SPEECH/

Viviane Reding

Member of the European Commission responsible for Information Society and Media

Securing personal data and fighting data breaches

EDPS-ENISA Seminar 'Responding to Data Breaches'

Brussels, 23 October 2009

Ladies and Gentlemen,

Let me begin by thanking our two hosts today, Mr Peter Hustinx and Mr Udo Helmbrecht, for giving me the opportunity to underline the importance of a strong European approach to the security of personal data.

I would also like to take the opportunity to thank Mr Hustinx and the staff of the European Data Protection Supervisor for their constructive role during the review of the telecom framework and express my hope that this cooperation will continue. Indeed I think that all parties involved in the legislative process – the European Parliament, the Council and the Commission – have valued highly their advice on privacy and data protection issues.

I warmly welcome Mr Helmbrecht in his new role at ENISA and am confident that he will lead the agency to the success we all need and expect.

And I must say the challenges that they will both face are very great. We have all heard examples of data breaches, the latest one only two weeks ago, a large European telecom provider found that hundreds of thousands of customer records had been stolen. And there are no doubt many more cases that we have not heard about. Yet if citizens have an underlying fear that their data may be lost or stolen they will not participate fully in the digital economy.

The Telecoms Reform has put the issue of mandatory notification of personal data breaches firmly on the European policy agenda. The reformed telecoms package, now awaiting final agreement, will establish rules concerning the prevention, management and reporting of data breaches in the electronic communications sector. As you are aware, the Commission will go a step further to extend the debate to generally applicable breach notification requirements and work on possible legislative solutions. This will be done in close consultation with the European Data Protection Supervisor and other stakeholders. I trust that today's seminar will be a valuable contribution to this endeavour.

I find it very reassuring that today's event is organised jointly by representatives of data protection and of Network and Information Security. This cooperation underlines the fact that privacy and information security are not in conflict with each other: **Without information security, protection of privacy and personal data is not possible**. Indeed, we must see challenges to personal data security in the broader context of the resilience of information and communication infrastructures.

A key principle of EU data protection law is that those who process personal data have to take the necessary security measures to counter the risks to this data.

With the telecoms reform, we are now strengthening and clarifying these rules: when a security breach happens, the operator will have **to inform** the authorities and those citizens who may face harm as a result of the loss of their personal data.

Furthermore, network operators must notify the competent national regulatory authority of a breach of security or loss of integrity that had a significant impact on the operation of networks or services.

In short: **Transparency and information will be the key new principles for dealing with breaches of data security.** I am grateful to the European Parliament which has helped to strengthen the legal responsibilities laid down by the new rules.

The new responsibilities for data security are a strong incentive for the managers of a company to make the necessary investments for the **prevention** of personal data breaches and for the resilience of network and information infrastructures. Here the European approach towards network and information security is clear: identify the responsibilities and provide the right (positive or negative) incentives for the stakeholders. **Those who profit from the information revolution must respond**

to the public policy responsibilities that come with it. It will of course not be possible to prevent **all** breaches. But operators must be prepared to minimise the risks by ensuring that **management** of incidents is planned and organized beforehand.

This regulatory response to data breaches stems from Europe's general vision of resilient ICT infrastructures and, even more important, of a "resilient society", where each actor accepts his share of the responsibility. **My vision is that security and data protection in the Information Society must be based on a comprehensive risk assessment and on management approaches, which take into account all hazards and threats, whether they come from cyber-attacks, from natural disruptions, or any other source.** I initiated this approach in 2006 and further strengthened it in 2009, in the broader context of the action plan on Critical Information Infrastructure Protection. We need to develop a risk management culture across society, also by providing and leveraging appropriate incentives to economic and social actors. These can be *negative* incentives, such as the obligation to notify breaches; or they can be *positive* incentives, such as exemption from liabilities for operators if they can demonstrate that they have put in place certain minimum security standards. I believe that there must be a clear allocation of responsibilities to help assess, manage and cushion risks.

However, technology and business are evolving very rapidly. New services and business models bring new types of risks to privacy and security. For example: social networking. It has, on the one hand, a strong potential for new forms of communication; but on the other hand it brings privacy concerns for internet users who put personal information online. We have seen this in Germany recently where sensitive data was illegally collected from one of the biggest German social networks, Schueler VZ. This clearly demonstrates that obligations to ensure protection against data breaches cannot be limited to electronic communications networks alone – but may need to be addressed in new EU rules which cover online services as well. The European Parliament is certainly right with calling on the Commission to study different legislative options to address this issue.

Our role is to understand what the public policy challenges are; identify the proper mechanisms to tackle them; and set the framework conditions - where necessary through sector-specific legislation.

The Commission has committed itself to reviewing Europe's general rules on protecting personal information, in the light of rapid technological development. At the same time, we will have to find agreement with our partners in other parts of the world, as the information society is becoming more and more global.

In 2010, the Commission intends to launch – as part of the ambitious European Digital Agenda advocated by President Barroso in his recent policy guidelines - a major initiative to modernise and strengthen network and information security policy in the EU. At the same time, I believe we should look at the emerging challenges for privacy and trust in the broad information society, with a particular emphasis on some of the outstanding issues which were raised during the discussions on the revision of the ePrivacy Directive, such as targeted advertising, convergence, the use of IP addresses and on-line identifiers.

It is absolutely essential that we find the right European responses to the concerns of European citizens about their fundamental rights to privacy and data protection. We cannot afford to lose their confidence in the information society, if we want the potential benefits of the digital economy to become reality. The support the Commission received for its proposals, aimed at the telecoms sector, was strong and encouraging. I look forward to today’s discussions, which I trust will provide an important initial contribution to the further process.

Thank you!