

# Data Breach Notifications

## ENISA's previous and current work

NIS Summer School

Hersonissos, 30<sup>th</sup> June 2011

# DBN study

## ★ Policy context

- ★ Review of ePrivacy Directive (2002/58/EC)
- ★ Article 4

## ★ Objectives

- ★ Survey/stock taking
- ★ Analysis

- Views and opinions
- Understanding of “personal data”
- Existing other fields models
- Differences between sectors

## ★ Conclusions / recommendations

- Undue delay
- Notification of citizens (if and what)
- Need of audit mechanisms
- Benefits from pan-EU approach

## ★ Methodology

- ★ Questionnaires
- ★ Interviews

# Data Protection Authorities

- ★ Definitions
- ★ Determination of breach
- ★ Determination of risk
- ★ Compliance
  - ★ Enforcement, audits, fines

# DPAs – notification and handling

- ★ Few formal procedures, some guidelines
- ★ Notification triggers – no formal criteria
- ★ Content of notification – not formalized
- ★ Means of communications – wide range
- ★ Undue delay

# DPAs – conclusions

- ★ Majority of DPAs support DBN
- ★ Concerns – budget, workload
- ★ Need for prioritization
- ★ Need for effective process
- ★ At the time of collecting data, any DPAs in “wait and see” mode

# Companies

- ★ General views
- ★ Sources, triggers, content of notifications
- ★ Notifications to Data Subjects
- ★ Relationship with regulators
- ★ Role of DPAs

# Companies – questionnaire

- ★ Best interest of customers, wish to be prepared
- ★ Some operators already issue notifications
- ★ DBN is a duty of
  - ★ 25% - regulatory affairs department,
  - ★ 50% - data protection officer
  - ★ 25% - mix of IT, security, legal, compliance
- ★ Few breaches – 2-5 in last two years
- ★ Notification of data subject – yes, but not always
- ★ “Seasonality” of data breaches
- ★ Distinctions
  - ★ IT-based / not IT-based
  - ★ Customer data / employee data

# Companies – notification and handling

- ★ Definitions – no challenges
- ★ Sources: other data processors, customers, media
- ★ Triggering events
  - ★ Impact on the brand
  - ★ Impact on the customer
  - ★ Case by case basis
  - ★ Few clear policies and criteria
  - ★ Faster notification if mandatory
- ★ Notifications to Regulatory Authorities
  - ★ Background facts
  - ★ Steps taken
  - ★ Communication with data subjects
  - ★ Steps taken for the future
- ★ Notifications to Data Subjects

# Companies – relationship with regulators

- ★ Need for clear guidelines
- ★ Expectations for constructive support, not fines
- ★ Cases of very good cooperation (brochures, web info, workshops)
- ★ Cases of bad cooperation (only sanctions)
- ★ Size of operator affects relationship

# Companies – conclusions

- ★ Satisfaction of current standards across EU
- ★ Triggers for DBN not clearly defined
- ★ Good awareness of legislation regarding DBN
- ★ High level of confidence in internal procedures
- ★ Concerns about being the only sector obliged for DBN
- ★ Assistance in interpretation of legislation needed

# Divergences DPAs / Operators

- ★ Undue delay
  - ★ Regulators: short deadline
  - ★ Operators: identifying and solving the problem as first priority
- ★ Traffic monitoring
  - ★ Regulators: privacy risk
  - ★ Operators: requested to analyze traffic by customers
- ★ Content of notifications
  - ★ Regulators: all necessary information
  - ★ Operators: information not affecting relations with customers
- ★ Audits and role of DPAs
  - ★ Regulators: performing audits is DPAs duty
  - ★ Operators: DPAs should provide guidance and support

# Conclusions

- ★ DBN will not contribute in data protection in short term
- ★ DBN will ensure information is given and actions taken
- ★ Problems are not country-specific (cloud!)
- ★ DPAs need resources
- ★ **Industry needs clear guidelines**

# Workshop 24<sup>th</sup> January 2011

## ★ Identified existing issues

- ★ Lack of unified approach among sectors and MSs
- ★ Different understanding of a breach
- ★ Lack of guidelines and best practices on:
  - Format of notifications
  - Technical measures for data protection
  - Follow-up actions after notifications
- ★ Economics of notifications
- ★ Cases of exemption from notifications

# Work programme 2011

- ★ Study: *Technological guidelines for the implementation of the Art. 4*
- ★ Method: Experts Group
  - ★ European Commission
  - ★ EDPS
  - ★ DPAs
  - ★ Industry
- ★ Expected outcome: October 2011

# Study 2010 – areas

## ★ Circumstances

- ★ Definition: ePrivacy Directive
- ★ Relation with security incident
- ★ Triggers of notifications to individuals

## ★ Procedures

- ★ Procedure of processing a breach [flowchart]
- ★ Undue delay
- ★ Channels of communications
- ★ Risk assessment of a breach [impact]
- ★ Cross-border cases
- ★ Collecting evidence
- ★ Internal procedure [roles, responsibilities]

## ★ Format

- ★ Content of notification
- ★ Technical format

## ★ Technological protection measures [exemptions]

- ★ Assessment of a risk of the occurrence of a breach
- ★ Residual risk
- ★ Unintelligible data disclosure
- ★ Organisational aspects

## ★ Inventory of breaches

- ★ Access protection
- ★ Content of inventory

# Thank you!

Sławomir Górniak,  
European Network and Information Security Agency  
Technical Competence Department

Email: [Slawomir.Gorniak@enisa.europa.eu](mailto:Slawomir.Gorniak@enisa.europa.eu)

## ★References

★<http://www.enisa.europa.eu/act/it/dbn>