Overzicht beveiligingsnormen relevant voor privacy

Piet Donga en Mirna Bognar

ING Bank Corporate Information Risk management

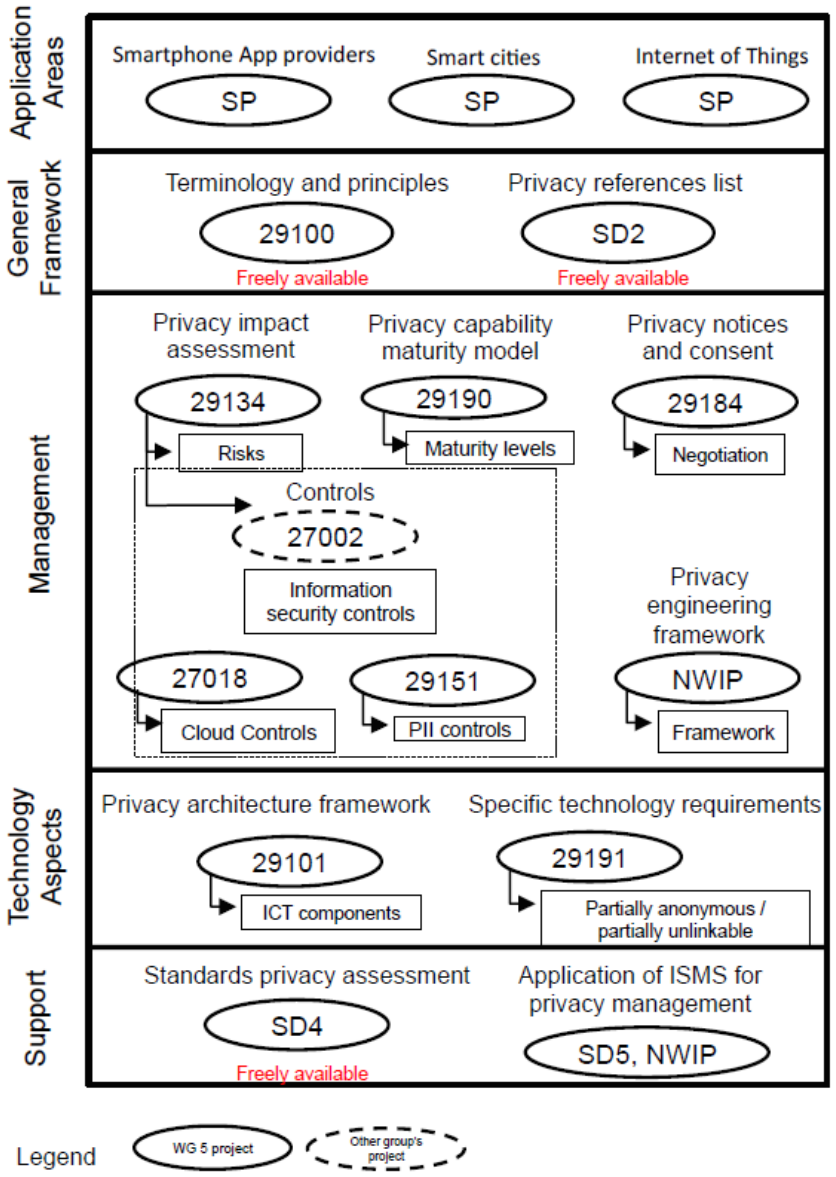
4 oktober 2016

Agenda

- Overzicht privacy-gerelateerde normen
  - WG 5 Roadmap
  - ISO29100 Privacy Framework
  - ISO29101 Privacy Architecture Framework
- Overzicht privacy-gerelateerde wet- en regelgeving
  - O.a. General Data Protection Regulation
- Rol Privacy Officer
  - Autoriteit Persoonsgegevens richtsnoer
  - ING invulling

Overzicht privacy-gerelateerde normen

- WG5



Overzicht privacy-gerelateerde normen

- ISO29100 Privacy Framework
  - Rollen
  - Controls and Requirements
  - Principles

Table 3 – The privacy principles of ISO/IEC 29100

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

Risk management is defined as "coordinated activities to direct and control an organization with regard to risk" (ISO Guide 73:2009). The privacy risk management process comprises the following processes:

- establishing the context, by understanding the organization (e.g., PII processing, responsibilities), the technical environment and the factors influencing privacy risk management (i.e. legal and regulatory factors, contractual factors, business factors and other factors);
- risk assessment, by identifying, analysing and evaluating risks to PII principals (risks that they can be adversely affected);
- risk treatment, by defining privacy safeguarding requirements, identifying and implementing privacy controls to avoid or reduce the risks to PII principals;
- communication and consultation, by getting information from interested parties, obtaining consensus on each risk management process, and informing PII principals and communicating about risks and controls; and
- monitoring and review, by following up risks and controls, and improving the process.

Overzicht privacy-gerelateerde normen

- ISO29101 Privacy Architecture Framework
  - Consistente, high-level aanpak implementatie privacy controls op ICT
  - Richtlijnen voor planning, ontwerp en implementatie ICT architecture
  - Privacy enhancing technologies (PETs) in dienst van bescherming persoonsgegevens

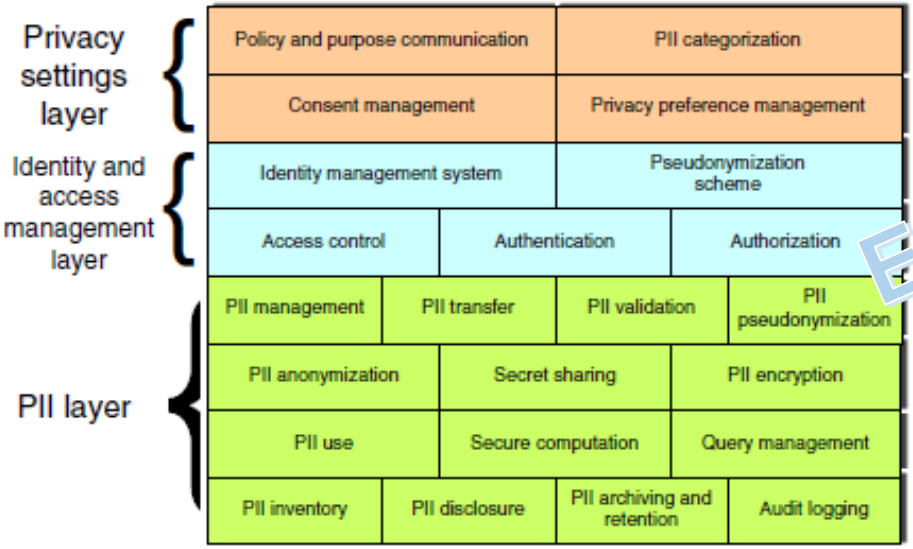


Figure 5 — The architecture of the ICT system of the PII processor

Overzicht privacy-gerelateerde wet- en regelgeving

- Europa:
  - Data Protection Directive 95/46 EC, bank secrecy regulations (in sommige landen)
- Buiten Europa:
  - Land-specifieke data protection en bank secrecy regulations
- Wereld-wijd:
  - Sector-specifieke regulations en gedragscodes betreffende gebruik van klantendata
- Aan de horizon:
  - EU General Data Protection Regulation (effectief vanaf 2018)

Generic Data Protection Regulation

- Status
  - Geadopteerd in mei 2016
  - Effectief per 2018 (2 jaar voor implementatie door bedrijven)
- Nieuw ten opzichte van bestaande wet- en regelgeving:
  - Verhoogde verantoordelijkheden voor Data Controllers om compliance te laten zien, in ruil voor melding van persoonsgegevens verwerking
  - Meer vereisten voor Data Processors
  - Meer rechten voor Data Subject
  - Vereisten voor melding datalekken
  - Verplichte Privacy Impact Assessment (PIA)
  - Boetes door lokale Data Protection Authoritiy

Rol van Privacy Officer

AUTORITEIT
PERSOONSGEGEVENS

- De werkzaamheden van een functionaris voor de gegevensbescherming kunnen onder meer zijn:
  - toezicht houden;
  - inventarisaties van gegevensverwerkingen maken;
  - meldingen van gegevensverwerkingen bijhouden;
  - vragen en klachten van mensen binnen en buiten de organisatie afhandelen;
  - interne regelingen ontwikkelen;
  - adviseren over technologie en beveiliging (privacy by design);
  - input leveren bij het opstellen of aanpassen van een gedragscode.

NEN

Voorbeeld: ING invulling