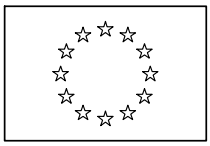

EUROPEAN COMMISSION

Brussels,
COM(2010) XXX final

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

"A comprehensive strategy on 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 strategy on 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 to the protection of personal data.**

Indeed technology nowadays allows individuals to disseminate 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 evident, but not unique, example of this phenomenon. "Cloud computing" - i.e., Internet-based computing whereby software, shared resources and information are on remote servers ("in the cloud") - also poses challenges to data protection, as it involves 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, **the means of collecting personal data have become increasingly sophisticated and less easily detectable**: for example, the use of cookies allows economic operators to better target individuals online with advertisements, thanks to the monitoring of their web browsing (so-called "behavioural advertising") and the growing use of geo-location devices makes it easy to determine the location of individuals simply because they possess a mobile phone. 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 effectively, to administer social security schemes or for taxation purposes, in the framework of their e-government applications etc.

---

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, 23.11.11995, 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.

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

In order to address this question, the Commission launched a process of review of the current legal framework, which started with a high level conference in May 2009, followed by a public consultation until the end of 2009[3] and by more targeted stakeholders' consultations throughout 2010[4]. A number of studies were also launched[5]. The results of this process confirmed that the core principles of the Directive are still valid and that its technologically neutral character should be preserved. However, several issues have been 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. It is to be noted that, in the electronic communication sector, this has been addressed by Directive 2002/58/EC (so-called "e-Privacy" Directive), which particularises and complements the general Data Protection Directive.[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, diminish 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, as well as to the allocation of responsibility for the data processing. As to international data

---

3 See the replies to the Commission's public consultation: http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm

4 Two targeted consultations (with public and private stakeholders) were organised on 29 June and 1st July 2010. Some of the stakeholders also sent written contributions as a follow up to the meeting. The Commission also consulted the Article 29 Working Party, which provided a comprehensive contribution to the 2009 consultation and adopted specific opinion in July 2010 on the accountability concept.

5 In addition to the *Study on the economic benefits of privacy enhancing technologies* (cit., footnote 2), see also: the EU study on the *Legal analysis of a Single Market for the Information Society, New rules for a new age, The future of online privacy and data protection*, (November 2009), and 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.

6 The e-Privacy Directive has been recently amended by Directive 2009/136/EC (to be transposed by May 2011) as part of the overall review of the regulatory framework for electronic communications.

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*

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.

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**[7]. The Lisbon Treaty provided the EU with additional means to achieve this: the 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 regulate, within a single legal instrument, data protection in the areas of police cooperation and judicial cooperation in criminal matters. The area of the 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 is committed to give the highest priority to ensuring respect for the fundamental right to data protection throughout the Union and across its policies, while at the same time enhancing its internal market dimension and facilitating the free flow of personal data.

This Communication intends to lay down the Commission's strategy 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, and 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 for the promotion of high data protection standards worldwide.

---

7 The need to provide a *comprehensive protection scheme*" on data protection, to "*ensure that the fundamental right to data protection is consistently applied* and to "*strengthen the EU stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention, as well as in [the EU] international relations*" has been stressed also in the Stockholm Programme (COM(2009)262 final of 10.6.2009; OJ C115/1, 4.5.2010) and in the Stockholm Action Plan (COM(2010), 171 final of 20.4.2010).

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

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

2. KEY OBJECTIVES OF THE COMPREHENSIVE STRATEGY ON DATA PROTECTION

2.1. Strengthening individuals' rights

2.1.1. Ensuring appropriate protection for individuals in all circumstances

The objective of the rules contained 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 Article 8 of the EU Charter of Fundamental Rights.

The concept of "personal data" is one of the key concepts for the protection offered to individuals by the current EU data protection instruments and triggers the application of the obligations incumbent to data controllers and data processors. The definition of "personal data" aims at covering all information relating to an identified or identifiable person. 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"[10]. This deliberate approach chosen by the legislator has the benefit of flexibility, allowing for its application to various situations and developments impacting 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 clear which approach should be followed, whether individuals enjoy data protection rights and whether data controllers should comply with the obligations provided by the Directive. National Data Protection Authorities have been confronted with cases where, on the one hand, the controller maintains that only scattered pieces of information are processed, without reference to a name or any other direct identifiers, and argues that the data should not be considered as personal data and not be subject to the data protection rules. On the other hand, the processing of that information only makes sense if it allows for the identification of specific individuals and treating them in a particular way[11].

At the same time, certain activities may still constitute an interference with fundamental rights, in the light of the jurisprudence of the European Court of Justice[12] and the European Court of Human Rights[13]. There may be situations which involve the processing of specific information, regardless of whether it is personal data or not, which should nevertheless be subject to protective measures under Union and national law. This may apply to key-coded data, geo-location data, or where the confidentiality and integrity in information-technology systems[14] must be ensured.

All the above issues therefore require careful examination.

---

10 See Recital 26 of Directive 95/46/EC

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

12 See for example Case C-101/01, 'Bodil Lindqvist', ECR [2003], I-1297, 96, 97 ECJ, and C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, ECR [2008] I-271.

13 See for instance Case of S. and Marper v. the United Kingdom, 4.12. 2008 (Application nos. 30562/04 and 30566/044.12.2008) and Rotaru v. Romania, judgment of 4 May 2000; no. 28341/95, § 55, ECHR 2000-V.

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

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**.

2.1.2. Increasing transparency

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.

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 on-line environment, where quite often privacy notices are difficult to access, unclear, non-transparent[15] and not always in full compliance with existing rules. A case where this might be so is online behavioural advertising, where 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 is collected, by whom, and for what purpose.

In this context, **minors** deserve specific protection, as they may be less aware of risks, consequences, safeguards and rights in relation to the processing of personal data[16].

The Commission will consider:

- introducing a **general principle of transparency** 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 **minors**;

- 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 lost, or accessed by unauthorised persons. The recent modifications to 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 such as the medical or the financial sector, the Commission will examine whether a general obligation to notify personal data breaches – both to data subjects and to Data Protection Authorities – should be introduced.

The Commission will:

- examine the possible modalities for the introduction in the general legal framework of a **general personal data breach notification**, including the addressees of such notifications and the threshold beyond which the obligation to notify should apply.

---

15 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 N° 282 : http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

16 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).

2.1.3. Enhancing control over one's own data

Among the preconditions for ensuring that individuals enjoy a high level of data protection, of significant importance 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**. In particular, 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 are enshrined in the EU Charter of Fundamental Rights[17] and already exist in the current legal framework but, given that the way in which they can be exercised is not harmonised, *de facto* actually exercising them is easier in certain Member States than in others. Moreover, this has become particularly challenging in the on-line 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 pertinent in this respect, as it constitutes significant challenge 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 to respond to individuals' requests, by allowing the exercise of rights by electronic means or by providing that right of access should be ensured free of charge as a principle);

- strengthening the so-called "**right to be forgotten**", i.e. the right of individuals to have their data deleted/removed when they are no longer needed for the purposes for which they were collected or when, in particular, processing is based on the person's consent, when he or she withdraws consent or when the storage period consented to has expired;

- guaranteeing "**data portability**", i.e., enabling an individual should be able to withdraw his/her own data (e.g., his/her photos, medical records or a list of friends) from an application or service and transfer them into another one, without hindrance from the data controllers[18].

2.1.4 Raising awareness

While transparency is essential, there is also the need to make the general public, and particularly young people, more aware of the risks related to the processing of personal data, as well as of their rights in that respect. 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[19]. Awareness rising activities should thus be encouraged and

---

17 Article 8(2) of the Charter states, in particular, that "Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".

18 The technical aspects of this – which go beyond the review of data protection rules - should also be examined.

19 See Flash Eurobarometer N° 225 – Data Protection in the European Union: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

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 consent

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[20]. 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 on-line 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, such as in the case of 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 an informed consent and ensure that the individual is fully aware that he or she consents, and to what data processing, in line with Article 8 of the EU Charter of Fundamental Rights.

The Commission will examine ways of:

- ensuring a **more harmonised implementation** of current rules on consent;

- **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[21]. However, there is a need to reconsider, in the light of technological and other societal developments, whether other categories of data could and should be added.

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

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

The Commission will consider whether:

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

- certain types of data that, in specific cases, could also be considered as 'sensitive', for example, **data related to minors**.

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 right to bring an action before the national courts** to data protection authorities and to civil society associations, including **consumer associations**;

- 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.

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 which is generally complete[22].

At the same time, the Directive allows the Member States a margin for manoeuvre in certain areas and authorises them to maintain or introduce particular rules for specific situations[23]. 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 problematic issues raised by private stakeholders, notably 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, which have 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, thus risking to affect the "equivalent (level of) protection" that the Directive is supposed to achieve and ensure.

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

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

In order to ensure a true level playing field for all data controllers who operate in different Member States, the Commission considers that **further harmonisation and approximation of data protection rules need to be provided at EU level**. The Commission will examine the means to achieve this.

2.2.2. Reducing the administrative burden

A concrete element for lessening the administrative burden and reducing costs for data controllers would be the **revision and simplification of the current notification system**[24]. 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 and 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**.

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 in 2003[25] already highlighted that the provisions related to applicable law[26] 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 different 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 the development of technologies: data controllers are increasingly operating in different 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)[27] to provide services from a distance and to process personal data in a virtual environment; and cloud computing makes it difficult to determine the location of personal data and of equipments used at any given time.

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

---

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

25 Report from the Commission - First Report on the implementation of the Data Protection Directive (95/46/EC) (COM (2003) 0265 final).

26 See Article 4 of Directive 95/46/EC.

27 The European Economic Area includes Norway, Liechtenstein and Iceland

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 their geographic location and of the 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 in those cases which are more and more frequent, 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 'accountability' principle[28]. This would not aim at increasing 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 above § 2.2.2).

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

– making the appointment of an internal independent **Data Protection Officer** mandatory and harmonising the rules related to their tasks and competences[29], while reflecting on the appropriate threshold not to impose undue administrative burdens, particularly on small and micro-enterprises;

– introducing an obligation in the legal framework 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;

– the concept of **"privacy by design"** and its concrete implementation, whereby data protection compliance would be embedded throughout the entire life cycle of technologies and procedures, from the early design stage to their deployment and use.

---

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

29 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).

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[30], have been rarely used so far and are not considered as satisfactory by private stakeholders (*see also below, § 2.4.1*).

Furthermore, the Commission considers it useful to explore the possible establishment of EU **certification schemes (e.g. "privacy seals")** for 'privacy-compliant' processes, technologies, products and services. This would not only give an orientation to the individual as user of such technologies, products and services, but also be relevant in relation to the responsibility of data controllers: the choice for such certified technologies, products or services could contribute to proving that the controller has fulfilled its obligations (*see above, §2.2.3*). Of course, it would be essential to **ensure the trustworthiness of such privacy seals** as well as to see how they can be articulated 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 (privacy seals)** for privacy aware technologies.

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, but not to the processing of personal data by police and judicial authorities in criminal matters. Various sector specific rules were adopted at EU level for police and judicial co-operation in criminal matters, in specific instruments, with particular data protection regimes, and/or referring to the rules in the Data Protection Convention of the Council of Europe (ETS 108) and – only for those Member States which have ratified it – to the Additional Protocol to that Convention (ETS 181)[31], as well as to the principles of non-legally binding Recommendation No. R (87) 15 of the Council of Europe regulating the use of personal data in the police sector[32]. As a result, the protection of personal data in this area is neither consistent nor uniform[33].

The general EU instrument in these areas is **Framework Decision 2008/977/JHA** on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. This instrument, while being a first step in establishing data protection rules

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

31 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows ETS No.: 181, available at: www.coe.int.

32 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 and available at: www.coe.int.

33 See an overview in Commission Communication "Overview of information management in the area of freedom, security and justice", COM (2010) 385.

for police and judicial authorities, **cannot be considered to ensure a level of protection equivalent to that offered by the Data Protection Directive, and does not achieve consistency with other legal instruments**. One of the major shortcomings of the Framework Decision is that it only applies to personal data that are or have been transmitted or made available between Member States, i.e., not to processing operations within the Member States, a distinction which is often very difficult to make in practice. In addition, since the Framework Decision only envisages minimum harmonisation of data protection standards, it does not achieve a free flow of personal data between competent authorities. It also **leaves a large room for manoeuvre to Member States for its implementation,** without any common procedures at EU level in order to contribute to the uniform application of such measures.

Moreover, the data protection provisions and supervisory mechanisms of other ex-third pillar acts, in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS), are not affected by the Framework Decision and thus maintain their specificities[34].

This situation directly affects, first of all, the power of 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). In addition, it may also hamper the exchange of necessary information between competent authorities to pursue objectives of general interest recognised by the Union, such as the fight against terrorism and organised crime, or the need to protect the rights and freedoms of others.

The objective of establishing a comprehensive and coherent system in the EU and vis-à-vis third countries entails **the need to consider a complete revision of the current rules on data protection in the area of police cooperation and judicial cooperation in criminal matters**, taking into account the specific nature of these fields and thus the specificities linked to the exchange of personal data in these areas[35].

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 at domestic level, while providing for the necessary **limitations** (e.g. concerning the right of access) and **derogations** (e.g., to the principle of transparency);

- examine the need for introducing specific provisions, 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);

- 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, to the new general legal data protection framework;

- 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.

---

[34] 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 and bodies, based on Regulation (EC) 45/2001.

[35] As indicated in Declaration 21 attached to the Lisbon Treaty.

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 data outside the EU/EEA area is the so-called **"adequacy procedure"**. 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. In some Member States adequacy is assessed in first instance by the organisation which itself transfers personal data to a third country, under the ex-post supervision of the data protection supervisory authority. This situation may lead to different approaches to the assessment of the level of adequacy of third countries and **entails the risk that the level of protection of data subjects is judged differently from one third country to the other**. In addition, the criteria, conditions and – for Commission adequacy decisions – procedures for the recognition of adequacy are currently not specified in detail in the current legal framework, which leads to varying practices.

In addition, for data transfers to third countries which do not ensure an adequate level of protection, the current Commission standard contractual clauses are not tailored to be used in non-contractual situations, such as in international agreements.

Other means that have been developed as a form of self-regulation (*see also above, § 2.2.4*) , such as internal company codes of conduct known as 'Binding Corporate Rules' (BCRs)[36], can also be a useful tool to lawfully transfer data between companies of the same corporate group. However, stakeholders have suggested that this mechanism could be further improved and its implementation eased.

There is therefore a **general need to improve the current mechanisms allowing for international transfers of 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, in order to ensure a **more uniform and coherent EU approach** vis-à-vis third countries and international organizations;

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

- to define **standard data protection clauses** to be used in international agreements, contracts, binding corporate rules or other legally binding instruments.

2.4.2. Promoting universal principles

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

---

[36] On BCRs and international transfers in general see: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

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[37].

As regards international technical standards, 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.

The Commission will:

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

- seek to secure that the international actions of the Union are grounded on the **principle of reciprocity of protection enjoyed by data subjects**, and in particular ensure that data subjects whose data are exported from the EU enjoy the same rights (including judicial redress) in third countries as third country nationals enjoy within the EU (reciprocal treatment);

- **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 organizations** 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 the data protection principles and rules is a key element to guarantee the respect of 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 the 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, having regard in particular to the recent ECJ case-law on their independence[38], and they should be provided with the necessary powers and resources to be able 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

---

37 See in particular the Data Protection Convention by the Council of Europe (ETS 108) and its Additional Protocol (ETS 181), which are open for accession by non-member States of the Council of Europe.

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

particularly the case where multinational enterprises (such as Internet companies) are based in several Member States and are exercising their activities in each of these countries.

In this respect, **an important role can be played by the Article 29 Working Party**[39], which already has the task, in addition to its advisory function[40], of contributing to the uniform application of EU data protection rules at national level. However, the continuing diverging 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 concept of "complete independence ";

- ways to **improving the cooperation and coordination between Data Protection Authorities** and ensure better enforcement of EU rules, particularly on issues having a cross-border dimension. This may include **strengthening the role of the Article 29 Working Party and providing it with additional powers in order to give a European response to breaches of data protection rules at EU level, or to create a European Data Protection Authority.**

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 businesses and individuals 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 strategy** 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.

---

[39] 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.

[40] 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.

On this basis, and following an impact assessment, the Commission's intention is to **present legislative proposals in 2011** aimed at revising the legal framework for data protection. Non-legislative measures, such as encouraging self-regulation and exploring the feasibility of an EU privacy seals, will be pursued in parallel.

At a later stage, the Commission will **assess the need to adapt EU specific data protection legal instruments** to the new general data protection framework.

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[41].

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.

[41] This also includes Council Framework Decision 208/977/JHA: Member States need to take the necessary measures to comply with the provisions of this Framework Decision before 27 November 2010. Commission powers based on Article 258 TFEU do not currently apply, however, in respect of the Framework Decision.