Privacy by design Guidelines: how to ensure that the citizen privacy is respected

Antonio Kung
EIP-SCC Citizen Focus

Context

- PRIPARE support action 2014-2015
  
  - pripareproject.eu

- Contribution to ISO
  
  - Rapporteur ISO Study period « privacy in smart cities »
  - Rapporteur ISO Study period « privacy guidelines in the IoT »
  - Contributor ISO 20547-4 Big data reference architecture – Security and privacy fabric

- Contribution to EIP-SCC
  
  - Commitment 7001
  - Citizen approach to data initiative
    - 2 webinars – One recommendation document
Initiative

• Citizen Centric Approach to Data – Privacy-by-design
  – Snowden revelations
  – Something must be done to protect a citizen's right to privacy

• Initiative leaders
  – Antonio Kung (chair)
  – Chris Cooper (co-chair)
GDPR: General Data Protection Regulation

Published on May 4th 2016
Enter into force on May 24th 2016
Apply on May 25th 2018

• Privacy-by-design (PbD) and by-default
• Privacy Impact Assessment (PIA)
• Data Protection Officers
  – All public authorities and companies processing personal data on a large scale
• Sanctions for breaches
  – up to 20,000,000 EUR
  – up to 4% of the annual worldwide turnover
# Stakeholder Concerns on Privacy

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Legal Compliance Level</th>
<th>Management Level</th>
<th>System Lifecycle Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Demand side</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy maker</td>
<td>Compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Operator</strong></td>
<td>Compliance requirements</td>
<td>Compliance</td>
<td>Compliance requirements</td>
</tr>
<tr>
<td>Data Controller</td>
<td>Regulation</td>
<td>Requirements</td>
<td>Privacy-by-Design</td>
</tr>
<tr>
<td><strong>Operator</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data processor</td>
<td>GDPR</td>
<td>PIA</td>
<td>PbD</td>
</tr>
<tr>
<td><strong>Supply side</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supplier</td>
<td>e.g. Operators Requirements</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Supply Side Concern

Smart City Application operator

Sensor

Device

Smart device

Cloud solution

Electronics

Security module

OS

Middleware

Purpose unknown

Small operator VS big operator

GDPR

PIA

PbD
What we want to Achieve

**Smart City Ecosystem**

**Demand side**
- Policy maker
- Operator
- Operator
- Supplier

**Supply side**
- Data Controller
- Data processor

**PRI Pare**
- PRI Pare methodology

**ISO**
- ISO 27550
- Privacy engineering guidelines

Global guidelines

Dedicated guidelines
Thanks

Antonio Kung