CREATE-IoT

H2020 Work Programme 2016-2017
H202-IoT-02-2016
Duration: 36 months

European Large-Scale Pilots Programme

CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT

H2020 – CREATE-IoT Project

Deliverable 05.07

Legal IoT Framework Common Event

Revision: 1.00
Due date: 30-06-2019 (m30)
Actual submission date: 19-07-2019
Lead partner: AS

European Commission

Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Summary					
No and name	**D05.07 Legal IoT Framework Common Event**				
Status	Released	**Due**	m30	**Date**	30-06-2019
Author(s)	P. Annicchino (AS), D. Stefanatou (AL), A. Kung (TL), O. Vermesan (SINTEF), R. Bahr (SINTEF)				
Editor	P. Annicchino (AS)				
DoW	Common event with the LSPs addressing IoT legal framework. The formal deliverable is the event arrangement itself. This document, thus, provides for a follow-up overview summarizing the discussions and the resulting findings.				
Comments					

Document history			
Rev.	**Date**	**Author**	**Description**
0.00	26-01-2019	SINTEF	Template/Initial version.
0.01	28-03-2019	SINTEF	Deliverable information.
0.02	26-08-2019	AS	ToC/Structure and collection of inputs
0.03	29-08-2019	AL/AS	Additional input across the document.
0.04	20-09-2019	AL /AS	Input on several sections.
0.05	23-09-2019	SINTEF	Updates across the document.
0.06	24-09-2019	AL	Provisioning of additional input across the document
0.07	30-09-2019	AS	Additional inputs
0.08	02-10-2019	AL	Additional revisions across the text. Update AUTOPILOT.
0.09	02-10-2019	AS	Review comments considered.
1.00	07-10-2019	SINTEF	Final version released.

Table of contents

1. Executive summary 4
1.1 Publishable summary 4
1.2 Non-publishable information 4

2. Introduction 5
2.1 Purpose and target group 5
2.2 Contributions of partners and attendance 5
2.3 Relations to other activities in the project and dissemination 5

3. Agenda of the Meeting and contributions from the LSPs 8
3.1 Introduction to the workshop 8
3.2 Personal wearables: Health, Living, Public Space, and in other domains 8
3.3 Moving sensors: Farm2Food, Mobility, Cities and in other domains 10
3.4 Industry 4.0, Cities, Water management, Energy, Construction, Living and in other domains 13

4. Key Takeaways 15

5. References 17

6. Appendices 18
6.1 Agenda of the workshop 18
6.2 Visual workshop material 23

1. EXECUTIVE SUMMARY

1.1 Publishable summary

The workshop, organized by the CREATE-IoT Project, on *"IoT and the Rule of Law*" expanded on the challenges raised by IoT technology on the Rule of Law aiming at, also, touching upon the potentially emerging opportunities. The workshop focused on the application domains covered by the EU-IoT LSPs Program, surfacing certain associated compliance challenges from their diverse viewpoints and how they tackled by each LSP and it brought forward to an extent issues of horizontal relevance (e.g. liability). Building on the experience of the current LSPs program, the workshop consolidated insights provided by the LSPs, thus, allowing to an extent for an overview across all projects in areas of common interest (e.g. DPO governance structure) that could be of help for the next IoT LSPs Program. The workshop confirmed in several ways that, in general, compliance with applicable laws, regulations and other norms constitute clearly the denominator of common interest for all LSPs; nevertheless, key considerations for compliance as to exactly 'what', essentially, varies due to the contextual differences. Overall, it is intended that the feedback gathered during the workshop will be considered for the WP05 deliverables due at the end of CREATE-IoT Project and, mainly, for D05.06 Legal IoT Framework Evaluation and Final Legal IoT Framework.

1.2 Non-publishable information

The document is public.

2. INTRODUCTION

2.1 Purpose and target group

The present report captures to an extent the discussion and the key messages of the D05.07 Legal IoT Framework Common Event[1], falling under Task T05.03: Legal support, accountability and liability. This event is part of the workshop series provided under Work Package 5 on "IoT Policy Framework - Trusted, Safe and Legal Environment for IoT". Overall, it is aimed that all workshops falling under WP5 provide for presentations of each LSP on the specific workshop topic to be addressed.

As far as the "*IoT and the Rule of Law"* workshop is concerned, it was anticipated that, besides the state of play (SOP) both with respect to the LSPs and the CSAs related to the particular topic, the discussion addresses the gaps between SOP and state of the art. Acknowledging the role of contextuality within the current IoT-LSPs Program and the different risks identified within the Rule of Law, the workshop discussions aimed at pointing at the denominator of common interest for all LSPs pertaining to this particular matter. The workshop was built upon the contributions of all LSPs, while being of open attendance for companies of all sizes and representatives from the public sector, including representatives from the services of the European Commission. The event arrangement itself constitutes the formal deliverable D05.07 mentioned above. This document, thus, provides for a follow-up overview of the workshop.

Overall, it is intended that the feedback gathered during the workshop is considered for the WP05 deliverables due at the end of CREATE-IoT Project and, mainly, for D05.06 Legal IoT Framework Evaluation & Final Legal IoT Framework.

2.2 Contributions of partners and attendance

AS has contributed to the organization of the workshop, including by providing for the logistical aspects and moderated one session. It also participated to the general discussion.

AL has contributed to the workshop by setting up the agenda in line with the scope and objectives of CREATE-IoT Project. Also, AL moderated one session and participated in the general discussion.

TL has contributed to the discussion, focussing on the relationship with standardisation.

The workshop was attended both in Brussels by around 30 people physically and online. Among them: representative of the LSPs; representatives of the Commission; representatives of SMEs; researchers of other institutions and research projects.

2.3 Relations to other activities in the project and dissemination

The workshop is part of the activities of CREATE-IoT WP05. Also, other WPs have contributed to the realization of the event. WP07 widely contributed to its dissemination. The workshop has been in fact promoted through different channels:

- AG05 mailing list.
- AG08 mailing list.
- IoT Security Cluster mailing list.
- Brussel Privacy Hub has been contacted to disseminate the event within their contacts.
- Cyberwatching.eu mailing list, portal and social media.

[1] The event took place on the 19th of July 2019, in Brussels.

Figure 1: Portal - The European watch on cybersecurity & privacy

Figure 2: Twitter - The European watch on cybersecurity & privacy

- CREATE-IoT social media

Figure 3: Twitter – The CREATE-IoT project

- LSPs web site

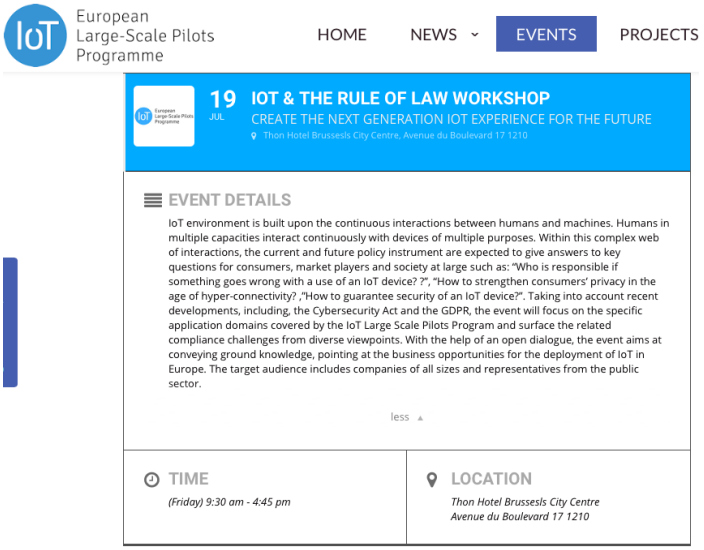


Figure 4: Portal - the European Large-Scale Pilots Programme

3. AGENDA OF THE MEETING AND CONTRIBUTIONS FROM THE LSPS

3.1 Introduction to the workshop

AL offered an introduction to the topic *"IoT and the Rule of law"*, pointing at the wide range of concepts falling under its scope. The introduction captured the momentum at EU level by referring to the measures announced by European Commission on the 17 July of 2019 in view of "strengthening the rule of law through increased awareness, an annual monitoring cycle and more effective enforcement"[2].

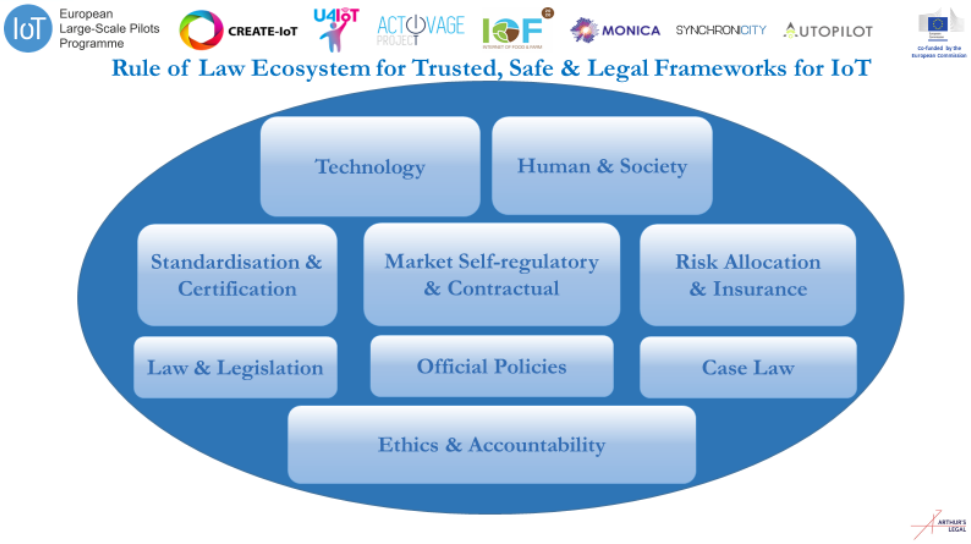


Figure 5: Rule of Law Ecosystem for Trusted, Safe & Legal Frameworks for IoT

The following sessions focused on the various application domains relevant for the LSPs and the specific challenges encountered with respect to the use of IoT technologies in the context of the currently ongoing EU-IoT LSPs Program. In the beginning of the workshop discussions, participants were informed in a clear manner that the discussions during the meeting sessions were recorded. There were no objections raised in this respect. The resulting audio file is available at the CREATE-IoT internal project repository.

Note that the agenda of the workshop is incorporated under the Appendices.

3.2 Personal wearables: Health, Living, Public Space, and in other domains

The representative from MONICA discussed the approach taken the project[3] focusing on the data protection strategy taken by the consortium and on the difficulties in building it. It also focused the presentation on some specific strategies (e.g. anonymization) and their impact on data protection. The representative from this particular LSP underlined the role of "collective accountability" for projects in order to bring them in line with data protection regulations. One of the important challenges for MONICA concerned the issue of "dynamic consent" or empowering the data subject to express, revoke consent in a cycle of information. To this extent specific measures have been taken to guarantee a full respect of the consent of the end-user. Another concern has been transparency and transfer of information to be provided to the public. In fact,

[2] Further information can be found at: https://europa.eu/rapid/press-release_IP-19-4169_en.htm
[3] Note that the representative from MONICA gave a presentation without the support of slides, hence, the absence of illustrations linked to the contribution from this particular LSP.

noise management and public events in wide open spaces, imply to take fully into consideration also safety and customer experience. In this context the project had to deal also with surveillance issues.

As far as the management of the project is concerned one important issue to be taken into consideration is the diversity of partners, in some cases it can create problems as there are information asymmetries. Also, often researchers and SMEs have different goals and these goals have to be achieved within the limits of the legal framework. In the context of data protection management, data flows among partners have been assessed and access requests have been dealt with. There has been an issue concerning the sharing of responsibilities among partners as DPO of the different partners are not necessarily also part of the project there a specific strategy had to be designed. A representative for each pilot was appointed to liaise with the local DPO. This has also involved the creation of a learning process among partners on data protection related issues. Since the strategy was developed also at the local level, path for info requests have been made clearer and also translated into local languages. All these issues have been addressed taking into consideration the peculiarities involved in the specific sector of wearables.

On behalf of the ACTIVAGE, the project representative presented remotely the main objectives of the ACTIVAGE IoT Ecosystem Suite (AIOTES) and the relevant ethical and legal challenges of this interoperable IoT environment.

Due to the multidisciplinary of the ACTIVAGE consortium, concrete common principles and policies of data management and also a data management strategy has been initiated to cope with the diverse use cases and the wide group of stakeholders (older adults, caregivers, health and social care, professionals) involved. In particular, the governance and management of big and sensitive data (health data) brought a number of a. challenges b. obligations and c. requirements in alignment also to the new regulation (GDPR).

Among the main challenges were to:

- Identify, collect and group similar data among different deployment sites.
- Coordinate efficiently the effort of diverse DSs in alignment to GDPR requirements.
- Regulate the activities of different entities/persons involved in data collection and processing activities.

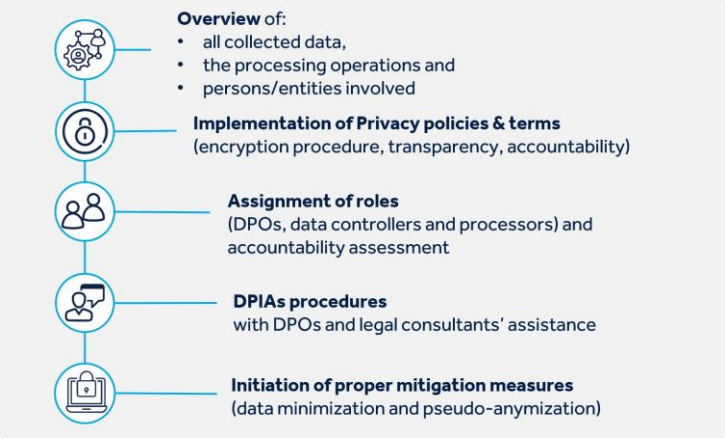


Figure 6: Presentation of ACTIVAGE

From the early beginning of the project and in the frame of pilots' operations, a concern of each deployment site and of the consortium as a whole, was to define a clear data management strategy where data protection and privacy issues have been integrated. In particular, data privacy and human rights' protection have been among the consortium's highest concerns and therefore an integral part of the whole management of the project. Nonetheless, as ACTIVAGE pilots were running before the GDPR launch, as the new regulation came into force in May 2018, the project consortium had to interpret the new requirements according to project's use

cases, needs and architecture, in order to initiate a trustworthy, reliable and widely acceptable IoT environment for end-users (elderly and caregivers). To this end, a number of policies, measures and activities have been defined and followed with consistency in order to achieve GDPR compliance.

However, applying in practice and evaluating the effectiveness of all these predefined measures and activities, a need emerged of regular re-assessment of the status of mandatory actions both at project and deployment site level. This re-assessment has been conducted with the support of DPOs per site, legal consultants and the ethical board, enabling the transparent monitoring of these processes.

Figure 7: Presentation of ACTIVAGE common objectives & ethics requirements

3.3 Moving sensors/actuators: Farm2Food, Mobility, Cities and in other domains

The LSP representative, on behalf of the AUTOPILOT project, discussed the challenges faced by consortium in the particular vertical of the self-driving vehicles. In this context, specific attention is needed to liability considerations, as well as to the different national regulations which are currently being enacted.

The AUTOPILOT project worked on a comprehensive automated/autonomous vehicles and IoT policy framework including trust, security, privacy and stakeholders engagement that includes a set of principles that form the basis of making rules and guidelines, and give an overall direction to planning, development and deployment of technologies and solutions for autonomous vehicles, IoT and AI systems.

The automated/autonomous vehicles and IoT policy framework proposed by AUTOPILOT has considered the specific requirements from the two fields, and the trust, security, privacy and data protection policies, the access to information policy, and the autonomous vehicles security and safety policies.

The automated/autonomous vehicle and IoT policy framework offers a starting point for understanding policy's impact on autonomous vehicles applications integrated with IoT services and is intended to guide the stakeholders involved in such complex ecosystems in developing, implementing, and maintaining a coherent policy that addresses trust, security, privacy and engagement elements.

In this context, the rule of law including the legal, regulations and liability issues are of paramount importance for automated/autonomous vehicles and IoT applications that form the basis for future Internet of Vehicles (IoV) applications.

The introduction of complex autonomous vehicles, IoT and AI systems adds a new layer of complexity to attributing liability for vehicle accidents. In this context, specific legislation should define how liability is apportioned when vehicles are sold as, and drivers/owners/users expect them to be, fully autonomous.

In these cases, attributing liability, fault and responsibility for insurance has to be clarified among the stakeholders involved in complex autonomous vehicles, IoT and AI applications.

Attributing liability in complex autonomous vehicles, IoT and AI applications is a difficult issue in order to establish the responsible stakeholder(s) for incidents (e.g. vehicle manufacturer, manufacturer of software, network providers, service providers, owners, users, etc.) caused by defects in the software interface between two vehicles or between a vehicle and the road, cyber-attacks on vehicles, defects in connectivity causing the incidents, etc.

AUTOPILOT project worked on providing an overview of the legislation related to automated/autonomous vehicles in European countries that host a demonstration pilot (Netherlands, France, Italy, France, Spain) and adding UK and Germany as other advanced markets. In addition. International legislation outside Europe was analysed for USA, China, Singapore and South Korea.

AUTOPILOT has used the KPMG autonomous vehicles readiness index results and the ranking of different countries around the world for 2018 and 2019 [4][5] that is based on four different criteria: policy and legislation, technology and innovation, infrastructure and consumer acceptance to identify the gaps among the different countries in Europe.

Figure 8: AUTOPILOT presentation

Elements identified by AUTIPILOT as legal issues around IoT and automated/autonomous vehicles are:

- Regulations
- Liability
  - Personal Injury
  - Cybersecurity and data breaches
  - Intellectual property ownership

  - Data and information
- Product liability
  - How will liability be apportioned?
  - Fleet Operator/Service Providers
  - Vehicle manufacturers
  - Technology companies/software manufacturers
  - Local government's responsible for maintaining infrastructure
  - Are autonomous vehicles treated as drivers and apply a negligence standard or as sophisticated technology and apply a product liability standard?

These elements need to include the new issues identified for IoT and automated/autonomous vehicles in the large-scale deployments such as:

- Regulations and legislation in different countries
- Cybersecurity in the context of a complex and heterogenous ecosystem for IoT and automated/autonomous vehicles applications
- Data privacy – vulnerabilities and legislation in different countries
- Need for legislation harmonisation at European and global level for IoT, automated/autonomous vehicles and cybersecurity
- Protecting Intellectual Property
- Protecting IP and trade secrets
- Insurance considerations
- Autonomous vehicle and IoT data vs. human data
- Convergence of technologies IoT, AI, Robotics, distributed ledger technologies (DLTs)
- Connectivity (V2X and IoT)

The representative from IoF2020 discussed the use cases of IoF2020 under the perspective of the role of law in smart farming.

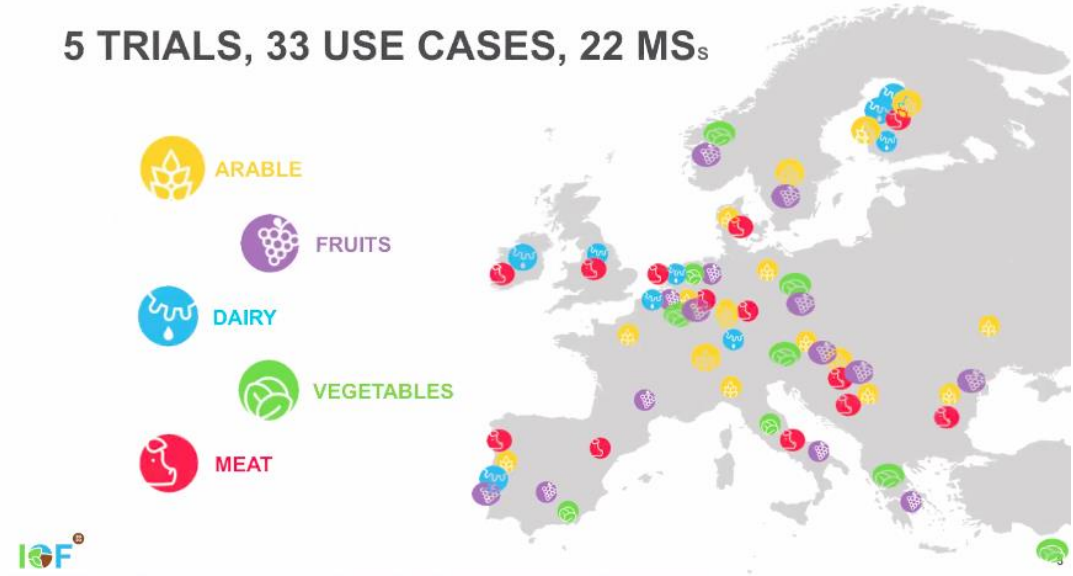


Figure 9: Presentation of IoF2020

Some of the use cases faced issues related to law and regulation, however all of them managed to find solutions to overcome them. None of the use cases so far reported on barriers or serious problems related to law and regulation. The project has worked on a specific WP dedicated to ethics. At the project level IoF2020 strongly recommends the uses cases to have good and explicit agreements on data exchange and IPR issues. In fact, the project has collected different templates and agreements which can be helpful in the use cases for the development of their technology. For this the use cases were advised to make a consortium agreement between the partners in the use case. For this it was suggested to use the DESCA template. The project has

recognized the sensitive nature of personal and non-personal data for farmers and therefore it has tried to clarify issues since the beginning of the implementation, and it tried to build trust through the work of an ethical team. In the meantime, the main representing organisations in agri-food (e.g. Copa-Cogeca, CEMA, IFOAM etc.) launched a code of conduct (CoC) for data exchange in agriculture. It is a set of principles to make transparent agreements on data exchange which has an important impact in the sector. Of course, when work is done in innovation context there is always an issue of "incomplete contracts" and therefore new and unforeseen issues may arise but at the project level there have been no major concerns. For instance, one issue that had to be addressed concerned the tracking of boxes that would imply automatically also the tracking of drivers carrying the boxes. An ethical issue addressed concerned the ownership of data collected by robots that farmer was claiming. In this case it is necessary to compensate the investment made to create the technological infrastructure to create the dataset. Finally, the project also developed a diagnostic tool that all the use-cases have to use to evaluate security.

In the annual partner event last March this CoC was promoted among the use cases, in particular the new use cases, to use this for their agreement. Because IoF2020 is a B-to-B project there are (so far) no privacy related issues. Overall the project has been working to guarantee the sustainability of the use-cases after the end of the research project.

Figure 10: IoF2020 presentation by George Beer (snapshot)

3.4 Industry 4.0, Cities, Water management, Energy, Construction, Living and in other domains

The representative from SYNCHRONICITY discussed the data management and privacy strategy adopted by the SYNCHRONICITY project. SYNCHRONICITY has developed a strategy in order to ensure full compliance with the highest ethical and legal standards. The strategy has taken into account some basic principles: the user/market acceptance; the consideration of legal, financial, political and reputational risks and the applicable EU norms on privacy.

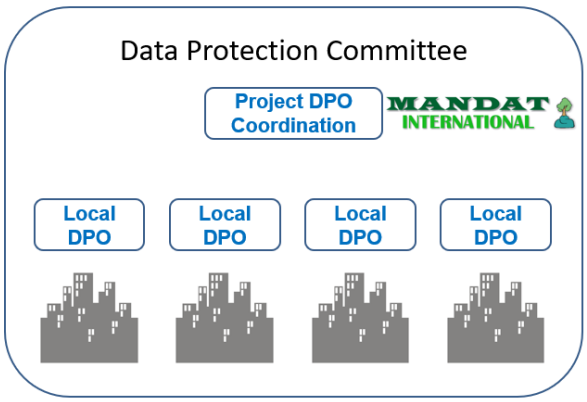


Figure 11. SYNCHRONICITY DPO strategy

During the presentation and the following discussion, it was highlighted how GDPR compliance is a very sensitive topic for smart cities as major data breaches can erode the trust in public institutions and also the political capital of politicians. In the case of research projects guaranteeing full compliance is also a way to preserve and protect the role of the European Commission given its key role in the funding of the projects.

A fundamental action is of course to analyse the different data flows and define a data management plan to be applied by the partners. There was, in this case, also a formal requirement to appoint a DPO according to article 37 of the GDPR. Formally speaking, it is also worth mentioning that the project is not a public entity but only a contract; the formal data controller is not the project but the municipality therefore each municipality needed to have a formal DPO appointed. There was work to be done to coordinate the work of the different DPOs. This has created a data protection distributed strategy which includes:

At the DPO level:

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

At project level:

- Data Protection Policy Coordination;
- Public Information and Contact;
- Reporting and data protection issues management.

SYNCHRONICITY also developed a dedicated DPIA for smart cities, which all cities have been required to perform and it is subject to continuous improvement. It also worked, especially with the city of Carouge on certification for smart cities. One of the challenges is to be able to provide complete and transparent information to citizens on IoT deployments. This is the project developed the Privacy App. Researchers involved in the project have highlighted some basic takeaways:

- GDPR is a research domain per se ad there is large potential for innovation;
- Take personal data protection seriously: don’t underestimate legal, financial and political risks;
- Identify and clarify DPO responsibilities;
- Continuous improvement process;
- Educate, educate, educate!
- Anticipate evolution and end-users' perceptions;
- Strong cross-fertilization potential.

4. KEY TAKEAWAYS

The workshop produced an overview of the compliance challenges and how they were tackled by the five (5) LSPs funded under the currently ongoing EU-IoT LSPs Program. Largely based on the experience gained, the discussion addressed issues pertaining to the separate application domains, but also of horizontal relevance[4]. The key messages to a great extent followed from the afternoon sessions allowing for an open discussion.

More specifically, it was emphasized that:

- The hyperconnectivity and continuous interaction between gadgets, sensors and people points to the rise of data and logs being produced, stored and processed both not only virtually and physically.
- The increased collection of data raises issues of authentication and trust.
- The proliferation of the amount of data in an IoT environment the challenge that data will be used for purposes in addition or other to those originally specified becomes even more important to consider.
- At the general level it was stressed how it must not be the intent of the law to govern this process in a way that hinders the advance of technology.
- Each pilot had to deal with a complex ecosystem of technologies and stakeholders, raising issues of integration and coordination;
- The concept of the rule of law has an important role to play in the consolidation of constitutional rights in the connected public sphere.
- Each pilot could exhibit commonalities at the level of architecture, interoperability, trustworthiness and practice. In terms of security most LSP used the STRIDE methodology. The counterpart LINDDUN [2] was mentioned as a possible common methodology for privacy;
- Each pilot has gained experience in data protection impact assessment in an ecosystem. This experience would be worth sharing, in particular how to organise a community of several stakeholders in an ecosystem in order to produce overall privacy impact assessment. In particular SYNCHRONICITY and CREATE-IoT have contributed to ISO/IEC 27570 [3] which describe five ecosystem processes (governance, risk management, engineering, citizen engagement, data exchange);
- The trustworthiness in ecosystems would require some further work on assurance in ecosystems;

Overall, the workshop discussion confirmed that compliance is essentially the denominator of common interest for all LSPs Projects. However, 'compliance to what' seems to differ according to each specific vertical/application domain. For example, compliance with IP law seems to be 'more relevant' for the scope of IoF2020, while compliance with the General Data Protection Regulation seems to be of direct relevance for the scope of ACTIVAGE (e.g. informing and obtaining the users consent, storing and handling their data via anonymization and pseudonymization and secondary use of data for medical research purposes) and SYNCHRONICITY (e.g. the need to prevent data breaches in cities)[5]. It should be stressed that

[4] Note that the considerations pertaining specifically to privacy will be to a large extent covered by the paper currently being drafted on *Internet of Things Deployments and Personal Data Protection: Lessons Learned from the European Large-Scale Pilots of Internet of Things.* The drafting is coordinated by Mandat International under the auspices of CREATE-IoT Project.

[5] Note the role of contextuality has been addressed under the WP05 deliverables submitted during Year 1 of CREATE-IoT Project and it will be further elaborated under the final versions due at the end of the project. It is aimed that the final versions encompass input from the respective common events.

the necessity to promote a "digital culture" where the protection of privacy is embedded has been highlighted by all LSPs.

Furthermore, the workshop has offered valuable feedback and know-how from LSPs that can be transferred to future research projects. In particular, the role and fundamental support of AGs has been discussed, as well as the necessity for the projects to set up DPO schemes appropriated for the scope of the projects and the synthesis of the consortia. In this respect, it was recommended that two viewpoints are taken in large scale pilots: first a practical operational viewpoint where the partners work in the pilot comply with GDPR. This involved specific coordination between DPOs; second a deployment viewpoint where the partners project anticipate work for privacy compliance when the transition from pilots to deployment takes place; It was emphasised, once again, the need to document properly the results of the LSPs and the need to transfer know-how to the new projects.

The next common event scheduled under WP05 is D05.09 on IoT Data Value Chain Model. The event is planned with the EC to take place on 27th January 2020, in Brussels.

5. REFERENCES

[1] CREATE-IoT WP05 deliverables (D05.01, D05.03, D05.05).
[2] LINDDUN – Privacy threat modelling. Online at: https://linddun.org/
[3] ISO/IEC 27570: Privacy guidelines for smart cities, (this standard is under development).
[4] Autonomous Vehicle Readiness Index: Assessing countries' openness and preparedness for autonomous vehicles, KPMG, 2018, online at: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/01/avri.pdf.
[5] Autonomous Vehicle Readiness Index: Assessing countries' openness and preparedness for autonomous vehicles, KPMG, 2018, online at: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf

6. APPENDICES

6.1 Agenda of the workshop

CREATE the Next Generation IoT eXperience for the Future

IoT & the Rule of Law

19 July 2019, Brussels

Thon Hotel Brussels City Centre

Avenue du Boulevard 17

1210 Brussels

IoT European Large-Scale Pilots Programme

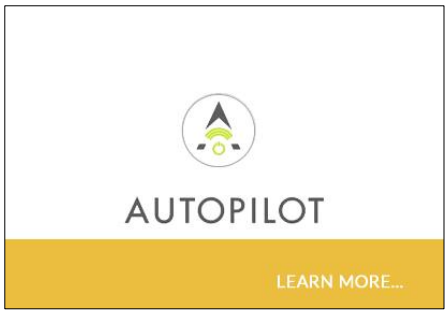
IoT environment is built upon the continuous interactions between humans and machines. Humans in multiple capacities interact continuously with devices of multiple purposes. Within this complex web of interactions, the current and future policy instrument are expected to give answers to key questions for consumers, market players and society at large such as: "Who is responsible if something goes wrong with a use of an IoT device? ?", "How to strengthen consumers' privacy in the age of hyper-connectivity? ,"How to guarantee security of an IoT device?". Considering recent developments, including, the Cybersecurity Act and the GDPR, the event will focus on the specific application domains covered by the IoT Large Scale Pilots Program and surface the related compliance challenges from diverse viewpoints. With the help of an open dialogue, the event aims at conveying ground knowledge, pointing at the business opportunities for the deployment of IoT in Europe. The target audience includes companies of all sizes and representatives from the public sector.

Agenda

09:30 – 10:00	**Registration**
Meeting Room: Oslo	
10:00 – 10:10	***Welcome and Introduction***
10:10 – 10:30	***"The Vast Domain of IoT & the Rule of Law"**, presentation by Arthur's Legal, CREATE-IoT.* The presentation will give an overview of the horizontal and vertical challenges in the IoT environment. It will pave the ground for the sessions to follow on the vertical challenges per application domain.
10:30-11:30	***"Personal Wearables (H2x): Health, Living, Public Space, and in other domains"*** Moderator: Pasquale Annicchino, Archimede Solutions, CREATE-IoT. Short presentations (10') by MONICA and ACTIVAGE on the respective compliance challenges encountered. The presentations will be followed by an open discussion with the audience.
11:30 – 12:45	***"Moving Sensors (M2x): Farm2Food, Mobility, Cities, and in other domains"*** Short presentations (10') by IoF2020 and AUTOPILOT on the respective compliance challenges encountered. The presentations will be followed by an open discussion with the audience.
12:45- 13:45	**Lunch Break and Networking**
13:45– 14:45	***"Long Term Fixed IoT Applications (M2x)": Industry 4.0, Cities, Water management, Energy, Construction, Living, and in other domains"*** Short presentation (10') by SYNCHRONICITY on the respective compliance challenges encountered. The presentations will be followed by an open discussion with the audience.
14:45-15:00	**Coffee Break**
15:00-15:45	***"Lessons learnt - sharing experiences from the IoT-LSPs Program"*** Panel: Representatives from the five (5) LSPs and the two (2) CSAs. Going beyond the compliance challenges discussed earlier, this session will allow for an open discussion on the experiences so far gained within the IoT-LSPs Program and, possibly, the arising business opportunities
15:45-16:30	***"The longer-term outlook: going beyond the IoT-LSPs Program"*** Panel: Representatives from the five (5) LSPs and DG CONNECT. The session will allow for an open discussion on future directions and regulatory developments relevant for IoT deployment in Europe, putting particular emphasis on issues such as product liability and the role of ethics.
16:30–16:45	***Closing remarks**: Franck Boissière, EC, DG CONNECT*

IoT European Large-Scale Pilots Programme Projects

ACTIVAGE - ACTIVATING INNOVATIVE IoT SMART LIVING ENVIRONMENTS FOR AGEING WELL - is building the first European interoperable and open IoT ecosystem enabling the deployment, at large scale, of a wide range of Active and Healthy Ageing IoT based solutions and services. To achieve this, ACTIVAGE is integrating thousands of devices to collect and analyse older adults' environmental and lifestyle information, identify their needs, and provide customized solutions, ensuring users' data privacy and security.



AUTOPILOT - AUTOMATED DRIVING PROGRESSED BY INTERNET OF THINGS – is developing an IoT connected vehicle platform and IoT architecture based on the existing and forthcoming standards, as well as open source and vendor solutions. The IoT ecosystem accommodates vehicles, road infrastructure and connected IoT objects, with particular attention to safety critical aspects of automated driving. The project develops a range of services combining autonomous driving and IoT, such as car sharing, autonomous valet parking, and better digital maps for autonomous vehicles.

CREATE-IoT - CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT - CREATE-IoT's stimulate collaboration between IoT initiatives, foster the take up of IoT in Europe and support the development and growth of IoT ecosystems based on open technologies and platforms. The work focuses on synchronisation and alignment on strategic and operational terms through frequent, multi-directional exchanges between the various activities under the IoT Focus Areas and the road-mapping with international initiatives.

IoF2020 - INTERNET OF FOOD AND FARM 2020 - is dedicated to accelerating the uptake of IoT technologies in the European farming and food chains and ultimately strengthening their competitiveness and sustainability. How? By demonstrating, together with end-users, the use of IoT in different use-cases spread throughout Europe, and focusing on 5 areas: dairy, meat, arable crops, fruits and vegetables. IoF2020 is designed to generate maximum impact right from the outset and in the long-run, bringing closer together and integrating the supply and demand sides of IoT technologies in the agri-food sector.

MONICA - MANAGEMENT OF NETWORKED IoT WEARABLES – VERY LARGE-SCALE DEMONSTRATION OF CULTURAL AND SOCIETAL APPLICATIONS - is a large-scale demonstration of how cities can use existing and new IoT solutions to meet sound, noise and security challenges at big open-air cultural and sports events, which attract and affect many people. Innovations include the establishment of sound zones at outdoor concerts for noise mitigation as well as security measures improving crowd information and management.

SYNCHRONICITY - DELIVERING AN IoT-ENABLED DIGITAL SINGLE MARKET FOR EUROPE AND BEYOND - brings together partners with worldwide outreach. The project represents the first attempt to deliver a digital single market for IoT-enabled urban services in Europe and beyond. With an already emerging foundation, based on OASC Minimal Interoperability Mechanism (MIMs), SYNCHRONICITY will establish a reference architecture model for the envisioned IoT-enabled city marketplace with identified interoperability points and interfaces and data models for different verticals.

U4IoT - USER ENGAGEMENT FOR LARGE SCALE PILOTS IN THE INTERNET OF THINGS - combines complementary Responsible Research and Innovation – Social Sciences and Humanities (RRI-SSH) expertise encompassing social and economic sciences, communication, crowdsourcing, living labs, co-creative workshops, meetups, and personal data protection to actively engage end-users and citizens in the large-scale pilots. U4IoT encompasses the whole lifecycle of end-user engagement in LSPs. Privacy-friendly crowdsourcing and survey tools enable to monitor the end-user perception and acceptance of IoT applications.

We are looking forward to seeing you

To promote and foster the take-up of IoT in Europe and to enable the emergence of an economically sustainable IoT ecosystem, the IoT European Large-Scale Pilots Programme projects are seeking to involve the IoT community across the value chain, from supply side to demand side.

Welcome to the IoT European Large-Scale Pilots Programme

A vibrant research, innovation, development and deployment IoT ecosystem across Europe!

6.2 Visual workshop material

Figure 11: The organizing team with Franck Boissière