Methods and Tools for GDPR Compliance through Privacy and Data Protection 4 Engineering

Status of Privacy Engineering Standardisation

Antonio Kung
Trialog, 25 rue du Général Foy 75008 Paris
antonio.kung@trialog.com

12 June 2019
Outline

- Speaker
- Ecosystem viewpoint: big change in standardisation
- Privacy engineering: new standards in the pipe
- IPEN in the loop: recommendation for best practice sharing on privacy engineering
Speaker

Engineering background

- Coordinator PRIPARE (pripareproject.eu) 2013-2015
  - Liaison with ISO/IEC JTC1/SC27/WG5
  - Member of OASIS (Privacy Management Reference Model - PMRM)

Active participation in privacy standards

- Privacy by design principles
  - Privacy by design for consumer goods and services (ISO 31700)

- Privacy engineering
  - Privacy engineering (ISO/IEC 27550 – to be published)
  - Big data – Security and privacy fabric (ISO/IEC 20547-4)
  - Smart cities - Privacy guidelines for smart cities (ISO/IEC 27570)
  - IoT - Security and privacy guidelines for IoT (ISO/IEC 27030)
  - Privacy preference management (ISO/IEC 27556)
  - Privacy engineering models - study
Administrator of IPEN wiki

12 June 2019

Status of privacy engineering standardisation

Slide 4
Methods and Tools for GDPR Compliance through Privacy and Data Protection Engineering

The ecosystem viewpoint

Big change in standardisation
The Ecosystem Viewpoint

Ecosystems
- Smart Cities
- IoT
- Big data

Domains
- Smart grid
- Health
- Transport

Technologies
- Blockchain
- AI
- Autonomous systems

Stakeholders
- Citizens
- Policy makers
- Business

Concerns
- Security
- Safety
- Trust
- Privacy

12 June 2019
Status of privacy engineering standardisation
Slide 6
An Integration Issue of Transversal Concern: Example of Security and Privacy

- **Security**:
  - 27001 Information security management systems — Requirements
  - 27009 Sector-specific application of 27001 – Requirements

- **Privacy**:  
  - 31700 Privacy-by-design for consumer goods and services
  - 29100 Privacy framework
  - 27552 Extension to 27001/27002 for privacy management – Requirements and guidelines

- **Risk analysis**
  - **Security**: 27005 Information security risk management
  - **Privacy**: 29134 Privacy impact assessment - Guidelines

- **Lifecycle engineering**
  - **Security**: 27101 Guidelines for cybersecurity framework
  - **Privacy**: 27550 Privacy engineering

- **Control design**
  - **Security**: 27002 Code of practice for information security controls
  - **Privacy**: 29151 Code of practice for personally identifiable information protection
  - 20889 Privacy enhancing data de-identification techniques
### ISO/IEC 17789 Cloud computing Reference Architecture

- ISO/IEC 23751 Data sharing agreement
  - Cloud service customer
  - Cloud service partner
  - Cloud service provider
  - Ecosystem guidance

### ISO/IEC 30141 IoT Reference Architecture

- ISO/IEC 27030 Security and privacy guidelines for IoT
  - IoT user
  - IoT service developer
  - IoT service provider
  - Ecosystem guidance

### ISO/IEC 20547-3 Big data Reference Architecture

- ISO/IEC 20547-4 Big data security and privacy
  - Big data service partner
  - Big data application provider
  - Big data provider
  - Big data consumer
  - Big data framework provider
  - Ecosystem guidance
ISO/IEC 27570 Privacy guidelines for smart cities

- Five processes
  - Governance
  - Risk management
  - Data exchange
  - Engineering
  - Citizen engagement

Best available techniques

Continuous improvement

Ecosystem Governance body

Organisation 1
Organisation N
Organisation N

12 June 2019
Example of 27556 Privacy Preference management

Functional Viewpoint

Privacy preference administration
Consent Information administration
Control Rule generation
Transparency administration
Privacy Preference Manager

Ecosystem Viewpoint

Data source collection → De-identification → Data transfer control → PII handling

Privacy preference manager
What is next?

- ISO/IEC JTC1 SG6 « Meta Reference Architecture » Workshop Montreal 20-22 August

- Will gather standard editors on important standards
  - Architecture (system, cloud, big data, IoT, smart city)
  - Cross cutting concern (security, privacy, safety, trust...)
  - Governance and continuous improvement

- Objective
  - Reach common understanding
  - Define shape of convergent standards
  - Define roadmap
Privacy engineering standards

New standards in the pipe
## Current work

| Principles | ISO 37100 | Privacy-by-design for consumer goods and services | Pending |
| ISO/IEC 29100 | Privacy framework | Published (free) |
| Mechanism | ISO/IEC 20889 | Data de-identification terminology and classification of techniques | Published |
| ISO/IEC 29184 | Online privacy notices and consent | Pending |
| Organisation practice | ISO/IEC 27550 | Privacy engineering for system life cycle processes | 2019 |
| ISO/IEC 27552 | Privacy information management -- requirements and guidelines | 2019 |
| ISO/IEC 27555 | Establishing a PII deletion concept in organisations | Pending |
| ISO/IEC 27556 | User-centric framework for privacy preference management | Pending |
| ISO/IEC 29134 | Privacy impact assessment guidelines | Published |
| ISO/IEC 29151 | Code of practice for PII protection | Published |
| ISO/IEC 29190 | Privacy capability assessment model | Published |
| Ecosystem practice | ISO/IEC 20547-4 | Big data security and privacy | Pending |
| ISO/IEC 27030 | Security and privacy guidelines for IoT | Pending |
| ISO/IEC 27570 | Privacy guidelines for smart cities | Pending |
| ISO/IEC 23751 | Data sharing agreements | Pending |
Privacy Engineering: Integrating privacy concerns

ISO/IEC 27550 Privacy Engineering for system lifecycle process
Beyond CIA

- Confidentiality
- Integrity
- Availability
- Unlinkability
- Intervenability
- Transparency

From ULD: ieee-security.org/TC/SPW2015/IWPE/2.pdf

ISO/IEC 27550 Privacy Engineering for system lifecycle process
<table>
<thead>
<tr>
<th>Property</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard privacy</td>
<td></td>
</tr>
<tr>
<td>Unlinkability</td>
<td>Linkability</td>
</tr>
<tr>
<td>Anonymity</td>
<td>Identifiability</td>
</tr>
<tr>
<td>Plausible deniability</td>
<td>Non-repudiation</td>
</tr>
<tr>
<td>Undetectability and unobservability</td>
<td>Detectability</td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Disclosure of information</td>
</tr>
<tr>
<td>Soft Privacy</td>
<td></td>
</tr>
<tr>
<td>Content awareness</td>
<td>Unawareness</td>
</tr>
<tr>
<td>Policy and consent compliance</td>
<td>Non compliance</td>
</tr>
</tbody>
</table>

ISO/IEC 27550 Privacy Engineering for system lifecycle process
### Design Strategy (J.H.Hoepman)


<table>
<thead>
<tr>
<th>Design strategy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data oriented strategies</strong></td>
<td></td>
</tr>
<tr>
<td>Minimize</td>
<td>Limit as much as possible the processing of PII</td>
</tr>
<tr>
<td>Separate</td>
<td>Distribute or isolate personal data as much as possible, to prevent correlation</td>
</tr>
<tr>
<td>Abstract</td>
<td>Limit as much as possible the detail in which personal data is processed, while still being useful</td>
</tr>
<tr>
<td>Hide</td>
<td>Prevent PII to become public or known.</td>
</tr>
<tr>
<td><strong>Process oriented strategies</strong></td>
<td></td>
</tr>
<tr>
<td>Inform</td>
<td>Inform PII principals about the processing of PII</td>
</tr>
<tr>
<td>Control</td>
<td>Provide PII principals control about the processing of their PII.</td>
</tr>
<tr>
<td>Enforce</td>
<td>Commit to PII processing in a privacy friendly way, and enforce this</td>
</tr>
<tr>
<td>Demonstrate</td>
<td>Demonstrate that PII is processed in a privacy friendly way.</td>
</tr>
</tbody>
</table>

ISO/IEC 27550 Privacy Engineering for system lifecycle process
What is next? New standards in the pipe
A possible scenario

ISO 31700
Privacy by design for consumer goods and services principles

SC27/WG5 study
Privacy engineering models

Privacy engineering (IS)

27550 Edition 2
(from TR to IS)
Liaison category C with ISO/IEC JTC1/SC27/WG5

| Sujet: Establishment for a category C Liaison between PRIPARE and JTC1/SC27/WG5 |
| De : Blandine GARCIA <GARCIA@ISO.org> |
| Date : 21/10/2014 00:29 |
| Pour : Antonio Kung <Antonio.Kung@TRIALOG.COM> |
| Copie à : Passia Krystyna Mrs <krystyna.passia@DIN.DE> |

Dear Mr. Kung,

We are pleased to announce you the establishment of the Liaison C with JTC1/SC27/WG5 and your registration in our Global Directory, as Liaison officer.

Best regards,

Mrs Blandine GARCIA
ISO/IEC Information Technology Task Force
ISO/IEC Project Manager
Standard Department
IPEN in the Loop: Recommendation for best practice sharing on privacy engineering
Creating a Virtuous Cycle

- Best practice sharing on privacy engineering will drive new standards
- Conditions
  - Community participation
    - e.g. H2020 cluster of GDPR projects
  - Repository operation
  - Content
    - Textual information (use case like)
    - Models
  - Management
    - Editorial and acceptance process
PDP4E Contribution to Best Practice Sharing

- Models for privacy engineering
  - IPR free
  - Guidelines for use
- Possible contributions
  - Use case for smart grid big data
  - Use case connected vehicles (C-ITS)

Repository of models for privacy engineering

Managed by IPEN community
Question?

antonio.kung@trialog.com
www.trialog.com