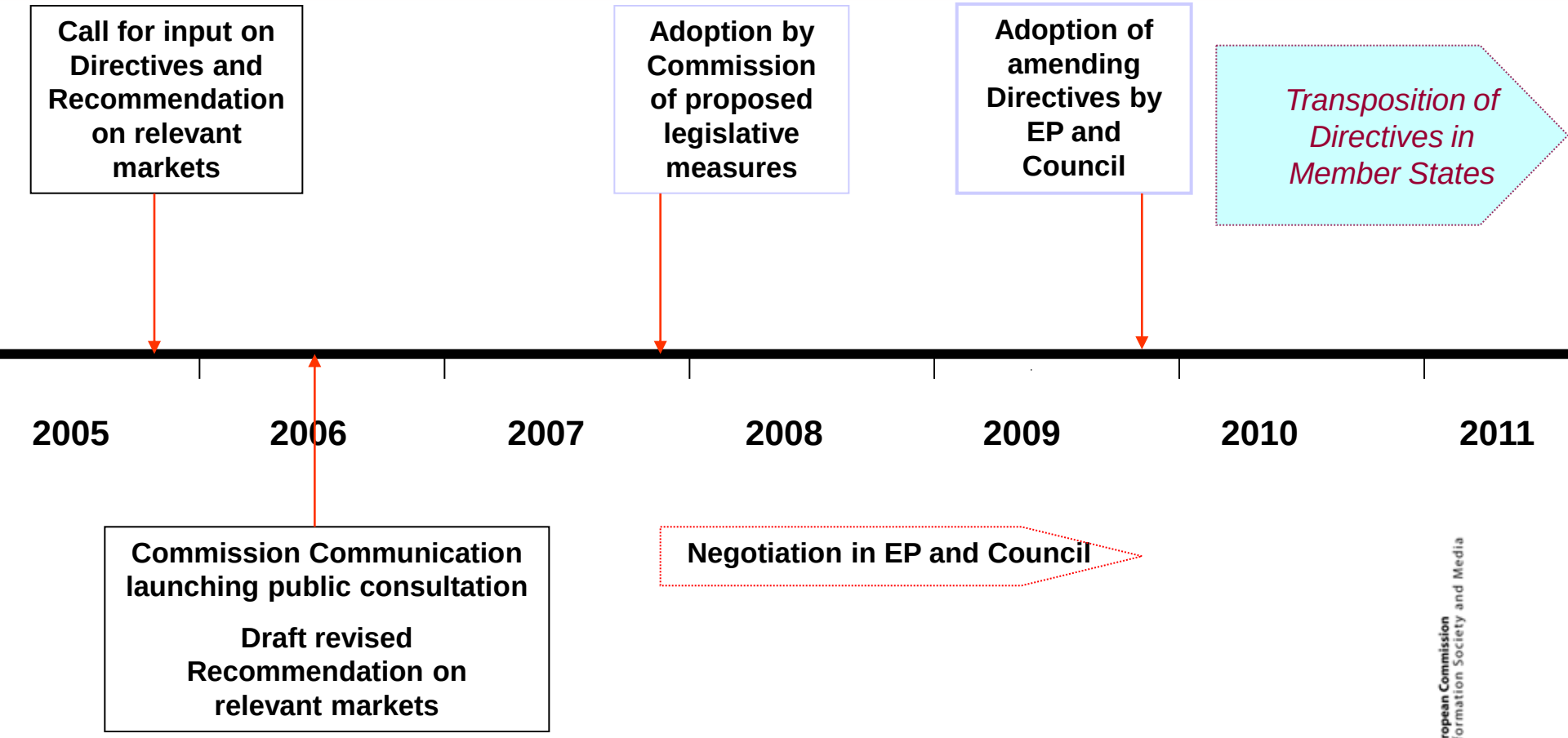
Reporting of Data Breaches

Achim Klabunde
European Commission
DG information Society and Media
Electronic Communications Policy

Overview

- Context
- Relevant provisions
- Tasks
- Procedure

Personal data breach notifications
Context: Telecom Reform Timeline



European Commission
Information Society and Media

Personal data breach notification: Motivation

(Recital 61):

> A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the subscriber or individual concerned. (…) A breach should be considered as adversely affecting the data or privacy of a subscriber or individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision of publicly available communications services in the Community. (…)

Personal data breach notification: Expected effect

> (…) the expected positive side-effect (…) [*of breach notification*] requirements would be an incentive for operators to "take security seriously" - operators, afraid of potential negative publicity (…) would increase their security budgets.

Impact assessment (SEC 2007 1472)

Personal data breach notification: Survey results

(…) when asked whether they would like to be informed if their personal data was lost, stolen or altered, 64% of Europeans responded positively "in all circumstances" and further 14% "in case there was a risk of a financial loss". Only 12% indicated that they would not like to be informed.

Impact assessment (SEC 2007 1472),

Data from Eurobarometer surveys

Commission commitment on personal data breaches

Declaration to the European Parliament

"… the obligation for providers of publicly available electronic communications services to notify personal data breaches makes it appropriate to extend the debate to generally applicable breach notification requirements …"

"The Commission will, therefore, without delay initiate the appropriate preparatory work, … the Commission will consult with the Article 29 Working Party and the European Data Protection Supervisor … ."

Personal data breach notifications in electronic communications: Relevant Changes to ePrivacy Directive

Changes in Directive 2002/58/EC:

Article 1 – Scope and aim

Article 2 – Definitions

Article 3 – Services concerned

Article 4 – Security of processing

Article 14a – Committee procedure

Article 15 – Application of 95/46

Article 15a – Implementation and enforcement

ePrivacy Directive amendments 1/4

Article 1: Scope and aim

- confidentiality

Article 2: Definitions

- Personal data breach

Article 3: Services concerned

- "Including networks supporting data collection and identification devices"

ePrivacy Directive amendments 2/4

Article 4: Security of processing

- List of minimum security measures for personal data
- notification of personal data breaches to authority and citizens
- national authority guidelines
- inventory of breaches
- harmonisation by Commission measures

ePrivacy Directive amendments 3/4

Article 14a: Committee procedure

- Communication Committee will assist Commission (Art 22 of Framework Directive 2002/21/EC)
- Regulatory procedure with scrutiny

Article 15: Application of 95/46

- Procedures for access to personal data and information to competent authority

ePrivacy Directive amendments 4/4

New Article 15a

- Effective, proportionate and dissuasive penalties for infringements
- NRA power to order the cessation of the infringements
- NRA investigative powers and resources, including the power to obtain any relevant information
- NRA may adopt measures to ensure effective cross-border cooperation

Commission follow-up tasks

- Support national transposition process
- Technical implementing measures for harmonisation
- Provide guidance to national authorities
- Prepare debate on broader personal data breach notifications

Technical implementing measures Procedure

- New procedure under Lisbon Treaty
- Preparation by Commission
- Stakeholder involvement
- Consultation of
  - ENISA
  - EDPS
  - Article 29 WP on Data Protection
- Communications Committee
- Parliamentary Scrutiny
- Adoption by Commission

Technical implementing measures Input

- National measures in Member States
- EDPS/ENISA Workshops
- ENISA Study
- Art 29 survey
- Own research
- Published research

Technical implementing measures: Encryption?

(Recital 64)

(…) due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. (…)

Technical implementing measures Elements

- "Best available technical and economic means of implementation"
- Effective technical protection measures
- Proportionate
- Effect on the investigation of a breach

A data breach has been detected …

- Who ?
- What ?
- Whom ?
- When ?
- How ?
- Why?

Notification rules in ePrivacy:

- Who must notify?
  - The data controller
- What must be notified?
  - nature of the data breach
  - contact points
  - recommended measures
  - Consequences of the breach
  - measures taken
- Whom to notify ?
  - Authority
  - subscriber or individual concerned
- When ?
  - Without undue delay
- How ?
  - notification format, procedure, circumstances – technical implementing measures
  - inventory of breaches
- Why?
  - Adverse effects on privacy and personal data
  - compliance audit
  - learn to avoid future events

Thank you