Data breaches and EU institutions

EUROPEAN DATA PROTECTION SUPERVISOR

European Data Protection Supervisor

The EDPS and data breaches

An opinion in April 2008

A second opinion in January 2009

Article 4.5 of Direction 2009/136/EC amending Directive 2002/58/EC (Consultation of ENISA, WP29 and EDPS)

EUROPEAN DATA PROTECTION SUPERVISOR

European Data Protection Supervisor

"Responding to data breaches“ I

London initiative (DPAs) Seminar – 3 April 2009

Objective: share experiences and best practices among DPAs

Sources of notification: complaints, inspections, investigations and….the data controller

Role of DPAs: investigation following a breach is not always conducted by the DPA

Digital evidences: need for computer forensics protocol

"Responding to data breaches“ II

EDPS/ENISA Seminar - 23 October 2009

Life cycle of a data breach:

- Prevention (standards and recognition, security measures, “experience feedback” and register, etc.)

- Management (zero risk, information sharing, CERT for EU institutions, evidences,)

- Notification (format, communication channel, law enforcement, the issue of the “when” and to “whom”,)

Regulation 45/2001…..

Article 35

Security

1. The Community institutions and bodies shall take appropriate technical and organisational measures to safeguard the secure use of the telecommunications networks and terminal equipment, if necessary in conjunction with the providers of publicly available telecommunications services or the providers of public telecommunications networks. Having regard to the state of the art and the cost of their implementation, These measures shall ensure a level of security appropriate to the risk presented.

2. In the event of any particular risk of a breach of the security of the network and terminal equipment, the Community institution or body concerned shall inform users of the existence of that risk and of any possible remedies and alternative means of communication.

A pioneer EU institution….

August 2006: Commission Decision C(2006) 3602 on the security of information system, (article 7.1)

" When a security incident covered by this Decision is detected in a Directorate-General, the Local Information Security Officer (LISO) shall be informed. LISOs shall at once inform their superiors and the Security Directorate."

May 2009: implementing rules for C(2006) 3602

" In the case of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data processed by Commission information systems, the system owner needs to inform the Data Protection Officer " (point 8.8.1) page 27.

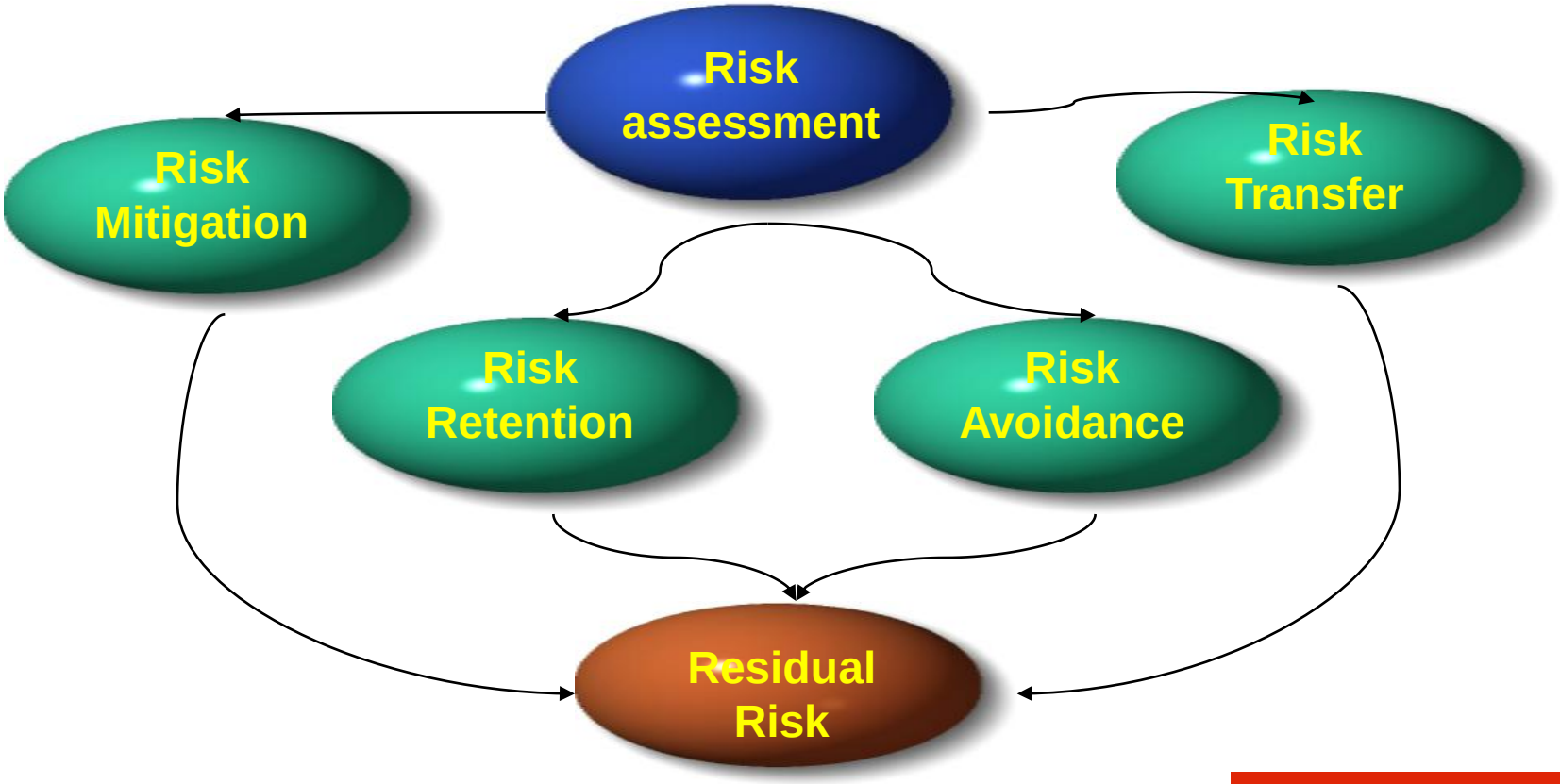
Security Incident or personal data breach or both....

Regulation 460/2004, Article 4(c) "network and information security" means the ability of a network or an information system to resist, at a given level of confidence, *accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems*;

A convergence which will requests organisational measures

The risk management approach and…

Reviewed Directive 2002/58 Article 4.1: "*Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented*. "



…The challenge of the residual risk

Article 4.3: "Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it. "

Who is going to be responsible for defining its level ?

How to communicate it ?

EUROPEAN DATA PROTECTION SUPERVISOR

European Data Protection Supervisor