How Data Privacy affects Applications and Databases

Dirk De Maeyer,
KPMG Advisory

OWASP

Contents

- Introduction
- Where do Application Security and Data Privacy meet ?
- Data Privacy - principles
- Expanding Information Security within Project/Application Development lifecycle

Introduction

- EU Directives
- Belgian laws
- Personal data
- Sensitive personal data

Legislation: EU Directives

- Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (**Data Privacy Directive**)

- Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (**Directive on electronic commerce**)

- Directive 2002/58/EC of 12 July 2002 on processing of personal data and the protection of privacy in the electronic communications sector (**Directive on privacy and electronic communications**)

Legislation: Belgium

- "Wet tot **bescherming van de persoonlijke levenssfeer** ten opzichte van de verwerking van persoonsgegevens" (8/12/1992, revisions 11/12/1998 and 26/02/2003)
- "**Wet elektronische handel**" (11/03/2003)
- "**Wet elektronische handel 2**" (11/03/2003)
- "**Wet betreffende de elektronische communicatie**" (13/06/2005)

Personal data

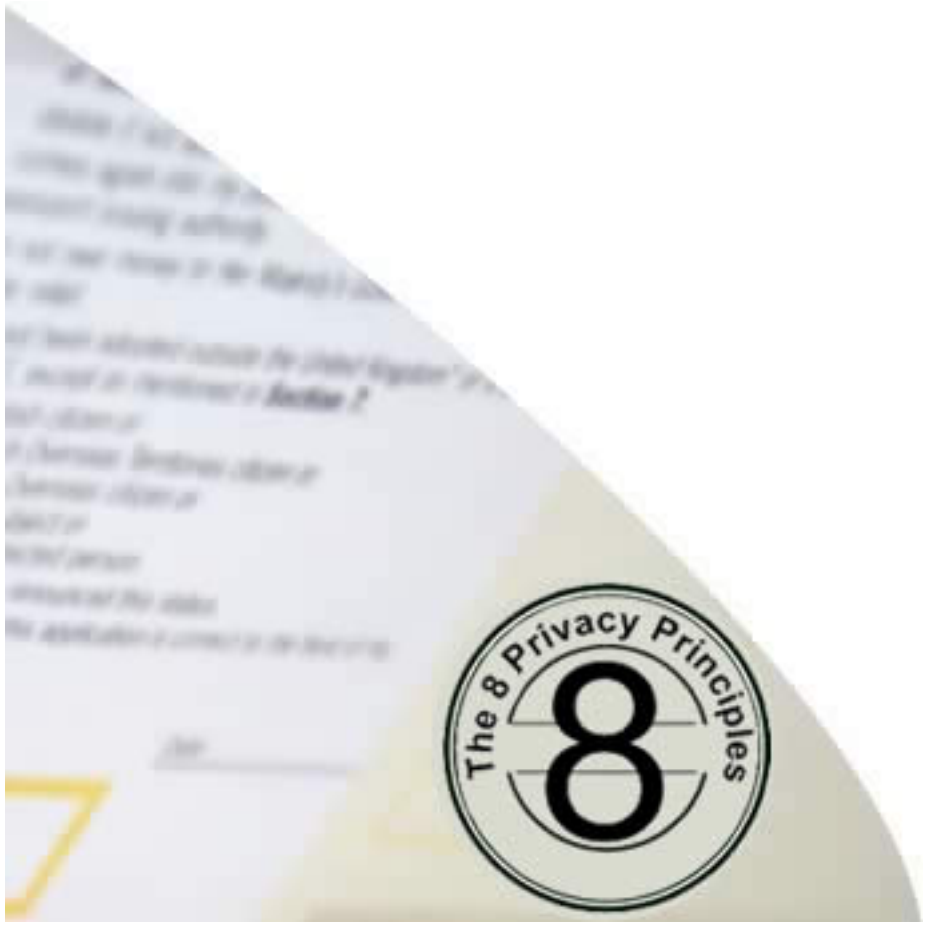
- **Personal** data
  - “any information relating to an identified or identifiable natural person ('data subject'); “
  - Examples: cookies, IP addresses, name, national number*, ...
- **Sensitive** personal data
  - “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. “
  - Also judicial: offences, criminal convictions, ...

Where do App. Security and Data Privacy meet ?

- “Forgetting” data privacy requirements during initiation phase
- Use of cookies
- Use of e-mail for publicity (opt-in)
- Vulnerabilities may lead to "unauthorized" access to personal data
- ...

Data Privacy - principles

- Fair processing
- Notice
- Choice
- Accuracy
- Security
- Access
- Onward Transfer
- Enforcement



Security and Data Privacy requirements

- Explicit requirements when registering with Belgian Data Protection Authority (Privacy Commission)*
  - Security policy
  - Security officer
  - Security organisation and people aspects
  - Physical and environmental security (incl. BU)
  - **Network security**
  - **Logical access security**
  - **Logging, monitoring, investigations**
  - Maintenance, supervision, control
  - Security incident and continuity management
  - Documentation

Expanding Information Security within Project/Application Development lifecycle

- Business Impact Assessment
  - Focus on Confidentiality, Integrity, Availability
  - Extend to include Data Privacy
- Data Privacy Questionnaires
  - Gathering responses on 8 principles
  - Example

Questions ?

Dirk De Maeyer
KPMG Advisory
ddemaeyer@kpmg.com