

Viviane Reding

Vice-President of the European Commission, EU Justice Commissioner

Building trust in the Digital Single Market: Reforming the EU's data protection rules

Check Against Delivery
Seul le texte prononcé fait foi
Es gilt das gesprochene Wort

Conference organised by the Industry Coalition for Data Protection - American Chamber of Commerce to the European Union

Brussels, 28 November 2011

Ladies and gentlemen,

I am delighted to be with you today to discuss the reform of the European Union data protection laws and its impact on businesses. The collection and storage of personal information are now essential elements of almost all companies' daily business – from insurance firms and banks to social media sites and search engines. Vast amounts of personal data are transferred and exchanged every day, across continents and around the globe in fractions of seconds.

To flourish, the digital economy needs trust. And trust is about the confidence consumers have when giving personal information online. It is all too easy for those who are in control of our data to keep it without enough guarantees. A lack of trust makes consumers hesitant to buy online and accept new digital services. Reliable and consistent rules are essential if we want the digital economy to grow. These rules should make citizens feel comfortable about using new technologies and services. We need a framework for privacy that protects consumers and encourages the digital economy. Privacy and data protection are also fundamental rights in Europe and part of the EU Treaties and the EU Charter of Fundamental Rights.

What are the challenges, then, that companies face under the current legal framework for data protection? What is hindering growth in the Digital Single Market? How can new European legislation overcome the current hurdles?

From a business perspective, I believe there are three main challenges.

Firstly, fragmented data protection rules make compliance costly for businesses.

At the moment, companies that operate in several Member States **must comply with different laws** and different decisions taken by data protection authorities in 27 Member States. A non-European company operating in the European Union has to abide by 27 different interpretations of the EU law on data protection. This is not helpful for businesses, and it is not helpful for citizens. The **administrative burden** associated with this fragmentation costs businesses an estimated **2.3 billion euros** per year.

The second main challenge is the effect of the current rules on the competitiveness of our Internal Market. The fragmentation, inconsistency and incoherence of 27 data protection laws make it difficult to sell or shop cross-border. They also create barriers to market entry, particularly for small and medium-sized companies.

The third challenge is that of uneven levels of protection for individuals across the EU.

The fragmentation of rules is not only an issue for businesses. Privacy concerns are amongst the most frequent reasons for people not buying goods and services online. More than two thirds (70%) of Europeans said they were concerned about how companies use this data and they think that they have only partial, if any, control of their own data. An overwhelming majority of 88% of Europeans believe that their personal data would be better protected if companies were obliged to have a Data Protection Officer. And more than 90% of Europeans want **the same data protection rights across the European Union**. These figures convey a strong message: Individuals don't always trust companies to keep their data safe. And they want the same level of protection wherever their data may be processed. Businesses understand that a high level of protection of privacy and personal data is a necessary condition to establishing a **relationship of trust** with their customers. The full potential of cloud computing, for example, can only be realised if it is seen as a trusted, reliable and safe way of storing data.

The existing European Union rules on data protection were adopted in 1995, when the full potential of the internet had not yet been realised. In 1993 the Internet carried only 1% of all telecommunicated information. By 2007, the figure was more than 97%. Although the basic principles and objectives of the 1995 Directive remain valid, these rules are not adapted to some new and emerging technologies and applications like social networks. We need to maintain both objectives of the original Directive, to ensure the free movement of personal data across the territory of the Union and to ensure a level of data protection. In a world of ever-increasing connectivity, **our fundamental right to data protection is being seriously tested.**

To address all of these challenges, the European Commission will propose a comprehensive data protection reform. To help businesses, I want to provide consistency and coherence. We need **legal certainty** and a **level-playing field** for all businesses that handle personal data of our citizens.

They need – the same as consumers – to have a '**one-stop-shop**' when it comes to data protection matters – one law and one single data protection authority for each business; that of the Member State in which they have their main establishment.

The authorities responsible for data protection must be provided with sufficient powers to enforce the law and they must have sufficient resources to exercise their powers.

At the same time, we must **strengthen coordination and cooperation** between national data protection authorities to make sure that the rules are **enforced consistently**. As a result, companies will be able to sell goods and services under the same data protection rules to 500 million people – a fantastic business opportunity!

To unleash the full potential of the Single Market, for growth, innovation, and job creation, we need to boost businesses in other ways. In addition to creating a level playing field for businesses in Europe, I want to drastically cut red tape by eliminating unnecessary costs and administrative burdens to create **a more business-friendly regulatory environment**. This means doing away with the general requirement to notify data processing to data protection authorities. Instead, we will focus on those requirements which enhance legal certainty and are of **real value**.

In a world where the free flow of data is imperative for our global businesses and physical boundaries are meaningless, we also need to rethink the way we transfer data. It seems odd to say that data held by a European company is adequately protected whilst it is inside the borders of the European Union, but not when it is transferred to a different part of that same company in Asia or South America, even when there are safeguards in place. In the internet age, data protection laws that apply only within a given territory do not reflect reality. Personal data is often collected in one place and processed in another. I want to improve the current system of binding corporate rules to make this type of exchange simpler and less burdensome and to cut down on the time and money invested by companies. I intend to propose a consistent and streamlined approval process with a **single point of contact** for companies amongst the data protection authorities. And once the binding corporate rules are approved by one data protection authority, I want them to be recognised by all the data protection authorities in the European Union. And there should be no need for additional national authorisation in case of further transfers.

Industry self-regulation has an important, complementary role to play in this reform. But let me be clear: self-regulation is not a fig leaf for non-compliance; self-regulation only works if there is strong, legally binding regulation in the first place. This is why I encourage codes of conduct for businesses in Europe provided that they are fully in line with European data protection law.

These are the ways in which the new rules will help businesses. But businesses also have responsibilities and I expect them to do their share by fully complying with data protection rules.

We need to increase the effectiveness of the fundamental right to the protection of personal data and **put individuals in control of their information**. And this is where business responsibility comes in. It is also in companies' interest to respect their customers' privacy and build up trust so people feel comfortable sharing their personal information.

Firstly, businesses must ensure **transparency** for individuals, who must be provided – in a simple and understandable language – with appropriate information about the processing of their data.

Internet users must be told which data is collected and for what purposes. They need to know how it might be used by third parties. They must know their rights and which authority to address if those rights are violated. They should be put in a position to make informed decisions about when to disclose their personal information.

Secondly, business responsibility means that whenever users give their agreement to the processing of their data, it has to be meaningful. In short, individuals should be well informed about privacy policies and their consent needs to be specific and given explicitly.

Thirdly, business responsibility means **better control** for individuals over their own data: that's why the reform will include **easier access** to one's own data. I want to give citizens better **data portability**. This means that if a user requests their information, it should be given to them in a widely used format which makes it simple to transfer elsewhere. I strongly believe that users should not be bound to one provider simply because it is inconvenient to move their information from one service to another. I also want to create a **right to be forgotten**, which will build on existing rules to better cope with privacy risks online. If an individual no longer wants their 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**.

Finally, business responsibility means that individuals are swiftly **informed** when their personal data is lost, stolen or breached. This year, we witnessed a massive security theft in online gaming services affecting millions of users around the world. This incident highlights why companies need to reinforce the security of the information they hold. Frequent data security breaches risk undermining consumers' trust in the digital economy. Our proposal will introduce a **general obligation** for data controllers to notify data breaches. In concrete terms, that means notifying data protection authorities and the individuals concerned when a data breach is discovered.

These are some of the main elements of the legislative package that I will propose early next year. We need to fix current weaknesses in the data protection framework and we will.

Everyone expects a **strong, consistent and future-proof framework for data protection, with consistent rules across all Member States and across all Union policies.** And I am determined to deliver.