COUNCIL OF THE EUROPEAN UNION

Brussels, 27 January 2012

5852/12

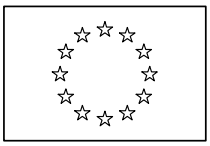
DATAPROTECT 8
JAI 43
MI 57
DRS 10
DAPIX 11
FREMP 6

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	27 January 2012
to:	Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.:	COM(2012) 9 final
Subject:	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

Delegations will find attached Commission document COM(2012) 9 final.

Encl.: COM(2012) 9 final



EUROPEAN COMMISSION

Brussels, 25.1.2012
COM(2012) 9 final

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)

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 have profoundly transformed the way in which an ever-increasing volume of 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 Europe's 250 million internet users. At the same time, personal data has become an asset for many businesses. Collecting, aggregating and analysing the 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, as well as in Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), and needs to be protected accordingly.

Lack of confidence makes consumers hesitant to buy online and accept new services. Therefore, a high level of data protection is also crucial to enhance trust in online services and to fulfil the potential of the digital economy, thereby encouraging **economic growth and the competitiveness of EU industries.**

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 if the Single Market is to function and to **stimulate economic growth, create new jobs and foster innovation**[2]. A modernisation of the EU's data protection rules, which strengthens their internal market dimension, ensures a high level of data protection for individuals, and promotes legal certainty, clarity and consistency, therefore plays

---

[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.

a central role in the European Commission's Stockholm Action Plan[3], in the Digital Agenda for Europe[4] and, more broadly, for the EU's growth strategy Europe 2020[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 effective protection of the fundamental rights and freedoms of individuals, remain valid. However, it was adopted 17 years ago when the internet was in its infancy. In today's new, challenging digital environment, existing rules provide neither the degree of harmonisation required, nor the necessary efficiency to ensure the right to personal data protection. That is why the European Commission is proposing a fundamental reform of the EU's data protection framework.

In addition, the Lisbon Treaty has created, with Article 16 TFEU, a new legal basis for a modernised and comprehensive approach to data protection and the free movement of personal data, also covering 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], which stress the need for the Union to "establish a comprehensive personal data protection scheme covering all areas of EU competence" and "ensure that the fundamental right to data protection is consistently applied".

To prepare the reform of the EU's data protection framework in a transparent manner, the Commission has, since 2009, launched public consultations on data protection[9] and engaged in intensive dialogue with stakeholders.[10] On 4 November 2010, the Commission published 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 was involved in an enhanced dialogue with Europe's national data protection authorities and with the European Data Protection Supervisor to explore options for more consistent application of EU data protection rules across all EU Member States[12].

---

3 COM(2010)171 final.

4 COM(2010)245 final.

5 COM(2010)2020 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.

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, EU Justice Commissioner Viviane 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, published at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm.

These discussions made clear that both citizens and businesses wanted the European Commission to reform EU data protection rules in a comprehensive manner. 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 cutting red tape for businesses**[14]. The Commission proposes that the new framework should 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 offences and related judicial activities.**

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 legislative act in the field of data protection today – the ways in which individuals are able to exercise their right to data protection are not sufficiently 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. This means that actually exercising such rights is more difficult in some Member States than in others, particularly online.

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

---

13 See the Impact Assessment SEC(2012)72.

14 This will include, at a later stage, amendments to align specific and sectoral instruments, for example Regulation (EC) No 45/2001, OJ L 8, 12.1.2001, p.1.

15 The Regulation also makes a limited number of technical adjustments to the e-Privacy Directive (Directive 2002/58/EC as last amended by Directive 2009/136/EC - OJ L 337, 18.12.2009, p. 11) to take account of the transformation of Directive 95/46/EC into a Regulation. The substantive legal consequences of the new Regulation and of the new Directive for the e-Privacy Directive will be the object, in due course, of a review by the Commission, taking into account the result of the negotiations on the current proposals with the European 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. A report on the implementation by Member States of the Framework Decision (COM(2012)12) is adopted as part of the data protection reform package.

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

18 Ibidem, p. 54.

to whom it is transmitted and for what purposes. Often, they 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 the network holds about him. In doing so, he realises that it 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 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 ensure that data is not made public;

- an explicit obligation for data controllers to delete an individual's personal data if that person explicitly requests deletion and where there is no other 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, concerns about privacy are among the most frequent reasons for people not buying goods and services online. Given the contribution of the Information and Communication Technology (ICT) sector to overall productivity growth in Europe – 20% directly from the ICT sector and 30% from ICT investments[19] – trust in such services is vital to stimulate growth in the EU economy and the competitiveness of European industry.

Data breach notifications

Hackers attacked a gaming service which targets users in the EU. The breach affected databases containing personal data (including names, addresses and possibly credit card data) of tens of millions of users worldwide. The company waited for a week before notifying the users concerned.

The reform of the EU's data protection rules will ensure this could no longer happen. The new rules will oblige companies:

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

- to notify data breaches to both the national data protection authority – within 24 hour of the breach being discovered, where feasible – and the individuals concerned without undue delay.

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

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

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

Improve individuals' ability to control their data, by:

- ensuring that, when their **consent** is required, it is **given explicitly, meaning that it is based either on a statement or on a clear affirmative action by the person concerned** and is 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 other 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, by:

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

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

- introducing **a general obligation**[20] for data controllers **to notify data breaches without undue delay** to both data protection authorities (which, where feasible, should be within 24 hours) and the individuals concerned.

Enhance the accountability of those processing data, in particular by:

- requiring data controllers to designate a **Data Protection Officer** in companies with more than 250 employees and in firms which are involved in processing operations which, by virtue of their nature, their scope or their purposes, present specific risks to the rights and freedoms of individuals ("risky processing");

[20] This is currently compulsory only in the telecommunications sector, based on the e-Privacy Directive.

- 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. The result is a **fragmented legal environment** which has created **legal uncertainty** and uneven protection for individuals. This has caused **unnecessary costs and administrative burdens** for businesses and is a disincentive for enterprises operating in the Single Market that may want to expand their operations across borders.

The resources and the powers of the national authorities responsible for data protection vary considerably among Member States[21]. In some cases, they are unable to perform their enforcement tasks satisfactorily. Cooperation among these authorities at European level – via the existing Advisory Group (the so-called Article 29 Working Party)[22] – does not always lead to consistent enforcement and also needs to be improved.

Consistent enforcement of data protection rules across Europe

A multinational company with several establishments in the EU has deployed an online 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 there was no such infringement of data protection laws. As a result, there was no consistent response among national data protection authorities to remedy this situation.

The reform of the EU's data protection rules will ensure that this could not happen in future, as:

- data protection requirements and safeguards will be set out in an EU Regulation with direct application throughout the Union;

- only the data protection authority where the company has its main establishment will be responsible for deciding whether the company is acting within the law;

- prompt, 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.

---

21 For more details on this aspect, see the Impact Assessment accompanying the legal proposals, SEC(2012)72.

22 The Article 29 Working Party was set up in 1996 (by Article 29 of Directive 95/46/EC) 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.

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 across 27 Member States and remove barriers to market entry, a factor of particular importance to micro, small and medium-sized enterprises.

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

To enhance the **Single Market dimension of data protection,** the Commission proposes to:

- lay down 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). Given their importance for the competitiveness of the European economy, special attention is given to the specific needs of micro, small and medium sized enterprises;

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

- **set up a 'one-stop-shop' system for data protection in the EU:** data controllers in the EU will only have to deal with **a 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;

[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.

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

- upgrade the Article 29 Working Party to **an independent European Data Protection Board** to improve its contribution to 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 to enhance synergies and effectiveness by foreseeing that the secretariat of the European Data Protection Board will be provided 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 Single Market. At the same time – in view of the fact that, as underlined by the Court of Justice of the EU[24], the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society[25] and be balanced with other fundamental rights, in accordance with the principle of proportionality[26] – the Regulation will include explicit provisions that ensure the respect of other fundamental rights, such as freedom of expression and information, the right to defence, as well as of professional secrecy (such as for the legal profession), without prejudicing the status of churches under the laws of the Member States.

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) allow the establishment of a comprehensive data protection framework ensuring a high level of protection for individuals' data, whilst respecting the specific nature of the field of police and judicial cooperation in criminal matters. In particular, it allows the revised EU data protection framework to cover both cross-border and domestic processing of personal data. This would reduce differences between the legislation in Member States, to the likely benefit of the protection of personal data overall. It could also lead to a smoother exchange of information between Member States' police and judicial authorities and thereby improve cooperation in the fight against serious crime in Europe. The processing of data by police and judicial authorities in criminal matters is currently principally covered by Framework Decision 2008/977/JHA, which pre-dates the entry into force of the Lisbon Treaty. The Commission has no powers to enforce its rules, as it is a Framework Decision, and this has contributed to uneven implementation. In addition, the scope of the Framework Decision is limited to cross-border processing

---

24 Court of Justice of the EU, judgment of 9.11.2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010], not yet officially reported.

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

26 Court of Justice of the EU, judgment of 6.11.2003, C-101/01, Lindqvist [2003] ECR I-12971, para 82-90; judgement of 16.12.2008, C-73/07, Satamedia [2008], ECR I-9831, para 50-62.

activities.[27] 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, in some cases, practical difficulties for police and other authorities for whom it may not be obvious whether data processing is to be purely domestic or cross-border; or to foresee whether 'domestic' data might become the object of a subsequent cross-border exchange.[28]

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

To ensure a high level of protection of personal data in the field of police and judicial cooperation in criminal matters and to facilitate exchanges of personal data between Member States' police and judicial authorities, the Commission is proposing, as part of the data protection reform package, a Directive which will:

- **apply general data protection principles** to police cooperation and judicial cooperation in criminal matters, while respecting the specific nature of these fields;[29]

- 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 cover the specific nature of law enforcement activities, including a distinction between different categories of data subjects** whose rights may vary (such as witnesses and suspects).

5. DATA PROTECTION IN A GLOBALISED WORLD

Individuals' rights must continue to be ensured when personal data is transferred from the EU to third countries, and whenever individuals in 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 a company or its processing facility.

---

27 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)).

28 This was confirmed by some Member States when replying to the Commission's questionnaire in relation to the Implementation Report on the Framework Decision (COM(2012)12).

29 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.

In today's globalised world, personal data is being transferred across an increasing number of virtual and geographical borders and stored on servers in multiple countries. More companies are offering cloud computing services, which allow customers to access and store data on remote servers. These factors call for an improvement in current mechanisms for transferring data to third countries. This includes adequacy decisions – i.e. decisions certifying 'adequate' data protection standards in third countries – and appropriate safeguards such as standard contractual clauses or Binding Corporate Rules[30], so as to secure a high level of data protection in international processing operations and facilitate data flows across borders.

Binding Corporate Rules

A corporate group regularly needs to transfer personal data from its affiliates based in the EU to its affiliates located in third countries. The group would like to introduce a set of Binding Corporate Rules (BCRs) to comply with EU law while 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.

Based on current practices agreed at the level of the Article 29 Working Party, 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 transfers covered by BCRs and this makes their adoption process very burdensome, costly, long and complex.

Following the data protection reform:

- this process will be simpler and more streamlined;

- BCRs will be validated only by one DPA, with mechanisms to ensure the swift involvement of other relevant DPAs;

- Once one authority has approved a BCR, it will be valid for the entire EU without needing any additional authorisation at national level.

To **address the challenges of globalisation**, flexible tools and mechanisms are needed – particularly for 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 goods and services are offered to individuals in the EU, or whenever their behaviour is monitored, **European rules shall apply;**

30 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 covered in Directive 95/46/EC but have developed as a matter of practice between DPAs, with the support of the Article 29 Working Party.

- any **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;

- 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 increasing number of companies involved in data processing activities, especially in cloud computing;

- engaging in **dialogue** and, where appropriate, **negotiations,** with third countries – particularly EU strategic partners and European Neighbourhood Policy countries – and relevant international organisations (such as the Council of Europe, the Organisation for Economic Cooperation and Development, the United Nations) to **promote high and interoperable data protection standards** worldwide.

6. CONCLUSION

The EU data protection reform aims to build **a modern, strong, consistent and comprehensive data protection framework for the European Union**. Individuals' fundamental right to data protection will be reinforced. Other rights, such as freedom of expression and information, the right of the child, the right to conduct a business, the right to a fair trial and professional secrecy (such as for the legal profession), as well as 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 the legal environment for businesses and the public sector substantially. This is expected to stimulate the development of the digital economy across the EU's Single Market and beyond, in line with the objectives of the Europe 2020 strategy and the Digital Agenda for Europe. Finally, the reform will enhance trust among law enforcement authorities in order to facilitate exchanges of data between them and cooperation in the fight against serious crime, while ensuring a high level of protection for individuals.

The European 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. Throughout this adoption process and beyond, especially in the context of the implementation of the new legal instruments, the Commission will maintain a **close and transparent dialogue with all interested parties** involving representatives from the private and public sector. This will include representatives from the police and the judiciary, electronic communications regulators, civil society organisations, data protection authorities and academics, as well as from specialised EU agencies such as Eurojust, Europol, the Fundamental Rights Agency, and the European Network and Information Society Agency.

In a context of constant development of information technologies and evolving social behaviour, such a dialogue is of the utmost importance to benefit from the input necessary to ensure a high level of data protection of individuals, the growth and

competitiveness of EU industries, the operational effectiveness of the public sector (including the police and the judiciary) and a low level of administrative burden.