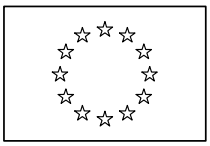

EUROPEAN COMMISSION

Brussels, 04.11.2010
COM(2010) 609/3

DRAFT VERSION

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

A comprehensive approach on personal data protection in the European Union

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

'A comprehensive approach on personal data protection in the European Union'

1. NEW CHALLENGES FOR THE PROTECTION OF PERSONAL DATA

The 1995 Data Protection Directive[1] set a milestone in the history of the protection of personal data in the European Union. The Directive enshrines two of the oldest and equally important ambitions of the European integration process: the protection of fundamental rights and freedoms of individuals and in particular the fundamental right to data protection, on the one hand, and the achievement of the internal market – the free flow of personal data in this case – on the other.

Fifteen years later, this twofold objective is still valid and the principles enshrined in the Directive remain sound. **However, rapid technological developments and globalisation have profoundly changed the world around us, and brought new challenges for the protection of personal data.**

Today technology allows individuals to share information about their behaviour and preferences easily and make it publicly and globally available on an unprecedented scale. Social networking sites, with hundreds of millions of members spread across the globe, are perhaps the most obvious, but not the only, example of this phenomenon. 'Cloud computing' - i.e., Internet-based computing whereby software, shared resources and information are on remote servers ('in the cloud') could also pose challenges to data protection, as it may involve the loss of individuals' control over their potentially sensitive information when they store their data with programs hosted on someone else's hardware. A recent study confirmed that there seems to be a convergence of views – of Data Protection Authorities, business associations and consumers' organisations – that risks to privacy and the protection of personal data associated with online activity are increasing[2].

At the same time, **ways of collecting personal data have become increasingly elaborated and less easily detectable.** For example, the use of sophisticated tools allows economic operators to better target individuals thanks to the monitoring of their behaviour. And the growing use of procedures allowing automatic data collection, such as electronic transport ticketing, road toll collecting, or of geo-location devices make it easier to determine the location of individuals simply because they use a mobile device. Public authorities also use more and more personal data for various purposes, such as tracing individuals in the event of an outbreak of a communicable disease, for preventing and fighting terrorism and crime more

---

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

2 See the *Study on the economic benefits of privacy enhancing technologies,* London Economics, July 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), p. 14.

effectively, to administer social security schemes or for taxation purposes, as part of their e-government applications etc.

All this inevitably raises the question whether existing EU data protection legislation can still fully and effectively cope with these challenges.

To address this question, the Commission launched a review of the current legal framework, with a high level conference in May 2009, followed by a public consultation until the end of 2009.[3] A number of studies were also launched.[4]

The findings confirmed that the core principles of the Directive are still valid and that its technologically neutral character should be preserved. However, several issues were identified as being problematic and posing specific challenges. These include:

- *Addressing the impact of new technologies*

Responses to the consultations, both from private individuals and organisations, have confirmed the need to clarify and specify the application of data protection principles to new technologies, in order to ensure that individuals' personal data are actually effectively protected, whatever the technology used to process their data, and that data controllers are fully aware of the implications of new technologies on data protection. This has been partially addressed by Directive 2002/58/EC (the so-called 'e-Privacy' Directive)[5], which particularises and complements the general Data Protection Directive in the electronic communications sector[6].

- *Enhancing the internal market dimension of data protection*

One of the main recurrent concerns of stakeholders, particularly multinational companies, is the lack of sufficient harmonisation between Member States' legislation on data protection, in spite of a common EU legal framework. They stressed the need to increase legal certainty,

---

3 See the replies to the Commission's public consultation: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. More targeted stakeholders' consultations were carried out throughout 2010. Vice-President Viviane Reding also chaired a high level meeting with stakeholders on 5 October 2010 in Brussels. The Commission also consulted the Article 29 Working Party, which provided a comprehensive contribution to the 2009 consultation (WP 168) and adopted a specific opinion in July 2010 on the accountability concept (WP 173).

4 In addition to the *Study on the economic benefits of privacy enhancing technologies* (cit., footnote 2), see also the *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments,* January 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). A study for an impact assessment for the future EU legal framework for personal data protection is also ongoing.

5 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), (OJ L 201, 31.7.2002, p. 37).

6 The Data Protection Directive 95/46/EC sets the data protection standards for all EU legislative acts, including the e-Privacy Directive 2002/58/EC (amended by Directive 2009/136/EC - OJ L 337, 18.12.2009, p. 11). The e-Privacy Directive applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks. It translated the principles set out in the Data Protection Directive into specific rules for the electronic communications sector. Directive 95/46/EC applies *inter alia* to non-public communication services.

lessen the administrative burden and ensure a level playing field for economic operators and other data controllers.

- *Addressing globalisation and improving international data transfers*

Several stakeholders highlighted that the increased outsourcing of processing, very often outside the EU, raises several problems in relation to the law applicable to the processing and the allocation of associated responsibility. As to international data transfers, many organisations considered that the current schemes are not entirely satisfactory and need to be reviewed and streamlined so as to make transfers simpler and less burdensome.

- *Providing a stronger institutional arrangement for the effective enforcement of data protection rules*

There is consensus among stakeholders that the role of Data Protection Authorities needs to be strengthened so as to ensure better enforcement of data protection rules. Some organisations also asked for increased transparency in the work of the Article 29 Working Party (*see 2.5. below*) and clarification of its tasks and powers.

- *Improving the coherence of the data protection legal framework*

In the public consultation, all stakeholders stressed the need for an overarching instrument applying to data processing operations in all sectors and policies of the Union, ensuring an integrated approach as well as seamless, consistent and effective protection.[7]

The above challenges **require the EU to develop a comprehensive and coherent approach** guaranteeing that **the fundamental right to data protection for individuals is fully respected within the EU and beyond**. The Lisbon Treaty provided the EU with additional means to achieve this: the EU Charter of Fundamental Rights - with Article 8 recognising an autonomous right to the protection of personal data - has become legally binding, and a new legal basis has been introduced[8] allowing for the establishment of comprehensive and coherent Union legislation on the protection of individuals with regard to the processing of their personal data and on the free movement of such data. In particular, the new legal basis allows the EU to have a single legal instrument for regulating data protection, including the areas of police cooperation and judicial cooperation in criminal matters. The area of Common Foreign and Security Policy is only partly covered by Article 16 TFEU, as specific rules for data processing by Member States must be laid down by a Council Decision based on a different legal basis[9].

Building on these new legal possibilities, the Commission will give the highest priority to ensuring respect for the fundamental right to data protection throughout the Union and all its policies, while at the same time enhancing the internal market dimension and facilitating the free flow of personal data. In this context, other relevant fundamental rights enshrined in the Charter, and other objectives in the Treaties, have to be fully taken into account while ensuring the fundamental right to the protection of personal data.

---

7 In separate contributions made after the end of the public consultation, Europol and Eurojust pleaded for nevertheless taking into account the specificities of their work regarding the coordination of law enforcement and crime prevention.

8 See Article 16 of the Treaty on the Functioning of the European Union (TFEU).

9 See Article 16(2), last paragraph, TFEU and Article 39 of the Treaty on the European Union (TEU).

This Communication intends to lay down the Commission's approach for modernising the EU legal system for the protection of personal data in all areas of the Union's activities, taking account, in particular, of the challenges resulting from globalisation and new technologies, so as to continue to guarantee a high level of protection of individuals with regard to the processing of personal data in all areas of the Union's activities. This will allow the EU to remain a driving force in promoting high data protection standards worldwide.

2. KEY OBJECTIVES OF THE COMPREHENSIVE APPROACH ON DATA PROTECTION

2.1. Strengthening individuals' rights

2.1.1. Ensuring appropriate protection for individuals in all circumstances

The objective of the rules in the current EU data protection instruments is **to protect the fundamental rights of natural persons and in particular their right to protection of personal data**, in line with the EU Charter of Fundamental Rights[10].

The concept of 'personal data' is one of the key concepts for the protection of individuals by the current EU data protection instruments and triggers the application of the obligations incumbent upon data controllers and data processors[11]. The definition of 'personal data' aims at covering all information relating to an identified or identifiable person, either directly or indirectly. To determine whether a person is identifiable, account should be taken of 'all the means likely reasonably to be used either by the controller or by any other person to identify the said person'[12]. This deliberate approach chosen by the legislator has the benefit of flexibility, allowing it to be applied to various situations and developments affecting fundamental rights, including those not foreseeable when the Directive was adopted. However, a consequence of such a broad and flexible approach is that there are numerous cases where it is not always clear, when implementing the Directive, which approach to take, whether individuals enjoy data protection rights and whether data controllers should comply with the obligations imposed by the Directive[13].

There are situations which involve the processing of specific information which would require additional measures under Union law. Such measures already exist in some cases. For example, storing of information in terminal equipment (e.g. mobile phones) is only allowed on condition that the individual has given his or her consent. This may also need to be addressed at EU level as regards e.g. key-coded data, location data, 'data mining' technologies allowing the combination of data from different sources, or cases where the confidentiality and integrity in information-technology systems[14] must be ensured.

---

10 See European Court of Justice, Cases C-101/01, 'Bodil Lindqvist', ECR [2003], I-1297, 96, 97, and C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, ECR [2008] I-271. See also the jurisprudence of the European Court of Human Rights, e.g. in cases: S. and Marper v. the United Kingdom, 4.12. 2008 (Application nos. 30562/04 and 30566/04) and Rotaru v. Romania, 4.5. 2000; no. 28341/95, § 55, ECHR 2000-V.

11 See the definitions of 'data controller' and 'data processor' in Article 2(d) and (e) of Directive 95/46/EC.

12 See Recital 26 of Directive 95/46/EC.

13 See for example the case of IP addresses, examined in the Article 29 Working Party Opinion 4/2007 on the concept of personal data (WP 136).

14 See for instance the judgement by the German Federal Constitutional Court (*Bundesverfassungsgericht*) of 27 February 2008, 1 BvR 370/07.

All the above issues therefore require careful examination.

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

2.1.2. Increasing transparency for data subjects

Transparency is a fundamental condition for enabling individuals to exercise control over their own data and to ensure effective protection of personal data. It is therefore essential that individuals are **well and clearly informed, in a transparent way**, by data controllers about how and by whom their data are collected and processed, for what reasons, for how long and what their rights are if they want to access, rectify or delete their data. The relevant provisions on the information to be given to the data subject[15] are not sufficient.

Basic elements of transparency are the requirements that the **information must be easily accessible and easy to understand, and that clear and plain language is used**. This is particularly relevant in the online environment, where quite often privacy notices are unclear, difficult to access, non-transparent[16] and not always in full compliance with existing rules. A case where this might be so is online behavioural advertising, where both the proliferation of actors involved in the provision of behavioural advertising and the technological complexity of the practice make it difficult for an individual to know and understand if personal data are being collected, by whom, and for what purpose.

In this context, **children** deserve specific protection, as they may be less aware of risks, consequences, safeguards and rights in relation to the processing of personal data[17].

The Commission will consider:

- introducing a **general principle of transparent processing** of personal data in the legal framework;

- introducing **specific obligations** for data controllers on the type of information to be provided and on the **modalities** for providing it, including in relation to **children**;

- drawing up one or more **EU standard forms** (‘**privacy information notices**’) to be used by data controllers.

It is also important for individuals to be informed when their data are accidentally or unlawfully destroyed, lost, altered, accessed by or disclosed to unauthorised persons. The recent revision of the e-Privacy Directive introduced a **mandatory personal data breach notification** covering, however, only the telecommunications sector. Given that risks of data breaches also exist in other sectors (e.g. the financial sector), the Commission will examine

15 See Articles 10 and 11 of Directive 95/46/EC.

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

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

the modalities for extending the obligation to notify personal data breaches to other sectors in line with the Commission declaration on data breach notification made before the European Parliament in 2009 in the context of the reform of the Regulatory Framework for Electronic Communications[18]. This examination will not affect the provisions of the e-Privacy Directive, which must be transposed into national laws by 25 May 2011[19]. A consistent and coherent approach on this matter will have to be ensured.

The Commission will:

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

2.1.3. Enhancing control over one's own data

Two important preconditions for ensuring that individuals enjoy a high level of data protection are **the limitation of the data controllers' processing in relation to its purposes (principle of data minimisation)** and the retention by data subjects of an **effective control over their own data**. Article 8(2) of the Charter states that 'everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'. Individuals should always be able to access, rectify, delete or block their data, unless there are legitimate reasons, provided by law, for preventing this. These rights already exist in the current legal framework. However, the way in which these rights can be exercised is not harmonised, and therefore exercising them is actually easier in some Member States than in others. Moreover, this has become particularly challenging in the online environment, where data are often retained without the person concerned being informed and/or having given his or her agreement to it.

The example of online social networking is particularly relevant here, as it presents significant challenges to the individual's effective control over his/her personal data. The Commission has received various queries from individuals who have not always been able to retrieve personal data from online service providers, such as their pictures, and who have therefore been impeded in exercising their rights of access, rectification and deletion.

Such rights should therefore be made more explicit, clarified and possibly strengthened.

The Commission will therefore examine ways of:

- strengthening the **principle of data minimisation**;

- **improving the modalities** for the actual **exercise of the rights of access, rectification, erasure or blocking of data** (e.g., by introducing deadlines for responding to individuals'

[18] 'The Commission takes note of the will of the European Parliament that an obligation to notify personal data breaches should not be limited to the electronic communications sector but also apply to entities such as providers of information society services […]. The Commission will, therefore, without delay initiate the appropriate preparatory work, including consultation with stakeholders, with a view to presenting proposals in this area, as appropriate, by the end of 2011 […]', retrievable at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//EN. See also recital 59 of Directive 2009/136/EC amending the e-Privacy Directive 2002/58/EC: 'The interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority.'

[19] Article 4 of Directive 2009/136/EC.

requests, by allowing the exercise of rights by electronic means or by providing that right of access should be ensured free of charge as a principle);

- clarifying the so-called '**right to be forgotten**', i.e. the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. This is the case, for example, when processing is based on the person's consent and when he or she withdraws consent or when the storage period has expired;

- complementing the rights of data subjects by ensuring '**data portability'**, i.e., providing the explicit right for an individual to withdraw his/her own data (e.g., his/her photos or a list of friends) from an application or service so that the withdrawn data can be transferred into another application or service, as far as technically feasible, without hindrance from the data controllers.

2.1.4. Raising awareness

While transparency is essential, there is also a need to make the general public, and particularly young people, more aware of the risks related to the processing of personal data and of their rights. A Eurobarometer survey in 2008 showed that a large majority of people in EU Member States consider that awareness of personal data protection in their own country is low[20]. Awareness raising activities should thus be encouraged and promoted by a broad range of actors, i.e. Member State authorities, particularly Data Protection Authorities and educational bodies, as well as data controllers and civil society associations. They should include non-legislative measures such as awareness campaigns in the print and electronic media, and the provision of clear information on web-sites, clearly spelling out data subjects' rights and data controllers' responsibilities.

The Commission will explore:

- the possibility for **co-financing awareness-raising activities on data protection** via the Union budget;

- the need for and the opportunity of including in the legal framework **an obligation to carry out awareness-raising activities** in this area.

2.1.5. Ensuring informed and free consent

When informed consent is required, the current rules provide that the individual's consent for processing his or her personal data should be a 'freely given specific and informed indication' of his or her wishes by which the individual signifies his or her agreement to this data processing[21]. However, these conditions are currently interpreted differently in Member States, ranging from a general requirement of written consent to the acceptance of implicit consent.

Moreover, in the online environment – given the opacity of privacy policies – it is often more difficult for individuals to be aware of their rights and give informed consent. This is even more complicated by the fact that, in some cases, it is not even clear what would constitute freely given, specific and informed consent to data processing, such as in the case of

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

[21] Cf. Article 2(h) of Directive 95/46/EC.

behavioural advertising, where internet browser settings are considered by some, but not by others, to deliver the user's consent.

Clarification concerning the conditions for the data subject's consent should therefore be provided, in order to always guarantee informed consent and ensure that the individual is fully aware that he or she is consenting, and to what data processing, in line with Article 8 of the EU Charter of Fundamental Rights. Clarity on key concepts can also favour the development of self-regulatory initiatives to develop practical solutions consistent with EU law.

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

2.1.6. Protecting sensitive data

The processing of sensitive data, i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life, is currently already prohibited as a general rule, with limited exceptions under certain conditions and safeguards[22]. However, in the light of technological and other societal developments, there is a need to reconsider the existing provisions on sensitive data, to examine whether other categories of data should be added and to further clarify the conditions for their processing. This concerns, for example, genetic data which is currently not explicitly mentioned as a sensitive category of data.

The Commission will consider:

- whether other categories of data should be considered as **'sensitive data'**, for example **genetic** data;

- further clarifying and **harmonising the conditions** allowing for the processing of categories of sensitive data.

2.1.7. Making remedies and sanctions more effective

In order to ensure the enforcement of data protection rules, it is essential to have **effective provisions on remedies and sanctions**. Many cases where an individual is affected by an infringement of data protection rules also affect a considerable number of other individuals in a similar situation.

The Commission will therefore:

- consider the possibility of **extending the power to bring an action before the national courts** to data protection authorities and to civil society associations, as well as to **other associations representing data subjects' interests**;

- assess the need for **strengthening the existing provisions on sanctions**, for example by explicitly including criminal sanctions in case of serious data protection violations, in order to make them more effective.

[22] Cf. Article 8 of Directive 95/46/EC.

2.2. Enhancing the internal market dimension

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

Data Protection in the EU has **a strong internal market dimension**, i.e., the need to ensure the free flow of personal data between Member States within the internal market. As a consequence, the Directive's harmonisation of national data protection laws is not limited to minimal harmonisation but amounts to harmonisation that is generally complete[23].

At the same time, the Directive gives the Member States room for manoeuvre in certain areas and authorises them to maintain or introduce particular rules for specific situations[24]. This, together with the fact that the Directive has sometimes been incorrectly implemented by Member States, has led to **divergences between the national laws implementing the Directive, which run counter to one of its main objectives, i.e. ensuring the free flow of personal data within the internal market**. This is true for a large number of sectors and contexts, e.g. when processing personal data in the employment context or for public health purposes. The lack of harmonisation is indeed one of the recurring and main problems raised by private stakeholders, especially economic operators, as it is an additional cost and administrative burden for them. This is particularly the case for data controllers established in several Member States and obliged to comply with the requirements and practices in each of these countries. Moreover, the divergence in the implementation of the Directive by Member States creates legal uncertainty not only for data controllers but also for data subjects, creating the risk of distorting the equivalent level of protection that the Directive is supposed to achieve and ensure.

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

2.2.2. Reducing the administrative burden

Providing a level-playing field will reduce the need to meet diverging national requirements and will thus considerably reduce the administrative burden for controllers. A further concrete element for lessening the administrative burden and reducing costs for data controllers would be the **revision and simplification of the current notification system**[25]. There is general consensus amongst data controllers that the current general obligation to notify all data processing operations to the Data Protection Authorities is a rather cumbersome obligation which does not provide, in itself, any real added value for the protection of individuals' personal data. Moreover, this is one of the cases where the Directive leaves a certain room for manoeuvre to Member States, which are free to decide about possible exemptions and simplifications, as well as the procedures to be followed.

A harmonised and simplified system would reduce costs as well as the administrative burden, especially for multinational companies established in several Member States.

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

---

23 European Court of Justice, C-101/01, 'Bodil Lindqvist', ECR [2003], I-1297, 96, 97.

24 *Ibidem*, 97. See also recital 9 of Directive 95/46/EC.

25 See Article 18 of Directive 95/46/EC.

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

The Commission's first report on the implementation of the Data Protection Directive as early as in 2003[26] highlighted the fact that the provisions on applicable law[27] were 'deficient in several cases, with the result that the kind of conflicts of law this Article seeks to avoid could arise'. The situation has not improved since then, as a result of which it is not always clear to data controllers and data protection supervisory authorities which Member State is responsible and which law is applicable when several Member States are concerned. This is particularly the case when a data controller is subject to different requirements from different Member States, when a multinational enterprise is established in more than one Member States or when the data controller is not established in the EU but provides its services to EU residents.

Complexity is also growing due to globalisation and technological developments: data controllers are increasingly operating in several Member States and jurisdictions, providing services and assistance around the clock. The Internet makes it much easier for data controllers established outside the European Economic Area (EEA)[28] to provide services from a distance and to process personal data in the online environment; and it is often difficult to determine the location of personal data and of equipment used at any given time (e.g., in 'cloud computing' applications and services).

However, the Commission considers that the fact that the processing of personal data is carried out by a data controller established in a third country should not deprive individuals of the protection to which they are entitled under the EU Charter of Fundamental Rights and EU data protection legislation.

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

2.2.4. Enhancing data controllers' responsibility

Administrative simplification should **not lead to an overall reduction of the data controllers' responsibility in ensuring effective data protection**. On the contrary, the Commission believes that their obligations should be more clearly spelt out in the legal framework, including in relation to internal control mechanisms and cooperation with Data Protection Supervisory Authorities. In addition, it should be ensured that such responsibility applies also to controllers who are subject to professional secrecy obligations (e.g. lawyers) as well as in those increasingly common cases where data controllers delegate data processing to other entities (e.g. processors).

The Commission will therefore explore ways of **ensuring that data controllers put in place effective policies and mechanisms to ensure compliance with data protection rules**. In doing so, it will take account of the current debate on the possible introduction of an

---

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

[27] See Article 4 of Directive 95/46/EC.

[28] The European Economic Area includes Norway, Liechtenstein and Iceland.

'accountability' principle[29]. This would not aim to increase the administrative burden on data controllers, since such measures would rather focus on establishing safeguards and mechanisms which make data protection compliance more effective while at the same time reducing and simplifying certain administrative formalities, such as notifications (*see 2.2.2 above*).

Promoting the use of Privacy Enhancing Technologies (PETs), as already pointed out in the 2007 Commission Communication on the issue, as well as of the 'Privacy by Design' principle could play an important role in this respect, including in ensuring data security[30].

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

- making the appointment of an independent **Data Protection Officer** mandatory and harmonising the rules related to their tasks and competences[31], while reflecting on the appropriate threshold to avoid undue administrative burdens, particularly on small and micro-enterprises;
- including in the legal framework an obligation for data controllers to carry out a **data protection impact assessment** in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance;
- further promoting the use of PETs and the possibilities for the concrete implementation of the concept of **'Privacy by Design'**.

2.2.5. Encouraging self-regulatory initiatives and exploring EU certification schemes

The Commission continues to consider that **self-regulatory initiatives** by data controllers can **contribute to a better enforcement of data protection rules**. The current provisions on self-regulation in the Data Protection Directive, namely the scope for drawing up Codes of Conduct[32], have rarely been used so far and are not considered satisfactory by private stakeholders.

Furthermore, the Commission will explore the possible creation of EU **certification schemes (e.g. 'privacy seals')** for 'privacy-compliant' processes, technologies, products and services[33]. This would not only give an orientation to the individual as a user of such technologies, products and services, but would also be relevant in relation to the responsibility of data controllers: opting for certified technologies, products or services could help to prove that the

---

29 See in particular the opinion adopted by the Article 29 Working Party on 13 July, 3/2010.

30 On PETs see: Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technology (PETs) - COM(2007) 228. The principle of 'Privacy by Design' means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal. This principle features inter alia in the Commission Communication on 'A Digital Agenda for Europe' - COM(2010) 245.

31 The current possibility for a data controller to appoint a Data Protection Officer in order to ensure, in an independent manner, compliance with the EU and national data protection rules and to assist individuals has been implemented in several Member States already (see e.g. the *Beauftragter für den Datenschutz* in Germany and the *correspondant informatique et libertés (CIL)* in France).

32 See Article 27 of Directive 95/46/EC.

33 On this aspect, see also the PETs Communication, cit. footnote 30.

controller has fulfilled its obligations (*see 2.2.4 above*). Of course, it would be essential to **ensure the trustworthiness of such privacy seals** and to see how they fit in with the legal obligations and international technical standards.

The Commission will:

- examine means of **further encouraging self-regulatory initiatives**, including the active promotion of Codes of Conduct;

- explore the feasibility of establishing **EU certification schemes** in the field of privacy and data protection.

2.3. Revising the data protection rules in the area of police and judicial cooperation in criminal matters

The Data Protection Directive applies to all personal data processing activities in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law', such as activities in the areas of police and judicial cooperation in criminal matters.[34] The Lisbon Treaty has however abolished the previous 'pillar structure' of the EU and introduced a new and comprehensive legal basis for the protection of personal data across Union policies.[35] Against this background, and in view of the EU Charter of Fundamental Rights, the Commission Communications on the Stockholm Programme and the Stockholm Action Plan[36] highlighted the need to have a 'comprehensive protection scheme' and to 'strengthen the EU's stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention'.

The EU instrument for the protection of personal data in the areas of police and judicial cooperation in criminal matters is **Framework Decision 2008/977/JHA**[37]. The Framework Decision is an important step forward in a field where common standards for data protection were very much needed. However, further work needs to be done.

The Framework Decision only applies to the cross-border exchange of personal data within the EU and not to domestic processing operations in the Member States. This distinction is difficult to make in practice and can complicate the actual implementation and application of the Framework Decision.[38]

Also, **the Framework Decision contains too wide an exception to the purpose limitation principle**. Another shortcoming is the lack of provisions that different categories of data should be distinguished in accordance with their degree of accuracy and reliability, that data

---

34 See Article 3(2), first indent, of Directive 95/46/EC.

35 See Article 16 TFEU.

36 See COM(2009) 262, 10.6.2009, and COM(2010) 171, 20.4.2010.

37 Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60). The Framework Decision only envisages minimum harmonisation of data protection standards.

38 This distinction does not exist in the relevant Council of Europe instruments such as: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No.: 108), its Additional Protocol regarding supervisory authorities and transborder data flows (ETS No.: 181) and Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, adopted on 17 September 1987.

based on facts should be distinguished from data based on opinions or personal assessments[39], and that a distinction should be made between different categories of data subjects (criminals, suspects, victims, witnesses, etc.), with specific guarantees laid down for data relating to non-suspects[40].

In addition **the Framework Decision does not replace the various sector-specific legislative instruments for police and judicial co-operation in criminal matters adopted at EU level**[41], in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS)[42], which either contain particular data protection regimes, and/or which usually refer to the data protection instruments of the Council of Europe. For activities within the area of police and judicial cooperation all Member States have subscribed to the Council of Europe Recommendation No R (87) 15, which sets out the principles of Convention 108 for the police sector. This is not, however, a legally binding instrument.

This situation may directly affect the possibilities for individuals to exercise their data protection rights in this area (e.g. to know what personal data are processed and exchanged about them, by whom and for what purpose, and on how to exercise their rights, such as the right to access their data).

The objective of establishing a comprehensive and coherent system in the EU and vis-à-vis third countries entails **the need to consider a revision of the current rules on data protection in the area of police cooperation and judicial cooperation in criminal matters.** The Commission stresses that the notion of a comprehensive data protection scheme does not exclude specific rules for data protection for the police and the judicial sector within the general framework, taking due account of the specific nature of these fields, as indicated by Declaration 21 attached to the Lisbon Treaty. This implies, for example, a need to consider the extent to which the exercise of certain data protection rights by an individual would jeopardise the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in a specific case.

The Commission will, in particular:

- consider the **extension of the application of the general data protection rules to the areas of police and judicial cooperation in criminal matters**, including for processing at domestic level while providing, where necessary, for harmonised **limitations** to certain data protection rights of individuals, e.g., concerning the right of access or to the principle of transparency;

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

---

39 As required by Principle 3.2 of Recommendation No R (87) 15.

40 Contrary to Principle 2 of Recommendation No R (87) 15 and its evaluation reports.

41 See an overview of such instruments in the Commission Communication 'Overview of information management in the area of freedom, security and justice' - COM(2010) 385.

42 Joint Supervisory Authorities have been set up by the relevant instruments to ensure data protection supervision, in addition to the general supervisory powers of the European Data Protection Supervisor (EDPS) over Union institutions, bodies, offices and agencies based on Regulation (EC) No 45/2001.

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

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

2.4. The global dimension of data protection

2.4.1. Clarifying and simplifying the rules for international data transfers

One of the means of enabling the transfer of personal data outside the EU and the EEA area is the so-called **'adequacy assessment'**. Currently, the adequacy of a third country – i.e., whether a third country ensures a level of protection that the EU considers as adequate – may be determined by the Commission and by Member States.

The effect of a Commission adequacy finding is that personal data can freely flow from the 27 EU Member States and the three EEA member countries to that third country without any further safeguard being necessary. However, the exact requirements for recognition of adequacy by the Commission are currently not specified in satisfactory detail in the Data Protection Directive. In addition, the Framework Decision does not provide for such a decision by the Commission.

In some Member States adequacy is assessed in the first instance by the data controller which itself transfers personal data to a third country, sometimes under the ex-post supervision of the data protection supervisory authority. This situation may lead to different approaches to assessing the level of adequacy of third countries, or international organisations, and **involves the risk that the level of protection of data subjects provided for in a third country is judged differently from one Member State to another**. Also, the current legal instruments include no detailed, harmonised requirements as to which transfers can be considered lawful. This leads to practices which vary from Member State to Member State.

In addition, as regards data transfers to third countries which do not ensure an adequate level of protection, the current Commission standard clauses for the transfer of personal data to controllers[43] and to processors[44] are not designed for non-contractual situations and, for example, cannot be used for transfers between public administrations.

Moreover, international agreements concluded by the EU or its Member States often require the inclusion of data protection principles and specific provisions. This may result in varying texts with inconsistent provisions and rights, and thus open to divergent interpretations, to the

---

[43] Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under the Directive 95/46/EC (OJ L 181, 4.7.2001, p. 19); Commission Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC (OJ L 6, 10.1.2002, p. 52); Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (OJ L 385, 29.12.2004, p. 74).

[44] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010, p. 5).

detriment of the data subject. As a consequence, the Commission announced that it would work on core elements for personal data protection in agreements between the Union and third countries for law enforcement purposes[45].

Other means that have been developed as a form of self-regulation, such as internal company codes of conduct known as 'Binding Corporate Rules' (BCRs)[46], can also be a useful tool to lawfully transfer personal data between companies of the same corporate group. However, stakeholders have suggested that this mechanism could be further improved and its implementation eased.

To address the issues identified there is a **general need to improve the current mechanisms allowing for international transfers of personal data**, while at the same time ensuring that personal data are adequately protected when transferred and processed outside the EU and the EEA.

The Commission intends to examine how:

- to **improve and streamline the current procedures** for international data transfers, including legally binding instruments and 'Binding Corporate Rules' in order to ensure a **more uniform and coherent EU approach** vis-à-vis third countries and international organisations;

- to **clarify the Commission's adequacy procedure** and better specify the **criteria and requirements** for assessing the level of data protection in a third country or an international organisation;

- to define **core EU data protection elements**, which could be used for all types of international agreements.

2.4.2. Promoting universal principles

Data processing is globalised and calls for the development of universal principles for the protection of individuals with regard to the processing of personal data.

The EU legal framework for data protection has often served as a **benchmark for third countries when regulating data protection**. Its effect and impact, within and outside the Union, have been of the utmost importance. The **European Union must therefore remain a driving force behind the development and promotion of international legal and technical standards for the protection of personal data**, based on relevant EU and other European instruments on data protection. This is particularly important in the framework of the EU's enlargement policy.

As regards international technical standards developed by standardisation organisations, the Commission believes that coherence between the future legal framework and such standards is very important to ensure a consistent and practical implementation of data protection rules by data controllers.

---

45 Stockholm Action Plan, cit. (footnote 36).

46 'Binding Corporate Rules' are codes of practice based on European data protection standards, 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. See: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

The Commission will:

- continue to **promote the development of high legal and technical standards of data protection** in third countries and at international level;

- strive for the **principle of reciprocity of protection** in the international actions of the Union and in particular regarding the data subjects whose data are exported from the EU to third countries;

- **enhance its cooperation, to this end, with third countries and international organisations**, such as the OECD, the Council of Europe, the United Nations, and other regional organisations;

- **closely follow up the development of international technical standards by standardisation organisations** such as CEN and ISO, to ensure that they usefully complement the legal rules and to ensure operational and effective implementation of the key data protection requirements.

2.5. A stronger institutional arrangement for better enforcement of data protection rules

The implementation and enforcement of data protection principles and rules is a key element in guaranteeing respect for individuals' rights.

In this context, **the role of the Data Protection Authorities (DPAs) is essential** for the enforcement of the rules on data protection. They are independent guardians of fundamental rights and freedoms with respect to the protection of personal data, upon which individuals rely to ensure the protection of their personal data and the lawfulness of processing operations. For this reason, the Commission believes that their role should be strengthened, especially having regard to the recent ECJ case law on their independence[47], and they should be provided with the necessary powers and resources to properly exercise their tasks both at national level and when co-operating with each other.

At the same time, the Commission considers that **Data Protection Authorities should strengthen their cooperation and better coordinate their activities**, especially when confronted by issues which, by their nature, have a cross-border dimension. This is particularly the case where multinational enterprises are based in several Member States and are carrying out their activities in each of these countries, or where coordinated supervision with the European Data Protection Supervisor (EDPS) is required[48].

In this respect, **an important role can be played by the Article 29 Working Party**[49], which already has the task, in addition to its advisory function[50], of contributing to the uniform application of EU data protection rules at national level. However, the continuing divergent

---

47 ECJ judgment of 9.3.2010, Commission v. Germany, Case C-518/07.

48 This is currently the case for large IT-systems, e.g., for the SIS II (cf. Article 46 of Regulation (EC) No 1987/2006 - OJ L 318, 28.12.2006, p. 4) and for the VIS (cf. Article 43 of Regulation (EC) No 767/2008 - OJ L 218, 13.8.2008, p. 60).

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

50 The Article 29 Working Party has the role of advising the Commission on the level of protection in the EU and in third countries and on any other measure relating to the processing of personal data.

application and interpretation of EU rules by Data Protection Authorities, even when challenges to data protection are the same across the EU, calls for a strengthening of the Working Party's role in coordinating DPAs' positions, ensuring a more uniform application at national level and thus an equivalent level of data protection.

The Commission will examine:

- how to **strengthen, clarify and harmonise the status and the powers of the national Data Protection Authorities** in the new legal framework, including the full implementation of the concept of 'complete independence'[51];

- ways to **improve the cooperation and coordination between Data Protection Authorities**;

- how to ensure a more consistent application of EU data protection rules across the internal market. This may include **strengthening the role of national data protection supervisors, better coordinating their work via the Article 29 Working Party (which should become a more transparent body), and/or creating a mechanism for ensuring consistency in the internal market under the authority of the European Commission**.

3. CONCLUSION: THE WAY FORWARD

Like technology, the way our personal data is used and shared in our society is changing all the time. The challenge this poses to legislators is to establish a legislative framework that will stand the test of time. At the end of the reform process, Europe's data protection rules should continue to guarantee a high level of protection and provide legal certainty to individuals, public administrations and businesses in the internal market alike for several generations. No matter how complex the situation or how sophisticated the technology, clarity must exist on the applicable rules and standards that national authorities have to enforce and that businesses and technology developers must comply with. Individuals should also have clarity about the rights they enjoy.

The **Commission's comprehensive approach** to address the issues and achieve the key objectives highlighted in this Communication will serve as a basis for further discussions with the other European institutions and other interested parties and will later be translated into concrete proposals and measures of both legislative and non-legislative nature. For this purpose, the Commission welcomes feedback on the issues raised in this Communication.

On this basis, following an impact assessment and taking into account the EU Charter of Fundamental Rights, the Commission will **propose legislation in 2011** aimed at revising the legal framework for data protection with the objective of strengthening the EU's stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention, taking into account the specificities of these areas. Non-legislative measures, such as encouraging self-regulation and exploring the feasibility of EU privacy seals, will be pursued in parallel.

As a second step, the Commission will **assess the need to adapt other legal instruments** to the new general data protection framework. This concerns, first of all, Regulation (EC) No

[51] See the ECJ judgment of 9.3.2010, Commission v. Germany, Case C-518/07.

45/2001, whose provisions will have to be adapted to the new general legal framework. The impact on other sectoral instruments will also need to be carefully examined at a later stage.

The Commission will also continue to ensure the proper monitoring of the correct implementation of Union law in this area, by pursuing an **active infringement policy** where EU rules on data protection are not correctly implemented and applied. Indeed, the current review of the data protection instruments does not affect the obligation of the Member States to implement and ensure the proper application of the existing legal instruments on the protection of personal data[52].

A high and uniform level of data protection within the EU will be the best way of endorsing and promoting EU data protection standards globally.

[52] This also includes Council Framework Decision 2008/977/JHA: Member States need to take the necessary measures to comply with the provisions of this Framework Decision before 27 November 2010.