Citizen Centric approach to data – GDPR revisited

Antonio Kung – Trialog – www.trialog.com
CEO
Chair EIP-SCC Citizen Approach to data
Editor ISO/IEC 27570 Privacy Guidelines for Smart Cities
Context

- **PRIPARE commitment 7001**
  - Standards on security and privacy
    - Liaison with ISO/IEC JTC 1/SC27/WG5
    - Editor ISO/IEC 27570 Privacy guidelines for smart cities
- **EIP-SCC initiative citizen centric approach to data**
  - GA 2015 Berlin: proposal for initiative
    - Nov 2015. Action Cluster meeting Brussels
    - April/May 2016. Two webinars on privacy for smart cities
  - GA 2016 Eindhoven: proposal for workshops in GDPR compliance
    - April 2016/Sept 2016: Espresso webinar / ERRIN workshop
    - Nov 2016. Action cluster meeting Brussels
    - March 2017/July 2017: Sharing cities PIA workshop
    - October 2017. Action Cluster meeting Brussels
  - GA 2017 Brussels: proposal for sharing GDPR compliance practice
    - Eurocities workshop
  - GA 2018 Sofia: Kicking off ISO/IEC 27570 Privacy guidelines for smart cities
Cities must Manage Ecosystems

Ecosystems

- Smart Cities
- IoT
- Big data

Domains

- Smart grid
- Transport
- Health

Concerns

- Security
- Safety
- Privacy

GDPR Revisited
Cities must Manage Ecosystems

- Municipality stakeholder
- Requests
  - PIA
  - Agreements For data exchange
- Integrator
- Supplier
- Data controller
- Data processor
- Citizen
- Comply
  - Privacy Obligations
  - PIA and PbD Purpose known
  - Requirements Purpose unknown

Contracts

Give consent

Agree

Apply

Apply

GDPR Revisited
Context of ISO/IEC 27570 Privacy guidelines for smart cities

- JTC1/SC27 Information security, cybersecurity and privacy protection
  - WG1 Information security management systems
  - WG2 Cryptography and security mechanisms
  - WG3 Security evaluation, testing and specification
  - WG4 Security controls and services
  - WG5 Identity management and privacy techniques

- Privacy for smart cities Study period
  - October 2015 - First study period (18 months) initiated by India
  - June 2017 – Second study period (6 months) Initiated by France further to contribution from JTC1/WG11 smart cities

- Privacy guidelines for smart cities ISO/IEC 27570 TS
  - Editors
    - Antonio Kung – France
    - Heung Youl Youm – Korea
  - 20 June 2018 – Registration – 1st WD
  - October 2018 – 2nd WD
  - May 2019 – 1st CD
  - Going for publication – mid 2020
The document takes a multiple agency as well as a citizen centric viewpoint, and provides guidance on how privacy standards can be used at a global level and at an organizational level for the benefit of citizens.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations that provide services in smart city environments.
### Smart Cities? Requirements?

<table>
<thead>
<tr>
<th>Slide</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>34</td>
<td>5. Privacy in Smart Cities</td>
<td>11</td>
</tr>
<tr>
<td>35</td>
<td>5.1 Smart cities</td>
<td>11</td>
</tr>
<tr>
<td>36</td>
<td>5.2 Actors</td>
<td>13</td>
</tr>
<tr>
<td>37</td>
<td>5.3 Use cases</td>
<td>15</td>
</tr>
<tr>
<td>38</td>
<td>5.4 Challenges</td>
<td>15</td>
</tr>
<tr>
<td>39</td>
<td>6 Requirements on smart city ecosystems</td>
<td>17</td>
</tr>
<tr>
<td>40</td>
<td>6.1 Requirements on governance chains</td>
<td>17</td>
</tr>
<tr>
<td>41</td>
<td>6.2 Requirements on supply chains</td>
<td>18</td>
</tr>
<tr>
<td>42</td>
<td>6.3 Requirements on data sharing chains</td>
<td>19</td>
</tr>
<tr>
<td>43</td>
<td>7 Standards for organizations in smart city ecosystems</td>
<td>20</td>
</tr>
<tr>
<td>44</td>
<td>7.1 Standards for privacy governance</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>7.2 Standards for privacy risk management</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>7.3 Standards for privacy engineering</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>8 Privacy guidelines for smart city processes</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>8.1 Privacy guidelines for the governance process</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>8.2 Privacy guidelines for the risk management process</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>8.3 Privacy guidelines for the engineering process</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>8.4 Privacy guidelines for the citizen engagement process</td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>8.5 Privacy guidelines for the data exchange and sharing process</td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>Annex A Requirements for templates and support documents</td>
<td>28</td>
</tr>
<tr>
<td>54</td>
<td>A.1 Privacy impact assessment</td>
<td>28</td>
</tr>
<tr>
<td>55</td>
<td>A.2 Data sharing agreement</td>
<td>28</td>
</tr>
<tr>
<td>56</td>
<td>A.3 PII processing declaration</td>
<td>28</td>
</tr>
<tr>
<td>57</td>
<td>Annex B Existing Initiatives for Smart Cities Privacy</td>
<td>29</td>
</tr>
<tr>
<td>58</td>
<td>B.1 Citizen-centric approach to data</td>
<td>29</td>
</tr>
<tr>
<td>59</td>
<td>B.2 Open data privacy playbook</td>
<td>29</td>
</tr>
</tbody>
</table>
ISO/IEC 30145 Smart Cities ICT Reference Framework

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Business</th>
<th>Citizens</th>
<th>Government organisations</th>
<th>Non Government organisations</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Vision &amp; Outcome</th>
<th>Well-being</th>
<th>Transparency</th>
<th>Sustainability</th>
<th>Economic development</th>
<th>Efficiency &amp; resilience</th>
<th>Collaboration</th>
<th>Innovation</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Business process framework</th>
<th>Business &amp; Operational processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>City Enterprise processes</td>
<td>Transport</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Governance &amp; Integration processes</th>
<th>Leadership &amp; direction</th>
<th>Stakeholder engagement &amp; citizen focus</th>
<th>Integrated portfolio management</th>
<th>Knowledge management</th>
<th>Integrated management</th>
<th>Integrated city systems engineering</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Knowledge management framework</th>
<th>Dynamic place</th>
<th>Measurement</th>
<th>Provenance</th>
<th>Validity</th>
<th>Place</th>
<th>Time</th>
<th>Trust</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Engineering management framework</th>
<th>Smart Application Layer</th>
<th>Data &amp; Services Supporting Layer</th>
<th>Computing &amp; Storage Layer</th>
<th>Network Communication Layer</th>
<th>Data Acquisition Layer</th>
<th>Security system</th>
<th>Construction system</th>
<th>Operation &amp; maintenance system</th>
<th>Identification system</th>
<th>Positioning system</th>
</tr>
</thead>
</table>

GDPR Revisited

May 17 2019
## ISO/IEC 30145 Smart cities ICT reference framework

### Engineering management framework

#### Smart Application Layer
- Smart government
- Smart transportation
- Smart education
- Smart healthcare
- Smart home
- Smart campus

#### Data & Services supporting layer

<table>
<thead>
<tr>
<th>Service integration</th>
<th>Service usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service acquisition &amp; aggregation</td>
<td>Service management</td>
</tr>
<tr>
<td>Service management</td>
<td>Service integration</td>
</tr>
</tbody>
</table>

#### Data integration

<table>
<thead>
<tr>
<th>Data sources</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fundamental data</td>
<td>Shared exchangeable data</td>
</tr>
<tr>
<td>Data acquisition &amp; aggregation</td>
<td>Data integration &amp; processing</td>
</tr>
<tr>
<td>Data processing</td>
<td>Intelligence mining &amp; analysis</td>
</tr>
<tr>
<td>Data management &amp; guidance</td>
<td>Data management &amp; guidance</td>
</tr>
</tbody>
</table>

#### Computing & storage layer

<table>
<thead>
<tr>
<th>Computing resource</th>
<th>Storage resource</th>
<th>Software resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public network</td>
<td>Privacy network</td>
<td></td>
</tr>
</tbody>
</table>

#### Network Communication Layer

<table>
<thead>
<tr>
<th>Data Acquisition Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor data acquisition</td>
</tr>
<tr>
<td>Human data acquisition</td>
</tr>
</tbody>
</table>
Smart City Ecosystems

- Ecosystem
  - Organisation
    - Process
      - Includes
        - Governance & Integration processes
        - Business & operation processes
        - Security and privacy processes

Follows

- Smart cities ICT Reference framework

Describes

Includes

Organisation

Implements

GDPR Revisited
## Examples of Ecosystems Concerns

<table>
<thead>
<tr>
<th>Governance level</th>
<th>Smart city is not able to track all data controllers or data processors. For instance not being able identify the data controllers or data processors that caused a breach.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Smart city is not able to enforce privacy policies in the governance chain. <em>Not being able to verify that all consents have been provided</em></td>
</tr>
<tr>
<td>Supply chain level</td>
<td>Privacy impact assessments are incorrect. <em>For instance supplier underestimate risks</em></td>
</tr>
<tr>
<td></td>
<td>Data controllers or data processors rely on suppliers of components that do not support some desired privacy controls. <em>For instance supplier providing data storage does not use state of the art protection capabilities.</em></td>
</tr>
<tr>
<td>Data sharing level</td>
<td>Lack of awareness from stakeholder in the data sharing chain of its obligations. <em>For instance a stakeholder provides personal data to a supplier without informing him.</em></td>
</tr>
<tr>
<td></td>
<td>Wrong assessment from a stakeholder that it is not a data controller or data processor. <em>For instance publishing open data that is not properly anonymized, or combining two datasets which do not contain personal data into a dataset which contains personal data.</em></td>
</tr>
</tbody>
</table>
Which standards to use?

Smart Cities experts

Smart Cities experts

Security and privacy experts

Security and privacy experts

Smart cities, security and privacy experts
Need to integrate privacy standards with other standards

ISO/IEC 27570 Privacy guidelines for smart cities

Privacy standards
- ISO/IEC 29100 privacy framework
- ISO/IEC 29134 privacy impact assessment guidelines
- ISO/IEC 27552 privacy control requirements
- ISO/IEC 29151 code of practice for PII protection
- ISO/IEC 27550 privacy engineering
- ISO/IEC 27556 privacy preference management

Smart city standards
- ISO/IEC 30145 Smart cities reference framework
- BSI PAS 183:2017 Guide to establishing a decision-making framework for sharing data and information services
- ISO 37156 Guidelines on Data Exchange and Sharing for Smart Community

Cloud standards
- ISO/IEC 17789 Cloud Computing Reference Architecture
- ISO/IEC 27018, Code of practice for protection of PII in public clouds acting as PII processors
- ISO/IEC 23751 Data sharing agreement framework

IoT standards
- ISO/IEC 30141 IoT Reference Architecture
- ISO/IEC 27030 security and privacy guidelines for IoT

Big data standards
- ISO/IEC 20547-3 Big data reference architecture
- ISO/IEC 20547-4 Big data security and privacy

JTC1/SC27/WG5
JTC1/WG11
JTC1/SC38
JTC1/SC41
JTC1/SC27/WG4
JTC1/SC42
JTC1/SC27/WG4 and WG5
Governance, Risk management, Engineering

- Governance
  - Privacy
  - Risk management
    - Security
      - Privacy
    - Security
      - Privacy
- Organisation process requirements
- Engineering
  - Privacy
  - ISO/IEC 27001 Information security management systems — Requirements
  - ISO/IEC 27009 Sector-specific application of ISO/IEC 27001 — Requirements
  - ISO/IEC 27002 Code of practice for information security controls
  - ISO/IEC 27003 Information security risk management
  - ISO/IEC 27550 Privacy guidelines for smart cities
  - ISO/IEC 27552 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management — Requirements and guidelines
  - ISO/IEC 27005 Information security risk management
  - ISO/IEC 29134 Privacy impact assessment - Guidelines
  - ISO/IEC 29100 Privacy framework
  - ISO/IEC 29151 Code of practice for personally identifiable information protection
  - ISO/IEC 29135 Privacy impact assessment — Guidelines
  - ISO/IEC 20889 Privacy enhancing data de-identification techniques
  - ISO/IEC 27570 Privacy guidelines for smart cities

GDPR Revisited
### Smart City Processes for Privacy

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>34</td>
<td>5 Privacy in Smart Cities</td>
<td>11</td>
</tr>
<tr>
<td>35</td>
<td>5.1 Smart cities</td>
<td>11</td>
</tr>
<tr>
<td>36</td>
<td>5.2 Actors</td>
<td>13</td>
</tr>
<tr>
<td>37</td>
<td>5.3 Use cases</td>
<td>15</td>
</tr>
<tr>
<td>38</td>
<td>5.4 Challenges</td>
<td>15</td>
</tr>
<tr>
<td>39</td>
<td>6 Requirements on smart city ecosystems</td>
<td>17</td>
</tr>
<tr>
<td>40</td>
<td>6.1 Requirements on governance chains</td>
<td>17</td>
</tr>
<tr>
<td>41</td>
<td>6.2 Requirements on supply chains</td>
<td>18</td>
</tr>
<tr>
<td>42</td>
<td>6.3 Requirements on data sharing chains</td>
<td>19</td>
</tr>
<tr>
<td>43</td>
<td>7 Standards for organizations in smart city ecosystems</td>
<td>20</td>
</tr>
<tr>
<td>44</td>
<td>7.1 Standards for privacy governance</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>7.2 Standards for privacy risk management</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>7.3 Standards for privacy engineering</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>8 Privacy guidelines for smart city processes</td>
<td>22</td>
</tr>
<tr>
<td>48</td>
<td>8.1 Privacy guidelines for the governance process</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>8.2 Privacy guidelines for the risk management process</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>8.3 Privacy guidelines for the engineering process</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>8.4 Privacy guidelines for the citizen engagement process</td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>8.5 Privacy guidelines for the data exchange and sharing process</td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>Annex A Requirements for templates and support documents</td>
<td>28</td>
</tr>
<tr>
<td>54</td>
<td>A.1 Privacy impact assessment</td>
<td>28</td>
</tr>
<tr>
<td>55</td>
<td>A.2 Data sharing agreement</td>
<td>28</td>
</tr>
<tr>
<td>56</td>
<td>A.3 PII processing declaration</td>
<td>28</td>
</tr>
<tr>
<td>57</td>
<td>Annex B Existing Initiatives for Smart Cities Privacy</td>
<td>29</td>
</tr>
<tr>
<td>58</td>
<td>B.1 Citizen-centric approach to data</td>
<td>29</td>
</tr>
<tr>
<td>59</td>
<td>B.2 Open data privacy playbook</td>
<td>29</td>
</tr>
</tbody>
</table>

**Smart Cities experts**
- Smart Cities experts
- Security and privacy experts
- Smart cities, security and privacy experts
Governance Process

- Description of activities
  - Establishment of privacy policies
  - Monitoring of their implementation in smart city service

- Guidelines for ecosystem coordination
  - Rules and policies of for chain of privacy governance;
  - Specify supervision requirements
  - Specify supervision process
  - Identify supervised organizations
  - Apply the supervision process

- Guidelines for organizations
  - Enrolment
  - Implement rules and policies
  - Apply supervision process
Risk Management Process

• Description of activities
  • System of system risk management
  • System-level risk management

• Guidelines for ecosystem coordination
  • SoS risk analysis leading to SoS controls
  • Mapping SoS controls to organisations

• Guidelines for organizations
  • System risk analysis leading to system controls
  • Implement controls
  • Apply risk mgt process

Can benefit from consistency with standards on risk management
Engineering Process

- **Description of activities**
  - Activities for privacy related to the lifecycle of a smart city service

- **Guidelines for ecosystem coordination**
  - Identify data processing operational requirements
  - Identify security and privacy requirements
  - Identify activities where privacy must be taken into account;
  - Map activities to the organizations of the ecosystem;
  - Establish coordination schemes

- **Guidelines for organizations**
  - Identify activities where privacy must be taken into account;
  - Identify the controls to be implemented
  - Establish the lifecycle process in accordance with coordination scheme

Can benefit from consistency with privacy engineering standards
Citizen Engagement Process

• Description of activities
  • Concertation with smart city citizens

• Guidelines for ecosystem coordination
  • Establish a citizen concertation process on privacy
  • Establish a citizen interaction process
    • Information, enquiries and complaints;
  • Establish review process of services involving citizens
  • Periodic citizen review of services
  • Establish coordination schemes

• Guidelines for organizations
  • Apply concertation support activities

Can benefit from consistency with citizen engagement practices and standards
Data Exchange and Sharing Process

- **Description of activities**
  - Integration of privacy in data exchange and sharing
  - Monitoring at smart city level

- **Guidelines for ecosystem coordination**
  - Specify the privacy impact assessment and sharing agreement templates to use
  - Establish security and privacy coordination schemes
    - measures for compliance, assurance and audit of practice.

- **Guidelines for organizations**
  - Use templates
  - Carry out data exchange and sharing activities in accordance with coordination scheme.

Will benefit with consistency with 37156 (TC268) and 23751 (JTC1/SC38)
Round Table

• Requirements and concerns

• Processes
  • Governance
  • Risk management
  • Engineering
  • Citizen engagement
  • Data sharing

• Use cases
Questions?

Antonio Kung - antonio.kung@trialog.com