EUROPEAN COMMISSION

Brussels, XXX
SEC(2012) 72/2

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

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.

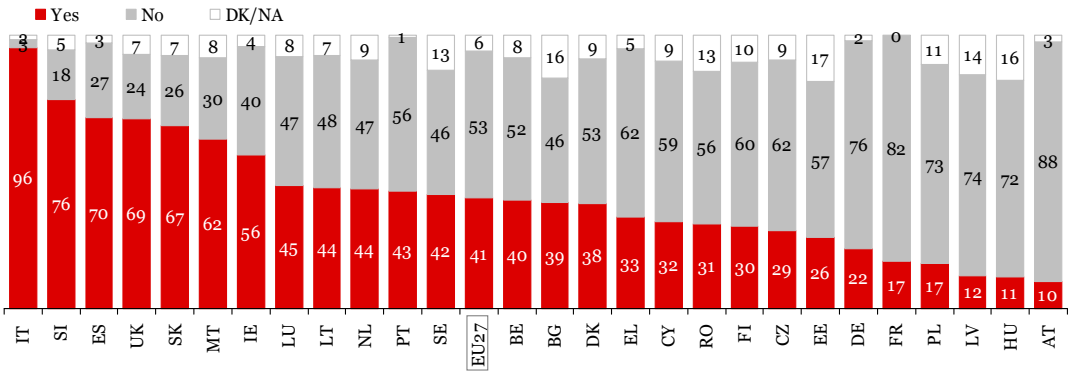
Two thirds of European citizens feel that the disclosure of personal data is a major concern for them and six in ten citizens consider that nowadays there is no alternative to disclosing personal data in order to obtain products and services[58]. Three quarters of citizens feel that they have either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

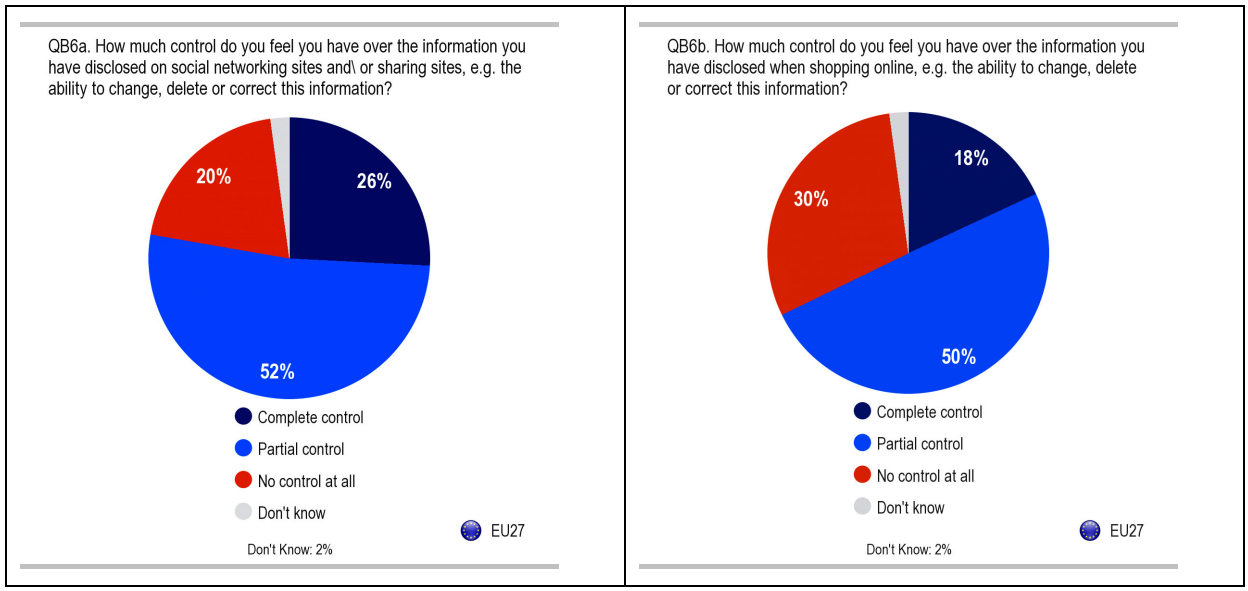
say they do not read them (25%), one in twenty say they do not know where to find them (5%) and almost one in ten ignore privacy statements (8%).[63]

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.

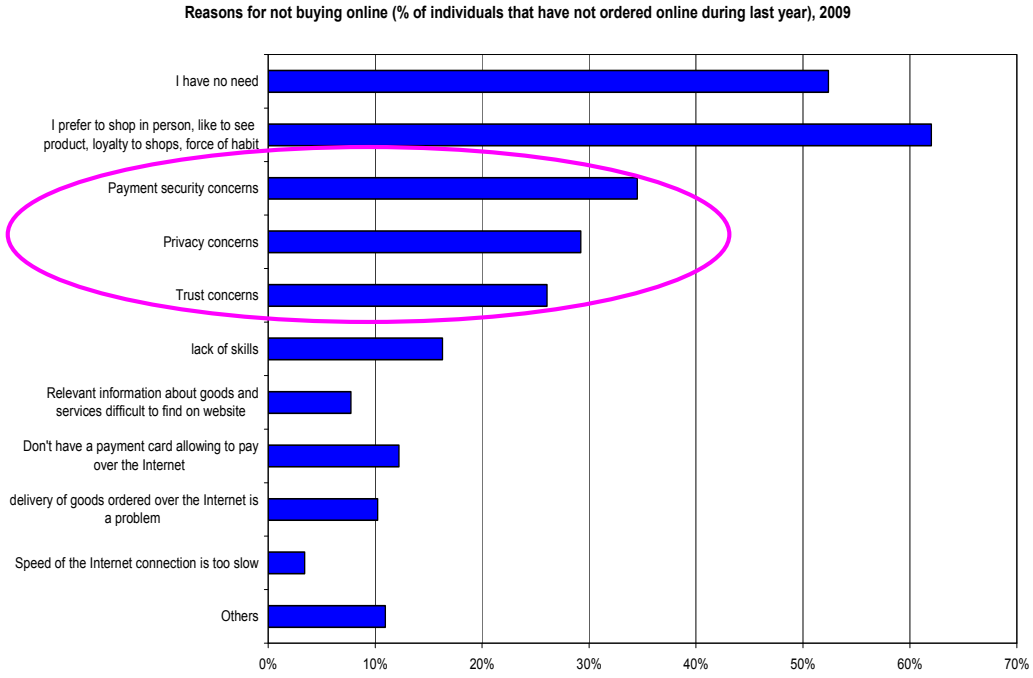
Individuals react on the increase of data breaches with raising concern. The percentage of individuals that would want to be informed when their personal data is lost, stolen or altered in any way is constantly increasing and has reached the level of 88% EU wide[75]**.** At present, EU wide harmonised 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