SYNCHRONICITY

CREATE-IoT

U4IoT

Privacy by Design Smart City

Dr Sébastien Ziegler – sziegler@mandint.org

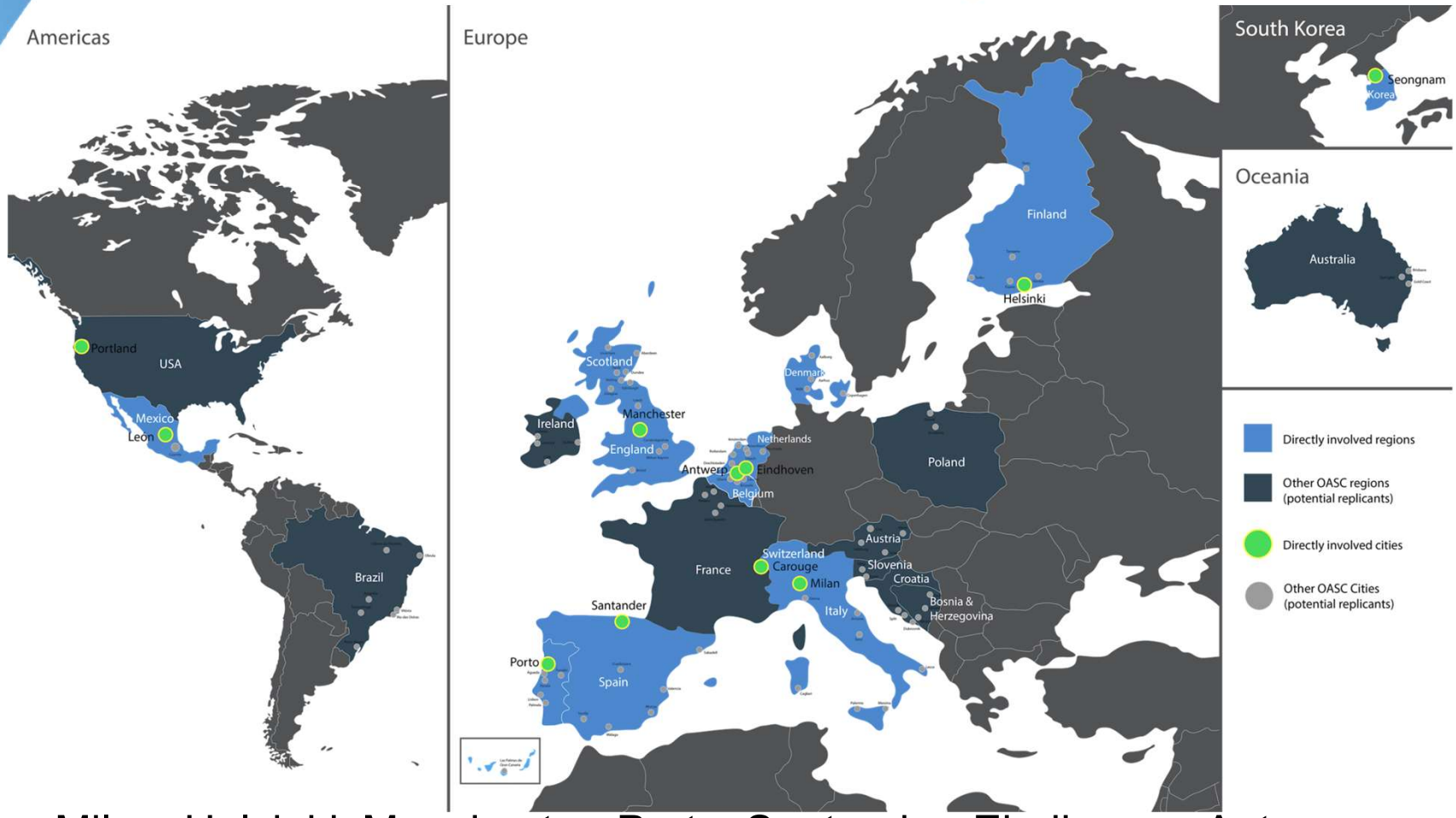
IoT Week 2019
Aarhus, Denmark, June 2019

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No732240

Co-funded by

Switzerland South Korea Mexico

SYNCHRONICITY



Milan, Helsinki, Manchester, Porto, Santander, Eindhoven, Antwerp, Carouge, Portland (US), Leon (Mexico), Seongnam (Korea)

SYNCHRONICITY

Interoperability

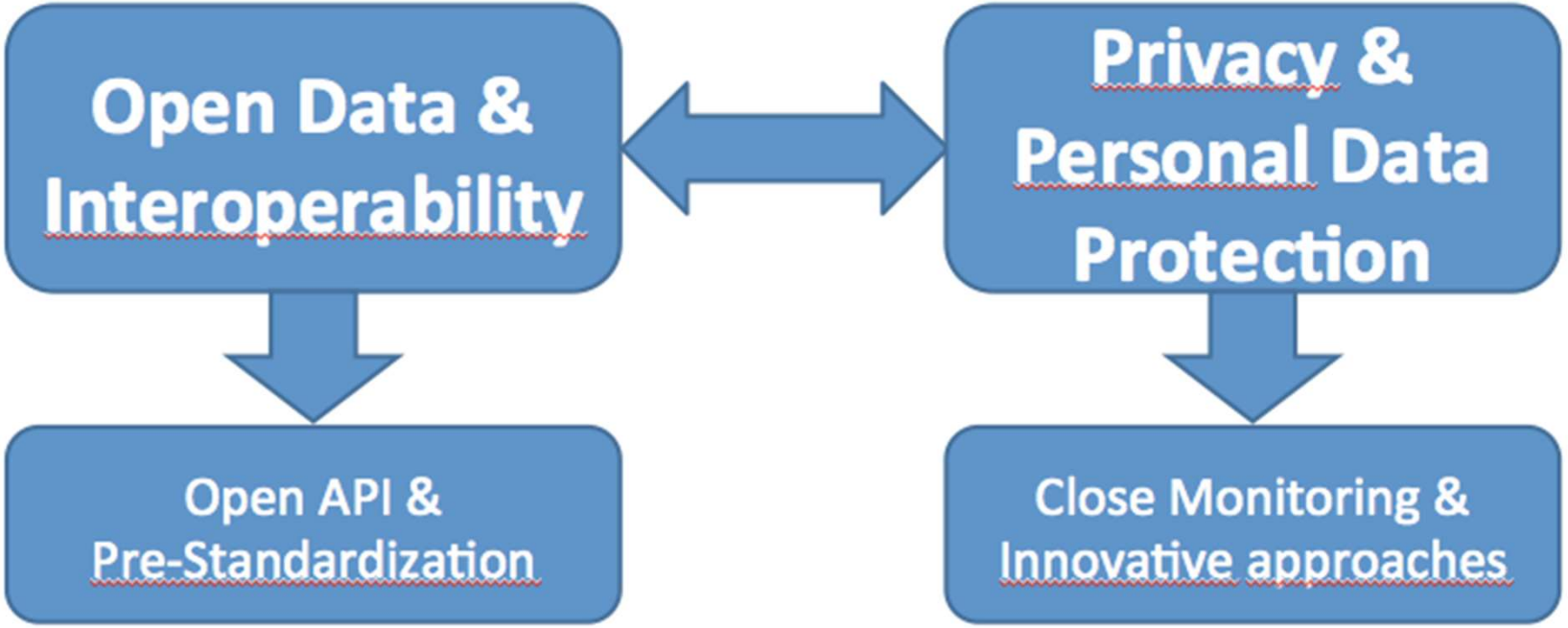
Shared Applications & Services

Data Analytics

European Digital Market

Open Data

Dilemma & Dual Strategy



Privacy & Data Protection Risks for smart cities

- User / Market Acceptance
- Legal Risks
- Financial Risks
- Political and Reputational Risks

Data Protection Objectives

- Ensure **full compliance** with the General Data Protection Regulation
- Identify and mitigate any privacy related **risks**
- Organize the **Data Protection Officer functions**
- Develop **specific tools and resources** for smart cities
- **Educate and promote data protection**

Data Management Plan

Detailed Data Management Plan
with guidelines for:

- Data Protection
- Open Data Access
- Data Processing and retention policy

Data Protection Officer

Article 37 Designation of the Data Protection Officer

1. The **controller and the processor shall designate a data protection officer** in any case where:

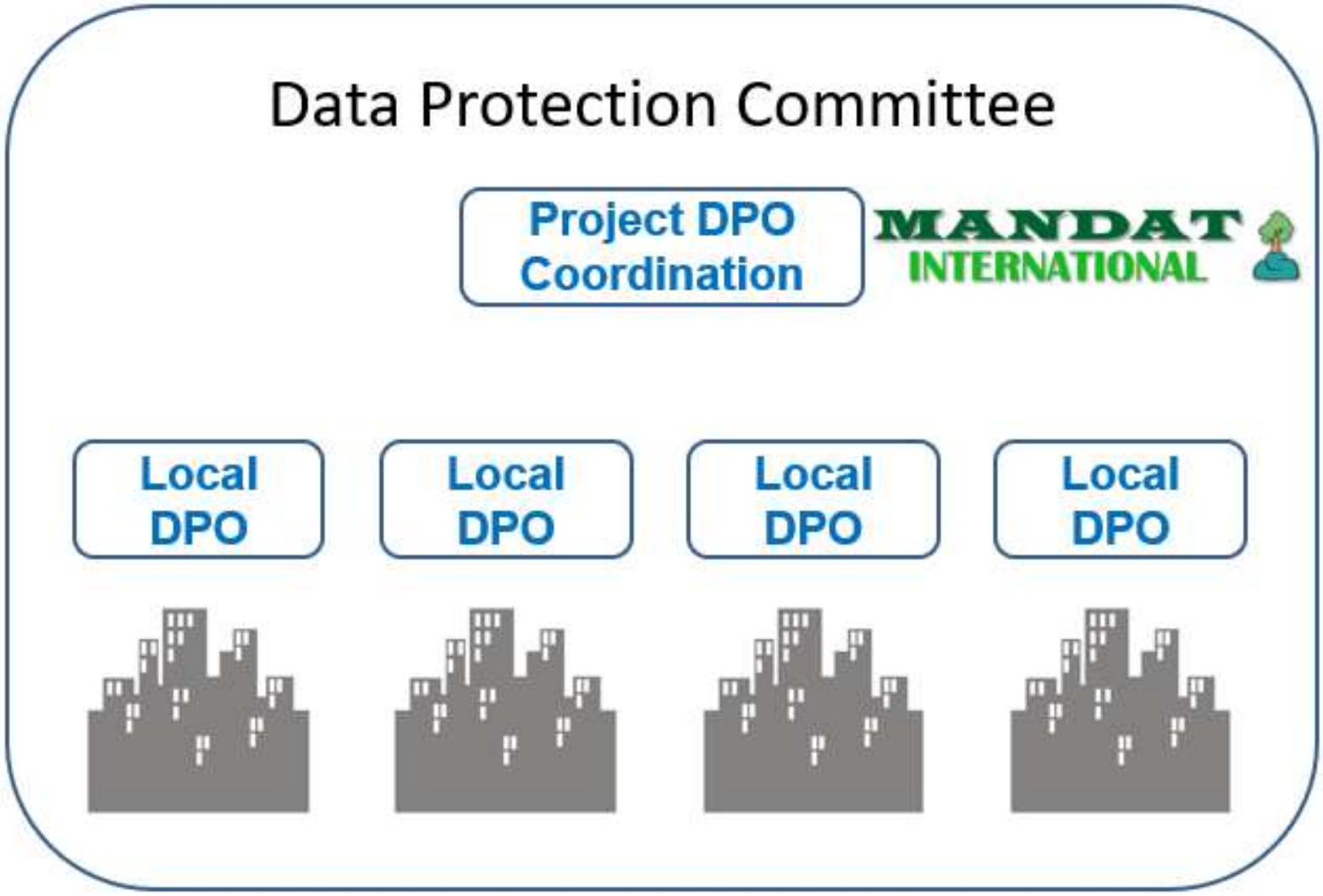
a. the **processing is carried out by a public authority or body**, except for courts acting in their judicial capacity;

b. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require **regular and systematic monitoring of data subjects on a large scale**; or

c. the core activities of the controller or the processor consist of **processing on a large scale of special categories of data** pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. **A group of undertakings may appoint a single data protection officer** provided that a data protection officer is easily accessible from each establishment. 3.Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

Data Protection Coordination



Data Protection Distributed Strategy

DPO Level

- DPO functions and responsibilities, including data protection and GDPR compliance monitoring
- Personal Data collection identification, including data controllers & processors identification
- Data Protection Impact Assessment (DPIA)

Project Level

- Data Protection Policy Coordination
- Public Information and Contact
- Reporting and DP Issues Management

Regular DPOs Telcos

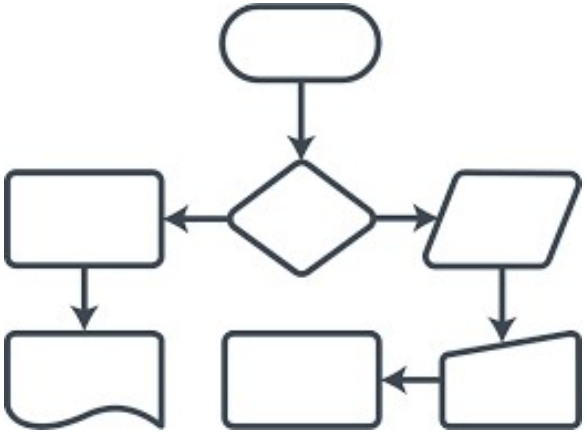
- Regular telcos
- Addressing identified needs
- DPIA support
- Information sharing

Data Protection by Design

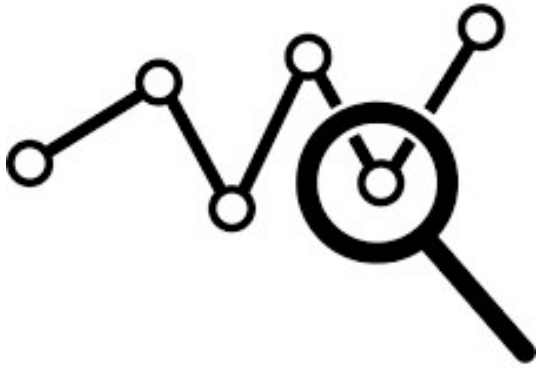
Article 25 Data protection by design and by default

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 for Smart Cities

DELIVERABLE 1.4

Dedicated DPIA developed for Synchronicity

All smart cities requested to perform the DPIA before starting data collection and formal experimentation

Continuous improvement based on cities feedbacks

Accountability tool to demonstrate compliance and respect for data protection

Data Protection Impact Assessment

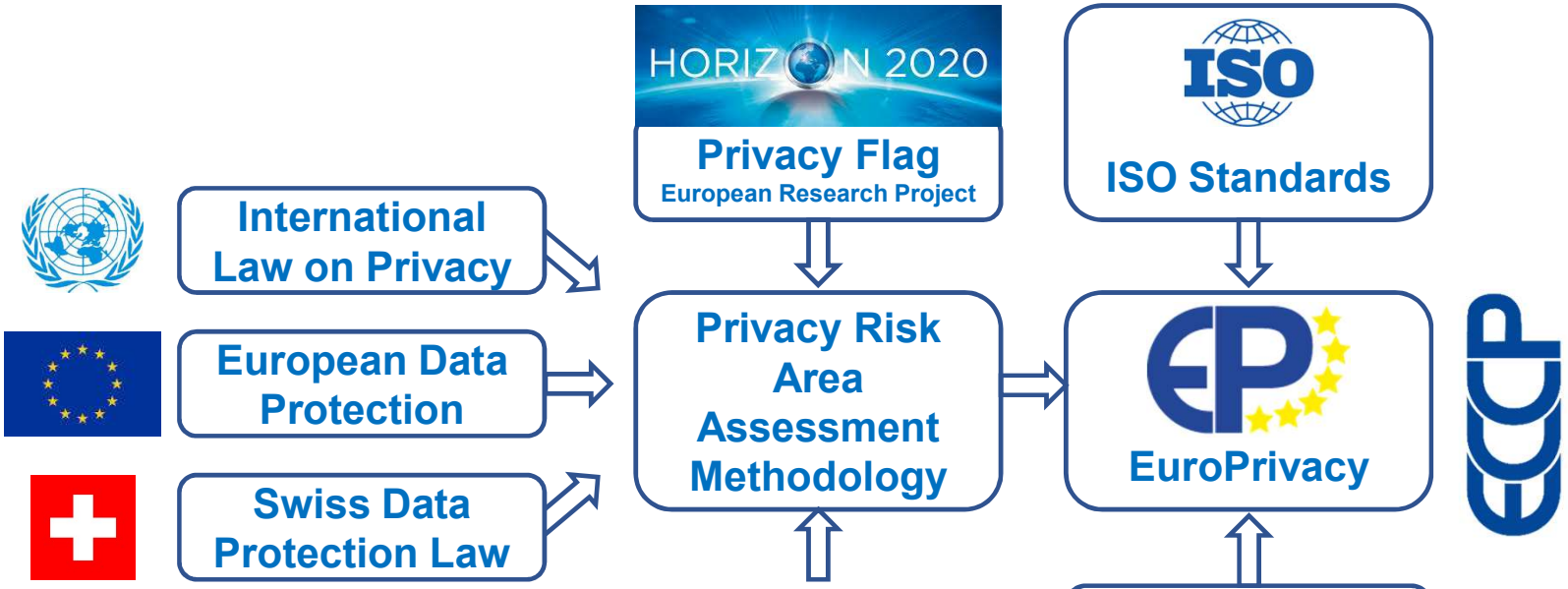
	Dataset #1	Dataset #2	Dataset #3
Title/name of the dataset			
Describe the Category of Internet of Things devices used to collect the data			
How many devices are deployed?			
Identification of Personal Data			
Any data that can be easily linked to individuals shall be considered as "personal data". Please 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 users or users' mobile devices (e.g. tablets, smartphones, smart watches 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			
For what purpose are you collecting these data?	**Autore:** According to Article 35 paragraph 7 of the GDPR, a PIA shall contain "*a systematic description of*		
Information			
Do you provide clear information to the public on the			
How is this information made accessible to the public?			
Is there a clear indication on how to contact the data controller and its data protection officer?			
Data Subject Rights			
Individuals whose data are collected keep rights on their data. Data Controller must ensure the respect of these			
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 city/partners 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 city/partners 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 secure any personal data and prevent unwanted access, modification or deletion. Do			

	FG #1	FG #2	FG #3
Date			
Duration			
Moderator's name			
Moderator's email			
How many participants			
Qualification of participants			
Stakeholders represented			
Please express your view on the objectives of the envisaged processing. Do you think that the city would provide you with a good service in pursuing			
What kind of your personal data are you willing to share with the			

Description of risk	Likelihood of risk (Low/Medium/High)	Severity of the risk impact (Low/Medium/High)	Countermeasures	Controller	Difficulty	Financial Cost	Term
Accidental or unlawful destruction of personal data							
Loss of personal data							
Alteration of personal data							
Unauthorized disclosure of, or access to, personal data							
Financial loss							
Discrimination							
Identity Theft							
Damage to the reputation							
Breach of professional secrecy							
Unauthorised reversal of pseudonymisation							
Other risks (please describe)							
Risk 1							
Risk 2							
Risk 3							
Risk 4							
Risk 5							
Risk 6							
Risk 7							
Risk 8							
Risk 9							
Risk 10							
Risk 11							

Europrivacy Gap Analysis and Certification of Smart Cities

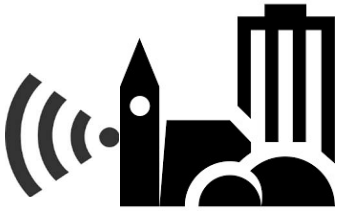
(based on H2020 Privacy Flag research project)



Privacy FLAG ANASTACIA SYNCHRONICITY

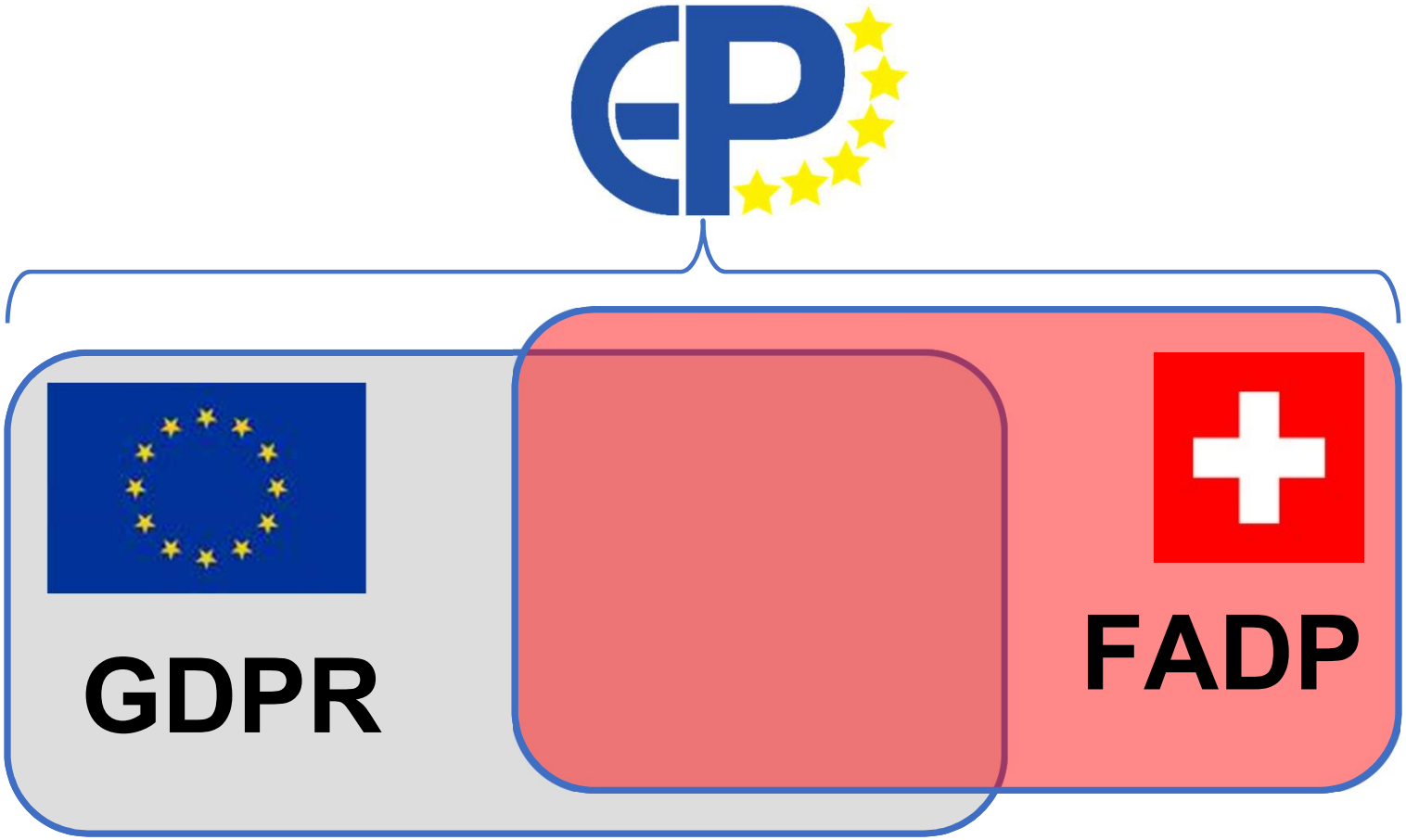
EuroPrivacy
Data Protection Certification

- → **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.com

Encompassing GDPR and National Obligations



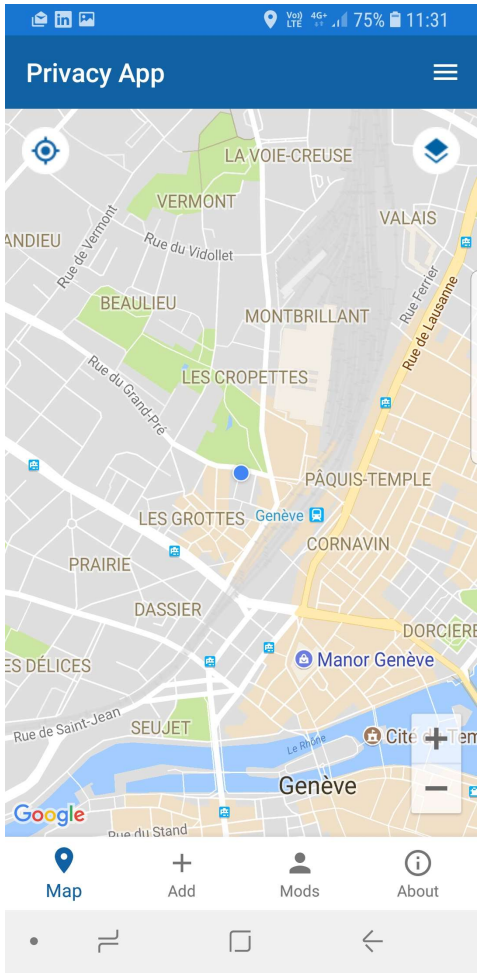
Duty to Inform

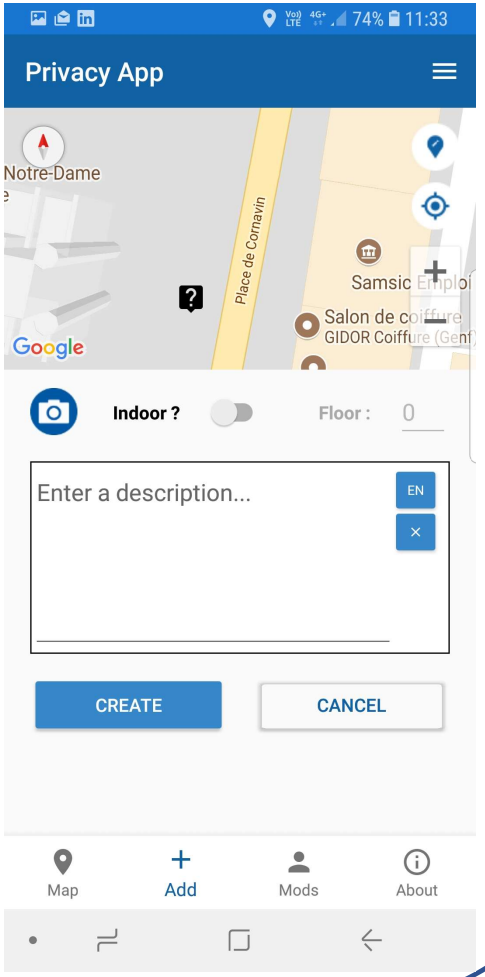
Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject

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.

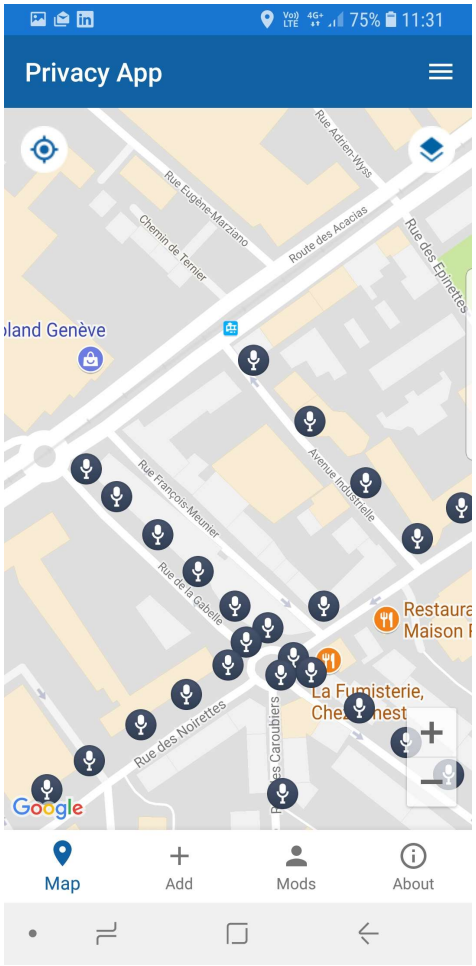
2.**The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. 3.

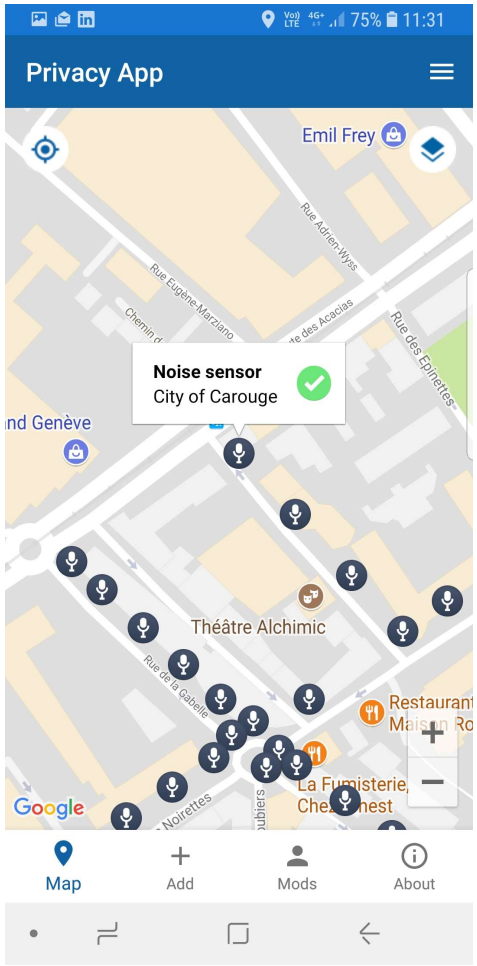
Privacy App

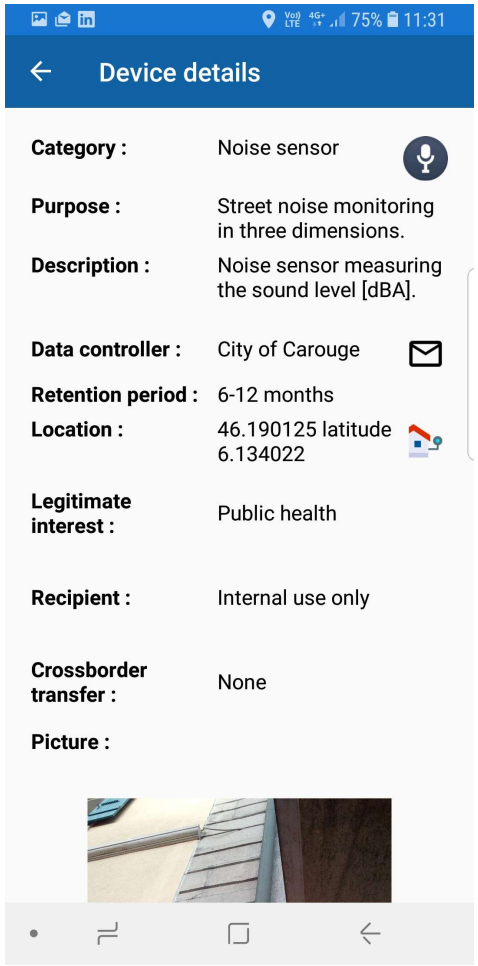

Privacy App
LA VOIE-CREUSE
VERMONT
VALAIS
BEAULIEU
MONTBRILLANT
LES CROPETTES
PÂQUIS-TEMPLE
LES GROTTES
Genève
CORNAVIN
PRAIRIE
DASSIER
Manor Genève
SEUJET
Genève
Google
Map
Add
Mods
About


Privacy App
Notre-Dame
Place de Cornavin
Google
Indoor ?
Floor :
0
Enter a description...
EN
CREATE
CANCEL
Map
Add
Mods
About

Privacy App


75% 11:31
Privacy App
Rue Adrien-Wyss
Rue Eugène-Marziano
Chemin de Terrier
Route des Acacias
Rue des Epinettes
Avenue Industrielle
Rue François-Maunier
Rue de la Gabelle
Rue des Noirettes
Google
Map
Add
Mods
About


75% 11:31
Privacy App
Emil Frey
Noise sensor
City of Carouge
Théâtre Alchimic
Google
Map
Add
Mods
About


75% 11:31
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 :

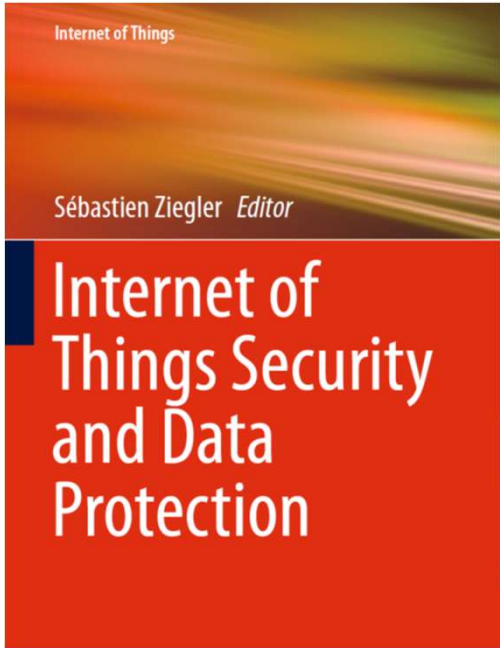
Key Lessons Learned

- GDPR is a research domain per se
  = large potential for innovation
- Underestimation of legal and financial risk; …and Political risk
- Identify and clarify the responsibilities: Mezzanine model
- Continuous improvement process
- Educate, educate, educate
- Be pragmatic and need-driven
- Anticipate evolution and end-user perception
- Strong cross-fertilization potential

More Information

Springer book on

IoT Security and Data Protection



IoT Experts

www.iotexperts.com

SYNCHRONICITY

Thank You !

Visit our website
synchronicity-iot.eu

Follow us on Twitter
@SyncCityIoT

Follow us on Facebook
@SynchroniCityiot

General information
info@synchronicity-iot.eu

Open Call enquiries
helpdesk@synchronicity-iot.eu

Dr Sébastien Ziegler
sziegler@mandint.org