EDPS - ENISA Seminar "Responding to Data Breaches"
European Parliament, Brussels, 23 October 2009

Introductory remarks

Peter Hustinx
European Data Protection Supervisor

Ladies and gentlemen,

It is a pleasure to welcome you at this seminar, hosted jointly by the European Data Protection Supervisor (EDPS) and the European Network and Information Security Agency (ENISA), with the generous and highly appreciated support of the European Parliament.

I would like to extend a special welcome to Commissioner Viviane Reding who has accepted to deliver a keynote speech. The political responsibility for today's subject is in your portfolio, but your active participation here underscores both the importance of the subject and your personal commitment to handling it properly and effectively.

I would like to extend a special welcome also to Dr. Udo Helmbrecht who recently started as the new Executive Director at ENISA. Please accept our best wishes for your task in developing the Agency and we look forward to a productive cooperation.

Relevance of data breach

'Security breach' and 'security breach notification' have been "far-away" concepts for a number of years, but that is no longer the case.

A growing number of data breaches are reported by the press, not only in the UK, but also in several other member states. In fact, this may well be a structural problem of the European information society. Our daily activities are more and more dependent

on the good performance of ICT. They are digitized as personal data and becoming more vulnerable.

The development of data breach legislation has now also reached Europe - see revision of Directive 2002/58/EC (e-Privacy). Not only is there a new obligation to notify breaches, but the Commission will also consult ENISA, WP29 and EDPS during the development of technical implementing rules.

Initially, this obligation will only apply to the Telecom and ISP sector, but it is also relevant in a wider context – both on line and off line - and therefore also important in the context of the review of Directive 95/46/EC and part of a larger trend towards better data governance and accountability.

In short: increasing relevance and horizontal perspective – two reasons for EDPS to invest in preparatory actions.

This seminar is the second of a set of initiatives. The first event took place last April. It was organised under the umbrella of the London initiative for Data Protection Authorities only, as a first step to exchange experiences and best practices, but the results have been taken on board in the preparation of this seminar and they will also be used during its follow up.

Structure of seminar

The seminar is organised according to the "life cycle" of a breach: prevention, management, notification. The selection of these topics intends to give a clear message to data controllers:

- First, strengthen the security measures to protect personal data. Moreover, set up the appropriate mechanisms to demonstrate that appropriate measures have been effectively put in practice.

- Second, zero risk/incident is utopian, unrealistic. Objective is to provide legal and technical certainty to all stakeholders from data controller to individual, in order

to mitigate the risks to an acceptable level. If a data breach occurs, ensure that you have the mechanisms in place to manage and report the breach.

Managing and reporting data breach will involve the intervention of many, different actors. A bilateral dialogue between data controllers and DPA is not sufficient. Responsibility and accountability of each actor have to be identified and addressed.

This should be seen as a collaborative exercise, in which the resulting security level will only correspond with the weakest link of this chain of actors (insurance company, law enforcement, technical processors, certification authorities, auditors, etc.).

Role of EDPS

The EDPS is now - and will also be in the future – involved with data breaches in EU institutions from a supervision point of view:

- Breaches in large scale IT systems: two notifications so far.
- European Commission has introduced in its new implementing rules on the security of information systems, the obligation to notify a data breach to its Data Protection Officer.
- Revision of Directive 2002/58 could also trigger revision of Regulation 45/2001 and introduce a wider obligation to notify security incidents.

The EDPS has supported the revision of Directive 2002/58 and will - together with WP29 - advise on implementing rules and other initiatives in this area.

Further remarks

Managing and reporting data breaches are a relatively new phenomenon. The pillars of security breach notification have been constructed, but there is still a long way to go for all of us: data controllers, data protection authorities, and other stakeholders.

Most important at this stage, is to understand the interconnections and to develop the right mix of measures to ensure an effective strategy and the right incentives for better

data security. We all need to learn at this stage and we hope at EDPS that today's meeting will serve this purpose.

On a more practical level, let me remind you that this seminar is held under the "Chatham House Rule". This means that participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

Two speakers were not able to confirm their attendance. A third speaker had some last minute problems. However, we expect a lively interaction in all three sessions today.

Let me now invite Commissioner Reding to take the floor for her keynote speech.