

# Data Protection



## *Progress on EU reform now irreversible after European Parliament vote*

Strasbourg, 12 March 2014

The European Parliament today cemented the strong support previously given at committee level to the European Commission's data protection reform ([MEMO/13/923](#) and [MEMO/14/60](#)) by voting in plenary with 621 votes in favour, 10 against and 22 abstentions for the the Regulation and 371 votes in favour, 276 against and 30 abstentions for the Directive). The reports of MEPs Jan-Philipp Albrecht and Dimitrios Droutsas, on which members of the European Parliament voted, are a strong endorsement of the Commission's data protection reform and an important signal of progress in the legislative procedure. The data protection reform will ensure more effective control of people over their personal data, and make it easier for businesses to operate and innovate in the EU's Single Market.

*« The message the European Parliament is sending is unequivocal: This reform is a necessity, and now it is irreversible. Europe's directly elected parliamentarians have listened to European citizens and European businesses and, with this vote, have made clear that we need a uniform and strong European data protection law, which will make life easier for business and strengthen the protection of our citizens, »* said **Vice-President Viviane Reding, the EU's Justice Commissioner.**

*« Data Protection is made in Europe. Strong data protection rules must be Europe's trade mark. Following the U.S. data spying scandals, data protection is more than ever a competitive advantage. I want to thank Mr Albrecht and Mr Droutsas for their committed and tireless work on the data protection reform. Today's vote is the strongest signal that it is time to deliver this reform for our citizens and our businesses. »*

## Next Steps

Today's plenary vote means the position of the Parliament is now set in stone and will not change even if the composition of the Parliament changes following the European elections in May.

It follows a positive vote from the leading Civil Liberties, Justice and Home Affairs Committee in October 2013 ([MEMO/13/923](#)).

To become law the proposed Regulation has to be adopted by the Council of Ministers using the «ordinary legislative procedure» (co-decision).

The European Parliament stands ready to negotiate with the Council of the EU as soon as the Council defines its position.

On 4 March 2014 Ministers in the Council discussed the data protection reform, focusing on its territorial scope and on aspects relating to international transfers ([MEMO/14/144](#) and [SPEECH/14/175](#)). Ministers [broadly supported](#) the principle that non-European companies when offering goods and services to European consumers, will have to apply the EU data protection law in full. The next meeting of Justice Ministers on the data protection reform will take place in June 2014.

European heads of state and government committed to a «timely» adoption of the new data protection legislation at a summit on 24 and 25 October 2013, which focused on the digital economy (see [Conclusions](#)).

## Background

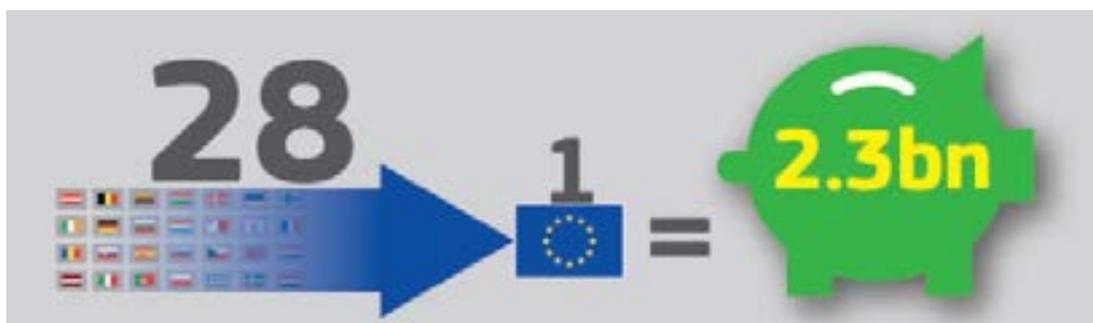
On 25 January 2012, the Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online data protection rights and boost Europe's digital economy (see [IP/12/46](#)). The Commission's proposals update and modernise the principles enshrined in the 1995 Data Protection Directive, bringing them into the digital age and building on the high level of data protection which has been in place in Europe since 1995.

## What will the data protection reform do for growth?

Data is the currency of today's digital economy. Collected, analysed and moved across the globe, personal data has acquired enormous economic significance. According to some estimates, the value of European citizens' personal data has the potential to grow to nearly €1 trillion annually by 2020. Strengthening Europe's high standards of data protection is a business opportunity.

The European Commission's data protection reform will help the digital single market realise this potential, notably through **three main innovations**:

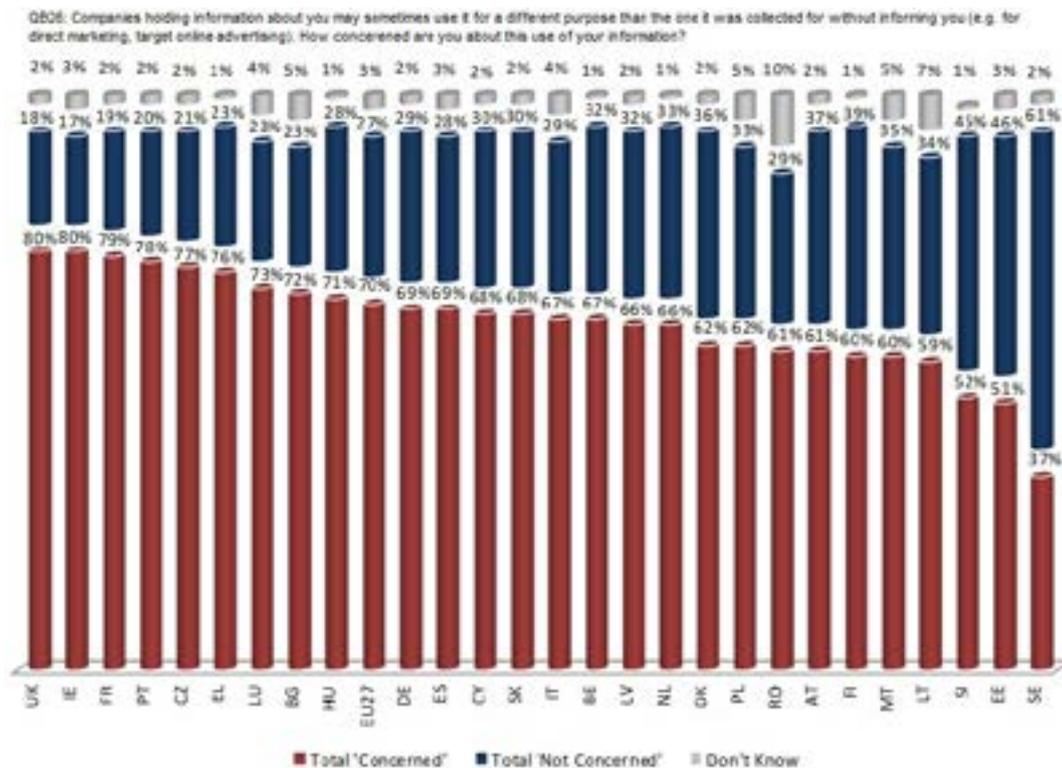
1. **One continent, one law:** The Regulation will establish a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws. Companies will deal with one law, not 28. The benefits are estimated at €2.3 billion per year.
2. **One-stop-shop:** The Regulation will establish a 'one-stop-shop' for businesses: companies will only have to deal with one single supervisory authority, not 28, making it simpler and cheaper for companies to do business in the EU.
3. **The same rules for all companies** – regardless of their establishment: Today European companies have to adhere to stricter standards than their competitors established outside the EU but also doing business on our Single Market. With the reform, companies based outside of Europe will have to apply the same rules. European regulators will be equipped with strong powers to enforce this: data protection authorities will be able to fine companies who do not comply with EU rules with up to 2% of their global annual turnover. European companies with strong procedures for protecting personal data will have a competitive advantage on a global scale at a time when the issue is becoming increasingly sensitive.



## What will the data protection reform do for citizens?

There is a clear need to close the growing rift between individuals and the companies that process their data:

- **Nine out of ten Europeans** (92%) say they are concerned about mobile apps collecting their data without their consent.
- **Seven Europeans out of ten** are concerned about the potential use that companies may make of the information disclosed.



Source: [Flash Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union, June 2011](#)

The data protection reform will strengthen citizens' rights and thereby help restore trust. Better data protection rules mean you can be more confident about how your personal data is treated, particularly online. The new rules will put citizens back in control of their data, notably through:

- **A right to be forgotten:** When you no longer want your data to be processed and there are no legitimate grounds for retaining it, the data will be deleted. This is about empowering individuals, not about erasing past events or restricting freedom of the press.
- **Easier access to your own data:** A right to data portability will make it easier for you to transfer your personal data between service providers.
- **Putting you in control:** When your consent is required to process your data, you must be asked to give it explicitly. It cannot be assumed. Saying nothing is not the same thing as saying yes. Businesses and organisations will also need to inform you without undue delay about data breaches that could adversely affect you.
- **Data protection first, not an afterthought:** 'Privacy by design' and 'privacy by default' will also become essential principles in EU data protection rules – this means that data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm – for example on social networks.

## What will the data protection reform do for SMEs?

The data protection reform is geared towards stimulating economic growth by cutting costs and red tape for European business, especially for small and medium enterprises (SMEs). First, by having one rule instead of 28 the EU's data protection reform will help SMEs break into new markets. Second, the Commission has proposed to exempt small and medium enterprises (SMEs) from several provisions of the Data Protection Regulation – whereas today's 1995 Data Protection Directive applies to all European companies, regardless of their size. Under the new rules, **SMEs will benefit from four reductions in red tape:**

- **Data Protection Officers:** SMEs are exempt from the obligation to appoint a data protection officer insofar as data processing is not their core business activity.
- **No more notifications:** Notifications to supervisory authorities are a formality and red tape that represents a cost for business of 130 million euro every year. The reform will scrap these entirely.
- **Every penny counts:** Where requests to access data are excessive or repetitive, SMEs will be able to charge a fee for providing access.
- **Impact Assessments:** SMEs will have no obligation to carry out an impact assessment unless there is a specific risk.

**The rules will also be flexible.** The EU rules will adequately and correctly take into account risk. We want to make sure that obligations are not imposed except where they are necessary to protect personal data: the baker on the corner will not be subject to the same rules as a (multinational) data processing specialist. In a number of cases, the obligations of data controllers and processors are calibrated to the size of the business and to the nature of the data being processed. For example, SMEs will not be fined for a first and non-intentional breach of the rules.

### Example

*A small advertising company wants to expand its activities from Spain to Italy. Its data processing activities will be subject to a separate set of rules in Italy and the company will have to deal with a new regulator. The costs of obtaining legal advice and adjusting business models in order to enter this new market may be prohibitive. For example, some Member States charge notification fees for processing data.*

*While the fee in Spain is zero, in Italy notification costs €150. The Commission's proposal will scrap all notification obligations and the costs associated with these. The aim of the data protection regulation is to remove obstacles to cross-border trade.*

## The European Parliament's LIBE committee confirms the main building blocks of the EU's data protection reform

In a speech on the data protection reform in March 2012, Vice-President Reding outlined the main building blocks of the reform ([SPEECH/12/200](#)). Two years later, all of these building blocks still form the heart of the data protection reform. This can be seen by comparing the [original Commission proposal](#) to the European Parliament text voted on today.

### Pillar one: One continent one law...

The European Parliament agrees that the new data protection law for the private and public sector should be a Regulation, and no longer a Directive.

## Commission Proposal

### Article 1: Subject matter and objectives

1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

## European Parliament Vote

### Article 1: Subject matter and objectives

1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

## ...with effective sanctions

The European Parliament agrees that national data protection authorities need to be able to impose effective sanctions in case of breach of the law. It has proposed strengthening the Commission's proposal by making sure that fines can go up to 5% of the annual worldwide turnover of a company (up from 2% in the Commission's proposal):

## Commission Proposal

### Article Article 79: Administrative sanctions

1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.  
  
(...)
6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

## European Parliament Vote

### Article 79: Administrative sanctions

1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article. The supervisory authorities shall co-operate with each other in accordance with Articles 46 and 57 to guarantee a harmonized level of sanctions within the Union. (...)
- 2a To anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following sanctions:
  - a. a warning in writing in cases of first and non-intentional non-compliance;
  - b. regular periodic data protection audits;
  - c. a fine up to 100 000 000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is greater.

## Pillar Two: Non-European companies will have to stick to European data protection law if they operate on the European market

For a strong European digital industry to compete globally we need a level-playing field. This is at the heart of the proposed EU data protection Regulation. Non-European companies, when offering services to European consumers, will have to apply the same rules and adhere to the same levels of protection of personal data. The reasoning is simple: if companies outside Europe want to take advantage of the European market with more than 500 million potential customers, then they have to play by the European rules. The European Parliament confirmed this important principle.

### Commission Proposal

#### Article 3: Territorial Scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
  - a. the offering of goods or services to such data subjects in the Union; or
  - b. the monitoring of their behaviour.

### European Parliament Vote

#### Article 3: Territorial Scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects in the Union by a controller or processor not established in the Union, where the processing activities are related to:
  - a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  - b. the monitoring of such data subjects.

## Pillar Three: The Right to be Forgotten/ The Right to Erasure

The right to be forgotten builds on already existing rules to better cope with data protection risks online. It is the individual who should be in the best position to protect the privacy of their data by choosing whether or not to provide it. It is therefore important to empower EU citizens, particularly teenagers, to be in control of their own identity online. If an individual no longer wants his or her personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system.

The right to be forgotten is of course not an absolute right. There are cases where there is a legitimate reason to keep data in a data base. The archives of a newspaper are a good example. It is clear that the right to be forgotten cannot amount to a right to re-write or erase history. Neither must the right to be forgotten take precedence over freedom of expression or freedom of the media. The right to be forgotten includes an explicit provision that ensures it does not encroach on the freedom of expression and information.

The European Parliament endorses all of these provisions. Furthermore, the compromise text reinforces the right to be forgotten by allowing citizens to obtain from third parties (to whom the data have been passed) the erasure of any links to, or copy or replication of that data. It also adds that citizens have the right to erasure where a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased.

## Commission Proposal

### Article 17: Right to be forgotten and to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
  - a. the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  - b. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
  - c. the data subject objects to the processing of personal data pursuant to Article 19;
  - d. the processing of the data does not comply with this Regulation for other reasons.
2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

## European Parliament Vote

### Article 17: Right to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, and to obtain from third parties the erasure of any links to, or copy or replication of that data, where one of the following grounds applies:
  - a. the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
  - b. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
  - c. the data subject objects to the processing of personal data pursuant to Article 19;
    - a. a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;
  - d. the data has been unlawfully processed.
- 1a The application of paragraph 1 shall be dependent upon the ability of the data controller to verify that the person requesting the erasure is the data subject.
2. Where the controller referred to in paragraph 1 has made the personal data public without a justification based on Article 6(1), it shall take all reasonable steps to have the data erased, including by third parties, without prejudice to Article 77. The controller shall inform the data subject, where possible, of the action taken by the relevant third parties.

## Pillar Four: A «One-stop-shop» for businesses and citizens

The European Parliament gave its support to the Commission's proposal to have a «one-stop-shop» for companies that operate in several EU countries and for consumers who want to complain against a company established in a country other than their own.

This is about simplification. Making it **simpler for businesses**: companies established and operating in several Member States will only have to deal with a single national data protection authority, in the country where they have their base: One interlocutor, not 28.

This also makes it **simpler for citizens** – who will only have to deal with the data protection authority in their member state, in their own language. They will no longer have to get on a plane to Dublin to plead their case, as the Austrian student Max Schrems has to do today with regards to Facebook.

## Commission Proposal

### Article 51: Competence

1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.
2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.
3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.

### Article 73: Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.

## European Parliament Vote

### Article 54a: Lead Authority

1. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, or where personal data of the residents of several Member States are processed, the supervisory authority of the main establishment of the controller or processor shall act as the lead authority responsible and be competent for the supervision of the processing activities of the controller or the processor in all Member States, in accordance with, without prejudice to the provisions of Chapter VII of this Regulation.

### Article 73: Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy and the consistency mechanism, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.

## For more information

Press pack: data protection reform:

[http://ec.europa.eu/justice/newsroom/data-protection/news/120125\\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm)

European Parliament – report on the Data Protection Regulation:

[http://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/libe/pr/922/922387/922387en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf)

Homepage of Vice-President Viviane Reding, EU Justice Commissioner:

[http://ec.europa.eu/commission\\_2010-2014/reding/](http://ec.europa.eu/commission_2010-2014/reding/)

Follow the Vice-President on Twitter: [@VivianeRedingEU](https://twitter.com/VivianeRedingEU)

## Press Contacts

Mina Andreeva (Spokesperson) - +32 229 13 82

Natasha Bertaud (Press Officer) - +32 2 296 74 56