euskaltel

Ibermática

IoT WEEK 2018

Global IoT Summit 2018

BILBAO JUNE 4-7 2018

iotweek.org

globaliotsummit.o
rg

“IoT Security & Data Protection at a Crossroad”

Sébastien Ziegler
Moderator
IoT Forum
President of the IoT Forum and Director Mandat International

Franck Boissière
European Commission, DG CONNECT
Internet of Things Unit
Policy Coordinator & Programme Officer

Roberto Cascella
ECSO - European CiberSecurity Organization
Senior Policy Officer

Juergen Neises
Fujitsu
EMEIA Enterprise & Cyber Security

Luca Bolognini
IIP - Istituto Italiano per la Privacy e la Valorizzazione dei Dati
President and CEO

May 25 2018

Why does it matter?

Universal applicability
for any personal data collected from EU residents

and:

Art 83, al 5

"Infringements of the following provisions shall (…) be subject to administrative fines **up to 20 000 000 EUR**, or in the case of an undertaking, **up to 4 % of the total worldwide annual turnover** of the preceding financial year, whichever is higher…"

Risk Management

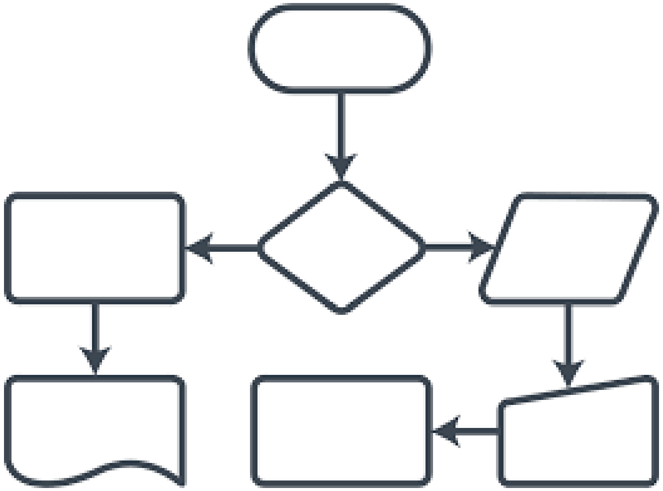
- ***End-user Acceptance***
- ***Legal Risks***
- ***Financial Risks***
- ***Reputational Risks***

Data Protection by Design

Article 25 Data protection by design and by default

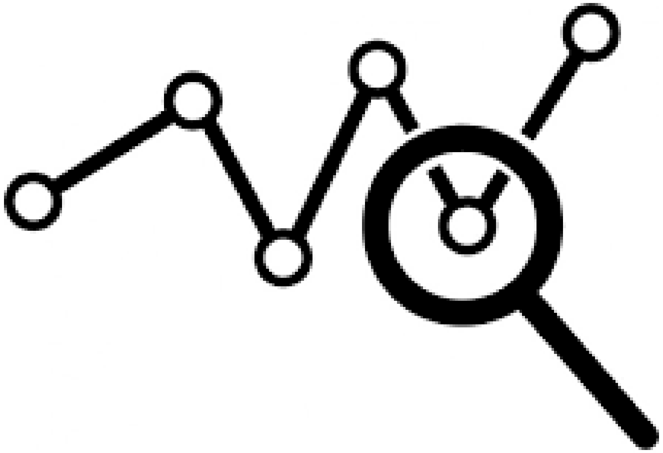
1.Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination 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
- Processes



Analysing:

- Compliance
- Risks
- Risks mitigation

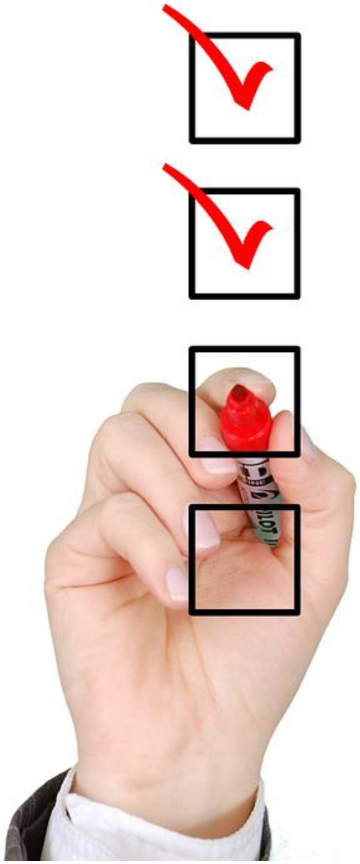
Data Protection Impact Assessment

Art 35, al 3

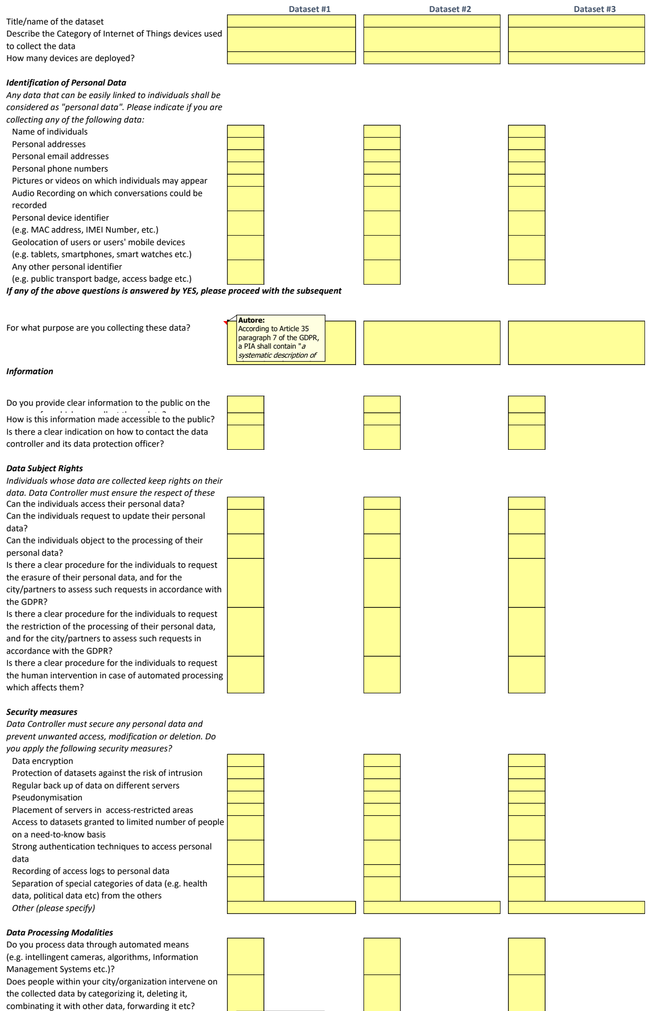
Where a type of processing **in particular using new technologies**, and taking into account the nature, scope, context and purposes of processing, is likely to result in high risk to the rights and freedoms of natural persons, **the controller shall**, prior to the processing, **carry out an assessment 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



Dr Sébastien Ziegler



	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 you apply the following security measures?			
Data encryption			
Protection of datasets against the risk of intrusion			
Regular back up of data on different servers			
Pseudonymisation			
Placement of servers in access-restricted areas			
Access to datasets granted to limited number of people on a need-to-know basis			
Strong authentication techniques to access personal data			
Recording of access logs to personal data			
Separation of special categories of data (e.g. health data, political data etc) from the others			
Other (please specify)			
Data Processing Modalities			
Do you process data through automated means (e.g. intellingent cameras, algorithms, Information Management Systems etc.)?			
Does people within your city/organization intervene on the collected data by categorizing it, deleting it, combinating it with other data, forwarding it etc?			

Duty to Inform

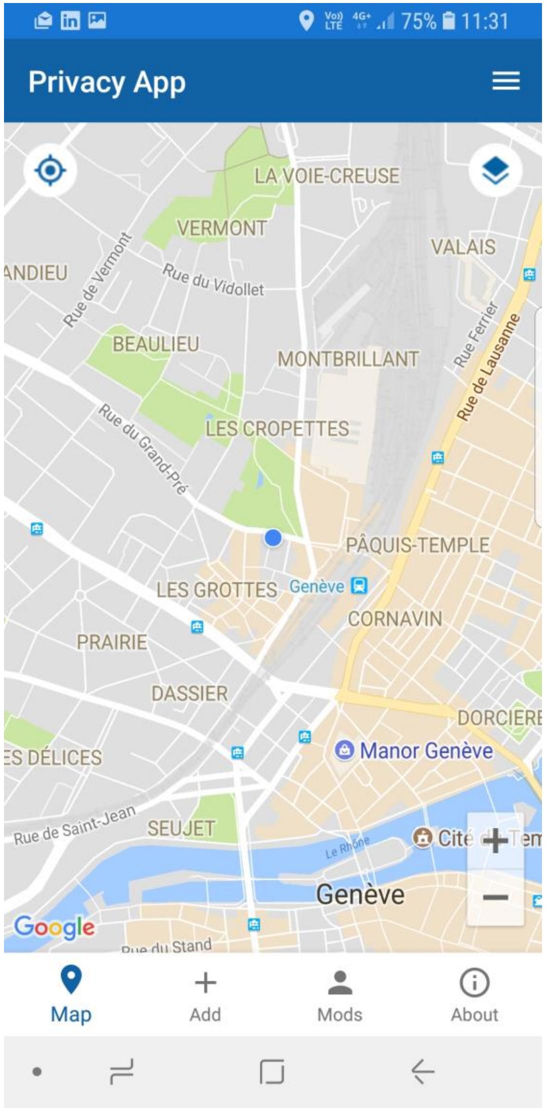
Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject

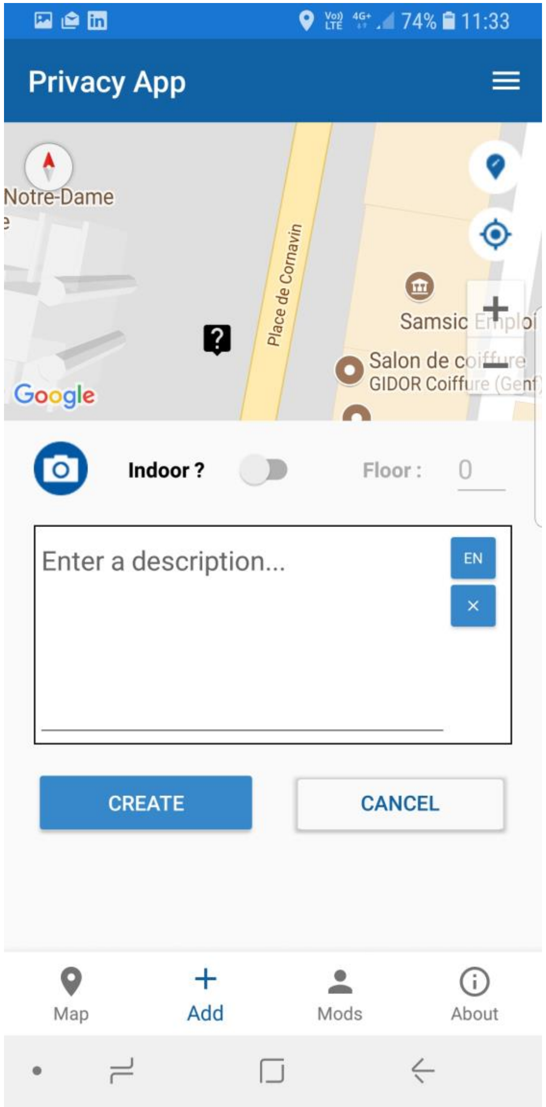
1.**The controller shall take appropriate measures to provide any information** referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 **relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form**, using clear and plain 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.

SYNCHRONICITY

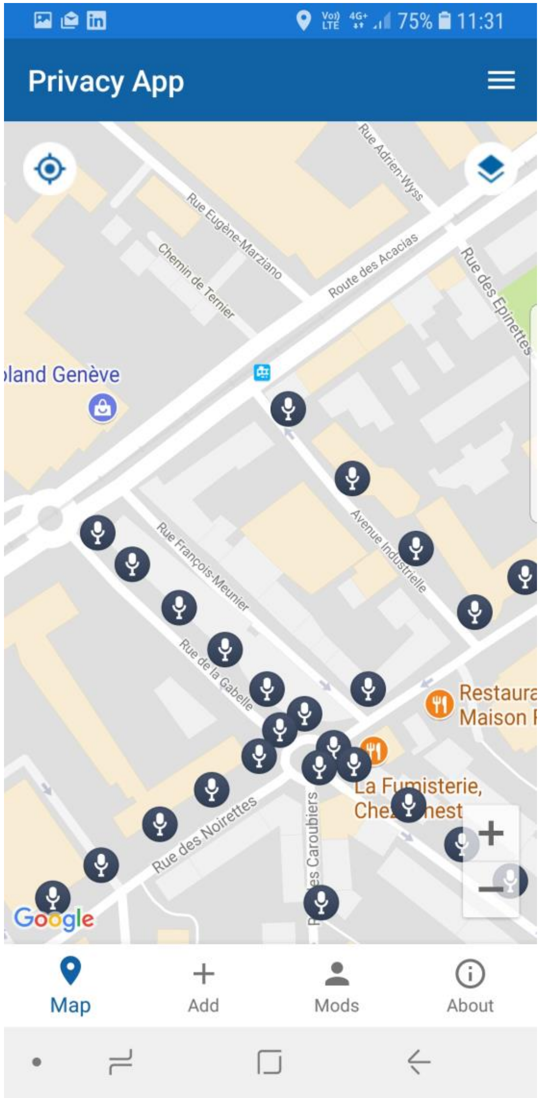
Privacy App

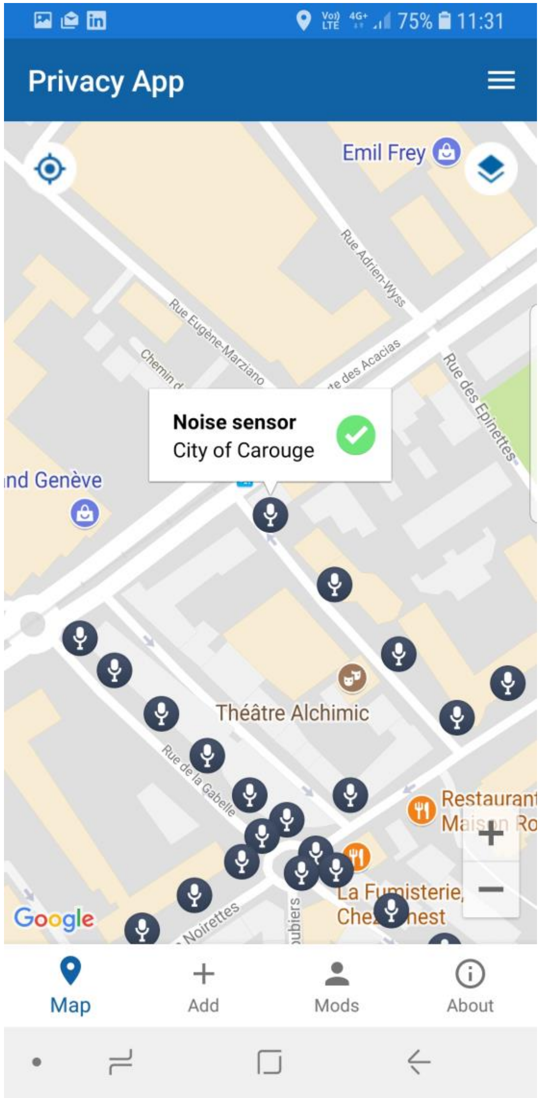


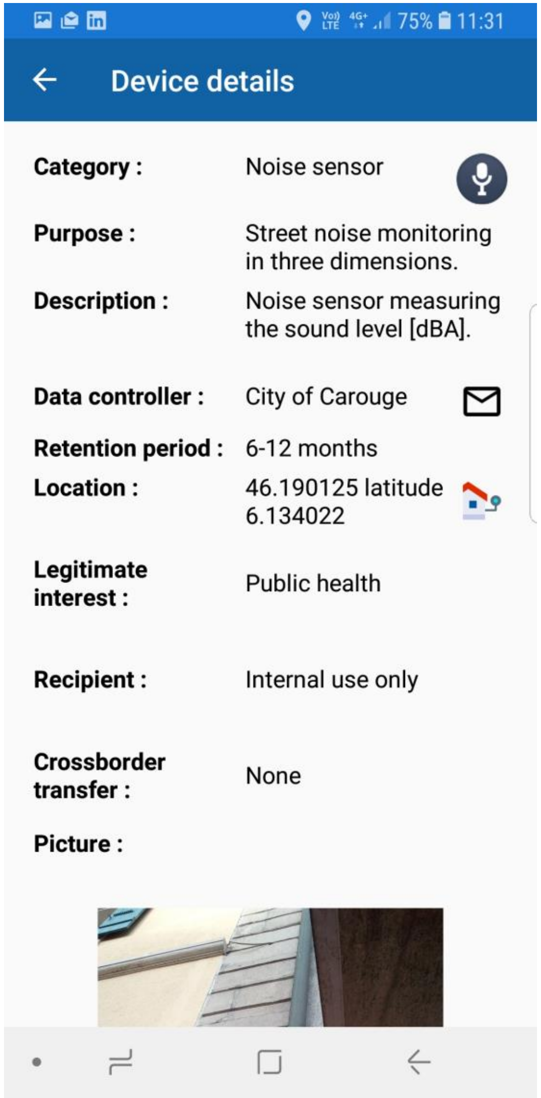


SYNCHRONICITY

Privacy App



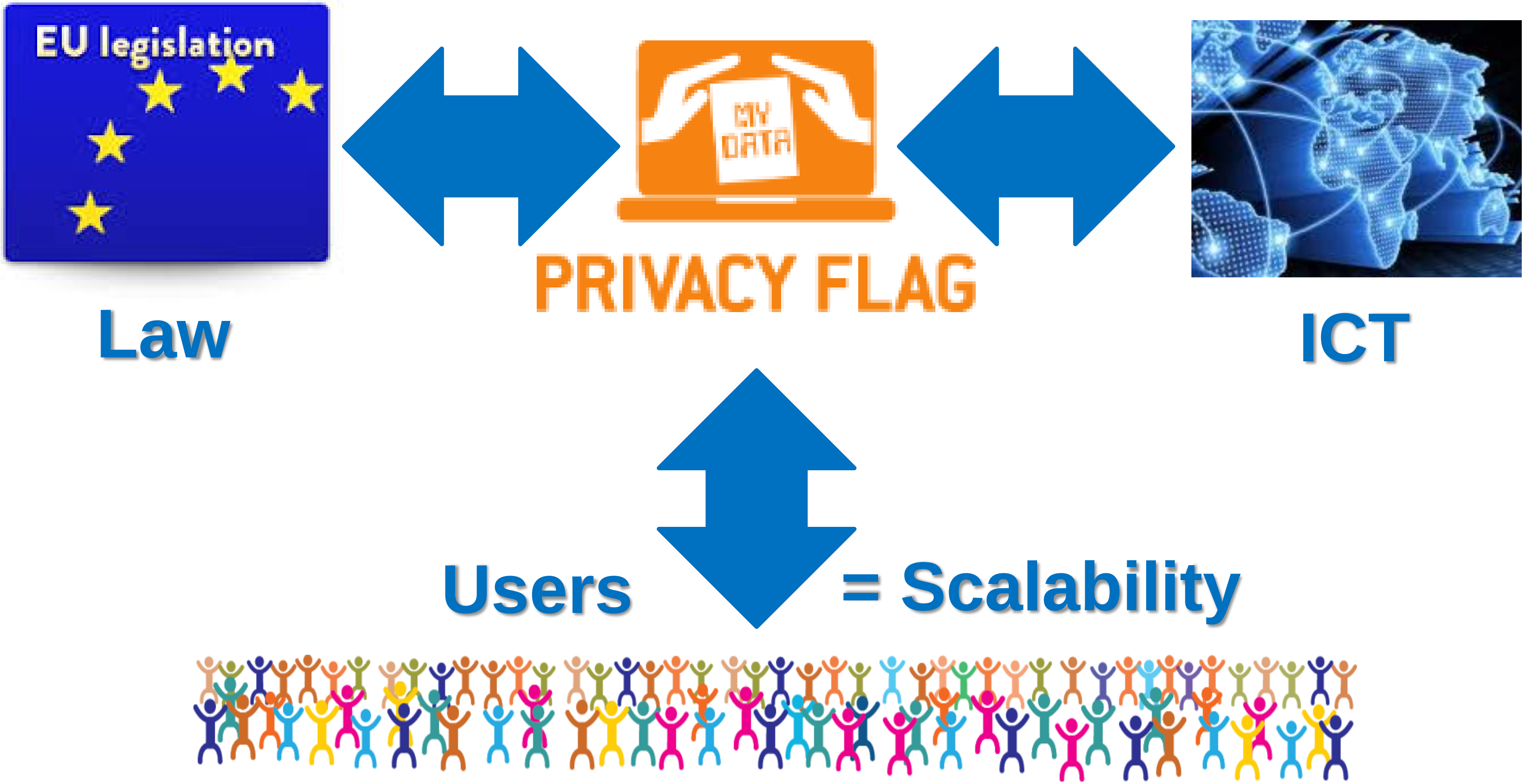



75% 11:31

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 :	

Privacy Flag Approach



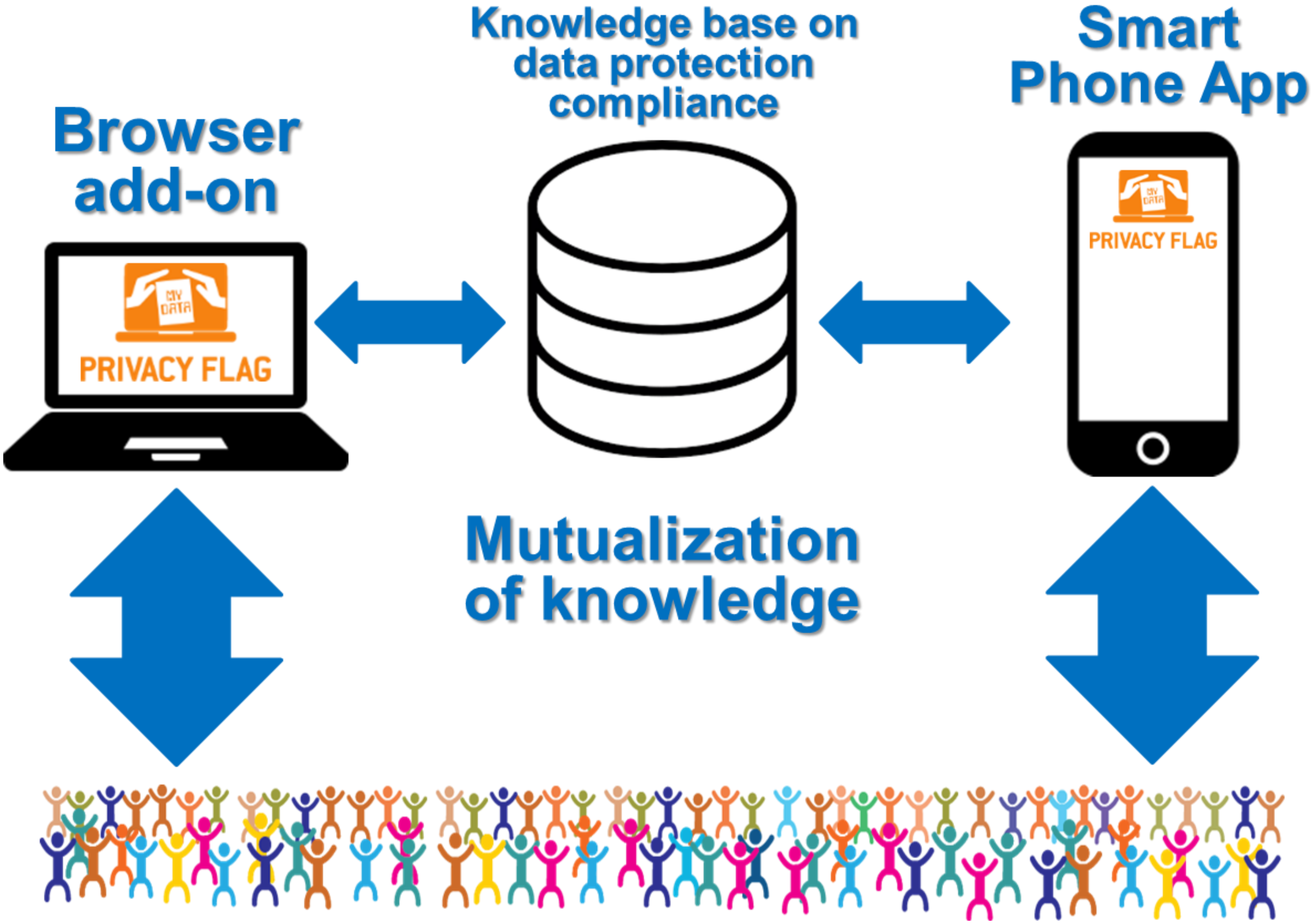
Law

ICT

Users

= Scalability

Crowdsourcing Model



Knowledge base on data protection compliance

Smart Phone App

Browser add-on

Mutualization of knowledge

Certification

Article 42 Certification

1.The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the **establishment of data protection certification mechanisms and of data protection seals and marks**, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

EuroPrivacy

Data Protection Certification

→ **Encompasses European (GDPR), national, and international obligations**

→ **Covers 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

Transitionning

Reactive Approach

Adapting Technology to GDPR

Proactive Approach

Leveraging Technology for GDPR

The ANASTACIA framework includes

1

Security development paradigm

based on the compliance to security best practices and the use of the security components and enablers (this will provide assisted security design, development and deployment cycles to assure security-by-design)

2

Distributed trust and security components and enablers

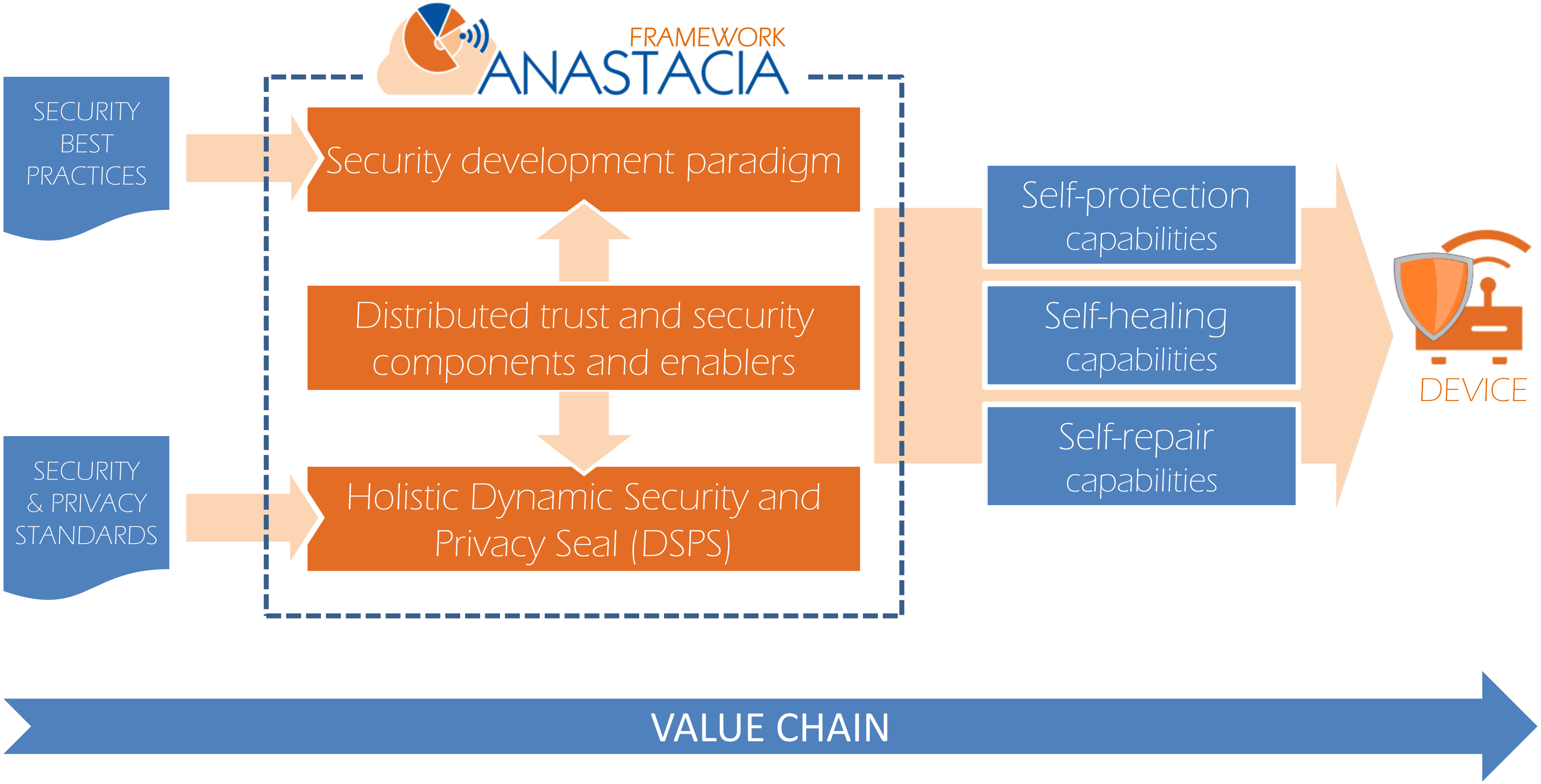
able to dynamically orchestrate and deploy user security policies and actions within complex and dynamic CPS and IoT architectures (online monitoring and testing techniques will allow more automated adaptation of the system to mitigate new and unexpected security vulnerabilities)

3

Holistic Dynamic Security and Privacy Seal (DSPS)

combining security and privacy standards and real time monitoring and online testing (this will provide quantitative and qualitative run-time evaluation of privacy risks and security levels, which can be easily understood and controlled by the final users)

DSPS in the context of ANASTACIA



FRAMEWORK ANASTACIA

SECURITY BEST PRACTICES

SECURITY & PRIVACY STANDARDS

Security development paradigm

Distributed trust and security components and enablers

Holistic Dynamic Security and Privacy Seal (DSPS)

Self-protection capabilities

Self-healing capabilities

Self-repair capabilities

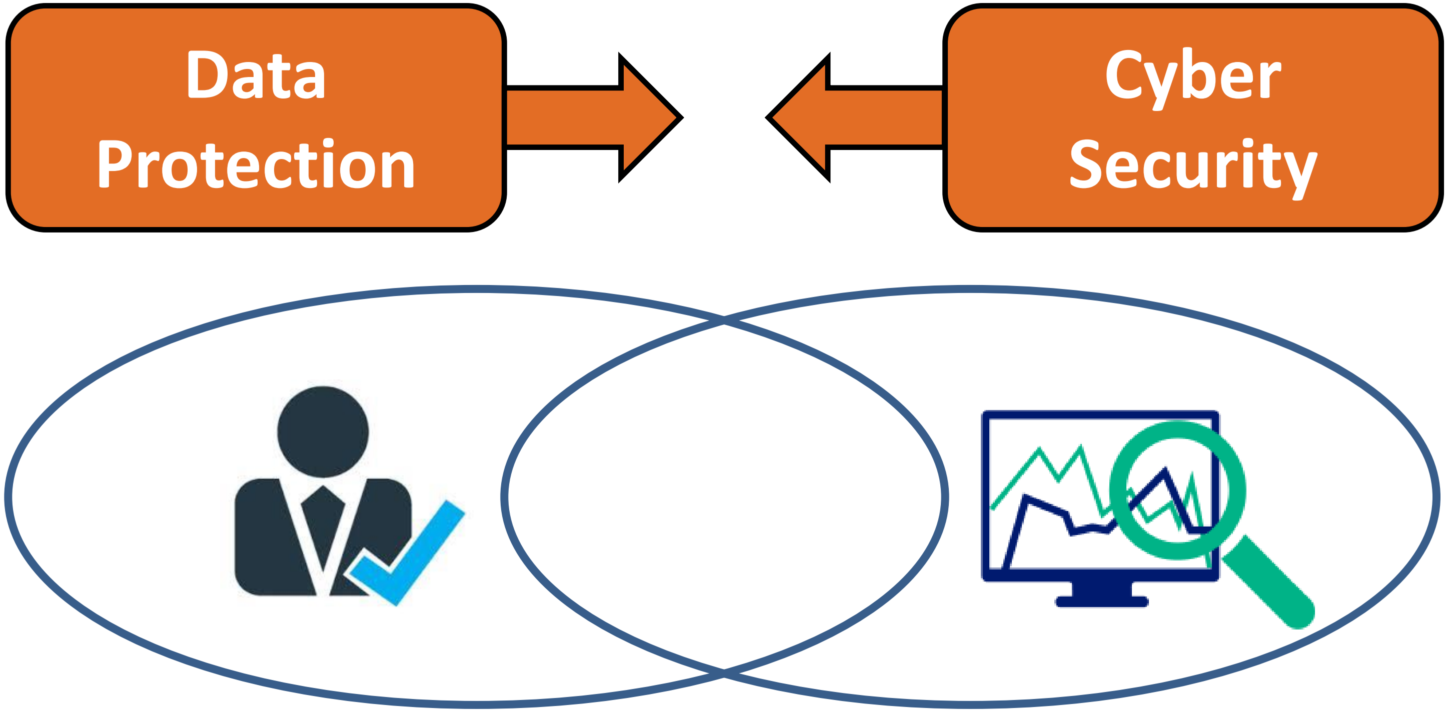
DEVICE

VALUE CHAIN

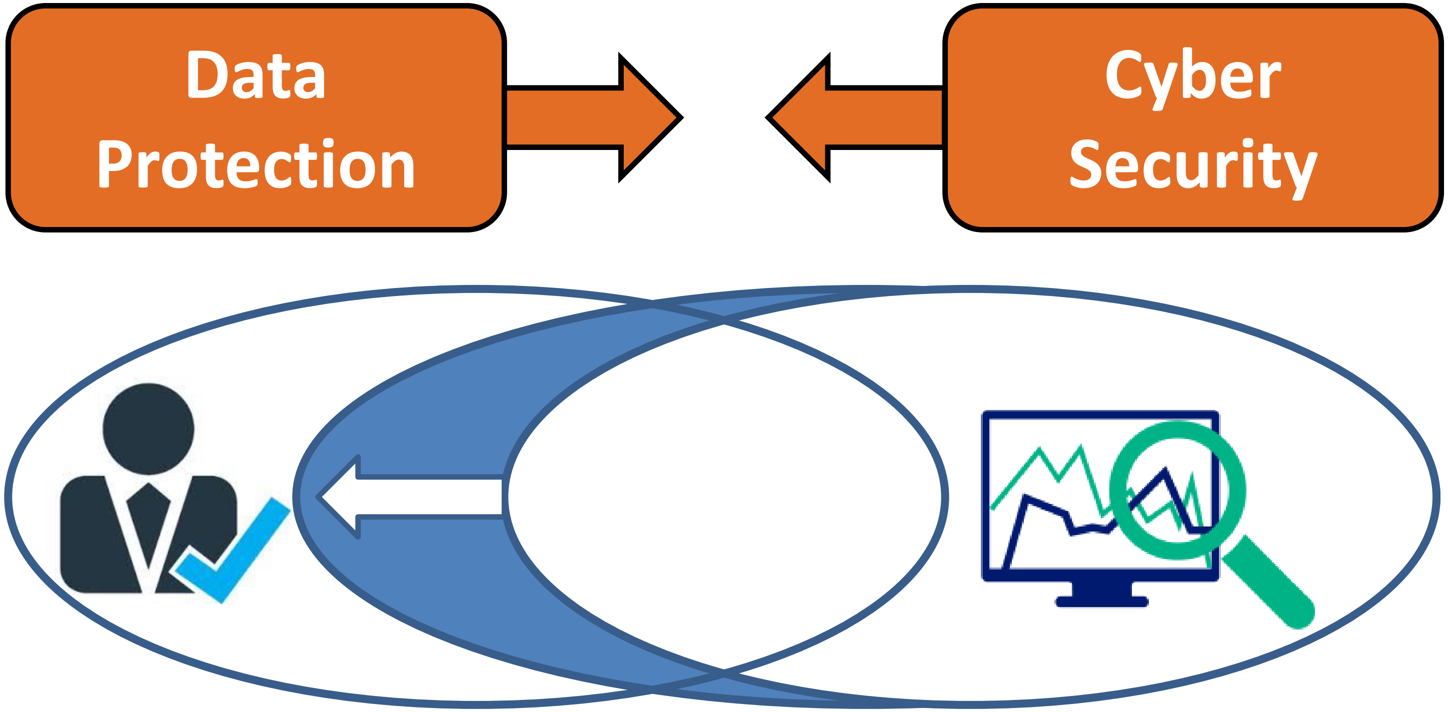
Dynamic Security and Privacy Seal (DSPS)

Real Time
Privacy & Security
Trustability

Asymetric Challenge



Assymetric Challenge



THANK YOU !

Sébastien Ziegler

sziegler@mandint.org
+41 79 750 53 83