



EU Data Protection Reform

What benefits for businesses in Europe?

Fact sheet | January 2016

Věra Jourová

Commissioner for Justice,
Consumers and Gender Equality



Directorate-General for
Justice and Consumers



The EU has reached political agreement on a [reform of data protection rules](#). Not only will the new set of rules bring citizens back in control of their personal data, it will also provide businesses with numerous benefits and opportunities. The reform will act as a key enabler of the [Digital Single Market](#), allowing European citizens and businesses to fully benefit from the digital economy.

What is the current situation? Why must it change?

Currently, businesses in the EU have to deal with 28 different data protection laws. This fragmentation is a costly administrative burden that makes it harder for many companies, particularly SMEs, to access new markets.

The reform will cut this red tape. For example, the new rules will do away with the current obligation for businesses to notify other national data protection authorities about the data they are processing, which currently costs businesses about **€130 million per year**.

What evidence is there?

Individuals and businesses expect data protection rules to be consistent and applied in a uniform manner across the EU. More than 90% of Europeans said they want the same data protection rights across the EU.

The data protection reform will help businesses regain consumers' trust to use their services. According to a 2015 Eurobarometer survey, eight out of 10 people feel that they do not have complete control of their personal data. Two-thirds of people are concerned they do not have complete control over their personal data online.

Businesses that fail to adequately protect individuals' personal data risk **losing their trust**. This trust, particularly in the online environment, is essential to encourage people to use new products and services.

Example 1: Allowing EU businesses to expand across borders

A small advertising company wants to expand its activities from France to Germany. Its data processing activities are currently 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 Data Protection Reform:

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. This will enable easier expansion of businesses across Europe.

Example 2: A level-playing field for EU and non-EU companies

An international company with several establishments in EU Member States has an online navigation and mapping system across Europe. 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 Data Protection Reform:

The new rules will establish one single 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. This levels the playing field for all businesses; it is about fair competition in a globalised world.

How will the new rules save money?

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**.

Example 3: Cutting costs

A chain of shops has its head office in France and franchised shops in 14 other EU countries. Each shop collects data relating to clients and transfers it to the head office in France for further processing.

With the current rules:

France's data protection laws apply to the processing done by head office, but individual shops still have to report to their national data protection authority, to confirm they are processing data in accordance with national laws in the country where they are located. This means the company's head office has to consult local lawyers for all its branches to ensure compliance with the law. The total costs arising from reporting requirements in all countries could be over €12,000.

With the Data Protection Reform:

The data protection law across all EU countries will be the same – one European Union – one law. This will eliminate the need to consult with local lawyers to ensure local compliance for the franchised shops. The result is direct cost savings and legal certainty.

How will the Data Protection Reform encourage innovation and use of big data?

According to some estimates, the value of European citizens' personal data could grow to nearly €1 trillion annually by 2020. The new EU rules will offer flexibility to businesses all while protecting individuals' fundamental rights.

'Data protection by design and by default' will become an essential principle. It will incentivise businesses to innovate and develop new ideas, methods, and technologies for security and protection of personal data. Businesses will have incentives to use techniques such as anonymisation (removing personally identifiable information), pseudonymisation (replacing personally identifiable material with artificial identifiers), and encryption (encoding messages so only those authorised can read it) to protect personal data. If personal data is fully anonymised, it is no longer personal data.

Personal data can be irreversibly anonymised by the business or, anonymised data can also be acquired for use in big data.

What is Big Data?

The term 'Big Data' refers to **large amounts of different types of data** produced from various types of sources, such as people, machines or sensors. This data could be climate information, satellite imagery, digital pictures and videos, transition records or GPS signals. **Big Data may involve personal data:** that is, any information relating to an individual, and 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.

Example 4: Driverless cars

The technology in driverless cars means more exchange of car data, including personal data. Data protection rules go hand in hand with innovative and progressive solutions. For example, in case of a crash, cars equipped with eCall emergency call system can automatically call the nearest emergency centre. This is an example of a workable and efficient solution in line with EU data protection principles. With the new rules, the function of eCall will become easier, simpler and more efficient in terms of data protection.

It is a data protection principle that when personal data is collected for one or more purposes it should not be further processed in a way that is incompatible with the original purposes. This does not prohibit processing for a different purpose or restrict 'raw data' for use in analytics. A key factor in deciding whether a new purpose is incompatible with the original purpose is whether it is fair. Fairness will consider factors such as; the effects on the privacy of individuals (e.g. specific and targeted decisions about identified persons) and whether an individual has a reasonable expectation that their personal data will be used in the new way. So in the example of the driverless cars, raw data can be used to analyse where the most accidents take place and how future accidents could be avoided. It can also be used to analyse traffic flows in order to reduce traffic jams.

Businesses should be able to anticipate and inform individuals of the potential uses and benefits of big data - even if the exact specifics of the analysis are not yet known. Businesses should also think whether the data can be anonymised for such future processing. This will allow raw data to be retained for big data, while protecting the rights of individuals.

Individuals will have more control. How will that help business?

The new right to **data portability** will allow individuals to move their personal data from one service provider to another. Start-ups and smaller companies will be able to access data markets dominated by digital giants and attract more consumers with privacy-friendly solutions. This will make the European economy more competitive.

Example 5: Benefits for individuals, benefits for businesses

A new small company wishes to enter the market offering an online social media sharing website. The market already has big players with a large market share. Under the current rules, each new customer will have to consider starting over again with the personal data they wish to provide to be established on the new website. This can be a disincentive for some people considering switching to the new business.

With the Data Protection Reform:

The right to data portability will make it easier for potential customers to transfer their personal data between service providers. This promotes competition and encourages new businesses in the marketplace.

What is the one-stop shop?

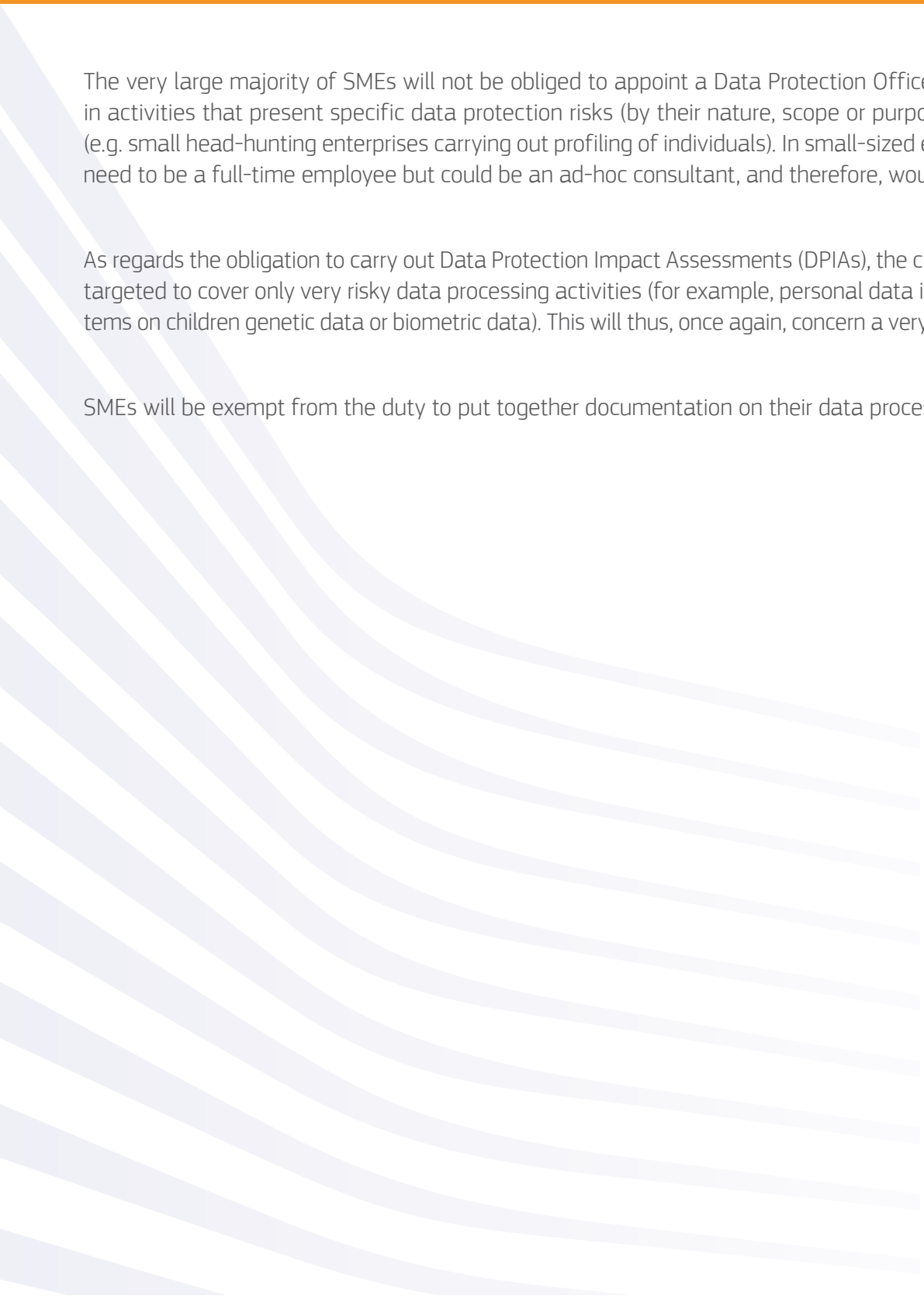
Within a single market for data, identical rules on paper are not enough. The rules must be applied in the same way everywhere. The 'one-stop-shop' will streamline cooperation between the data protection authorities on issues with implications for all of Europe. Companies will only have to deal with one authority, not 28.

It will ensure legal certainty for businesses. 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.

What are the benefits for smaller companies (SMEs)?

SMEs will fully benefit from a simplification of the regulatory environment. A special recital 11 in the Regulation makes the "think small first" dimension of the proposal particularly visible.

The specific situation of SMEs has been duly taken into account in our reform proposals, and care has been taken not to impose undue administrative burden upon them.



The very large majority of SMEs will not be obliged to appoint a Data Protection Officer. Only those engaged in activities that present specific data protection risks (by their nature, scope or purposes) will be concerned (e.g. small head-hunting enterprises carrying out profiling of individuals). In small-sized enterprises, this will not need to be a full-time employee but could be an ad-hoc consultant, and therefore, would be much less costly.

As regards the obligation to carry out Data Protection Impact Assessments (DPIAs), the criteria are very narrowly targeted to cover only very risky data processing activities (for example, personal data in large scale filing systems on children genetic data or biometric data). This will thus, once again, concern a very small portion of SMEs.

SMEs will be exempt from the duty to put together documentation on their data processing activities.