

Viviane Reding

Vice-President of the European Commission, EU Justice Commissioner

**The EU Data Protection Reform 2012:
Making Europe the Standard Setter for
Modern Data Protection Rules in the
Digital Age**

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

Innovation Conference Digital, Life, Design

Munich, 22 January 2012

Ladies and gentlemen,

I am glad to be back at the DLD (Digital, Life, Design). Since its foundation in 2005, this one-of-a kind conference allows people from business, technology, media and politics to exchange dreams and experiences about the transformation of markets, culture and society through digital technologies and the Internet. This transformation calls for a special political contribution: a contribution which the European Commission is about to present. This will be a fundamental reform of the common European rules that govern the free movement of personal data in Europe's single market and the best possible protection of such data in the digital age.

You know more than anybody else: today, we live in a world of breathtaking possibilities. We can instantly send messages to people on another continent with the tap of a finger on a screen. We can instantly update our friends and family about the birth of a child or the latest holiday pictures. We can entrust our private data to a cloud service provider without knowing where and how this personal data will be stored and processed.

All these technological developments are welcome drivers of innovation, growth and jobs creation.

However, technological changes also bring about new regulatory challenges. The Internet, cloud computing, and mobile devices allow each of us to access our data everywhere and at any time. Our data races from Munich to Miami and to Hong Kong in fractions of a second. In this new data world, we all leave digital traces every moment, everywhere.

Does this matter? Do people care about how their data is protected? Do our rules need to be strengthened to give people more confidence and to make it easier for businesses to operate on Europe's digital single market?

The simple answer is: yes. In Europe, people do care. 72 percent of Europeans said in a recent poll that they are concerned about how companies use their personal data.

Businesses are worried too. Are their data secured in the cloud? Why do they need to face outdated rules? Why should they face 27 different regulations if they want to work on the whole of the EU continent? Why can't they have legal certainty when making the 500 million European citizens their potential customers?

We need to take these worries serious. We need to give an answer to citizens and businesses alike.

The current EU Data Protection laws date from 1995, from pre- Internet times.

In 1993, the Internet carried only 1% of all telecommunicated information. Today, the figure has risen to more than 97%.

Today personal data has become one of companies' most valuable assets: the market for analysis of large sets of data is growing by 40% per year worldwide. The Internet economy will continue to grow exponentially under one pre-condition: trust has to prevail.

Personal data is the currency of today's digital market. And like any currency it needs stability and trust. Only if consumers can 'trust' that their data is well protected, will they continue to entrust businesses and authorities with it, buy online, and accept new services – the new services, you in this audience, invent and develop. Reliable, consistently applied rules make data processing safer, cheaper and inspire users' confidence.

We can only imagine how technology will change our lives tomorrow. The details we do not know yet. That is why the new regulatory environment has to be future-proof, be technology-neutral. That's why 'privacy by design' has to become standard. It is

necessary to eliminate the current barriers in our digital market to allow inventors to move forward with ideas and seize the opportunities. We have to restore the trust of citizens and businesses in the new internet developments.

This week, I will present my proposals for a reform of the EU's data protection rules. But already today, I can outline to you the main characteristics of the new legislation which will make the Digital Single Market more accessible for both businesses and consumers, which will make Europe more competitive and which will become an international standard-setter in terms of modern data protection rules.

I will start out by briefly describing where we are today and then outline my vision of how the reform of the EU's data protection rules will reduce burdens on companies and better protect our citizens.

We currently have a real patchwork of data protection laws in Europe. Companies in Europe have to deal with 27 often conflicting data protection laws with data protection authorities that apply the law in different ways. Legal uncertainty and legal fragmentation are a burden for those companies – both small and large – that want to do business in Europe's Single Market. This fragmentation of data protection laws in Europe is not only an extra cost for business, but it is also holds back economic growth and innovation.

In addition, companies very often are burdened with red tape: cumbersome and costly notification requirements for processing data without bringing a feeling of safety to the citizens. On the contrary, privacy concerns are one of the most frequent reasons why people don't buy goods and services online.

This needs to be changed.

To address all these challenges, **I will propose this week a comprehensive reform of the data protection rules.** There will be two legislative texts to accomplish these goals:

First, a Regulation to enhance opportunities for companies that want to do business in the EU's internal market, while ensuring a high level of data protection for individuals.

Second, a Directive to ensure a smoother exchange of information between Member States' police and judicial authorities in the fight against serious crime while at the same time protecting people's fundamental right to data protection.

The new rules will **help businesses in three ways.**

Firstly, they create legal certainty. Secondly, they simplify the regulatory environment. And thirdly, they provide clear rules for international data transfers.

Let's look at the **first point** (legal certainty) in more detail. Instead of a patchwork of 27 different rules in 27 countries, there will be one law that will apply to all Member States in the European Union and to all companies which are offering their goods and services to consumers in the EU – even if their servers are based outside of the European Union.

The directly applicable Regulation will create a strong, clear and uniform legislative framework that will help unleash the potential of the Digital Single Market. It will do away with the fragmentation that will save businesses around 2.3 billion euros per year. The new Regulation will remove barriers to market entry – a factor of particular importance to small and medium-sized enterprises.

The savings will be achieved by a series of measures. First, by **simplifying the regulatory environment** and by **drastically cutting red tape.** No more general notification requirements. Instead, companies across Europe will be themselves

responsible and accountable for the protection of personal data in their business field. They will have to appoint a data protection officer – a requirement that businesses here in Germany are already very familiar with. The scrapping of the general notification rule alone brings about savings worth 130 million euro a year.

Second, there will be a regulatory '**one-stop-shop**' for businesses for all data protection matters. A company will have to comply with one law for the whole of the EU territory. It will only have to deal with one single data protection authority. It will be the data protection authority of the Member State in which the company has its main establishment.

It will not matter anymore which data protection authority deals with a case. All data protection authorities in whichever EU country will have the same **adequate tools and powers** to enforce EU law. Data protection authorities should be able to deal with complaints, carry out investigations, take binding decisions and **impose effective and dissuasive sanctions, whether the French, the Irish, the Romanian or the Bavarian data protection authority is in charge of a case**. This will give the legislation the necessary 'teeth' so the rules can be enforced.

Data protection authorities must be **independent** from political and economic interests and have **sufficient resources** to do their job. They will need to work closely together – especially in cross-border cases – to make sure that the rules are **enforced consistently** across Europe.

The **third element** to ease burdens on companies is to ensure **clear rules for international data transfers**. In a world where the free flow of data is fundamental to business models and physical boundaries are meaningless, we need to rethink the way we transfer data. It seems odd 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 need to take account of this global dimension. If they only focus on the activities of a company within a given country, they will not reflect reality.

Personal data can be collected in Berlin and processed in Bangalore. I therefore want to improve the current system of **binding corporate rules** to make these exchanges less burdensome and more secure. I will propose a consistent and streamlined approval process with a **single point of contact** for companies. And once the binding corporate rules are approved by one data protection authority, they will be recognised by all the data protection authorities in the European Union. There should be no need for additional national authorisation in case of further transfers.

As a result, companies will be able to sell goods and services under the same data protection rules to 500 million people – this can be a very interesting business opportunity!

This is what Europe can do to help the Digital Single Market take off. This is what Europe can do to work towards global standards.

But you, businesses handling personal data, have a critical role to play as well. If we want to give a real meaning to the fundamental right to the protection of personal data, if we want **individuals to be in control of their information**, then **business responsibility** has to come in. It makes good business sense to respect customers' privacy and build up trust so people feel secure sharing their personal information on your platform, on your service.

Here, **transparency** is the name of the game.

First, people need to be **informed** about the processing of their data in simple and clear language. Internet users must be told which data is collected, for what

purposes and how long it will be stored. 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. People need to be able to make an informed decision about what to disclose, when and to whom.

Second, whenever users give their agreement to the processing of their data, it has to be meaningful. In short, people's **consent** needs to be specific and given explicitly.

Thirdly, the reform will give individuals **better control** over their own data. I will include **easier access** to one's own data in the new rules. People must be able to easily take their data to another provider or have it deleted if they no longer want it to be used.

The new rules will provide for **data portability**. Another important way to give people control over their data: the **right to be forgotten**. I want to explicitly clarify that people shall have the right – and not only the ‘possibility’ – to withdraw their consent to the processing of the personal data they have given out themselves.

The Internet has an almost unlimited search and memory capacity. So even tiny scraps of personal information can have a huge impact, even years after they were shared or made public. The right to be forgotten will build on already existing rules to better cope with privacy 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. By the way, 81% of German citizens are worried they are no more in control of their personal data!

If an individual no longer wants his 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 and legally justified interest 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 of the total erasure of history. Neither must the right to be forgotten take precedence over freedom of expression or freedom of the media.

The new EU rules **will include explicit provisions that ensure the respect of freedom of expression** and information. After all, I have been the EU's Media Commissioner for many years, and I will never compromise in the fight for the fundamental rights of freedom of expression and freedom of the media. This also holds true in the field of data protection, which is another important fundamental right, but not an absolute one.

Finally, individuals must be swiftly **informed** when their personal data is lost, stolen or hacked. Whether user data gets stolen from an online gaming service, or credit card details are hacked on a firms' website: these security breaches affect millions of users around the world. There were recently many serious data breach incidents which highlight why companies need to reinforce the security of the information they hold. Frequent data security breaches risk undermining consumers' trust in the digital economy. I will therefore introduce a **general obligation for data controllers to notify data breaches**. Companies that suffer a data leak must inform the data protection authorities and the individuals concerned, and they must do so without undue delay. As a general rule, without undue delay means for me ‘within 24 hours’.

Ladies and gentlemen,

We will get a **strong, consistent and future-proof framework for data protection, applied consistently across all Member States and across all European Union policies**. We will make our data protection legislation fit for the digital age so it encourages innovation and development of new technologies and services.

We will adjust the rules to the reality of multinational businesses. And will adjust the rules to the reality of people's lives. Europeans live, work, shop and travel freely in the EU, so their data must travel freely as well: Freely and safely. The reform will become a golden opportunity for business: complying with the EU's laws on data protection will lead to a competitive advantage. European data protection rules will become a trademark people recognise and trust worldwide. I would welcome if everyone here put these new rules to life.

Allow me a last point.

For some time there has been a heated debate about the freedom of the Internet. According to the Fundamental Rights Charter, the freedom of expression and the freedom of information are basic rights for the European citizens. They are directly linked to a free internet which has thus to be preserved.

But those are not the only freedoms. The right of the creator to the content and fruits of his creation are equally important. This right also has to be preserved.

In order to achieve this, European policy aims at equilibrating the respect of both rights. Freedom of information and copyright must not be enemies; they are partners!

The protection of creators must never be used as a pretext to intervene in the freedom of the Internet. That is why for Europe, blocking the Internet is not an option.