Security as a key element of Privacy and Data Protection

Dr. Udo Helmbrecht, Executive Director, ENISA

Madrid 24 May 2010

ENISA Role

★ Rationale

ENISA is an Agency for network and information security, which pro-actively advises the European Commission, the European Parliament and the Council and promotes co-operation among governments, businesses and NGOs to the benefit of citizens in the European Union.

★ ENISA was established in March 2004

- ★ to ensure a high and effective level of network and information security within the Community;
- ★ to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union,
- ★ thus contributing to the smooth functioning of the Internal Market.

ENISA in the area of Privacy

Previous work (examples)

- "Cloud computing"
- "Web 2.0 Security and Privacy"
- "Technology-induced challenges in Privacy & Data Protection in Europe"
- "Privacy Features of European eID Card Specifications"

2010

- Work Programme: Stock taking of authentication and privacy mechanisms in view of Art. 4 of the ePrivacy directive
- A major initiative relevant to network and information security is the recently adopted review of the EU electronic communications regulatory framework and in particular, the new provisions of articles 13a and 13b of the Framework Directive[1] and article 4 of the e-Privacy Directive[2].
- These provisions aim at strengthening obligations for operators to ensure security and integrity of their networks and services, and to notify breaches of security, integrity and personal data to competent national authorities. ENISA is called upon supporting the Commission and the Member States by providing its expertise in developing appropriate implementing measures.

[1] Directive 2009/140/EC
[2] Directive 2002/58/EC

Cloud computing (2009)

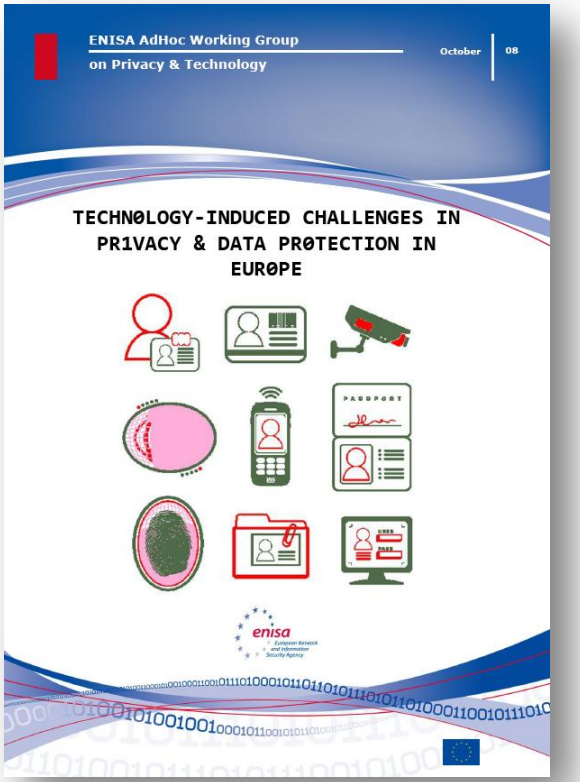
- "Cloud computing: Benefits, risks and recommendation for information security"
- We recommend that the European Commission study or clarify the following:
  - certain issues related to the Data Protection Directive and the recommendations of the Article 29 Data Protection Working Party;
  - cloud providers obligation to notify their customers of data security breaches;
  - how the liability exemptions for intermediaries arising from the eCommerce Directive articles 12-15 apply to cloud providers;
  - how best to support the minimum data protection standards

Web 2.0 Security and Privacy (2008)

- Web 2.0 has brought a sea-change in the way knowledge and information is managed.
- Vulnerabilities of Web 2.0 identified in this paper are:
  - identity theft,
  - extortion via botnets,
  - financial loss,
  - loss of privacy
  - and damage to reputation
- Addressing the risks:
  - Technology
  - Governement Policy
  - Research
  - Awareness Raising
  - Standardisation
  - Provider measures
  - Secure development initiatives

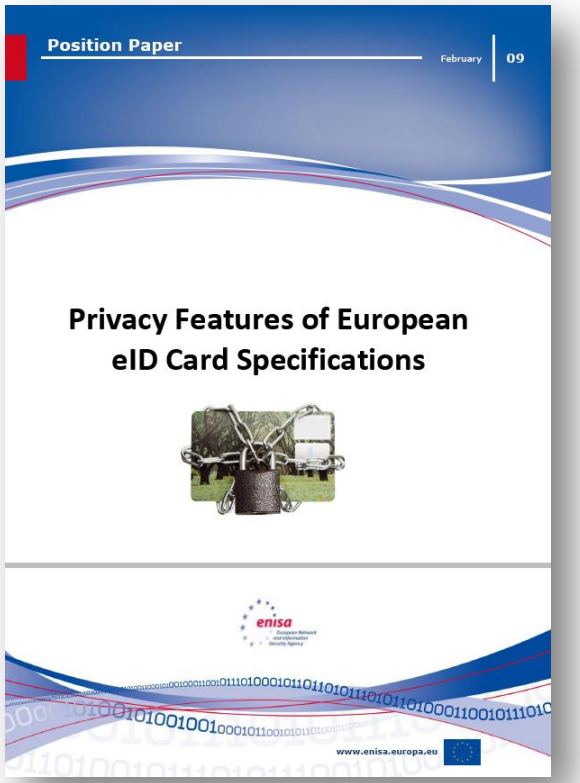
ENISA Ad Hoc Working Group on Privacy & Technology (2008)

- ★ Technology-induced challenges in Privacy & Data Protection in Europe
- ★ Recommendations (examples)
  - ★ e-inclusion programmes
  - ★ User assistance tools
  - ★ Identity management



Privacy Features of European eID Card Specifications (2009)

- The aim of this paper is to allow easy comparison between privacy features offered by European eID card specifications and thereby to facilitate identification of best practice.
- This paper gives a brief overview of the range of privacy features available,
- The main focus of this paper is to map the implementation of these features in the various national ID card schemes.



Art. 4 – ePrivacy directive

- "Citizens' Rights" Directive (Directive 2009/136/EC) Amendments to Directive 2002/58/EC - ePrivacy Directive. This is part of the Telecom Reform package
- Article 4. "Security of processing", is of relevance due to a new obligation on “security breach notification” and the consulting role of ENISA to the Commission on adoption of certain procedures.
- Art 4.(3)
  In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.

Art. 4 – 2011

- Work Programme 2011 will include the tasks of ENISA according to Art. 4 (5)

Art. 4 (5)
In order to ensure consistency in implementation the Commission may, following consultation with (among others) ENISA, adopt:

- **technical implementing measures** concerning the circumstances,
- **format and procedures** applicable to the information and
- **notification requirements**