GRAF & PITKOWITZ
RECHTSANWÄLTE GMBH

Dr. Ferdinand Graf

Responding to a Data Breach >> the European Perspective

ABA Data Breach Panel
August 9, 2013
San Francisco

I. General

- **European Definition of a Data Breach**
  - "a breach of security leading to the **accidental** or **unlawful** destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed"

- **European Examples**
  - HM Revenues and Customs (governmental entity in the UK) in 2007
  - Sony (UK) in 2011;
  - Nokia (Finland) in 2011

II. Current Legal Framework: EU

- **Regulations:** directly applicable and legally binding in every EU member state; to be applied by all member state courts

- **Directives:** framework legislation; EU member states have – limited - discretion when implementing a directive into national law

  – **Example**: current Data Protection Directive 95/46/EC ("*Data Protection Directive*") protects natural persons only; Austria provides for data protection both for natural and legal persons

- **Data Protection Authority ("*DPA*"):** No central European data protection authority; national authorities execute EU and local law provisions

III. Current Legal Framework: EU

- **Directive 95/46/EC ("*Data Protection Directive*")**
  - First community wide data protection framework
  - Defines data subjects' rights
  - Requires establishment of national DPAs
  - No rules on data breach notification

- **Directive 2002/58/EC as amended by Directive 2009/136/EC ("*ePrivacy directive*")**
  - Limited scope: only applicable to the electronic communication sector
  - For the first time rules on data breach notification >> obligatory notice to national DPA and affected data subject

IV. Current Legal Framework: Austria

- **Data Protection Act 2000 (*Datenschutzgesetz* 2000, "DSG")**

  – Independent DPA (to be newly structured under 2013 amendment); decisions can be appealed to state courts
  – Protection of data as a constitutional right
  – Applies to natural and legal persons; also takes effect *inter privatos*
  – Data transfers outside the European Economic Area (EU, Norway, Liechtenstein, Iceland) require prior approval by the Austrian DPA but exemptions apply to: US Safe Harbor, EU Standard Contractual Clauses and Binding Corporate Rules
  – Penalties up to EUR 25,000 which are very low compared to other EU member states

V. Current Legal Framework: Austria

- **Data Breach Notification Duty**

  – Section 24 para 2a DSG:

  "If the controller learns that data from his data application are **systematically** and **seriously misused** and the data subject may suffer **damages**, he shall immediately inform the data subject in an appropriate manner. Such obligation does not exist if the information – taking into consideration that only minor damage to the data subject is likely and the cost of the information to all persons concerned - would require an **inappropriate effort**."

VI. Current Legal Framework: Austria

- **Data Breach Notification Duty**
  - Enacted in 2010; Austria was the second EU member state establishing a data breach notification duty
  - All personal data is covered (not limited to sensitive data)
  - Limited to “systematic“ and “serious” misuse of data – no definitions of these terms in the DSG
  - Data controller must inform the affected data subject in an “appropriate way”; no obligation to inform the DPA
  - Penalties of up to EUR 10,000 for breach

VII. Current Legal Framework: Other Member States

- **Germany**
  - General breach notification duty, but limited to “special” data
  - Obligation to inform DPA and data subjects
  - Penalties of up to EUR 300,000
- **UK**
  - Breach notification duty limited to electronic communication sector
  - Recommendation of the DPA to report “serious breaches” to DPA
  - Penalties of up to GBP 500,000
- **France**
  - Breach notification duty limited to electronic communication sector
  - Penalties of up to EUR 300,000 for natural persons and up to EUR 1,500,000 for legal persons

VIII. Future Legal Framework: EU

- **Proposed New EU Data Protection Regulation**
  - Presented by the European Commission on January 25, 2012

- **Extended Territorial Scope of the New Regulation**
  - Data processing of controllers established **within** the EU
  - Data processing of controllers established **outside** the EU: Processed data of data subjects residing in the EU in connection with the offering of goods or services or the monitoring of their behavior

IX. Future Legal Framework: EU

- **Data Breach Notification Duty**
  - Within 24 hours: Notification to DPA and, in case of adverse effects, the affected data subject
  - Duty to recommend measures to mitigate the possible damage

- **Significantly Increased Penalties**
  - Fines up to EUR 1,000,000 or 2% of an enterprise's annual turnover
  - Fines shall be "effective, proportionate and persuasive"

X. Action Items

- **How to Guard Against a Data Breach**
  - Establishing physical and electronic security systems
  - Limiting data access to certain employees and companies
  - Implementing joint security policies
  - Encrypting and storing of sensitive data on separate databases
  - Contractual risk transfer to third parties and insurances

XI. Action Items

- **How to Respond to a Data Breach**
  - Joint development of emergency plans with legal, public relations, IT, and crisis management departments
  - Designate a data protection officer (required for companies employing more than 250 persons) or other contact persons where information can be obtained
  - Establishing sufficient resources to promptly inform authorities and data subjects
  - Determination of notification requirements