail, given national divergences, but costs will be higher MS whose DPAs are currently under-resourced. • New cooperation and mutual assistance mechanism between DPAs would entail additional costs (including administrative burden) for national DPAs, in terms of additional resources.. • Additional tasks of EDPS for providing the secretariat of the EU Data Protection Board are likely to require an average increase of its annual budget by about €3 million, including additional human resources. *Administrative burden* • Introducing a general obligation to notify data breaches to DPAs and individuals imposes additional administrative burden estimated at €20 million per annum. • Introducing a general obligation for data controllers to be able to demonstrate compliance with data protection law is estimated to impose additional administrative burden of approximately €580 million per annum.

Policy Option	Magnitude of Economic Impacts	Benefits	Costs
Policy Option 3	Far-reaching	*Administrative burden* • The total abolition of notifications – while maintaining prior checks in case of risky processing - would greatly simplify the regulatory environment and reduce administrative burden by approximately €130 million per annum (fees excluded).	*Compliance costs* • Eliminating the general notification requirement will have a negative impact on those DPAs for whom this currently represents an important – if not exclusive – source of financing • Making a hierarchy between grounds for processing with consent as the primary ground would make the processing of personal data more difficult, cumbersome and costly for businesses. • Expanding the categories of sensitive data to biometric, financial and children's data would entail costs as it would require data controllers to adapt their procedures and technical systems to more stringent rules concerning the processing of such data. • Specifying detailed criteria and thresholds for notifying data breaches would provide more legal certainty but is also likely to impose undue costs on data controllers. • An EU-wide certification system would be a resource-intensive option. • Budgetary impacts of setting up a regulatory EU Data Protection Agency would be significant. For comparison, the overall 2011 budget for the EDPS amounts to €7.6 million, the EU Fundamental Rights Agency's budget was €20 million and that for the European Network and Information Security Agency was €8.1 million. It is expected that a regulatory agency for data protection would require an annual budget of approximately €7-15 million.

7. COMPARING THE OPTIONS

7.1.1. Analysis

7.1.1. Policy Option 1

Measures under Policy Option 1 would lead to low levels of compliance and administrative costs, especially for private data controllers, as most of the additional costs would fall on national and EU public authorities (e.g. financing for awareness-raising activities, encouragement of PETs and of privacy certification schemes).

However, at the same time it would only have a limited positive impact on the identified problems and on achieving the policy objectives.

In terms of political feasibility, although the policy proposals that have been included in Policy Option 1 are generally not controversial, this policy option is likely to be met with resistance by stakeholders as a result of its limited scope and impact on the problems, and would be considered as not ambitious enough.

7.1.2. Policy Option 2

As regards the first and second objectives, measures under Policy Option 2 are a considerably further-reaching and more ambitious package of proposals, particularly of regulatory nature. It will lead to a ***significant reduction of fragmentation and legal uncertainty.*** It can be expected to have a much greater impact in addressing the identified problems and achieving the policy objectives.

On balance, the compliance and administrative costs associated with the proposals included in this policy option are expected to be reasonable in view of the benefits and savings of **about *€2.3 billion*** in terms of administrative burden that can be achieved (*see Annex 9*).

This option will ensure a better and consistent enforcement overall. The abolition of notifications in favour of a much simpler 'basic registration system' would also simplify the regulatory environment and reduce the administrative burden.

As to its political feasibility and stakeholders' acceptance, it is expected to be positively received by economic operators, as it would reduce their overall compliance costs, particularly those linked to the currently fragmented rules. The strengthening of data protection rights would be welcomed by the data protection community and DPAs in general. The EP report on this issue has likewise called for providing a uniform and high level of protection of individuals, while Council conclusions have called for the new legal framework to provide for a higher level of harmonisation than the current one.

As regards the third general objective, this option would contribute to achieving the objectives of ensuring more coherence and consistency of data protection rules in the area of police cooperation and judicial cooperation in criminal matters by repealing the Framework Decision, and eliminating gaps in particular by extending its scope to "domestic" processing.

7.1.3. Policy Option 3

As regards the first and second general objectives, measures under Policy Option 3 are those having the greatest impact on the problems and on the achievement of the objectives. They include most of the measures in Policy Option 2, while being more far-reaching under

several aspects (e.g. more detailed rules on certain sectors, abolition of notifications and the establishment of a European Data Protection Agency).

They would therefore have a high and positive impact in terms of both reducing costs linked to legal fragmentation and enhancing individuals' rights. Moreover, it would maximise the consistency and coherence of data protection rules in the former third pillar and raise the data protection standards in that context.

However, some of the measures included under this option either have ***high compliance*** costs or are likely to encounter a strong opposition from stakeholders.

As to the third general objective, Policy Option 3 may raise difficulties: the simultaneous amendment of all former third pillar instruments would be very complex and politically unfeasible, as Member States will not accept endangering existing forms of cooperation between law enforcement authorities without an in-depth assessment, involving them, of any envisaged modification.

It would therefore be, overall, a rather ***controversial option*** with some measures raising strong opposition from stakeholders.

7.2. Summary table comparing the policy options

Comparison of Policy Options					
	Baseline Scenario (BS)	**PO1: Soft action**	**PO2 Modernised legal framework**	**PO3: Detailed legal rules at EU level**	**Preferred Option**
Effectiveness regarding objective 1: Creating a level playing field in the internal market					
Harmonise and clarify EU data protection rules and procedures	-- Fragmentation and uncertainty aggravate.	+ Limited but positive effect of interpretative communications from the Commission, promotion of PETs and standardisation.	+++ Very positive effect due to the large reduction of legal uncertainties, harmonised obligation and simplification of international transfers	++ Very positive effect due to the maximum reduction of disparities between Member States. However, no flexibility for Member States to adapt to national specificities	+++ PO2+ elements of PO1
Ensure consistent enforcement of data protection rules	-- No EU wide coordination of enforcement.	+ Limited but positive effect of coordination tools for the WP 29.	+++ Positive effect due to the introduction of a country of origin principle, mechanism guaranteeing consistency of DPAs decisions and competence for the Commission to adopt implementing measures and/or delegated acts	++ Very positive. An EU data protection agency would guarantee consistency of decisions at EU level. However difficult to reconcile with EU Law. Harmonised criminal sanctions would strengthen the effect.	+++ PO2+elements of PO1

Comparison of Policy Options					
	Baseline Scenario (BS)	**PO1: Soft action**	**PO2 Modernised legal framework**	**PO3: Detailed legal rules at EU level**	**Preferred Option**
Effectiveness regarding objective 2: Reinforcing individuals' right to data protection					
Put individuals in control of their personal data	-- Fragmentation and uncertainty increase and continue to undermine trust.	+ Limited legal clarifications would only slightly improve the individual rights.	+++ Positive impact of "right to be forgotten", "data portability", addition of genetic data to sensitive data	+++ Increased protection of individuals by extending definition of sensitive data further to children data, financial data and biometric data	+++ PO2
Protect individuals data wherever they data are processed	-- Increasing problem with the development of cloud computing.	- Limited amendments to adequacy would improve some specific situations.	+++ Positive impact of new applicable law rules for controllers established outside the EU	+++ Additional positive impact of mandatory EU wide certification mechanisms allowing individuals to select controllers based on their certification level	+++ PO2
Reinforce the accountability of those processing personal data	-- No incentive beyond basic compliance, fragmentation prevents effective self regulation.	-- Limited but positive effect of interpretative communication from the Commission.	++ Individuals will benefit from the new obligations of controllers and strengthened independence and powers of DPAs e.g. Data protection impact assessment, privacy by design and data minimisation principle.	+++ Better protection of individuals through collective redress. The EU agency have a positive impact, as a single contact point for individuals	++ PO2

Comparison of Policy Options					
	Baseline Scenario (BS)	**PO1: Soft action**	**PO2 Modernised legal framework**	**PO3: Detailed legal rules at EU level**	**Preferred Option**
Effectiveness regarding objective 3: Including police and judicial co-operation in the EU data protection framework					
Reinforce the data protection framework facilitating the police co-operation and judicial co-operation in criminal matters	-- Inconsistencies and gaps aggravate and continue to affect a smooth co-operation	N/A	++ Enhancing the coherence and contributing to eliminate gaps	++ Further strengthening data subjects rights and higher level of protection	++ PO2
Lisbonize data protection rules in the ex third pillar while respecting specificities	-- Fragmentation and low level of harmonisation continue	N/A	++	++	++ PO2

Comparison of Policy Options					
	Baseline Scenario (BS)	**PO1: Soft action**	**PO2 Modernised legal framework**	**PO3: Detailed legal rules at EU level**	**Preferred Option**
Economic and financial impacts					
Impact on economic operators (including SMEs)	-- No reduction of current obligations of business and public authorities Current poor level of trust in the online sector would be maintained.	-- Simplified notifications would help SMEs and business operating cross border. Self regulation, promotion of PETs and awareness raising have a positive limited impact on the trust in the digital environment.	++ Overall net savings of 2.3 billion Euros compared to the baseline scenario for businesses operating cross border due to increased harmonisation and coordinated enforcement. Limited new obligations to improve compliance (DPOs mainly for large companies) and detect failures (data breach notifications)	+ Collective redress increases risk of litigation. Legislation to the detail could slow innovation. Detailed obligations could create additional compliance costs for business Negative impact on public authorities who rely on the notifications for their funding. But positive impact for economic stakeholders	+ PO2 + encouragements of PETS, certification and awareness raising
Budgetary impact (EU and national budget)	- EU: Continuing financing projects within the fundamental right program MS: No budgetary impact	- EU: Cost of a single platform for notification Cost of IT tools for the WP 29 Cost of awareness raising activities MS: no costs	+ EU: Cost of reinforcing the EDPS who would manage the consistency mechanism and provide the secretariat of WP 29 (0,85M€/year). MS: Public authorities shall be reinforced to deal with their reinforced powers.	-- EU: Cost of introducing an agency MS: Agency would take over some of the current tasks of MSes, reducing their costs	+ PO2

Comparison of Policy Options					
	Baseline Scenario (BS)	**PO1: Soft action**	**PO2 Modernised legal framework**	**PO3: Detailed legal rules at EU level**	**Preferred Option**
Cutting red tape	--- Total admin burden cost equals €5.3 billion per annum Continuing national divergences and multiple requirements on businesses	+ Limited reduction of the administrative burden through a single system for notification and streamlined adequacy mechanism	++ The administrative burden costs related to legal fragmentation would be drastically reduced (€2.9 billion yearly saving leading to a € 2.3 billion overall net saving) Positive effect due to the abolition of notifications (while maintaining prior checks for risky processing)	+++ Complete abolition of notification of processing would largely eliminate administrative burden. EU agency single point of contact for cross border business	+++ PO2 PO3 for notification €2.9 billion yearly reduction in administrative burden
Simplification	--	+ Streamlined adequacy will accelerate the recognition of third countries. Otherwise, no simplification	++ General reduction of compliance and admin burden costs, limited administrative burden in case of failure (data breach notifications) is introduced	+++ The detailed rules may lead to more cases of non compliance and misunderstandings from businesses	++ PO2
Social impact and Fundamental Rights					
	-	+ Limited positive impact, in the fundamental rights dimension	+++ Benefits on freedom of expression, non discrimination, and right to a judicial remedy.	+++ The restrictive measures under this option create only a limited positive impact, while possibly	+++ PO2

Comparison of Policy Options					
	Baseline Scenario (BS)	**PO1: Soft action**	**PO2 Modernised legal framework**	**PO3: Detailed legal rules at EU level**	**Preferred Option**
			No limitation to the freedom to conduct a business	limiting the freedom to conduct a business.	
Environmental impact					
	No impact	No impact	No impact	No impact	No impact
Feasibility					
	Low	Medium	Medium/high	Low/medium	Medium/high

7.3. Preferred Option

The Preferred Option consists of most of the measures of Policy Option 2, which are those most likely to ensure the achievement of public policy objectives without excessive compliance costs, combined with:

– One key element of Policy Option 3: the ***abolition of the notification obligations*** (except in cases of prior checks: risky processing), which would simplify the regulatory environment further and totally eliminate the administrative burden required by this obligation (which would partly remain with a basic registration system). This is called for by a large majority of stakeholders and would have a limited negative impact on some DPAs (*see under § 6 above);*

– Some soft measures from Policy Option 1: the encouragement of greater uptake of PETs and privacy certification schemes and awareness-raising activities for individuals, particularly children.

Table 4 - Summary of preferred Policy Option

Problem	Preferred Policy Option
PROBLEM 1: - Barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement **General Objective: To enhance the internal market dimension of data protection**	• Abolishing notifications of processing operations altogether, while maintaining prior checks for risky processing requiring prior checking (*from Policy Option 3)* • Simplifying the provisions on applicable law, to ensure that data controllers are always subject to legislation of one Member State only (or EU Regulation) and supervision of only one supervisory authority; • Amending substantive rules to remove explicit margins for manoeuvre for Member States and increase clarity and precision of the rules in general; • Giving the Commission the competence to adopt implementing acts or delegated acts where there is a need for uniform implementation of specific provisions, or when there is a need to supplement or amend specific non-essential data protection provisions, ensuring that the interests of SMEs are taken into account when these measures are developed (in accordance with the "think small first" principle). ***Simplifying rules and procedures for transfers of personal data to third countries*** by giving the Commission exclusive competence for adequacy decisions, introducing more flexibility, extending the scope of BCRs to include data processors and introducing a clear definition of "groups of companies". Moreover, prior authorisations will be deleted in the large majority of cases.. • Introducing specific provisions to safeguard the competitiveness of the EU economy and take into account the relatively weaker position of SMEs in markets, in the context of: information requirements; responsibilities of the data controller and joint controllers; documentation to be kept by controllers; notification of data breaches to the data subject; data protection impact assessments; processing of health data; and administrative sanctions. • Reinforcing and harmonising DPA tasks and powers and obliging Member States through the EU legal instrument to ensure provide adequate resources; • Harmonising offences subject to administrative sanctions, with low minimum thresholds to prevent unrealistic sanctions on SMEs; • Providing for mutual recognition of DPAs' decisions and increased co-operation via a consistency mechanism and mutual assistance operated, under the supervision of the Commission, through a European Data Protection Board with a possibility for the Commission to intervene to

	ensure swift compliance with EU law; • Ensuring the independence and effectiveness of the new European Data Protection Board by establishing the EDPS as responsible for its secretariat (instead of the Commission). • Encouragement of awareness-raising activities for SMEs to ensure adequate knowledge and understanding of the new legal framework
PROBLEM 2: Difficulties for individuals to stay in control of their personal data **General Objective: To increase the effectiveness of the fundamental right to data protection**	• Funding of awareness-raising activities for individuals, particularly children (*from Policy Option 1)* • Encouraging greater uptake of Privacy Enhancing Technologies by business and voluntary privacy certification schemes/privacy seals (*from Policy Option 1)* • Further clarifying the concept of personal data; • Clarifying the modalities for consent; • Including genetic data into the category of "sensitive data" and harmonising exceptions to the processing of sensitive data; • Clarifying the application of rules including for children (e.g. in the context of the right to be forgotten, clearer information, prohibition of profiling); • Clarifying provisions relating to processing by individuals for private purposes ("household exemption"); • Strengthening data controllers' responsibility and accountability, including by extending data controllers' obligations to data processors and creating stronger transparency obligations for data controllers (e.g. giving individuals clear and intelligible information); • Introducing Data Protection Officers (DPOs) for public authorities, companies above 250 employees and companies performing risky processing (i.e. excluding micro- enterprises and SMEs not involved in risky processing); • Introducing Data Protection Impact Assessments (DPIAs) for processing operations likely to present specific risks, e.g. when processing biometric data; • Introducing a "data protection by design" principle; • Introducing a general obligation to notify data breaches to DPAs within 24 hours after becoming aware of the breach (if feasible), and without undue delay to individuals. • Strengthening and harmonising provisions on how individuals can exercise their rights of access and rectification to personal data (e.g. free of charge); • Introducing a right to data portability, giving individuals the possibility to withdraw their personal data from a service provider and process them themselves or transfer them to another provider, as far as this is technically feasible; • Strengthening the right of individuals to have their personal data deleted ("right to be forgotten"); • Strengthening the right of associations to bring action before courts on behalf of individuals;.
PROBLEM 3: Gaps and inconsistencies in the protection of personal data in the field of police and judicial cooperation in	• Extended scope of rules in this area to cover domestic data processing; • Stricter rules on limiting data processing to the purposes compatible with those of its initial collection; • Providing minimum conditions for the right of access for individuals; • Adding genetic data to the categories of sensitive data, • Codifying selected principles based on the Council of Europe Recommendations and best practices regarding law enforcement and data protection (e.g. distinction between categories of data subjects);

criminal matters **General Objective: Enhance the coherence of the EU data protection framework**	• Establishing mechanisms fostering common interpretation at EU level (extended competence of the WP29 and the Commission).

The Preferred Option is estimated to reduce overall administrative burden by about €2.3 billion per annum. Most of this reduction will come from the important reduction of fragmentation in national data protection rules, which currently imposes significant compliance costs on economic operators and affects the free flow of personal data in the EU. It will hence have significant positive impacts on the EU internal market.

The Preferred Option is also expected to ***substantially strengthen data subjects' rights*** and the control over their data – including in the area of police cooperation and judicial cooperation in criminal matters thus enhancing the fundamental right to data protection and at the same time effective police and justice cooperation.

Some additional compliance costs are expected to accrue from the strengthened data protection rules, but a strong data protection regime in Europe can offer a competitive advantage for the European economy. The Eurobarometer survey[117] and other sources[118] suggest that consumers are more likely to patronise businesses with strong privacy and data protection records. Studies also indicate that loss of customers accounts for 60% of the total costs of a data breach[119]. ***Privacy and data protection can increase consumer confidence.*** The Eurobarometer survey finds that fewer than four in ten Europeans trust shops, department stores, phone companies, mobile phone companies, internet service providers, and internet companies to protect their data.[120] Enhanced data protection could enable European companies to ***capture the market share of Europeans who do not shop online because of a lack of trust*** that their information is secure, win customers who leave organisations with poor data protection records and retain their existing customers.

Requiring companies to adopt high standards of data protection can also lead to long-term improvements for European businesses. Non-EU companies which do not have appropriate standards will be limited in their ability to operate within the EU, and European companies will be at the forefront if similarly high standards are adopted in third countries. Thus, regulation could act as a stimulus to ***innovation*** and to data protection-friendly business models. Furthermore, strong data protection regimes could offer an opportunity to innovate in other ways. For example, privacy enhancing technologies or privacy by design and data protection consulting are sectors which could benefit from an environment where enhanced data protection is the norm. ***European industry could become world leaders in privacy enhancing technology or privacy by design solutions, drawing business, jobs and capital to the European Union*** (*see also Annex 10 on the impact of the preferred option on competiveness*).

---

117 EB2011.

118 Information Commissioner's Office (UK), *The Privacy Dividend: The Business Case for Investing in Proactive Privacy Protection*, March 2010

119 Ponemon Institute and Symantec, *2010 Annual Study: U.S. Cost of a Data Breach*, 2011.

120 EB2011.

The Preferred Option includes a balanced solution also in relation to problem 3, as it strengthens individuals' rights, eliminates gaps and reduces inconsistencies as regards data protection in the area of police and judicial cooperation in criminal matters, while limiting the potentially high impacts – *vis-à-vis* Member States' law enforcement authorities – that would derive from an immediate amendment of all ex-third pillar instruments.

7.4. Impacts on simplification of the Preferred Option

The data protection reform package forms part of the Commission's rolling simplification programme. The simplification will benefit individuals, private sector operators, public authorities, including police and judicial authorities in particular by bringing the following improvements:

- enhanced legal certainty as regards applicable rights and obligations, reduction of the current legal fragmentation, and reduction of costs and administrative burden caused by them;
- simplification of the regulatory environment by streamlining obligations and procedures involved in protecting personal data with more focus on risky processing activities;
- clearer rights for individuals and clearer obligations for those processing personal data;
- more coherence and consistency in the field of the former third pillar and as regards functions of the WP29 and the EDPS.

As regards ***administrative burden***, significant reductions will be the consequence, in particular, of the abolition of the notification system and of simplified procedures for international transfers. The "one-stop-shop" for data controllers will also greatly reduce compliance costs. Compliance costs and administrative burden related to the introduction of a principle of transparency, the notification of data breaches and the establishment of a new co-operation and co-ordination mechanisms are justified by enhanced quality and efficiency of individuals rights.

Table 5 below provides an overview of envisaged changes to the current regulatory framework which contribute to its reduction both in terms of enhanced quality and efficiency.

Current provisions in the regulatory framework	Changes envisaged in the future framework	Expected impacts on simplification
<u>Information of Individuals</u> **Art 10 and 11** of Directive 95/46/EC establish the obligations of data controllers with regards to **information to be given to the data subject** (i.e. identity of data controller and his representative; purposes of the processing for which the data are intended; recipients of the data; information on rights of access) ►***Significant administrative burden is incurred by data controllers as a result of this***	**Introduction of an explicit principle of transparency** - Benefit for data subjects This would ensure that data processing is "transparent" to data subjects. **Information requirements** would be clarified. I**ntelligible information, using clear and plain language** will have to be provided to individuals and I particular to children.	**- Better information for data subjects** - **Greater legal clarity** for data controllers. ►***Data controllers' are expected to incur one-off compliance costs for taking the necessary measures in order to provide the updated information.*** ***This cost is justified by the***

obligation	Additional information like the contact details of the DPAs and specific rights will have to be provided. As regards controller, model for privacy notices will be introduced (via implementing measures or delegated acts).	***enhanced quality of information (and hence protection) to data subjects.*** ***Estimated to approximately €180 million per annum in Annex 9.***
<u>Notification</u> **Art 18** requires data controllers (under certain conditions) to **notify to national DPA** the automatic processing of personal data. ► ***Significant administrative burden is incurred by data controllers as a result of this obligation, particularly by data controllers processing personal data in more than one Member State, as they have to notify DPAs in all the MS they operate in.***	**Abolition of the existing system of obligations** of notification	- Significant simplification effects for **data controllers** processing personal data in more than one MS that will no longer be obliged to notify to data protection authorities in any MS ►***Significant reductions in administrative burden incurred by data controllers, estimated to €80 million per annum in Annex 9***
<u>Applicable law</u> Applicable law provisions are contained in Art 4 of Directive 95/46/EC ►***These provisions do not impose administrative burden, but they do create significant compliance costs***	**Clarification of the provisions** on applicable law, including the current determining criteria (if Directive – or EU Regulation) One law applicable to one controller	- **Improved legal certainty for data controllers** ►***No impact on administrative burden*** ►**Compliance costs will be reduced**
<u>Notification of data breaches</u> There is no obligation in Directive 95/46/EC to notify data breaches to data subjects. Currently this obligation is only found in the ePrivacy Directive (2009/138/EC).	Extension of the data breach notification to all sectors	- Enhanced legal clarity as to which areas this obligation covers ►***Increases in the administrative burden for data controllers, estimated at approximately €20 million in Annex 5.***
<u>Transborder data flows</u> Articles 25 and 26 of Directive 95/46/EC foresee an adequacy procedure for international transfers, which according to	Simplifying rules and procedures for transfers of personal data to third countries by giving the Commission exclusive competence for	- Simplified procedures for international transfers facilitate the flow of data to third countries.

stakeholders should be streamlined	adequacy decisions, extending the scope of BCRs to include data processors and introducing a clear definition of "groups of companies". Moreover, prior authorisations will be deleted in the large majority of cases.	►***Administrative burden linked with authorization for trans-border data flows will be reduced.***
<u>Data protection rules for police and judicial cooperation</u> **Framework Decision 2008/977/JHA:** ►***No administrative burden imposed by these provisions***	Eliminating the protection loopholes including as regards internal processing activies and improving the consistency of data protection rules in the area of police cooperation and judicial cooperation in criminal matters: While general rules and principles would be the same as those covering other areas already covered under the scope of Directive 95/46/EC, some specific rules would be foreseen to take account of the specificities of this area – in addition to the changes already foreseen under Policy Option 1	- **Enhanced legal clarity for Member States and data controllers** - **Clarifications of data subjects in** the area of police cooperation and judicial cooperation in criminal matters - More consistency would exist also as regards transfers to third countries, given the enhanced Commission's role in declaring adequacy. ►***No impact on administrative burden***
<u>Enforcement/Governance</u> Art. 28 of the Directive establishes national DPAs responsible for monitoring data protection in the Member States. Art 29 establishes an advisory body on data protection to the Commission ►**Significant compliance costs** for public authorities	Establishment of a **new mechanism of co-operation and co-ordination between national DPAs** An **enhanced role and more resources to Art 29 WP**	- **Increased efficiency and effectiveness** in the system of governance and on enforcement ►***May entail some additional administrative burden and compliance costs for public authorities***

8. MONITORING AND EVALUATION

This section describes the monitoring and evaluation that could be applied to assess the impact of the preferred option. The approach to monitoring and evaluation is outlined with respect to the three main problems that the preferred policy option will address.

The first evaluation will take place 3 years after the entry into force of the legal instruments. An explicit review clause, by which the Commission will evaluate implementation, will be included in the legal instruments. The Commission will subsequently report to the European Parliament and the Council on its evaluation. Further evaluations will have to take place every four years. The Commission methodology on evaluation will be applied. These evaluations will be conducted with the help of targeted studies on the implementation of the legal

instruments, questionnaires to national data protection authorities, expert discussions, workshops, Eurobarometers, and so forth.

The legal instrument will also explicitly provide that the evaluations will support the possibility for the Commission, to submit additional legislative or non-legislative proposals and/or implementing measures, if deemed necessary.

Table 6: Monitoring and evaluation

Problem	Monitoring indicators	Tools
1. Fragmentation, legal uncertainty and inconsistent enforcement	• Time and costs spent by data controllers complying with legislation in 'other Member States' • The level of harmonisation of national data protection rules • Human resources available to DPAs • Powers available to DPAs (including independence) • Levels of sanctions imposed • Use made of DPOs • Use made of DPIA	• Periodic surveys of data controllers • Analyses of complaints • Comparative implementation reports at EU-level. • Surveys of DPAs and/or descriptive analyses of information in annual reports • Surveys of data controllers of different types and in key sectors • Case studies of particular issues to identify successful enforcement mechanisms.
2. Difficulties for individuals to stay in control of their personal data	• The numbers of complaints received from data subjects and compensation received by data subjects • Indications of harm suffered by data subjects as a result of violations of data protection rights • The numbers of prosecutions of data controllers • The value of fines imposed on data controllers responsible for breaches of data protection. • The confidence of data subjects in putting personal data on line and benefitting from online services • Internet usage or to be monitored through surveys.	• Trend analysis, bearing in mind that new data should be collected • Assessments of harm suffered by data subjects. • Monitoring figures on complaints to DPAs through DPA's Annual Activity Reports.
3. Inconsistencies and gaps in the protection of personal data in the field of police and judicial cooperation in criminal matters and inconsistency of the rules	• Complaints received • Incidences of data subjects having their rights breached as a result of unlawful data processing (press reports etc) • Confidence of data subjects in law enforcement agencies • Descriptions of data protection practices in different MS	• Surveys of law enforcement agencies to assess the effectiveness of measures in the preferred option. • Surveys of data subjects • Case studies and peer reviews of aspects of law enforcement affected by measures in the preferred option

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/EC[121] 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

[121] 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.

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.

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/EC[122] 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/EC[123] 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 45/2001[124] 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

---

122 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.

123 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.

124 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.

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 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 authorities[125]. Several instruments exist with specific data protection regimes or with data protection clauses.

Since 2008 ***Council Framework Decision 2008/977/JHA***[126] 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 2001[127], 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

---

125 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.

126 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.

127 See below under 2.7

(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.

ANNEX 2

EVALUATION OF THE IMPLEMENTATION OF THE DATA PROTECTION DIRECTIVE

9. CONTEXT OF THE EVALUATION

The Commission's reports on the implementation of the Data Protection Directive 95/46/EC[128] found in 2003[129] and in 2007[130] 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 studies[131], of opinions of the

---

128 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).

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

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

131 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;

Article 29 Working Party,[132] and of a survey launched by the Commission in relation to certain aspects of the Directive, to which 22 Member States responded.

10. KEY PROVISIONS OF DIRECTIVE 95/46/EC

10.1. Definitions and concepts

10.1.1. 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 laws[133], 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.[134] 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

---

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.

[132] 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.

[133] 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 Directive[133] (e.g. France, Slovenia, Spain) or other minor amendments.

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

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, 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 France[135], Ireland[136]). ECJ case law on the confidentiality of electronic communications[137] 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

---

135 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.

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

137 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.

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.[138] 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"[139], clarifying, particularly, the elements of "any information", "relating to", and "natural person", and pointing to recital 26 of the Directive as an essential 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.

10.1.2. 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

---

138 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.

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

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"[140], 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.

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

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.

10.1.3. 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,[141]

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

employment[142], schools,[143] and the medical sector[144], 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 advertising[145], 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.

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

10.2.1. 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.[146]

---

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

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

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

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

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

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 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[147] - referring to the "correspondence and the holding of records of addresses"[148] – 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.[149]

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 networking[150]. 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

147 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.

148 Cf. recital 12 of the Directive.

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

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

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.

10.2.2. 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 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.[151] 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.[152]

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

---

151 ECJ, Case C-73/07, Satamedia , 16.12.2008.

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

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.

As regards the disclosure of information to the public or to third parties, the ECJ[153] 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.

10.3. The applicable law - Article 4

The Commission's first report on the implementation of the Data Protection Directive[154] 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.

---

153 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.

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

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 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 Party[155] - 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

[155] Opinion 1/2008, 4.8.2008 (WP 148).

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 opinion[156] 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.

10.4. 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 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.

---

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

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***[157], 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.

10.5. 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 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

[157] Opinion 3/2010, 13.7.2010 (WP 173).

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 ECJ[158] and the European Court of Human Rights[159] 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 legitimate[160].

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.

158 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.

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

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

10.6. 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[161], stated that there could be little, if anything, more private to the individual than the knowledge of his genetic make-up[162]. 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.

---

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

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

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 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.

10.7. 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.[163]

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-transparent[164] 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 data[165], 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

---

163 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.

164 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).

165 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).

identity theft[166]. The recent revision of the e-Privacy Directive[167] 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.

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.

10.8. 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

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

167 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.

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.[168]

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 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 environment[169].

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

---

168 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

169 See http://online.wsj.com/article/SB10001424052748703396604576087573944344348.html.

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 charge[170]. 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.

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

10.9.1. 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 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

[170] EB 2011.

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.

10.9.2. 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.[171] 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.

10.10.Remedies and Sanctions - Articles 22 and 24

10.10.1. 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

[171] 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).

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.

10.10.2. 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.

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

10.11.1. 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.[172] 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 Members 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

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

findings covering not all but only specific transfers of personal data to a particular third country.[173]

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 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.

10.11.2. 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 2010[174], 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

---

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

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

differently. In some Member States, the DPA still needs to authorise the transfer, whereas in other Member States such authorisation is not required.

10.11.3. 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.[175] 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***. 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 tool[176] and discouraged several other companies, potentially keen on using them[177]. 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

---

175 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.

176 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.

177 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.

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.

10.12.National Data Protection Authorities and enforcement - Article 28

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

The requirement of "***complete independence***" has been clarified in a recent ECJ ruling[178], 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). 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*

[178] C-518/07, *European Commission v. Germany*, 9.3.2010.

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.

10.12.2. 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.

10.12.3. 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.

10.12.4. 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,

DPAs 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.

10.12.5. 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.

10.12.6. 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 Data[179].

[179] ETS No. 108.

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.

10.13.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***[180] - 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 Party[181] – 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

[180] 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 .

[181] 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).

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".

11. 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

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

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

The general **Data Protection Directive 95/46/EC**[182] 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.[183] 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.[184] 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 matters[185].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)[186] and – for those Member States which have ratified it – to the Additional Protocol to that Convention (ETS 181)[187], as well as to the principles of the non-legally binding Recommendation No. R (87) 15

---

182 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).

183 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".

184 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).

185 See the list at the end of this annex.

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

187 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').

of the Council of Europe regulating the use of personal data in the police sector (Police Recommendation)[188], which sets out the principles of Convention 108 for the police sector.

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

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

Framework Decision 2008/977/JHA[189] had to be implemented by Member States by 27 November 2010 (Article 29(1)).[190] 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/JHA[191] 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).

---

188 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').

189 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').

190 See separate implementation report, COM(….).

191 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).

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.[192] As held by the ECJ in a number of cases[193], the rules on the protection of 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.[194]

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.[195] The

---

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

193 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.

194 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.

195 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.

European Parliament[196], the Conference of Data Protection Authorities[197], 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 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 retention[198]. The Framework Decision therefore fails to address this legal uncertainty.[199]

12.2.2. 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

---

196 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)).

197 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.

198 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).

199 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.

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 Aricle 126) or additionally to the Additional Protocol with the Police Recommendation (Prüm Decision Article 25).

12.2.3. 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 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.

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

12.3.1. 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**[200]**,** 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**[201]**,** 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**[202], 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 files[203], and on Europol's relations with partners, including the exchange of personal data and classified information[204];

- Amending Decision 2009/426/JHA to the Decision establishing **Eurojust**[205] 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**[206] also states that the Framework Decision applies to personal data exchange within its scope (recital 19 in the preamble);

---

200 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).

201 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).

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

203 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).

204 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).

205 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)

206 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).

- Decision 2009/917/JHA establishing the **Customs Information System (CIS)**[207], 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**[208] 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.

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.

12.3.2. 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':**

---

207 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).

208 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).

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.[209] The importance of such review is important both to ensure individuals' rights and for the efficient operation of police services.

---

[209] 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.

- **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")[210]. 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 (Article17 (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 Decision[211]

---

210 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 appliy, in particular, in France and Belgium.

211 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).

(Article 14) and the CIS Decision (Article 22). All these instruments require the right of 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 (Article17 (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) DPFD).

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 Norway[212] or the Agreement between the European Union and Iceland and Norway on the application of certain provisions of the Prüm Decision[213]. 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).

---

212 OJ L 292, 21.10.2006, p. 2.

213 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).

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.[214].

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.

13. 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).

13.1. Fundamental Rights Standards

13.1.1. 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*[215], concerning the lack of independence of the national supervisory authorities, and *Schecke et al.*[216] 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'.

---

214 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).

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

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

13.1.2. 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'.[217] In *M.S. v. Sweden*[218], 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'.

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 details[219]; the recording of fingerprinting, photography and other personal information by the police[220]even if the police register is secret[221]; the collection of medical data and the maintenance of medical records[222]; the compulsion by state authorities to reveal details of personal expenditure (and thus intimate details of private life)[223]; records relating to past criminal cases[224]; information relating to terrorist activity[225], collecting personal information in order to protect national security[226].

13.1.3. 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*".

---

217 See X and Y v Netherlands, judgement of 26 march 1985, para 23.
218 M.S. v Sweden, judgment of 27 August 1997.
219 Appl. No. 9072/82, X v. the United Kingdom, 6 Oct. 1982, 30 DR 229.
220 Murray v. the United Kingdom, judgment of 28 Oct. 1994, Series A no. 300-A.
221 Leander v. Sweden, judgment of 26 March 1987, Series A no. 116.
222 Appl. No. 14661/81, 9 July 1991, 71 DR 141.
223 Appl. No. 9804/82, 7 Dec. 1982, 31 DR 231.
224 Friedl v. Austria, Comm. Rep., 19 May 1994, p. 20.
225 McVeigh, O'Neill and Evans v. the United Kingdom, 18 March 1981, DR 24 p. 15.
226 Leander v. Sweden, judgment of 26 March 1987, para. 59.

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 question[227].

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*",[228] the grounds for that interference must be examined, which involves three cumulative conditions[229] that the interference or infringement must:

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

- 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"[230];

- rules involving negative consequences for individuals should be clear and precise and their application predictable for those subject to them[231];

- that the measure must be foreseeable, i.e. drawn up with sufficient precision to enable the individual to regulate his conduct"[232]. 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*"[233].

- 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".* [234]

---

227 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).

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

229 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.

230 See paragraph 52 of the aforementioned Rotaru judgment.

231 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.

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

233 See paragraph 99 of the aforementioned Marper judgment.

234 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)

(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*"[235]. 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".[236]

The objective pursued must in effect be reconciled with the fundamental rights set forth in Articles 7 and 8 of the Charter.[237] 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*".[238]

As they constitute exceptions to the fundamental rights, grounds for interference are "*to be interpreted narrowly*"[239] and "*must apply only in so far as is strictly necessary*"[240].

A limitation imposed on the rights in question, is justified only if it is "*proportionate to the legitimate aim pursued*"[241] 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"*.[242] 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*".[243]

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*".[244]

---

which overturned a decision authorising searches by electronic profiling, through cross-checking data in a number of databases.

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

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

237 See paragraph 76 of the aforementioned Schecke Judgment.

238 See paragraph 77 of the aforementioned Schecke Judgment.

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

240 See paragraph 77 of the aforementioned Schecke judgment.

241 See paragraph 71, Schecke judgment.

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

243 See paragraph 83 of the aforementioned Österreichischer Rundfunk judgment.

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

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 ECHR[245]. *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*"[246].

ECHR case law:

In Leander v Sweden[247], 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[248], 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[249], 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.

In S. and Marper v. United Kingdom[250] 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.

---

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

246 Marper judgment, paragraphs 119 and 125.

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

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

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

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

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 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

13.2. 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 receive[251].

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

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

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.[252]

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

[252] 288 out of the 305 responses are available on the website.

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).

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 strenghen self-regulation or self-enforcement. Indeed, a number of public authorities argued that the issue at hand is less the strenghening of rights but rather the proper application of the existing Directive. Other stakeholders, including business assocations, 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.

DPAs 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 treshhold, 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 occuring 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 strenghen 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 strenghening 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 negativelly 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 necessairly 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 thay 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 strenghtening 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 simply 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 pubic 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 defined 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 ilustrated 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

14. POLICY OPTION 1: SOFT ACTION

14.1.1. 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 cases[253]. 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 areas[254].

---

253 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).

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

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 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, shoulc 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 costs[255], 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;

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

- 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

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 matter[256] – 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

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

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.

14.1.2. 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

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 € 80M[257]. 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 shown[258], 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

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

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

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.

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.

14.1.3. 2. POLICY OPTION 2 - MODERNISED LEGAL FRAMEWORK

14.1.4. 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 powers[259], 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 States[260].

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.

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 system[261]. However, if the registration

---

259 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.

260 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).

261 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).

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"[262].

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 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

---

[262] See Advice Paper of WP29 on notifications, p.6.

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 lose, 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 that 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 s 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 ore 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 States 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)

14.1.5. 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 study[263] 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 extend 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 or 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 definition[264]. 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

263 Timelex study on case-law regarding IP addresses […]

264 [Examples to be added]

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 processing[265], 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 2011[266].

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'[267]) 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 consent[268].

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

---

[265] Art 29 opinion on Internet of /19992000

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

[267] For example, in the Greek version of the Directive and in EL national law.

[268]

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 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" case[269], 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.[270]

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

---

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

270 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 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.

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 date 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 a 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.

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 Institute[271] - 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.

14.1.6. 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.

---

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

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 more intrusive. The increased harmonisation of the conditions for access to one's own personal data, or i or the distinction to be made between various categories of data subjects (criminal suspects, victims, witnesses, etc.) would strenghten 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 lacking[272].

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.

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

14.1.8. 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

[272] See the Implementation report of the Framework Decision (COM…)…

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

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 processing[273].

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

---

273 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.

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
- 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.

14.1.9. 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 al 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 law[274].

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.[275]

Nonetheless, given that the Commission has conducted a wide public consultation on the issue of collective redress[276] 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.

14.1.10. 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 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.

---

[274] 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

[275] 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

[276] http://ec.europa.eu/justice/news/consulting_public/news_consulting_0054_en.htm

ANNEX 6

DETAILED ASSESSMENT OF IMPACTS OF THE INTRODUCTION OF

DATA PROTECTION OFFICERS (DPOS) AND DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

15.

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.

- ***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.[277]

	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***

[277] 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

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 assume 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:

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 DPIA[278]:

[278] 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.

- 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 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.

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.[279]

[279] 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.

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:

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.

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.[280]
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.

[280] As stated above, this labour rate is the EU figure for external consultations.

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.

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[281]

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.[282]
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.

[281] This figure also corresponds to stakeholder feedback for a large multi-national as to expected costs in conducting a privacy impact assessment.

[282] This labour rate is the EU figure for external consultations.

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.

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 provided 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

o 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 rules[283]. Other compliance costs imposed by existing legislation and the preferred option are beyond the scope of this analysis.

o 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**

[283] 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."

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.

- 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[284]	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[285], it can be assumed that approximately **42**% of the total number of companies can be *practically* considered as data	2010	Data Protection SME Panel	**8,821,638**

[284] 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

[285] SME Panel on data protection, Questions 7 (36% compliance) and 9 (48% compliance).

controllers within the meaning of the Directive. ***This is the approximate total number of enterprises/data controllers on which the administrative burden of the Directive is actually imposed***.			

- 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 2008[286] and 2010[287] 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	2008, 2011	2008 EUROSTAT figures	1,852,544

[286] Flash Eurobarometer 224 – Business attitudes towards cross-border sales and consumer protection, available at http://ec.europa.eu/consumers/strategy/docs/fl224%20_eurobar_cbs_summary.pdf (survey of managers of companies over 10 employees). This figure is extrapolated to companies of less than 10 employees.

[287] 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

engaged in cross-border trade		on enterprises in the EU, Flash EB 300.	
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)**			**926,272**

- 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 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 notification[288], 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)

[288] 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.

- 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.

(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 EU[289]; 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

[289] 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.

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).

ANNEX 10

IMPACTS OF THE PREFERRED OPTION ON COMPETITIVENESS

16. 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.

17. COST AND PRICE COMPETITIVENESS

17.1. 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.

17.2. 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.

17.3. 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*).

18. CAPACITY TO INNOVATE

18.1. 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.

18.2. 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.

18.3. 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.

19. INTERNATIONAL COMPETITIVENESS

19.1. 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.

19.2. 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.

19.3. Summary

19.3.1. 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 businesses function. In protection i cost to a lim
		Introducing demonstrate law is estim 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.	