

Brussels, 25 January 2012

Data protection reform: Frequently asked questions

Why do we need to reform the EU data protection rules?

With social networking sites, cloud computing, location-based services and smart cards, we leave digital traces with every move we make. We need a robust set of rules to make sure people's right to personal data protection – recognised by Article 8 of the EU's [Charter of Fundamental Rights](#) – is made effective.

The right to the protection of personal data is also explicitly stated in Article 16 of the [Treaty on the Functioning of the European Union](#). This gave the EU new responsibilities to protect personal data in all areas of EU law, including police and judicial cooperation.

In Europe, legislation on data protection has been in place since 1995. The [Data Protection Directive](#) guarantees an effective protection of the fundamental right to data protection. But differences in the way that each Member State implements the law have led to inconsistencies, which create complexity, legal uncertainty and administrative costs. This affects the trust and confidence of individuals and the competitiveness of the EU economy. The current rules also need modernising – they were introduced at a time when many of today's online services and the challenges they bring for data protection did not yet exist.

Are people concerned about how their personal data is used?

According to a recent Eurobarometer ([IP/11/742](#)), 70% of Europeans are concerned that their personal data may be misused. They are worried that companies may be passing on their data to other companies without their permission. Many users – especially young people – are not aware of **privacy policies** when they create a profile on a social networking site. When people surf the net, they are also not aware that their search data could be used by online advertisers. Therefore, privacy policies must be written in **clear, plain language**. Companies should be transparent about their privacy statements.

74% of Europeans think that disclosing personal data is increasingly part of modern life, but at the same time, 72% of Internet users are worried that they give away too much personal data, according to the Eurobarometer survey. They feel they are not in complete control of their data. This erodes their trust in online and other services and holds back the growth of the digital economy in general.

What is personal data?

Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address. The EU's Charter of Fundamental Rights says that everyone has the right to personal data protection in all aspects of life: at home, at work, whilst shopping, when receiving medical treatment, at a police station or on the Internet.

What will change under the proposals?

The Commission's proposals update and modernise the principles enshrined in the 1995 Data Protection Directive to guarantee privacy rights. They focus on: reinforcing individuals' rights, strengthening the EU internal market, ensuring a high level of data protection in all areas (including police and criminal justice cooperation) ensuring proper enforcement of the rules, facilitating international transfers of personal data and setting global data protection standards.

The proposed changes will give people more control over their personal data and make it easier to access it. They are designed to make sure that people's personal information is protected – no matter where it is sent, processed or stored – even outside the EU, as may often be the case on the internet.

How will the changes help improve personal data protection for individuals?

- A reinforced '**right to be forgotten**' will help people better manage data protection risks online: people will be able to delete their data if there are no legitimate reasons for retaining it.
- Wherever **consent** is required for data to be processed, it will have to be given **explicitly**, rather than assumed as is sometimes the case now. In addition, people will have easier **access to their own data** and be able to transfer personal data from one service provider to another more easily.
- There will be increased **responsibility and accountability** for those processing personal data: for example, companies and organisations must notify the national supervisory authority of serious **data breaches** as soon as possible (if feasible, within 24 hours)..
- People will be able to refer cases where their data has been breached or rules on data protection violated to the **data protection authority** in their country, even when their data is processed by an organisation based outside the EU.
- EU rules will apply even if personal data is **processed abroad** by companies that are active in the EU market. This will give people in the EU confidence that their data is still protected wherever it may be handled in the world.

How will they help businesses?

- By implementing a single set of rules on data protection, valid across the EU, thereby replacing the current patchwork of national rules in 27 Member States, increasing legal certainty and making it easier to trade and do business in Europe's Single Market. This will lead to a **net saving for companies** estimated to amount to €2.3 billion a year.
- By simplifying the regulatory environment by cutting red tape and abolishing formalities such as general notification requirements for companies, saving businesses around €130 million a year.
- Companies will only have to deal with a single national data protection authority in the EU country where they have their main base. At the moment, companies that are active throughout the EU must notify up to 27 different national authorities of data processing.
- The new rules will create advantages for EU companies in global competition, as they will be able to offer their customers assurances of strong data protection whilst operating in a simpler regulatory environment.

How will the rules be enforced?

Under the new proposals, there will be only one set of data protection rules and one responsible data protection authority – the national authority of the Member State in which the company has its main establishment. This '**one-stop-shop**' for data protection will greatly simplify the way businesses and citizens interact with data protection laws and give incentives to trade and invest cross-border in the internal market, as opposed to the current situation where businesses are supervised by a different authority in each Member State they are established.

Are there any penalties?

The Regulation provides for sanctions that are proportionate and dissuasive. For first offences, the national supervisory authorities may send a warning letter. For serious violations (such as processing sensitive data without an individual's consent or on any other legal grounds) supervisory authorities shall impose penalties up to €1 million or up to 2% of the global annual turnover of a company. The fines start out at €250,000 or up to 0.5% of turnover for less serious offences (a company charges a fee for requests from a user for his data) and move up to €500,000 or up to 1% for not supplying information to a user or for not having rectified data.

What about the economy?

A stronger, simpler and clearer data protection framework will encourage companies to get the most out of the Digital Single Market, fostering economic growth, innovation and job creation. This will especially help small and medium-sized enterprises.

For companies offering cloud services – remote storing and processing of data on computer servers – the trust in the EU's coherent regulatory regime will be a key asset and attractive point for investors.

Having the same rights across the EU will also boost individuals' confidence in the fact that the protection they get for their data will be equally strong, wherever their data is processed. This will improve trust in online shopping and services, helping to boost demand in the economy.

Both for citizens and business, these reforms will help break down barriers that are hindering Europe's response to the crisis.

What about the use of data by police and judicial authorities?

A new Directive will apply general data protection principles and rules to police and judicial cooperation in criminal matters. These rules will apply to both domestic processing and cross-border transfers of data. Having the same law in all EU Member States will make it easier for our police forces to work together in exchanging information. This will help fight crime more effectively. If people's personal data is shared in this way, they can be confident that it will be protected by the same law everywhere and that your fundamental right to data protection will be respected.

What are the next steps?

The Commission's proposals will now be passed on to the European Parliament and EU Member States (meeting in the Council of Ministers) for discussion. The Regulation will be enforceable in all Member States two years after it has been adopted. Member States will also have a period of two years to transpose the provisions in the Directive into national law.

Further information

Press pack: data protection reform:

http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

European Commission – data protection:

<http://ec.europa.eu/justice/data-protection>

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

<http://ec.europa.eu/reding>

Justice Directorate General Newsroom:

http://ec.europa.eu/justice/news/intro/news_intro_en.htm