Trust in the context of smart cities
Synchrogenicity: Privacy by Design
Strategy for Smart Cities

Connected Smart Cities
Brussels, January 17, 2019
Dilemma & Dual Strategy

Open Data & Interoperability
- Open API & Pre-Standardization

Privacy & Personal Data Protection
- Close Monitoring & Innovative approaches
Privacy Risks for smart cities

- Citizens / Users Acceptance
- Legal Risks
- Financial Risks
- Political and Reputational Risks
Data Protection Coordination

Data Protection Committee

Project DPO Coordination

Local DPO  Local DPO  Local DPO  Local DPO
Data Management Plan

Detailed Data Management Plan with guidelines for:
- Data Protection
- Open Data Access
- Data Processing and retention policy
Article 25 Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
Privacy by Design

Mapping:
- Stakeholders
- Data nature & flows
- Processes

Analysing:
- Compliance
- Risks
- Risks mitigation
Data Protection Impact Assessment

Art 35, al 3
Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of processing, is likely to result in high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A data protection impact assessment referred to in paragraph 1 shall in particular be required in case of:

• ...
• A systematic monitoring of a publicly accessible area on a large scale.
## Data Protection Impact Assessment

<table>
<thead>
<tr>
<th>Dataset #1</th>
<th>Dataset #2</th>
<th>Dataset #3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title/name of the dataset</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Describe the Category of Internet of Things devices used to collect the data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>How many devices are deployed?</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Identification of Personal Data

Any data that can be easily linked to individuals shall be considered as "personal data". Indicate if you are collecting any of the following data:

- Name of individuals
- Personal addresses
- Personal email addresses
- Personal phone numbers
- Pictures or videos on which individuals may appear
- Audio-Recording on which conversations could be recorded
- Personal device identifier (e.g., MAC address, IMEI number, etc.)
- Geolocation of any or users' mobile devices (e.g., location, smartphone, smart watch etc.)
- Any other personal identifier (e.g., public transport badge, access badge etc.)

If any of the above questions is answered by YES, please proceed with the subsequent steps.

### Data Subject Rights

- **For what purpose are you collecting these data?**
- **Do you provide clear information to the public on how this information made accessible to the public?**
  - [ ] Yes
  - [ ] No
- **Is there a clear indication on how to contact the data controller and its data protection officer?**
  - [ ] Yes
  - [ ] No

### Data Subject Rights

- **Individuals whose data are collected have rights on their data. Data Controller must ensure the respect of these rights**
  - Can the individuals access their personal data?
  - Can the individuals request to update their personal data?
  - Can the individuals object to the processing of their personal data?
  - Is there a clear procedure for the individuals to request the erasure of their personal data, and for the datacontroller to assess such requests in accordance with the GDPR?
  - Is there a clear procedure for the individuals to request the restriction of the processing of their personal data, and for the datacontroller to assess such requests in accordance with the GDPR?
  - Is there a clear procedure for the individuals to request the human intervention in case of automated processing which affects them?

### Security measures

- **Data Controller must ensure any personal data and prevent unwanted access, modification or deletion. Do you apply the following security measures?**
  - Strong authentication techniques to access personal data
  - Access-restricted areas
  - Geolocation of users or users' mobile devices
  - Personal device identifier
  - Personal address
  - Personal phone numbers
  - Personal email addresses
  - Personal identifiers
  - Accidental or unlawful destruction of personal data
  - Loss of personal data
  - Alteration of personal data
  - Loss of personal data
  - Accidental or unlawful destruction of personal data
  - Loss of personal data
  - Alteration of personal data
  - Loss of personal data

### Countermeasures

- **Description of risk**
- **Likelihood of risk (Low/Medium/High)**
- **Severity of the risk impact (Low/Medium/High)**
- **Controller**
- **Difficulty**
- **Financial Cost**
- **Term**

### Risk Analysis

- **Risk 1**
  - **Description of risk**
  - **Likelihood of risk (Low/Medium/High)**
  - **Severity of the risk impact (Low/Medium/High)**
  - **Controller**
  - **Difficulty**
  - **Financial Cost**
  - **Term**

- **Risk 2**
  - **Description of risk**
  - **Likelihood of risk (Low/Medium/High)**
  - **Severity of the risk impact (Low/Medium/High)**
  - **Controller**
  - **Difficulty**
  - **Financial Cost**
  - **Term**

- **Risk 3**
  - **Description of risk**
  - **Likelihood of risk (Low/Medium/High)**
  - **Severity of the risk impact (Low/Medium/High)**
  - **Controller**
  - **Difficulty**
  - **Financial Cost**
  - **Term**

### Qualification of participants

- **Stakeholders represented**
- **Moderator's name**
- **Moderator's email**
- **Number of participants**
- **how many participants**
GDPR Certification Process
**EuroPrivacy** based on H2020 Privacy Flag research project

1. International Law on Privacy
2. European Data Protection
3. Swiss Data Protection Law

- Privacy Flag European Research Project
- Privacy Risk Area Assessment Methodology
- ISO Standards
- EuroPrivacy
- Archimede Solutions
→ Encompassing EU (GDPR), national, and international obligations

→ Addressing emerging technologies
  Smart Cities, Big data, Internet of Things, etc…

→ Hybrid Scheme encompassing both:
  - Products & Services (ISO 17065)
  - Information Management Systems (ISO 17021-1)

→ ISO compliant
  and easily combined with ISO/IEC 27011

www.europrivacy.org
Duty to Inform

Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.
Privacy App

**Device details**

- **Category:** Noise sensor
- **Purpose:** Street noise monitoring in three dimensions.
- **Description:** Noise sensor measuring the sound level (dBA).
- **Data controller:** City of Carouge
- **Retention period:** 6-12 months
- **Location:** 46.190125 latitude, 6.134022
- **Legitimate interest:** Public health
- **Recipient:** Internal use only
- **Crossborder transfer:** None
- **Picture:**
Key Lessons Learned

• Privacy by design in smart cities is a research domain per se with a large potential for innovation
• Legal and financial risk underestimated
  Need to address the Political risk
• Identify and clarify the responsibilities
• Continuous improvement process
• Educate, educate, educate
• Be pragmatic and need-driven
• Anticipate evolution and end-user perception
• Strong cross-fertilization potential
SYNCHRONICITY

THANK YOU!

Dr Sébastien Ziegler
sziegler@mandint.org