EUROPEAN COMMISSION

Brussels, XXX
[…](2011) XXX draft

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

Safeguarding Privacy in a Connected World
A European Data Protection Framework for the 21st Century

(Text with EEA relevance)

1. TODAY'S CHALLENGES TO DATA PROTECTION

The rapid pace of technological change and globalisation has profoundly transformed the scale and the way in which personal data is collected, accessed, used and transferred. New ways of sharing information through social networks and storing large amounts of data remotely have become part of life for many of the 250 million internet users in Europe. At the same time, personal data has become an asset for many businesses. Collecting, aggregating and analysing data of potential customers is often an important part of their economic activities[1].

In this new digital environment, **individuals have the right to enjoy effective control over their personal information**. Data protection is a fundamental right in Europe, enshrined in Article 8 of the Charter of Fundamental Rights of the European Union. This fundamental right has to be protected accordingly, while respecting other fundamental rights. A high level of data protection is also crucial to enhance trust in online services and to fulfil the potential of the digital economy, thus encouraging **economic growth and the competitiveness of EU industries.** A lack of confidence makes consumers hesitant to buy online and accept new services.

Modern, coherent rules across the EU are needed for data to flow freely from one Member State to another. Businesses need clear and uniform rules that provide legal certainty and minimise the administrative burden. This is essential for the single market to function and to **stimulate economic growth, create new jobs and foster innovation**[2]. Data protection therefore plays a central role not only in the European Commission's Stockholm Action Plan[3], but also in the Europe 2020 Strategy[4] – the EU's growth strategy – and in the Digital Agenda for Europe[5].

The EU's 1995 Directive[6], the central legislative instrument for the protection of personal data in Europe, was a milestone in the history of data protection. Its objectives, to ensure a functioning single market and an effective protection of the fundamental rights and freedoms of individuals, remain valid. However, it was adopted 16 years ago when the Internet was in its infancy. Now, in this new, challenging, digital environment, the existing rules provide neither the degree of harmonisation required, nor the necessary efficiency to ensure the right to personal data protection. The European Commission is therefore now proposing a fundamental reform of the EU's data protection framework.

In addition, the Lisbon Treaty has created, with Article 16 of the Treaty on the Functioning of the European Union (TFEU), a new foundation for a modernised and

---

1 The market for the analysis of very large sets of data is growing by 40% per year worldwide: http://www.mckinsey.com/mgi/publications/big_data/.

2 See also the conclusions of the European Council of 23 October 2011, which stressed the "key role" of the Single Market "in delivering growth and employment", as well as the need to complete the Digital Single Market by 2015.

3 COM(2010)171 final.

4 COM(2010)2020 final.

5 COM(2010)245 final.

6 Directive 95/46/EC on the protection of individuals with regard to the protection of personal data and on the free movement on such data, OJ L 281, 23.11.1995, p. 31.

comprehensive approach to data protection and the free movement of personal data, including in the area of police and judicial cooperation in criminal matters[7]. This approach is reflected in the European Commission's Communications on the Stockholm Programme and the Stockholm Action Plan[8].

To prepare the reform of the EU's data protection framework in a transparent manner, the Commission has launched, since 2009, public consultations on data protection[9] and engaged in an intense dialogue with stakeholders[10]. On 4 November 2010, the Commission issued a Communication on a comprehensive approach on personal data protection in the European Union[11] which set out the main themes of the reform. Between September and December 2011, the Commission in addition engaged in an enhanced dialogue with Europe's national data protection authorities and with the European Data Protection Supervisor to explore options for achieving a more consistent application of EU data protection rules across all EU Member States[12].

These discussions made clear that both citizens and businesses wanted the European Commission to substantially reform EU data protection rules. After assessing the impacts of different policy options[13], the European Commission is now proposing **a strong and consistent legislative framework across Union policies, enhancing individuals' rights, the single market dimension of data protection and drastically cutting red tape for businesses**[14]. The Commission proposes that the new framework will consist of:

– A **Regulation** (replacing Directive 95/46/EC) setting out a general EU framework for data protection[15];

– and a **Directive** (replacing Framework Decision 2008/977/JHA[16]) setting out rules on the protection of personal data processed for the purposes of **prevention, detection, investigation or prosecution of criminal**

---

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

8 COM(2009)262 and COM(2010)171 respectively.

9 Two public consultations have been launched on the data protection reform: one from July to December 2009 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm) and a second one from November 2010 till January 2011 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm).

10 Targeted consultations were organised in 2010 with Member State authorities and private stakeholders. In November 2010, Vice-President Reding organised a roundtable on the data protection reform. Additional dedicated workshops and seminars on specific issues (e.g. data breach notifications) were also held throughout 2011.

11 COM(2010)609.

12 See the letter of EU Justice Commissioner Viviane Reding of 19 September 2011 to the members of the Article 29 Working Party.

13 See the Impact Assessment (COM(…)).

14 This will include, at a later stage, amendments to align specific and sectoral instruments, in particular Regulation (EC) N° 45/2011 (OJ L 8, 12.1.2001, p.1) and acts in the area of police cooperation and judicial cooperation in criminal matters.

15 The legal relationship of the new Regulation and the new Directive with the e-Privacy Directive and other specific rules on data protection will be the object of an evaluation by the Commission, taking into account the negotiations on the current proposals with the Parliament and the Council.

16 Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p.60.

offences and related judicial activities. This legislative proposal is accompanied by a report on the implementation by Member States of Framework Decision 2008/977/JHA.

This Communication sets out the main elements of the reform of the EU framework for data protection.

2. PUTTING INDIVIDUALS IN CONTROL OF THEIR PERSONAL DATA

Under Directive 95/46/EC – the EU's main data protection law today – the ways in which individuals are able to exercise their right to data protection are not harmonised across Member States. Nor are the powers of the national authorities responsible for data protection harmonised enough to ensure consistent and effective application of the rules. The consequence is that actually exercising these rights is more difficult in some Member States than in others, particularly online.

This is due to the sheer volume of data collected everyday, and the fact that users are often not fully aware of their data being collected. Although many Europeans consider that the disclosure of personal data is increasingly a part of modern life[17], 72% of internet users in Europe still worry that they are asked for too much personal data online[18]. They feel that they are not in control of their data: they are not properly informed of what happens to their personal information, to whom it is transmitted and for what purposes. They often do not know how to exercise their rights online.

"Right to be forgotten"

A European student, who is a member of an online social networking service, decides to request access to all the personal data it holds about him. In doing so, he realises that the social network collects much more data than he was aware of and that some personal data that he thought had been deleted were still being stored.

The reform of the EU's data protection rules will ensure that this will no longer happen in the future by introducing:

- an explicit requirement that obliges online social networking services (and all other data controllers) to minimise the volume of users' personal data that they collect and process;

- a requirement that the default settings are that data is not made public;

- an explicit obligation for data controllers to delete an individual's personal data once the concerned individual requests deletion expressly and where there is no legitimate reason to retain it. In this specific case, this would oblige the social network provider to delete the student's data immediately and completely.

As highlighted in the Digital Agenda for Europe, privacy concerns are amongst the most frequent reasons for people not buying goods and services online. Given the contribution of the Information and Communication Technology (ICT) sector to

[17] See Special Eurobarometer 359 – *Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011, p. 23.

[18] Ibidem, p. 54.

overall productivity growth in Europe – 20% directly from the ICT sector and 30% from ICT investments[19] –, trust in such services is vital for stimulating growth in the EU economy and the competitiveness of European industry.

Data breach notifications

A gaming service which targets users in the EU has been subject to a security breach by hackers. The breach affected databases containing personal data (including names, addresses and possibly credit card data) of tens of millions of users worldwide. The company delayed notification of the breach to the concerned users for a week after it had been discovered.

The reform of the EU's data protection rules will ensure that this will no longer happen in the future. Companies will be obliged by the new EU rules:

- to strengthen their security measures to prevent and avoid breaches;

- to notify data breaches to both the national data protection authority and the individuals concerned within 24 hours of a breach being discovered.

The aim of the new laws proposed by the Commission today is to strengthen rights, to give people efficient and operational means to make sure that they are fully informed about what happens to their personal data and to enable them to exercise their rights more effectively.

To strengthen the right of individuals to data protection, the Commission is proposing new rules which will:

Increase individuals' ability to control their data, namely by:

- ensuring that, when their **consent** is required, it is **given explicitly i.e. must be based on an affirmative action by the person concerned** and must be freely given;

- equipping Internet users with an effective **right to be forgotten** in the online environment: the right to have their data deleted if they withdraw their consent and if there are no legitimate grounds for retaining the data;

- guaranteeing **easy access to one's own data** and a **right to data portability**: a right to obtain a copy of the stored data from the controller and the freedom to move it from one service provider to another, without hindrance;

- reinforcing **the right to information** so that individuals fully understand how their personal data is handled, particularly when the processing activities concern **children.**

Improve the means for individuals to exercise their rights, namely by:

- strengthening national **data protection authorities' independence and powers,** so that they are properly equipped to deal effectively with complaints, in

[19] See Digital Agenda for Europe, cit., p.4.

particular the powers to carry out effective investigations, take binding decisions and impose effective and dissuasive sanctions;

- enhancing **administrative and judicial remedies** when data protection rights are **violated**. In particular, qualified associations will be able to bring actions to court on behalf of the individual.

Reinforce data security, in particular by:

- encouraging the use of **privacy enhancing technologies** (technologies which protect the privacy of information by minimising the storage of personal data), **privacy-friendly default settings** and **privacy certification schemes;**

- introducing **a general obligation**[20] for data controllers **to immediately notify data breaches** to both the individuals concerned and data protection authorities.

Enhance the accountability of those processing data, namely by:

- requiring data controllers to designate a **Data Protection Officer** in the public sector, in companies with more than 250 employees and in firms which are involved in risky processing;

- introducing the **Privacy by Design principle** to make sure that data protection safeguards are taken into account at the planning stage of procedures and systems;

- introducing the obligation to carry out **Data Protection Impact Assessments** for organisations involved in risky processing.

3. DATA PROTECTION RULES FIT FOR THE DIGITAL SINGLE MARKET

Despite the current Directive's objective to ensure an equivalent level of data protection within the EU, there is still considerable divergence in the rules across Member States. As a consequence, data controllers may have to deal with 27 different national laws and requirements within the EU. The result is a **fragmented legal environment** which has created **legal uncertainty** and unequal protection for individuals. This has caused **unnecessary costs and administrative burdens** for businesses and constitutes a disincentive for enterprises operating in the single market who may wish to expand their operations cross-border.

The resources and the powers of the national authorities responsible for data protection vary considerably between Member States[21]. In some cases this means that they are unable to perform their enforcement tasks satisfactorily. Cooperation between these authorities at European level – via the existing Advisory Group (the

[20] This is currently compulsory only in the telecoms sector, based on the e-Privacy Directive (Directive 2002/58/EC as last amended by Directive 2009/136/EC - OJ L 337, 18.12.2009, p. 11).

[21] For more details on this aspect, see the Impact Assessment accompanying the legal proposals, COM(…)…

so-called Article 29 Working Party)[22] – does not always lead to consistent enforcement and therefore also needs to be improved.

Consistent enforcement of data protection rules across Europe

A multinational company with several establishments in the EU has deployed a virtual mapping system across Europe which collects images of all private and public buildings, and may also take pictures of people on the street. In one Member State, the inclusion of un-blurred pictures of persons unaware that they were being photographed was considered to be unlawful while in other Member States this did not infringe data protection laws. Consequently national data protection authorities took different measures to remedy this situation.

The reform of the EU's data protection rules will ensure that this can no longer happen in future, because:

- the data protection requirements and safeguards will be harmonised across Member States by means of an EU Regulation;

- the independence of national data protection authorities will be further reinforced;

- only the data protection authority where the company has its main establishment will be responsible to take decisions against the company;

- a swift and effective coordination between national data protection authorities – given that the service is directed at individuals in several Member States – will help ensure that the new EU data protection rules will be applied and enforced consistently across all Member States.

National authorities need to be reinforced and their cooperation strengthened to guarantee the consistent enforcement and, ultimately, uniform application of rules across the EU.

A strong, clear and uniform legislative framework at EU level will help to unleash the potential of the digital single market and foster economic growth, innovation and job creation. A Regulation will do away with the fragmentation of legal regimes between the 27 Member States and barriers to market entry, which is of particular importance to small and medium-sized enterprises.

The new rules will also provide an advantage for EU companies in global competition, as they will be able to offer their customers assurances, backed up by a regulatory framework, that valuable personal information will be treated with the necessary care and diligence. Trust in the coherent regulatory regime of the EU will be a key asset for service providers and an incentive for investors looking for optimal conditions when locating services.

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

In order to enhance the **single market dimension of data protection,** the Commission proposes to:

- **harmonise** data protection rules at EU level through a Regulation directly applicable in all Member States[23] which will put an end to the cumulative and simultaneous application of different national data protection laws; this will lead to a net **saving for companies of about €2.3 billion a year in terms of administrative burdens alone;**

- **simplify the regulatory environment by drastically cutting red tape** and doing away with **formalities** such as general notification requirements (leading to net savings of €130 million a year in terms of administrative burdens alone);

- **further enhance the independence and the powers of national data protection authorities (DPAs)** to enable them to carry out investigations, take binding decisions and impose effective and dissuasive sanctions, as well as oblige Member States to provide them with **sufficient resources**;

- **set up a one-stop-shop system for data protection in the EU:** data controllers in the EU will only have to deal with **one single DPA**, namely the DPA of the Member State where the company's main establishment is located;

- create the conditions for **swift and efficient cooperation between DPAs** including the obligation for one DPA to carry out investigations and inspections upon request from another, and to mutually recognise each other's decisions;

- **set up a consistency mechanism** at EU level, which will ensure that decisions by a DPA which have a wider European impact take full account of the views of other concerned DPAs and are fully in compliance with Union law;

- upgrade the Article 29 Working Party to **an independent European Data Protection Board** to better contribute to a consistent application of data protection law and to provide a strong basis for cooperation among data protection authorities, including the European Data Protection Supervisor; and enhance synergies and effectiveness by providing that the secretariat of the European Data Protection Board will be hosted by the European Data Protection Supervisor.

The new EU Regulation will ensure a robust protection of the fundamental right to data protection throughout the European Union and strengthen the functioning of the internal market. At the same time, it will include explicit provisions that ensure respect of other fundamental rights, such as freedom of expression and information and the right to defence, as well as of professional secrecy (e.g. for the legal profession) and does not prejudice the status of churches under the laws of the Member States.

[23] A Directive is proposed to define the rules applicable to the area of police cooperation and judicial cooperation in criminal matters (see § 4 below), which will allow for more flexibility for Member States in this specific area.

4. THE USE OF DATA IN POLICE AND CRIMINAL JUSTICE COOPERATION

The entry into force of the Lisbon Treaty and in particular the introduction of a new legal basis (Article 16 TFEU) provide the opportunity to achieve a comprehensive data protection framework ensuring both a high level of protection for individuals' data in the field of police and judicial cooperation in criminal matters and a smoother exchange of information between Member States' police and judicial authorities. This will improve cooperation in the fight against serious crime in Europe.

Data protection in the field of police cooperation

As part of an ongoing criminal investigation, a police authority in one Member State (country A) is requested by the police of another Member State (country B) to check whether DNA found at a crime scene is related to three individuals who are known to be in country B and whether there is additional personal data (for example, their names) available in case of a positive match. However, given the limited harmonisation at EU level of rules on DNA processing and exchange for law enforcement purposes, the police officer in country A handling the request is not sure whether the national law of country B offers sufficient data protection safeguards in relation to DNA data and therefore is not able to respond swiftly to the request for information.

The reform of the EU's data protection rules will ensure that this can no longer happen in future, because:

- rules on the processing of genetic data will be more harmonised, in line with the case-law of the European Court of Human Rights. This will make it easier for police authorities in the EU to exchange such data when investigating serious crimes;

- the same data protection rules will apply to data transfers within a Member State and across borders. This will facilitate the practical application of the new rules by national judicial and police authorities which often cannot identify easily in advance whether a case is a purely domestic one or has a cross-border dimension.

This protection should be extended to cases where data from the private sector may be required and used by law enforcement authorities in a variety of circumstances: data related to bank transfers, data collected when buying an airline ticket, or traffic and telecommunication data, for example.

The processing of data by police and judicial authorities in the criminal field is currently covered principally by Framework Decision 2008/977/JHA, which pre-dates the entry into force of the Lisbon Treaty. In view of its nature as a Framework Decision, the Commission has no powers to enforce its rules, which has contributed to its very uneven implementation. In addition, the scope of this Framework Decision is limited to cross-border processing activities[24]. This means that the processing of personal data that has not been made the subject of exchanges is currently not covered by EU rules governing such processing and protecting the fundamental right to data protection. This also creates a practical difficulty for police and other authorities who are not always able to easily distinguish between purely domestic

[24] More precisely, the Framework Decision applies to personal data that are or have been transmitted or made available between Member States or exchanged between Member States and EU institutions or bodies (see Article 1(2)).

and cross-border processing or to foresee whether certain data may become the object of a cross-border exchange at a later stage[25].

Article 16 TFEU provides a legal basis to cover both cross-border and domestic processing of personal data. A consistent application would also help in coping with different national 'rules of origin' and varying standards that affect both the level of protection of individuals' data and the efficiency of law enforcement cooperation.

The EU's new reformed data protection framework therefore aims to ensure a consistent, high level of data protection in this area to **enhance mutual trust between police and judicial authorities of different Member States, thus facilitating the free flow of data and cooperation between police and judicial authorities**.

To extend stronger protection of personal data to the field of police and judicial cooperation in criminal matters and to facilitate at the same time exchanges of personal data between Member States' police and judicial authorities, the Commission is proposing a Directive which will:

- **apply general data protection principles and rules** to the area of police cooperation and judicial cooperation in criminal matters, while respecting the specific nature of these fields[26];

- provide for **minimum harmonised criteria and conditions on possible limitations** to the general rules. This concerns, in particular, the rights of individuals to be informed when police and judicial authorities handle or access their data. Such limitations are necessary for the effective prevention, investigation, detection or prosecution of criminal offences;

- establish **specific rules to cater for the specific nature of law enforcement activities, including** for the processing of **genetic data** for the purposes of criminal investigation;

- **distinguish between the various categories of data subjects** whose rights may vary (e.g. witnesses and suspects).

5. SETTING GLOBAL STANDARDS FOR DATA PROTECTION

Individuals' rights must continue to be ensured when personal data is transferred from the EU to third countries, and whenever individuals in the Member States are targeted and their data is used or analysed by third country service providers. This means that EU data protection standards have to apply regardless of the geographical location of the company or its processing facility.

[25] This was confirmed by several Member States when replying to the Commission's questionnaire in relation to the Implementation Report on the Framework Decision (COM(2012)…).

[26] Cf. Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, as annexed to the Final Act of the Intergovernmental Conference which adopted the Lisbon Treaty.

The increasingly globalised nature of data flows, the multiplication of actors in areas such as cloud computing and the fact that personal data is being transferred across an increasing number of virtual and geographical borders and stored on servers in multiple countries, all call for an improvement of the current mechanisms for transfers of data to third countries. This includes adequacy decisions and appropriate safeguards such as standard contractual clauses or Binding Corporate Rules[27] – with the twofold aim of securing a high level of data protection in international processing operations and facilitating data flows across borders.

Binding Corporate Rules

A corporate group needs to transfer personal data from its affiliates based in the 27 EU Member States to its affiliates located in third countries on a regular basis. The group would like to introduce a set of Binding Corporate Rules (BCRs) in order to be compliant with EU law whilst also limiting the administrative requirements for each individual transfer. In practice, BCRs ensure that a single set of rules would apply throughout the group instead of various internal contracts.

Today the recognition that a company's BCRs provide adequate safeguards implies a thorough review by three DPAs (one "lead" and two "reviewers") but may also be commented on by several others. Furthermore, many Member States' laws require additional national authorisations for the transfers covered by the BCRs and this makes their adoption process very burdensome, costly, long and complex.

Following the data protection reform:

- a simpler and more streamlined process will take place;

- BCRs will be validated only by the lead DPA. Mechanisms are foreseen to ensure the swift involvement of other concerned DPAs;

- Once a BCR is validated by one authority, it will be valid for the whole EU without needing any additional authorisation at national level.

To address the challenges of globalisation, it is therefore necessary to provide flexible tools and mechanisms – particularly to businesses operating worldwide – while guaranteeing protection of individuals' data without any loopholes, the Commission is proposing the following measures:

- **clear rules** defining when **EU law is applicable to data controllers established in third countries**, in particular by specifying that whenever processing activities are **directed at individuals in the EU**, **European rules shall apply;**

- any decisions certifying data protection standards in third countries (**adequacy decisions)** will be taken by the European Commission on the basis of explicit and clear criteria, including in the area of police cooperation and criminal justice;

[27] Binding Corporate Rules (BCRs) are codes of practices based on European data protection standards, approved by at least one DPA, which organisations draw up voluntarily and follow to ensure adequate safeguards for categories of transfers of personal data between companies that are part of the same corporate group and that are bound by those rules. They are not explicitly foreseen in Directive 95/46/EC but have developed as a matter of practice between DPAs, with the support of the Article 29 Working Party.

- legitimate flows of data to third countries will be made easier by reinforcing and simplifying **rules on international transfers** to countries not covered by an adequacy decision, in particular by streamlining and extending the use of tools such as **Binding Corporate Rules,** so that they can be used to cover **data processors** and within **groups of companies**, thus better reflecting the multiplicity of actors involved in data processing activities, especially in cloud computing;

- engaging in **dialogue** and, where appropriate, **negotiations,** with third countries – particularly EU strategic partners – and relevant international organisations (e.g. Council of Europe[28], OECD, UN) to **promote high and interoperable data protection standards** worldwide.

6. CONCLUSION

The EU data protection reform aims at building **a modern, strong, consistent and comprehensive data protection framework** for the European Union**.** The fundamental right to data protection will be given effect. Other rights, such as freedom of expression and information, the right to defence and professional secrecy (e.g. for the legal profession) and the status of churches under Member States' laws will be respected.

The reform will first of all benefit individuals by strengthening their data protection rights and their trust in the digital environment. The reform will furthermore simplify substantially the legal environment for businesses and the public sector, thus stimulating the development of the digital economy across the EU single market and beyond, in line with the objectives of the Europe 2020 strategy and the Digital Agenda for Europe. Last but not least, the reform will enhance trust between law enforcement authorities and facilitate the exchanges of data between them, thereby improving cooperation in the fight against crime, while ensuring a high level of protection for individuals.

The Commission will work closely with the European Parliament and the Council to ensure an agreement on the EU's new data protection framework by the end of 2012. It will continue to maintain a close dialogue, throughout this process and beyond, with all interested parties to benefit from the input necessary, including on ICT developments and evolving social behaviour, in order to ensure both a high level of protection of individuals as well as the growth and competitiveness of EU industries.

[28] The Commission will work together with the Council of Europe on the ongoing revision of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (n° 108) in order to ensure its coherence with the reform of the EU data protection framework.