

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines



Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

**IOT4SCC: Joint Workshop on IoT for Smart Cities & Communities Platform Convergence:
Breakout C, 7 June 2018**

Outline on Session on Personal Data Protection Strategies and Guidelines



European
Large-Scale Pilots
Programme

Session 1 (12.30 - 13.30)

- Citizen viewpoint for smart cities
 - Mara Balestrini, Ideas for change
- Privacy-by-design viewpoint for smart cities
 - Antonio Kung, Trialog
- Introduction to smart city use case session
- Selection of smart city use case

Session 2 (14.30-15.30)

- Practice / Legal and ethical compliance viewpoint for smart cities
 - Pasquale Annicchino, Archimede Solutions
- Smart city use case session
 - Breaches
 - Threats and consequences
 - Measures
- Conclusion

Citizen viewpoint for smart cities

 **IoT Week Bilbao 2018**
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Mara Balestrami, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Privacy-by-design Viewpoint for Smart Cities



Antonio Kung, Trialog, France

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Antonio Kung



European
Large-Scale Pilots
Programme

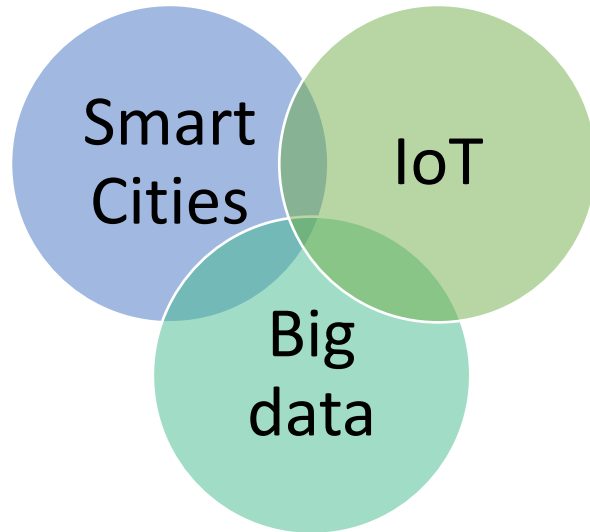
- European projects: PRIPARE, Create-IoT...
- IPEN wiki (ipen.trialog.com)
- EIP-SCC Citizen approach to data: privacy-by-design
 - Workshop London (March 2017)
 - Workshop Milan (July 2017)
 - Workshop Brussels – Eurocities (January 2018)
- Involved in standardisation
 - ISO/IEC 27570 - Privacy guidelines for smart cities
 - ISO/IEC 27030 - Security and privacy guidelines for IoT
 - ISO/IEC 27550 - Privacy engineering for system life cycle processes
 - ISO/IEC 30147 - Methodology for implementing and maintaining trustworthiness of IoT systems and services
 - ISO/IEC 20547-4 – Big data reference architecture – Security and privacy



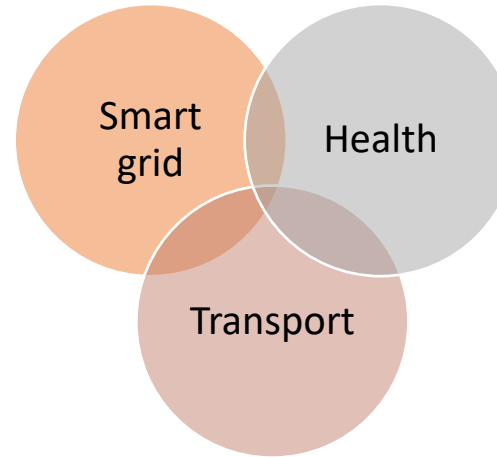
ICT Trend towards Complex Ecosystems



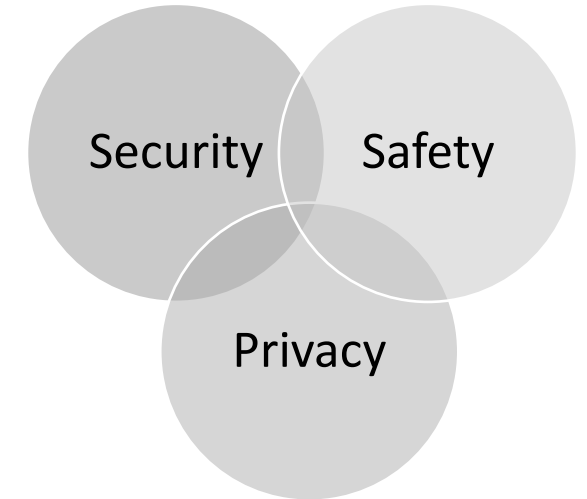
European
Large-Scale Pilots
Programme



Ecosystems



Domains



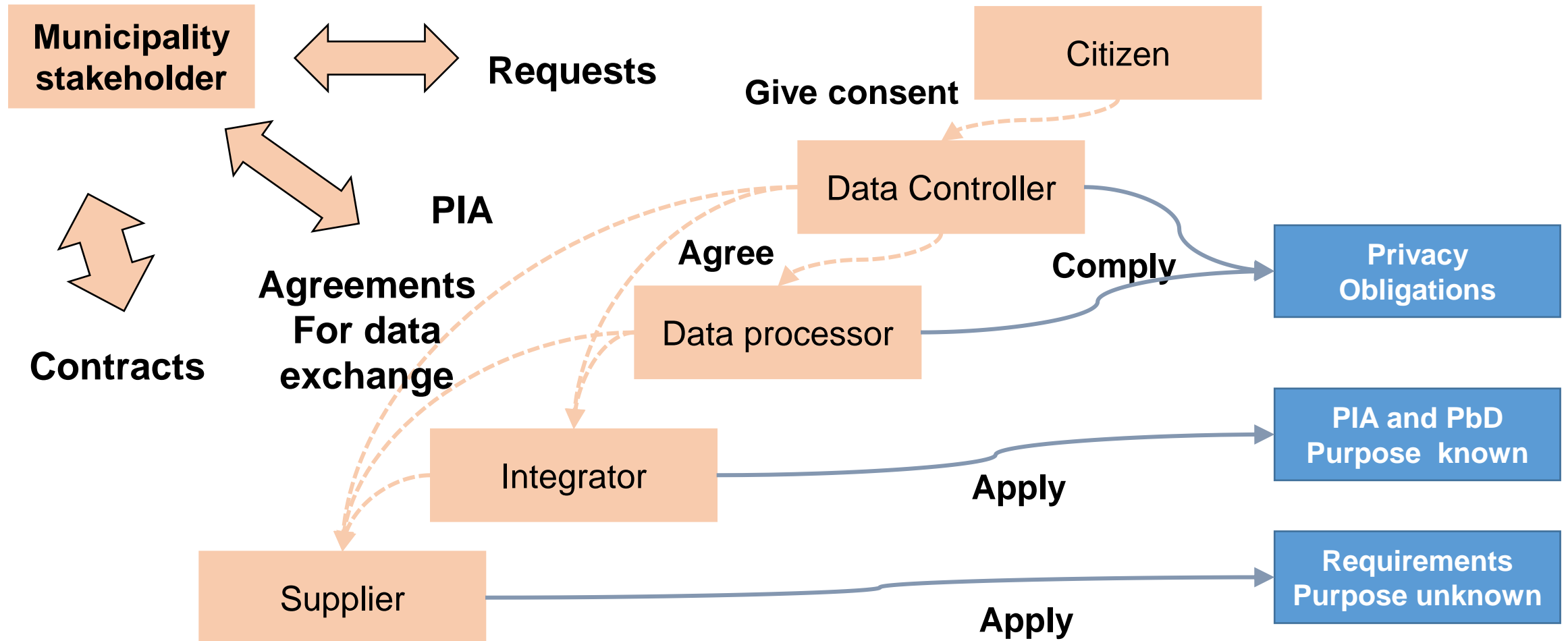
Concerns



Smart Cities Deal with Ecosystems



European
Large-Scale Pilots
Programme



CREATE-IoT



ACTIVAGE
PROJECT



MONICA

SYNCHRONICITY



7

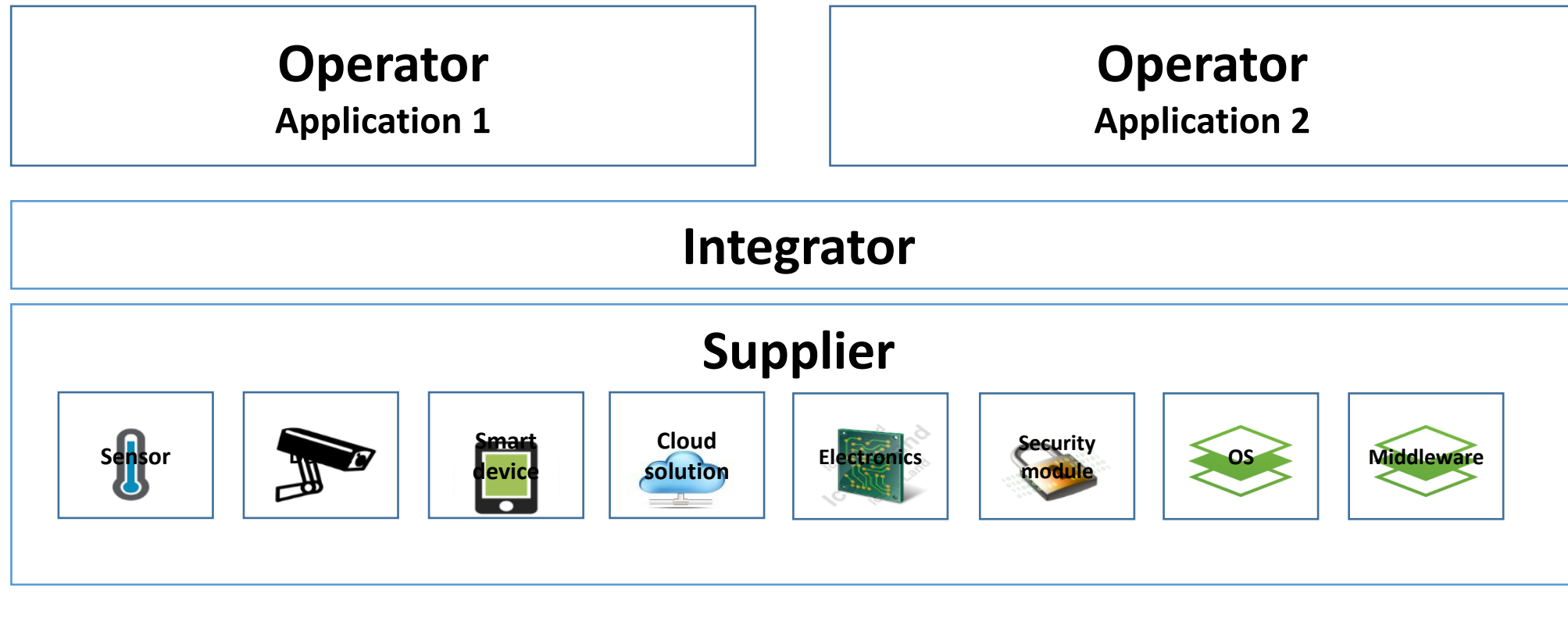
Co-funded by the European Commission



Ecosystems Involve Supply Chains



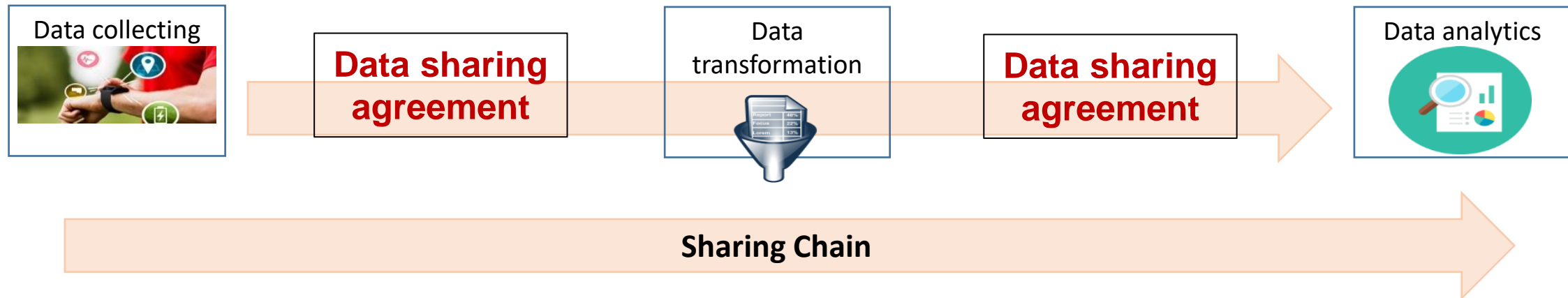
European
Large-Scale Pilots
Programme



Ecosystems Involve Business Exchange



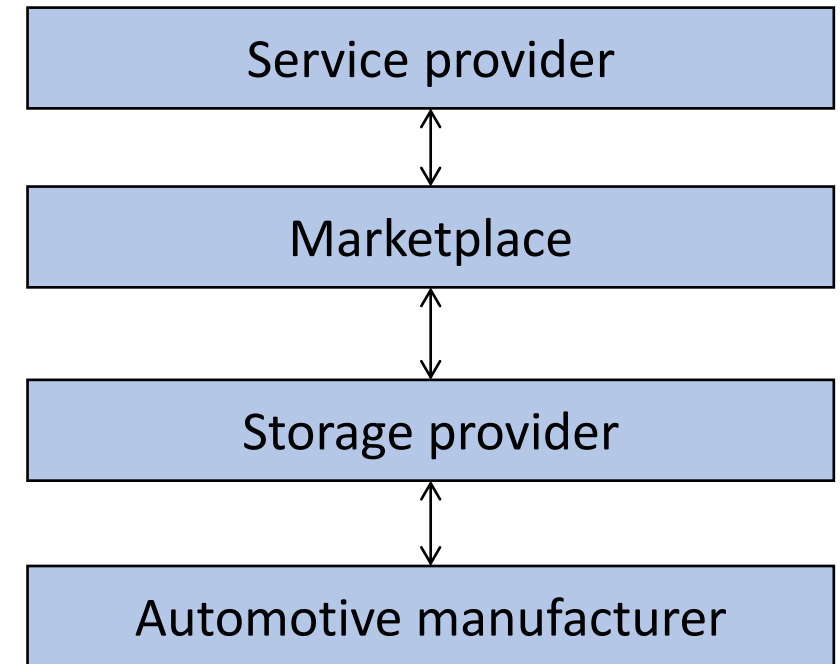
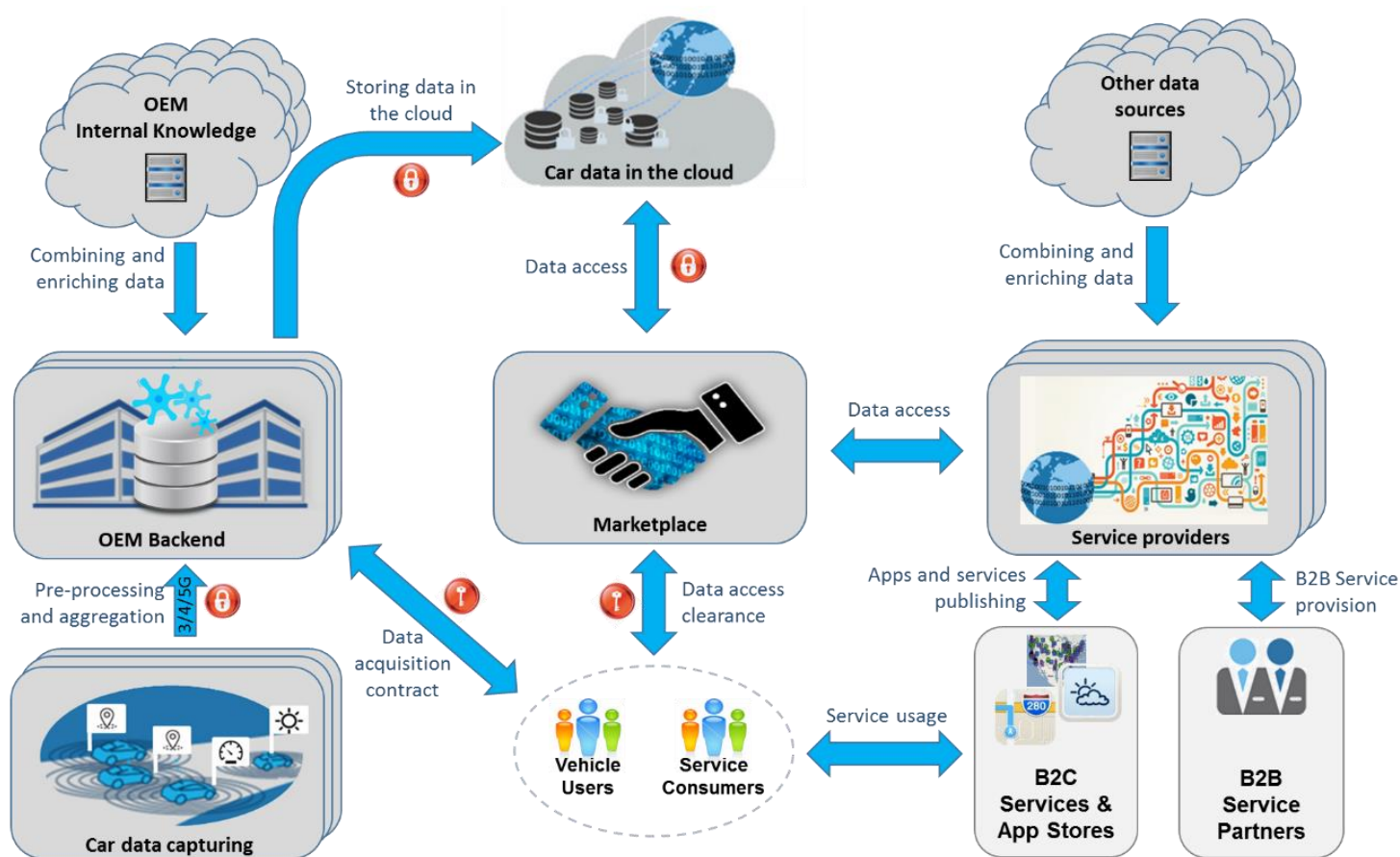
European
Large-Scale Pilots
Programme



Example of Big Data Ecosystem: AutoMat



European
Large-Scale Pilots
Programme



Need to coordinate between ecosystem stakeholders



European
Large-Scale Pilots
Programme

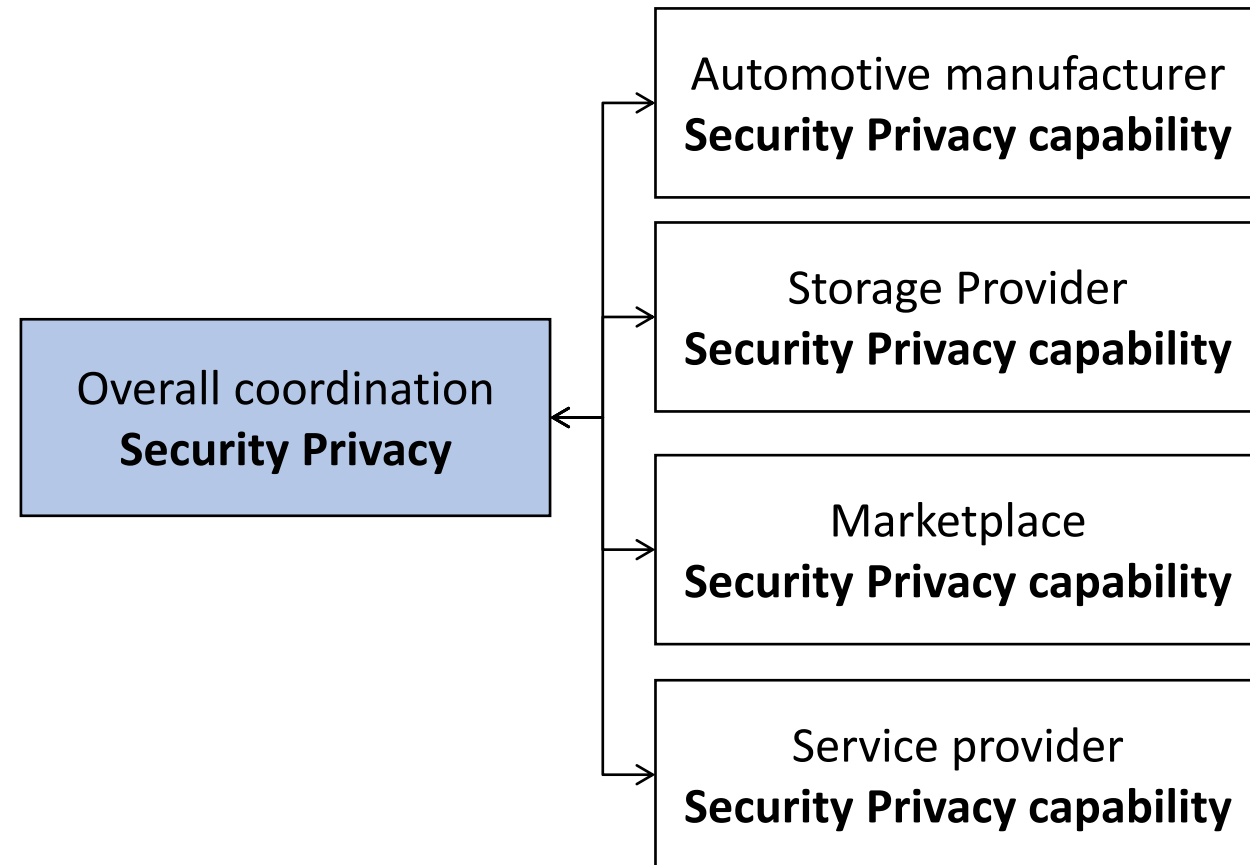
- Example of coordination needs

- **Privacy compliance**

- Global privacy impact assessment vs organisation PIA
 - PII tracking e.g. upon user consent removal
 - Data breach management

- **Cybersecurity compliance**

- Global risk analysis vs organisation risk analysis
 - Cybersecurity incident management

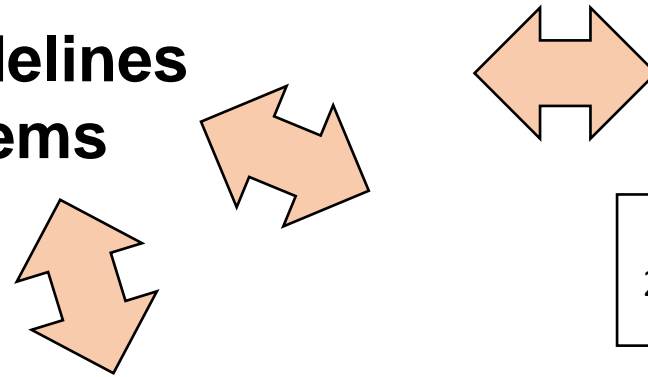


Impact on Standards Landscape



European
Large-Scale Pilots
Programme

Additional guidelines For ecosystems



Privacy Standards for Smart Cities
27570 Privacy guidelines

Privacy Standards for Big Data
20546-4 Security and privacy

Privacy Standards for IoT
27030 Security and privacy guidelines

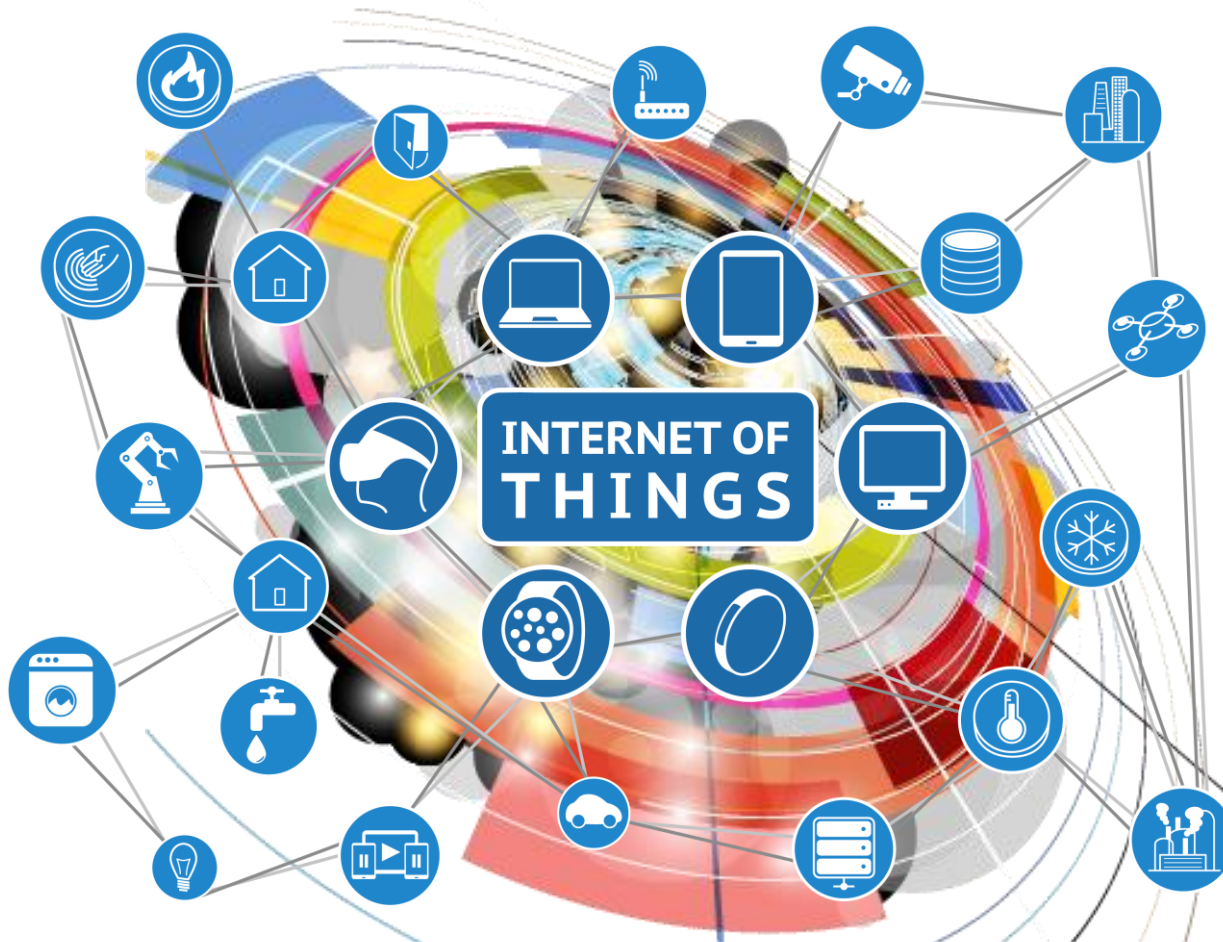
General Privacy Standards

Privacy framework 29100
Privacy impact assessment 29134
Privacy engineering 27550
Code of practice 29151
Privacy Information management systems 27552
OASIS-PMRM

Thank You!



European Large-Scale Pilots Programme



www.european-iot-pilots.eu

www.create-iot.eu



@IOTEULSP



@IoT_euLSP



@CREATE-IoT



@CreateloT_eu

The CREATE-IoT project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732929.

email: antonio.kung@trialog.com



ACTVAGE
PROJECT



MONICA

SYNCHRONICITY



Introduction to smart city use case session



Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

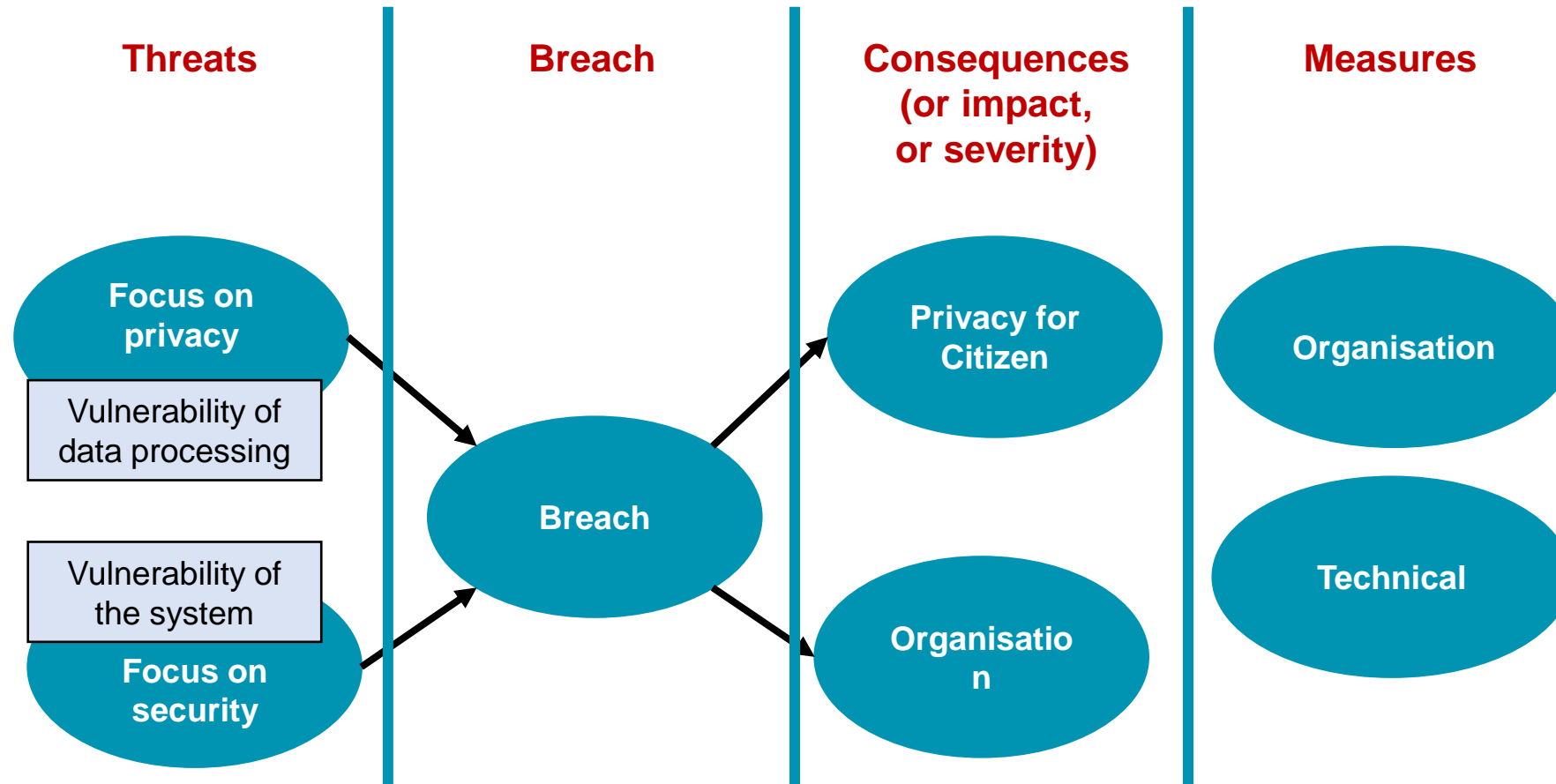
IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

- Many such sessions carried out since 2017
- Participative approach
 - Citizen, Policy makers, Engineers
- Templates based on standards
- Content : impact analysis
 - Breaches
 - Threats and consequences
 - Measures

Security and privacy assessment (based on ISO/IEC 27550)



European
Large-Scale Pilots
Programme



Risk map (based on CNIL guidelines)



European
Large-Scale Pilots
Programme

Maximum Impact	Must be avoided or reduced		<div>A</div> <div>O</div> Absolutely avoided or reduced	
Significant Impact				
Limited Impact	These risks may be taken		Must be reduced	
Negligible Impact				
	Negligible Likelihood	Limited Likelihood	Significant Likelihood	Maximum Likelihood

Example

- Breach: Alice attendance to an Alcoholics Anonymous meeting is made public
- Threat and consequence
 - Threat: Some one hacks into the attendance management system and retrieves the log of attendance
 - Consequence
 - Likelihood significant
 - Impact
 - for Alice could be maximum
 - For the organisation could be significant



Threats (based on LINDDUN and STRIDE)



European
Large-Scale Pilots
Programme

Threat	Property
Linkability	Unlinkability
Identifiability	Anonymity
Non-repudiation	Plausible deniability
Detectability	Undetectability and unobservability
Disclosure of information	Confidentiality
Unawareness	Content awareness
Non compliance	Policy and consent compliance

Threat	Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Nonrepudiation
Information disclosure	Confidentiality
Denial Of Service	Availability
Elevation of privilege	Authorization

Security Measures (based on ISO/IEC 27000)



European
Large-Scale Pilots
Programme

Category	Sub-categories
Policies	Management direction
Organization	Internal organisation Mobile devices and teleworking
Human resource security	Prior to employment During employment Termination and change of employment
Asset management	Responsibility for assets Information classification
Access control	Business requirements of access control User access management User responsibilities System and application access control Media handling
Cryptography	Cryptographic controls
Physical and environmental security	Secure areas Equipment

Category	Sub-categories
Operation security	Operational procedures and responsibilities Protection from malware Backup Logging and monitoring Control of operational software Technical vulnerability management Information systems audit considerations
Communication security	Network security management Information transfer
System acquisition, development and maintenance	Security requirements Security in development processes Test data
Suppliers relationships	Security in supplier relationships Supplier service delivery management
Incident management	Management of incidents and improvements
Business continuity	Information security continuity Redundancies
Compliance	Compliance (legal and contractual) Information security reviews



CREATE-IoT
28 Mai 2018



MONICA

SYNCHRONICITY



19

Co-funded by the European Commission



Atelier cyber Trialog

Privacy measures (based on ISO/IEC 27552)



European
Large-Scale Pilots
Programme

Category	Measures for Data Controllers
Conditions for collection and processing	Identify and document purpose
	Identify lawful basis
	Determine when and how consent is to be obtained
	Obtain and record consent
	Privacy impact assessment
	Contracts with PII processors
	Records related to processing PII
Rights of PII principals	Determining PII principals rights and enabling exercise
	Determining information for PII principals
	Providing information for PII principals
	Provide mechanism to modify or withdraw consent
	Provide mechanism to object to processing
	Sharing the exercising of PII princ
	Correction or erasure
	Providing copy of PII processed
	Request management
	Automated decision taking

Category	Measures for Data Processors
Conditions for collection and processing	Cooperation agreement
	Organization's purposes
	Marketing and advertising use
	Infringing instruction
	PII controller obligations
	Records related to processing PII
Rights of PII principals	Obligations to PII principals

Privacy measures (based on ISO/IEC 27552)



European
Large-Scale Pilots
Programme

Category	Measures for Data Controllers
Privacy-by-design and by-default	Limit collection
	Limit processing
	Define and document PII minimization and de-identification objectives
	Comply with data minimization and de-identification use
	PII de-identification and deletion
	Temporary files
	Retention
	Disposal
	Collection procedures
	PII transmission controls
PII sharing, transfer and disclosure	Identify basis for PII transfer
	Countries and organisations to which PII might be transferred
	Records of transfer of PII
	Records of PII disclosure to third parties
	Joint controller

Category	Measures for Data Processors
Privacy-by-design and by-default	Temporary files
	Return transfer or disposal of PII
	PII transmission controls
PII sharing, transfer and disclosure	Basis for transfert of PII
	Countries and organisations to which PII might be transferred
	Records of PII disclosure to third parties
	Notification of PII disclosure requests
	Legally binding PII disclosures
	Disclosure of subcontractors used to process PII
	Engagement of a subcontractor to process PII
	Change of subcontractor to process PII

The five Results of a Workshop



European
Large-Scale Pilots
Programme

[1] Description of system component, data flow, data process	[2] Breaches, Threats and consequences
[3] Risk map	[4] Measures
[5] Conclusions / Actions	



CREATE-IoT



ACTIVAGE
PROJECT



MONICA

SYNCHRONICITY



22

Co-funded by the European Commission

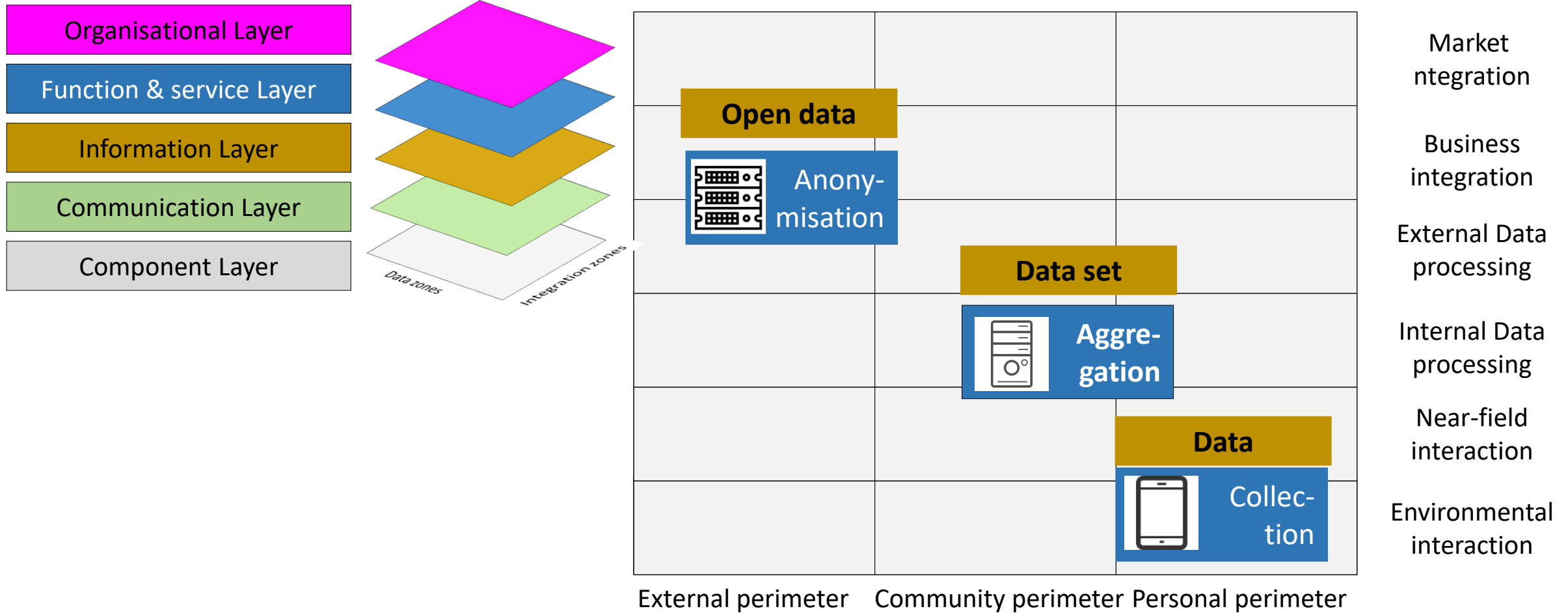


Atelier cyber Trialog

Example: open data



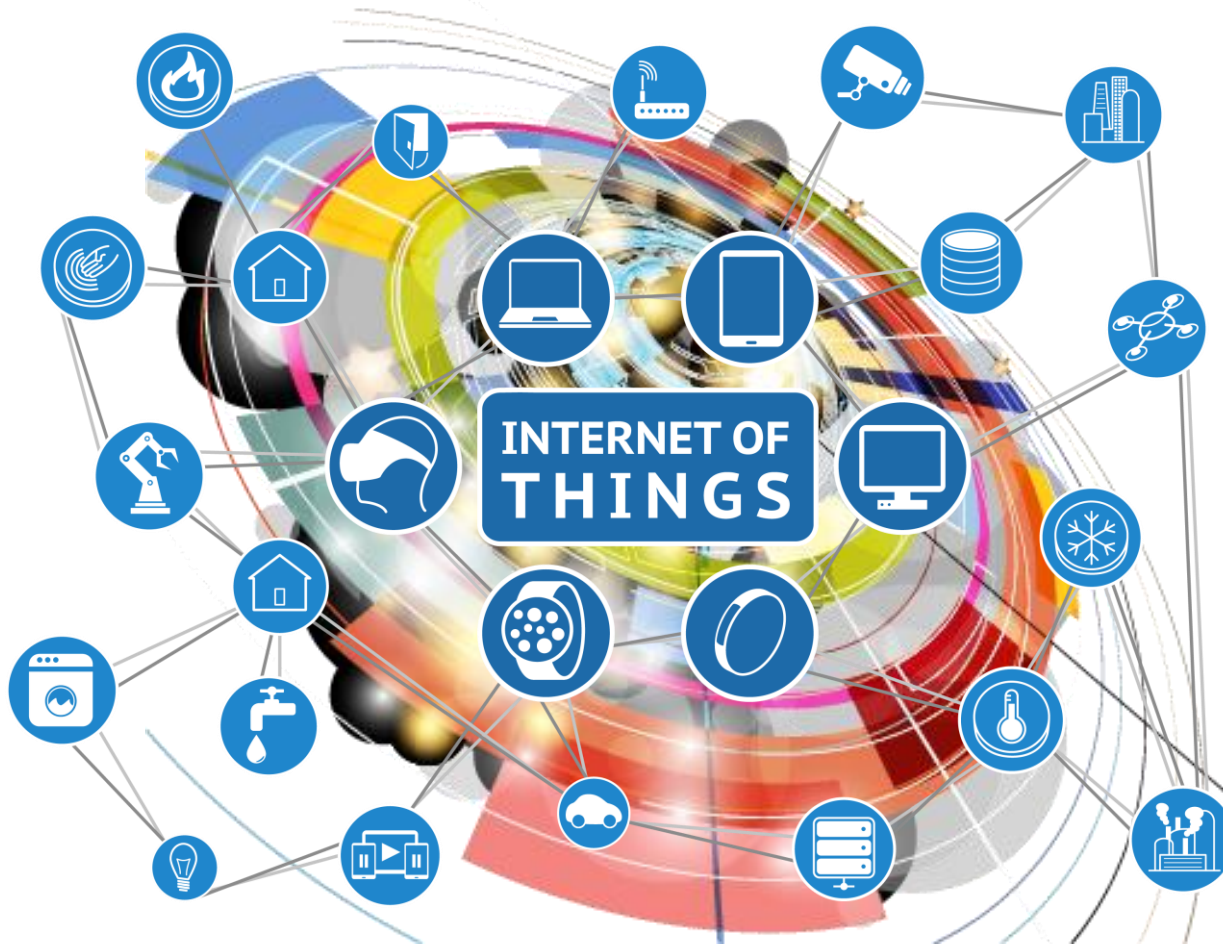
European
Large-Scale Pilots
Programme



Thank You!



European Large-Scale Pilots Programme



www.european-iot-pilots.eu

www.create-iot.eu



@IOTEULSP



@IoT_euLSP



@CREATE-IoT



@CreateloT_eu

The CREATE-IoT project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732929.

email: antonio.kung@trialog.com



ACTVAGE
PROJECT



MONICA

SYNCHRONICITY



Selection of Use Case



Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Use case



European
Large-Scale Pilots
Programme

- Open data
 - Data collected from citizen activities (e.g. smart phones)
 - Data aggregated and anonymised by smart city service
- Other use case
 - Bike sharing application based on smart phone
 - Service provider wishes to trade collected data(e.g. status of road)
 - Specific IoT devices added for instance RFID sensors

Legal and Ethical Compliance Viewpoint for Smart Cities



Pasquale Annicchino, Archimede Solutions, Switzerland

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Smart city use case session: Breaches

 **IoT Week Bilbao 2018**
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

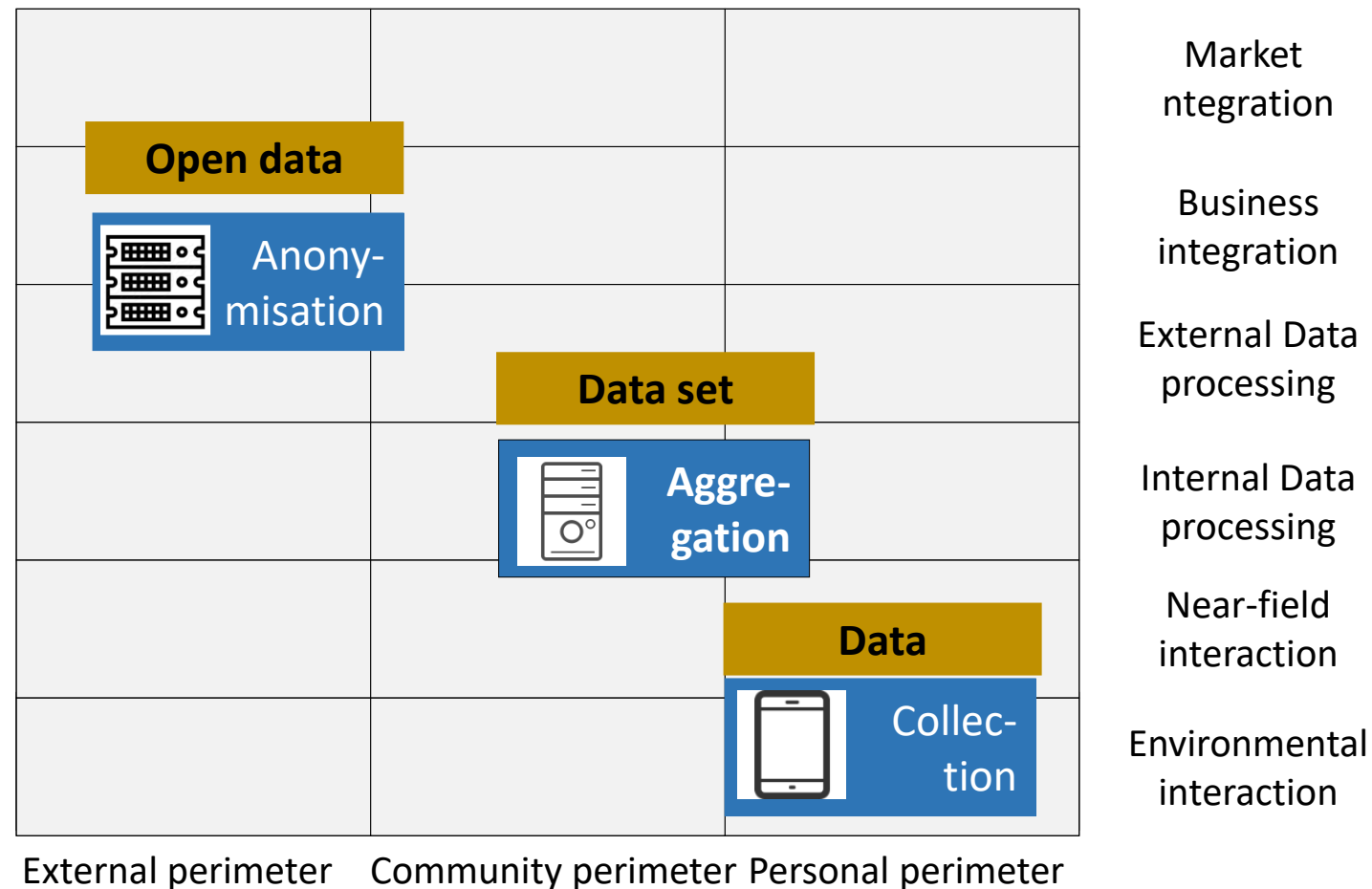
IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Open Data Breaches



European
Large-Scale Pilots
Programme

- Massive personal data leak
- Massive business data leak
- Fake data

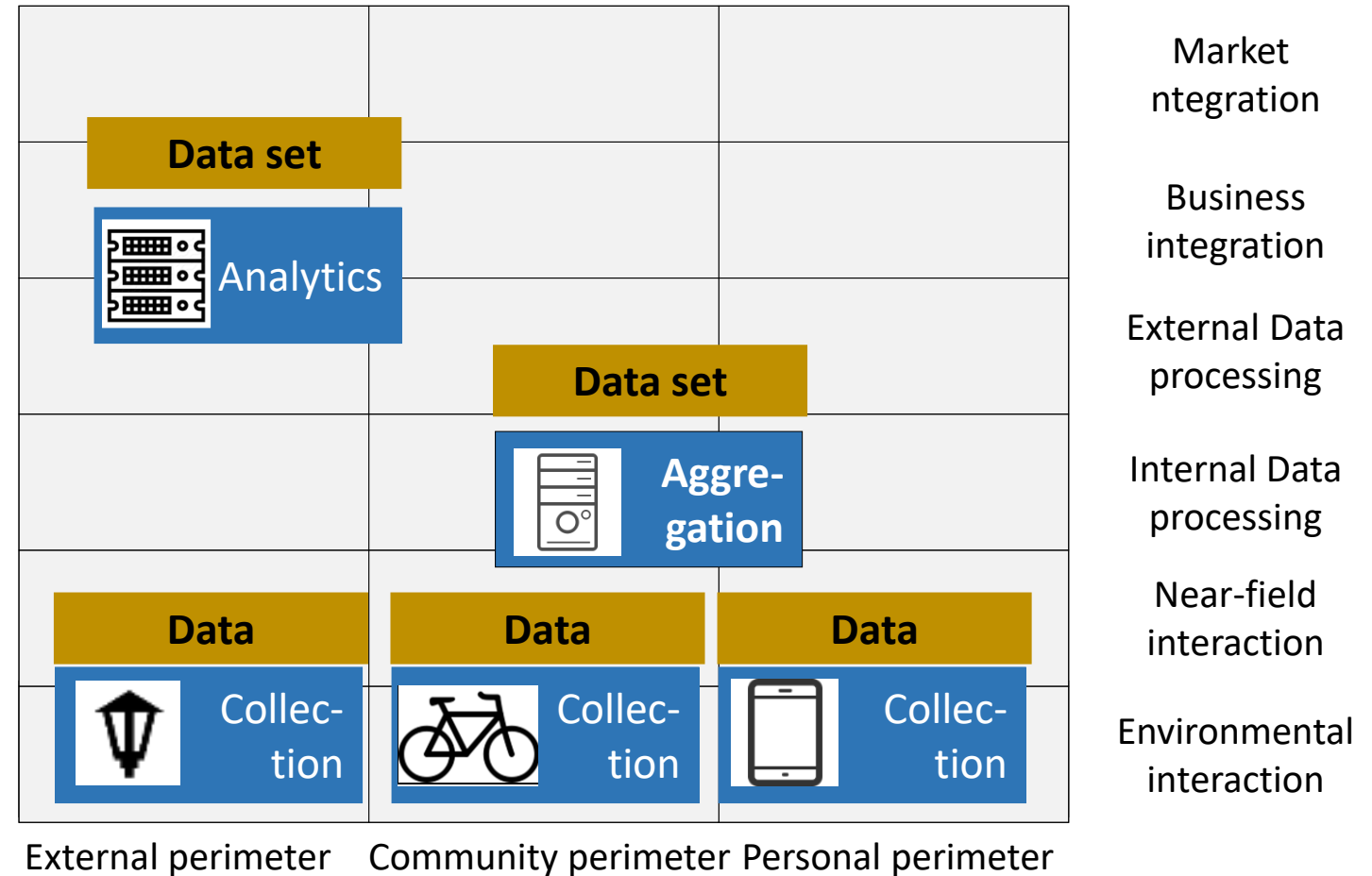


Bike Sharing Breaches



European
Large-Scale Pilots
Programme

- Massive personal data leaks
- Injecting fake data
- Manipulation of data to get commercial advantage
- Misuse of the location of individual data



Smart city use case session: Threats and Consequences

 **IoT Week Bilbao 2018**
4-7 JUNE 2018, BILBAO (SPAIN)
EUSKALDUNA CONFERENCE CENTRE

Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

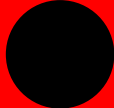
IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Open Data Threat and Consequences



European
Large-Scale Pilots
Programme

- Massive privacy leak
 - **Weak anonymization**
- Massive business data leak
- Fake data

Maximum Impact	Must be avoided or reduced	 Absolutely avoided or reduced		
Significant Impact				
Limited Impact	These risks may be taken	Must be reduced		
Negligible Impact				
	Negligible Likelihood	Limited Likelihood	Significant Likelihood	Maximum Likelihood

Bike Sharing Threat and Consequences



European
Large-Scale Pilots
Programme

- Massive personal data leaks
- Injecting fake data
 - Using bikes to simulate bumps
- Manipulation of data to get commercial advantage
 - Unauthorised access to companies' system
- Misuse of the location of individual data

Maximum Impact	Must be avoided or reduced		Absolutely avoided or reduced	
Significant Impact				
Limited Impact	These risks may be taken		Must be reduced	
Negligible Impact				
	Negligible Likelihood	Limited Likelihood	Significant Likelihood	Maximum Likelihood



CREATE-IoT



ACTIVAGE
PROJECT



MONICA

SYNCHRONICITY



33

Co-funded by the European Commission



Smart city use case session: Measures



Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Use Case Measures



European
Large-Scale Pilots
Programme

- Open data use case Incident management
 - Smart city PR, Smart city management team
 - Periodic incident drill
 - Remove open data repository
 - Removing the data
 - Maintain traceability of open data processing
 - Information security (access)
 - To have updated anonymization processes
 - Transparency
- Bike sharing session
 - Fake data
 - Plausibility check
 - Anomaly detection

Smart city use case session: Conclusions



Antonio Kung, Trialog, France
Mara Balestrani, Ideas for change, Spain

IoT and Smart Cities: Personal Data Protection Strategies and Guidelines, 7 June 2018

Conclusion: ISO/IEC 27570 Privacy guidelines for smart cities



European
Large-Scale Pilots
Programme

- Time line

- February 2018 - Acceptance of project
- May 2018 - 1st Working draft
- February 2021 or earlier - Standard publication

1	Reference number of working document: ISO/IEC JTC 1/SC 27 N 1276
2	Date: 2018-06-03
3	Reference number of document: ISO/IEC WD 27570
4	Committee identification: ISO/IEC JTC 1/SC 27/WG 5
5	Secretariat: DIN
6	
7	
8	
9	Information technology — Security techniques — Privacy
10	guidelines for smart cities
11	<i>Technologies de l'information — Techniques de sécurité — Lignes directrices pour la vie privée dans les villes</i>
12	<i>intelligentes</i>
13	

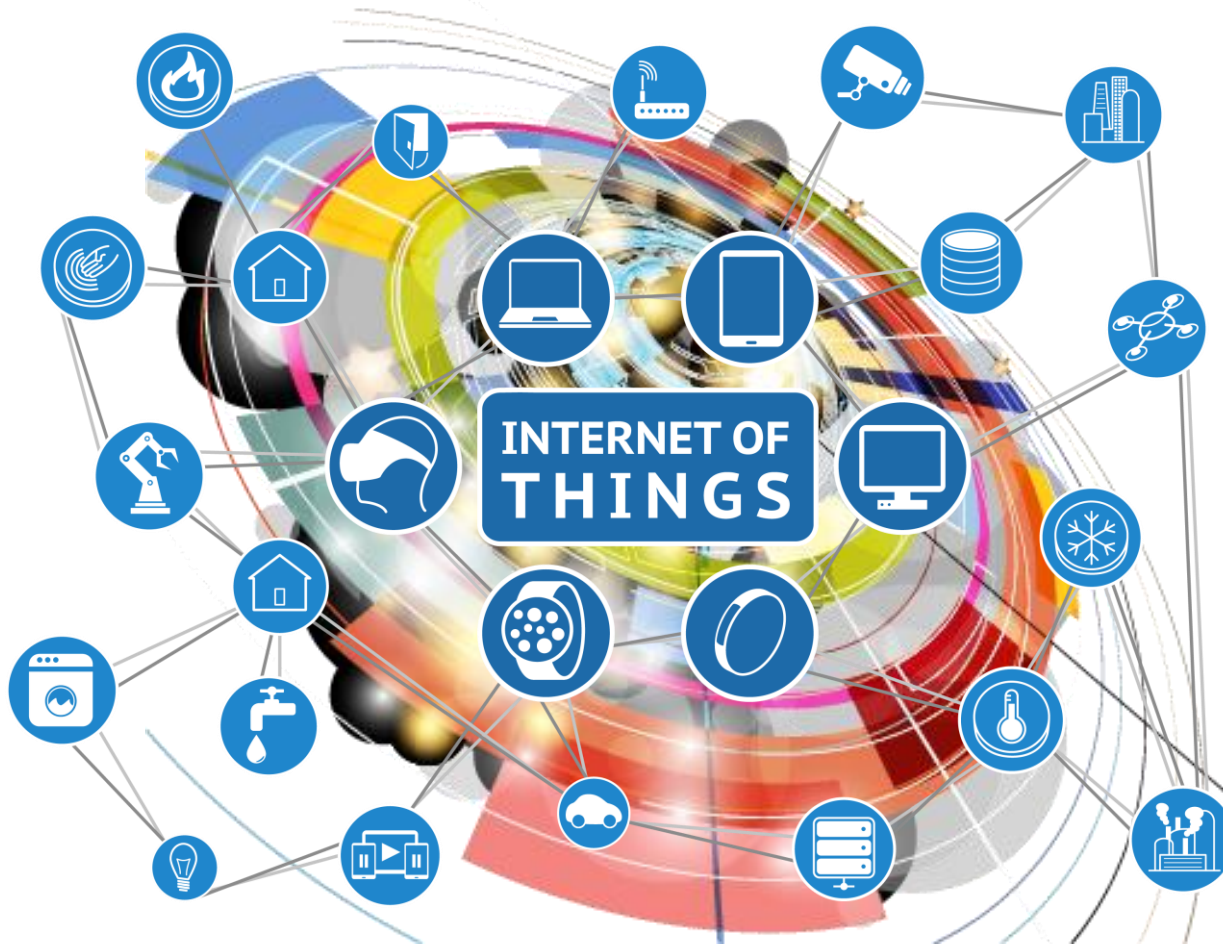
- Current content

- Privacy in smart cities
 - Actors
 - Use cases example
 - Challenges for privacy
 - Common threats and risks
- Guidelines for ecosystem coordination
 - Organisation application of security and privacy processes
 - Ecosystem application of security and privacy processes
- Guidelines for smart city processes
 - Governance
 - Requirements
 - Risk analysis
 - Life cycle
 - Citizen engagement

Thank You!



European Large-Scale Pilots Programme



www.european-iot-pilots.eu

www.create-iot.eu



@IOTEULSP



@IoT_euLSP



@CREATE-IoT



@CreateloT_eu

The CREATE-IoT project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732929.

email: antonio.kung@trialog.com



ACTVAGE
PROJECT



MONICA

SYNCHRONICITY

