



## Stronger data protection rules for Europe

Luxembourg, 15 June 2015

### Stronger data protection rules for Europe

More than 90% of Europeans are concerned about mobile apps collecting their data without their consent. Today, an important step was taken to finalise EU data protection rules to help restore that confidence.

Ministers in the Council reached a General Approach on the new data protection rules, confirming the approach taken in the Commission's proposal back in 2012 (see [IP/12/46](#)). The proposed rules received the backing of the European Parliament in March 2014 ([MEMO/14/186](#)).

### How do EU data protection rules contribute to boosting the Digital Single Market?

Completing the [Digital Single Market](#) is one of the top priorities of the European Commission. The internet and digital technologies are transforming our world. But existing barriers online mean citizens miss out on goods and services, internet companies and start-ups have their horizons limited, and businesses and governments cannot fully benefit from digital tools.

With a fully functioning Digital Single Market, we can create up to €415 billion in additional growth, hundreds of thousands of new jobs, and a vibrant knowledge-based society (see [IP/15/4919](#)).

But if citizens do not trust online services, they will not benefit from all the opportunities presented by technology. Confidence is paramount, but it is still far from a reality.

Data protection reform will address this lack of trust. It will strengthen citizen's rights such as the right to be forgotten, the right to data portability and the right to be informed of personal data breaches. The reform gives national regulators enforcement powers to ensure that these new rules are properly applied. They will be able to impose fines of up to 2% of a company's annual worldwide turnover.

### What are the main benefits of the EU Data Protection Reform?

The European Commission's proposals for a comprehensive reform of the EU's 1995 Data Protection Directive aim to strengthen privacy rights and boost Europe's digital economy. The Commission's proposals update and modernise the principles enshrined in the 1995 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. A clear definition of personal data will be established in the regulation to ensure harmonised implementation of the rules across the EU. The legislation is technologically neutral: this means that it will not go out of date, enabling innovation to continue to thrive under the new rules.

### What are the main benefits for citizens?

The data protection reform will strengthen citizens' rights and thereby help restore trust. Nine out of ten Europeans say they are concerned about mobile apps collecting their data without their consent; seven out of ten are concerned about the potential use that companies may make of the information disclosed.

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 provided that 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 (see section on right to be forgotten for more details).
- **Easier access to your own data:** Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way. Moreover, a **right to data portability** will make it easier for you to transfer your personal data between service providers.
- **The right to know when your data has been hacked:** For example, companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible (if feasible within 24 hours) so that users can take appropriate measures.
- **Data protection first, not an afterthought:** 'Data protection by design' and 'Data protection 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 or mobile apps.

### **What are the benefits for businesses?**

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 four main innovations:

- **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.
- **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; and easier, swifter and more efficient for citizens to get their personal data protected.
- **The same rules for all companies – regardless of where they are established:** Today European companies have to adhere to stricter standards than companies 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. We are creating a level-playing field. Moreover rules for **international transfers** of data are streamlined, through simplified approval of binding corporate rules. This will foster international trade while ensuring continuity of protection for personal data.
- **European regulators will be equipped with strong enforcement powers:** data protection authorities will be able to fine companies who do not comply with EU rules up to 2% of their global annual turnover. The European Parliament has even proposed to raise the possible sanctions to 5%.

### **What are the benefits 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 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 every year. The reform will scrap these entirely.
- **Every penny counts:** Where requests to access data are manifestly unfounded or excessive, 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. 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.

### **What is the "consistency mechanism" proposed in the EU data protection reform?**

Within a single market for data, identical rules on paper will not be enough. We have to ensure that the rules are interpreted and applied in the same way everywhere. That is why our reform introduces a [consistency mechanism](#) to streamline cooperation between the data protection authorities on issues with implications for all of Europe.

### **What is the one-stop shop and how does it work?**

At present, a company processing data in the EU has to deal with 28 national laws and with even more national and local regulators.

#### **- For businesses**

The regulation will create a regulatory **"one-stop shop"** for business: companies will only have to deal

with one supervisory authority, not 28.

The flaws of the present system were illustrated in the Google Street View case. The actions of a single company affected individuals in several Member States in the same way. Yet they prompted uncoordinated and divergent responses from national data protection authorities.

The one-stop shop will ensure legal certainty for businesses operating throughout the EU and bring benefits for individuals and data protection authorities.

Businesses will profit from faster decisions, from one single interlocutor (eliminating multiple contact points), and from less red tape. They will benefit from consistency of decisions where the same processing activity takes place in several Member States.

#### **- For citizens**

With the new rules, **individuals will always be able to go to their local data protection authority**. The aim is to improve the current system in which individuals living in one Member State have to lodge a complaint with a data protection authority of another Member State, where the company is based. At the moment, when a business is established in one Member State, only the Data Protection Authority of that Member State is competent, even if the business is processing data across Europe.

This makes it **simpler for citizens** – who will only have to deal with the data protection authority in their member state, in their own language. The proposal gives citizens the right to take a company processing their data to court in their home Member State. Everyone therefore have a right of administrative and judicial redress.

#### **How will the regulation work in practice?**

**Example 1:** a multinational company with several establishments in EU Member States has an online navigation and mapping system across Europe. This system collects images of all private and public buildings, and may also take pictures of individuals.

*With the current rules:*

The data protection safeguards upon data controllers vary substantially from one Member State to another. In one Member State, the deployment of this service led to a major public and political outcry, and some aspects of it were considered to be unlawful. The company then offered additional guarantees and safeguards to the individuals residing in that Member State after negotiation with the competent DPA, however the company refused to commit to offer the same additional guarantees to individuals in other Member States.

Currently, data controllers operating across borders need to spend time and money (for legal advice, and to prepare the required forms or documents) to comply with different, and sometimes contradictory, obligations.

*With the new rules:*

The new rules will establish a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws. Any company - regardless of whether it is established in the EU or not - will have to apply EU data protection law should they wish to offer their services in the EU.

**Example 2:** a small advertising company wants to expand its activities from France to Germany.

*With the current rules:*

Its data processing activities will be subject to a separate set of rules in Germany 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.

*With the new rules:*

The new data protection rules 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.

#### **How does the Council confirm the Commission's approach?**

The Council agrees upon many of the fundamental pillars of the [Commission's proposal](#):

#### **- One continent, one law**

The Council agrees that the new data protection law for the private and public sector should be a Regulation, and no longer a Directive. The Regulation will establish a single, pan-European law for data protection meaning that companies can simply deal with one law, not 28. The new rules will bring benefits of an estimated €2.3 billion per year.

## **Non-European companies will have to respect 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. 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 and its more than 500 million potential customers, then they have to play by the European rules.

The Council confirmed this important principle.

### **- Stronger rights for citizens, including the right to be forgotten**

The new rules will give citizens stronger rights, ensuring that citizens can be in control of their own personal data. The right to be forgotten builds on already existing rules to better cope with data protection risks online – in particular, the right to erasure. Citizens should be in a position to protect the privacy of their data by choosing whether or not to provide it. It is therefore important to empower EU individuals, 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 database. 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 legislation concerning the right to be forgotten **includes an explicit provision that ensures it does not encroach on the freedom of expression and information.**

The Council endorses the right to be forgotten.

### **- A "One-stop shop" for businesses and citizens**

The "one-stop shop" is about simplification:

- it makes it **simpler for businesses** established and operating in several Member States. They will only have to deal with a single national data protection authority, in the country where they have their main base: one interlocutor, not 28.

- it 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.

### **- Effective sanctions**

The Council agrees that national data protection authorities need to be able to impose effective sanctions in case of breach of the law. It has maintained the Commission's proposal that fines going up to €1 million, or, in case of a company, 2% of the annual worldwide turnover of that company can be applied.

**For more information:**

[IP/15/5176](#)

MEMO/15/5170

General public inquiries:

[Europe Direct](#) by phone [00 800 67 89 10 11](tel:0080067891011) or by [email](#)