V. 8.5
February 2020

PERSONAL DATA PROTECTION FOR INTERNET OF THINGS DEPLOYMENTS:

LESSONS LEARNED FROM THE EUROPEAN LARGE-SCALE PILOTS OF INTERNET OF THINGS

CREATE-IoT U4IoT ACTIVAGE PROJECT AUTOPILOT IoF 2020

MONICA SYNCHRONICITY

Foreword

The European Commission has financed an ambitious research programme on the Internet of Things (IoT) comprised of five Large Scale Pilots (LSPs) encompassing various application domains and two Coordination & Support Actions (CSAs). After the formal launch of the EU-IoT LSPs Program in January 2017, the General Data Protection Regulation (GDPR) became applicable in May 2018 creating an impact for organizations of all sizes, even if they are located outside the territory of the EU.

The purpose of this document is to present lessons learned and good practices necessary for enhanced personal data protection. Methodologies, strategies and the most relevant enablers developed by the five LSPs and their supporting CSAs provide an example on how to ensure the compliance of IoT technologies with the GDPR Regulation. This Guideline is intended for the international audience, including industry, the research community, public administration and standardization bodies.

While the following good practices are the result of several years of research and experience acquired through the European research programme supported by the European Commission, it presents the research community views and perspectives in a fully independent manner. Its content does not engage the European Union and its bodies in any way.

Partners and Contributors

These Guidelines have been developed as a collaborative exercise among the five LSPs and their supporting CSAs, namely Activage, Autopilot, IoF2020, Monica, Synchronicity, Create-IoT and U4IoT. All the above-mentioned projects have received financial support from the Horizon 2020 European Union research programme (H2020). The editorial work has been coordinated by Mandat International in line with the scope of Create-IoT project and, in particular, with the 'Work Package 5: IoT Policy Framework - Trusted, Safe and Legal Environment for IoT' and in collaboration with the Activity Group 5 coordinated by Archimede Solutions. The work has been further supported by the following team:

Editors and Main Contributors

- Sebastien Ziegler (Lead Editor, Mandat International - Create IoT)
- Pasquale Annicchino (Archimede Solutions - Create IoT)
- Dimitra Stefanatou (Arthur's Legal – Create-IoT)
- Sofia Segkouli (CERTH/ITI - Activage)
- Ali Padyab (LTU - U4IoT)
- Rita Bhandari (Ertico - Autopilot)
- Simone van Der Burg (WUR - IoF2020)
- Carlotta Firmani (Thales Group - Autopilot)
- Antonio Kung (Trialog – Create IoT)
- Adrián Quesada Rodríguez (Mandat International - Synchronicity)
- Renáta Radócz (Mandat International - Synchronicity)
- Trine F. Sørensen (In-JeT ApS – MONICA)

This document also benefited from the following contributors:

Konstantinos Votis, Nikolaos Kaklanis, Stefanos Stavrotheodoros, Dimitrios Tzovaras (Information Technologies Institute-ITI, Centre for Research and Technology Hellas-CERTH, Thessaloniki, Greece); Pilar Sala (Mysphera S.L, Spain; ITACA-SABIEN, Universitat Politècnica de València, Spain); Juan Mario Lecumberri Ciáurriz ⁽Iniciativa Social Integral, Valencia, Spain); Giuseppe Fico, Alejandro Medrano (Life Supporting Technologies – Universidad Politécnina de Madrid, Spain), Ana Maria Pacheco Huamani (Archimede Solutions), Arthur van der Wees (Arthur's Legal - Create-IoT).

The editorial coordination and publication of the white paper has been led by Mandat International, alias International Cooperation Foundation, in the context of the Create-IoT European research project.

Table of contents

1. Introduction

1.1 Scope of the Document

Personal data protection constitutes a fundamental right enshrined in European law. As such, it is fully applicable to the Internet of Things (IoT). The five Large Scale Pilots (LSPs) funded by the Horizon 2020 European research programme offered an excellent opportunity to research and demonstrate how to comply with this requirement across diverse application domains:

- Smart living environments for ageing well with ACTIVAGE;
- Autonomous vehicles in a connected environment with AUTOPILOT.
- Smart farming and food security with IoF2020;
- Wearables for smart ecosystems with MONICA;
- Smart cities and communities with SYNCHRONICITY.

The present document leverages on and shares the experience acquired through these five LSPs in relation to privacy by design and personal data protection. Its purpose is to produce an overview of the most relevant methodologies, strategies and enablers developed by the five European LSPs and the two Coordinated & Support Actions (CSAs) to ensure IoT compliance with the GDPR. These Guidelines synthetizes their main achievements in the forms of practical lessons learned, data protection guidelines and identified enablers aiming to support the implementation of personal data protection in practice. It is intended to be itereatively complemented and enhanced by future large-scale pilots.

1.2 Target Audience

The aim of this document is to disseminate lessons learned to:

- future large-scale pilots and deployments of Internet of Things;
- the research community;
- the international audience, including industry, public administration and standardization bodies.

1.3 Methodology

These good practices are the result of interdisciplinary and collaborative effort among the participating projects. Independently from the Guidelines, each project developed specific activities to ensure complete compliance with the applicable data protection regulation in diverse contexts. Create-IoT has been in charge of supporting the LSPs and facilitating their collaboration and convergence through several cross-project activity groups. One of these activity groups had the mandate to focus on data protection.

The present report has been elaborated in parallel to the development of the LSPs and has been discussed through several meetings, including conferences such as the IoT Week (www.iotweek.org). Each project has brought its own perspective. Contributions were discussed and integrated together in order to extract and share the most relevant lessons learned. It has resulted in a collective work aimed at presenting the main results of the LSPs program on IoT deployments with regards to personal data protection.

Figure 1 shows the matrix approach used by the LSPs to develop synergies, including in the domain of data protection, security and privacy:

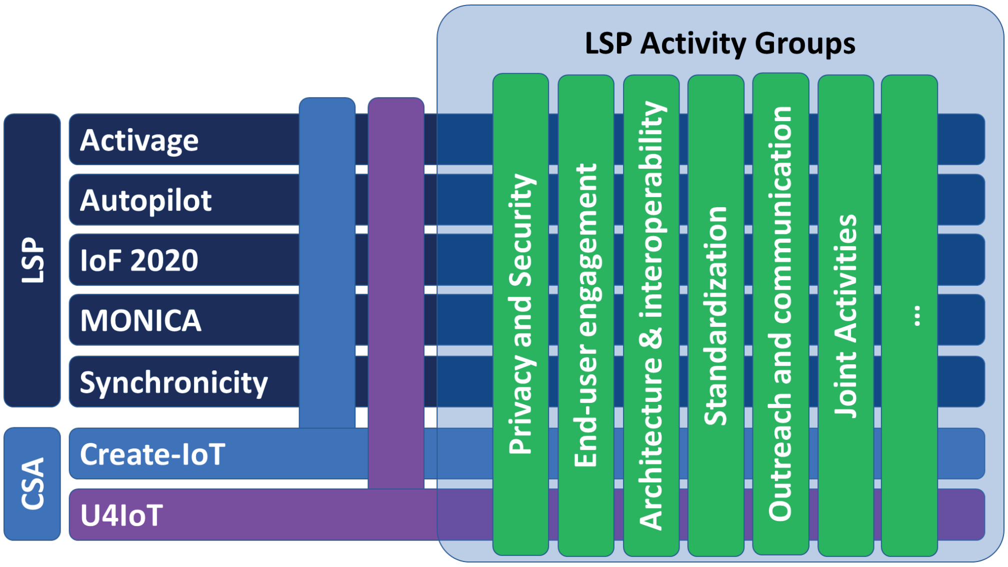


Figure 1: Matrix Approach used by LSPs and CSAs.

1.4 An Iterative and Continuous Process

Ensuring full compliance of IoT deployments with the GDPR and related obligations is challenging when such deployments are exposing data subjects to a large surface of risks. The fast pace of technology evolution in the domain of data analytics, miniaturization and Artificial intelligence, requires developers to adopt an iterative process aiming at continuous improvement. The current Guidelines intend to serve to future research and Large-Scale Pilots and may be revised accordingly. As an example, Figure 2 depicts the interconnection between the LSPs that participated in this document and the subsequent research projects:

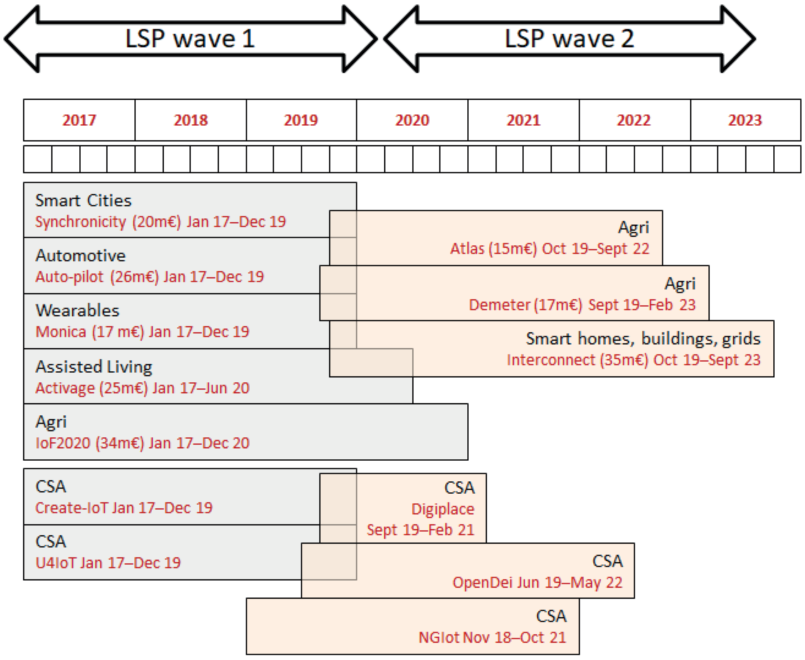


Figure 2: LSPs and CSAs waves.

1.5 Structure

The following document intends to shed light upon how an IoT ecosystem can be fully compliant with the existing regulatory framework and, in particular, with the GDPR regulation through the examples and practical experiences of five application domains. After the first introductory chapter, **Chapter 2** introduces GDPR as a regulatory landscape and describes the five LSPs and two CSAs.

Chapter 3 focuses on the privacy by design and privacy by default frameworks, including the role of technical and organizational measures to implement data protection principles in practice.

Although some essential concepts are the same for all LSPs, the five domains are unique on their own. They all required independent methodologies to be developed and a specific approach to data protection. **Chapter 4** explores their domain specific experience in relation to compliance and operation in the new IoT ecosystem.

Big data and privacy are key factors that LSPs have to take into account to benefit from the impacts of new technologies. Nonetheless, there are precarious areas that must be regulated clearly. **Chapter 5** gathers the experience of project partners in risk assessment and introduces privacy enhancing technologies, trusted frameworks and other specific solutions that prioritize trust-building and compliance.

Privacy by design and by default are recent concerns and standardization bodies only offer few standards. **Chapter 6** explores four types of existing standards (principles, mechanisms, organizational level practice and ecosystem level practice), highlighting the standard development that has been influenced and will be influenced by LSPs and CSAs.

Chapter 7 offers guidelines and recommendations through both vertical and horizontal experiences and know-how to answer this question. Lessons learned from the five LSPs can offer useful insights for future research to the IoT community.

Chapter 8 identifies research needs and challenges that were identified by the project partners. It describes some key research areas to be addressed in the future.

Chapter 9 concludes the document and the lessons learned by the European Large-Scale Pilots. It is followed by **Chapter 10**, which provides the list of references and a short bibliography, and by the **Annexes**.

2. Setting the Scene

2.1 The Regulatory Landscape

The Guidelines focus on the compliance IoT large scale pilots with the European data protection regulation and more specifically with four normative references:

- The General Data Protection Regulation (GDPR) itself: Regulation 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- The Directive on privacy and electronic communications: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector.
- The Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
- The Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

European General Data Protection Regulation (GDPR)

The protection of personal data is a fundamental right in the European Union. Article 8 of the EU Charter for fundamental rights provides that: "*1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority*".

In order to make the protection of this right effective, the European Union has enacted different legislative instruments. Among them, the most important one is the General Data Protection Regulation (GDPR), which provides high level of data protection. As opposed to the former personal data protection regime that required Member States to transpose the Data Protection Directive into the respective national law, the GDPR is directly applicable in all EU Member States. It has been designed to provide a common legal framework for data protection law and to protect the data assets and privacy of individuals within the EU. Nonetheless, companies outside EU may also be subject to the GDPR if the "establishment" of a company collects personal data of an EU citizen or addresses the EU market, even if the establishment is located outside the EU.

GDPR is a comprehensive legislation with several implications:

- Enhanced personal rights for data subjects, such as the right to be forgotten, the right to data portability, the right to information on processed personal data, etc.
- Increased importance of prior informed consent to hold and process data and the ability of data subjects to withdraw consent at any time.
- Data Protection by design and by default with strict data minimization requirement.
- Requirement to appoint a Data Protection Officer (DPO).
- Requirement to perform Data Protection Impact Assessments (DPIAs) to identify and mitigate the risk for the rights and freedom of natural persons.
- A stringent sanctions regime with the possibility to impose substantial fines for non-compliance (up to 4% of the global turnover of non-complying companies).

2.2 Large Scale Pilots

The European Commission supported the LSPs for demonstrating and assessing the potential of the Internet of Things in five application domains: assisted living, connected vehicles, smart farming, wearables and smart cities. Here is a brief overview of these five LSPs:

Activage – ACTivating InoVative IoT smart living environments for AGEing well

ACTIVAGE is a multi-centric LSP in which each Deployment Site (DS) included a number of stakeholders (e.g. older people, formal and informal caregivers, service providers AHA services, health care/social care administration, technological infrastructure and technology providers) in the Active Health and Ageing (AHA) network. The main aim was to build the first European IoT Ecosystem Suite (AIOTES), a set of Techniques, Tools and Methodologies for interoperability between different layers of heterogeneous IoT Platforms. Each DS used one or more IoT platforms (FIWARE, SOFIA2, UniversAAL, SensiNact, OpenIoT, IoTivity and SENIORSOME). In order to create an open AHA ecosystem, ACTIVAGE initiated a key component of interoperability between these IoT platforms, which ensures privacy and security. Along with the interoperability of IoT platforms, a number of Qualified Key Performance Indicators (KPIs) were used in terms of the local and a Global evaluation framework. More information is available at https://www.activageproject.eu/.

Autopilot - Automated driving progressed by Internet of Things

AUTOPILOT is a European funded project that intended to develop Autonomous Driving (AD) use cases by augmenting AD with Internet of Things technologies and infrastructures.

The overall objective of AUTOPILOT was to bring together relevant knowledge and technology from the automotive and the IoT value chains in order to develop IoT-architectures and platforms which would bring Automated Driving towards a new dimension.

The ideal way of assuring data protection and cybersecurity in a connected car is to build it from the start, by design. This means that for connected cars and, more generally, to contribute to the system data protection, security must be built together with car manufacturers and equipment makers from the first stage of vehicle architecture. More information is available at https://autopilot-project.eu/.

IoF2020 – Internet of Food and Farm 2020

The Internet of Things has revolutionary potential. A smart web of sensors, actuators, cameras, robots, drones and other connected devices allows for an unprecedented level of control and automated decision-making. The project Internet of Food & Farm 2020 (IoF2020) explored the potential of IoT-technologies for the European food and farming industry.

The goal was ambitious; to make precision farming a reality and to take a vital step towards a more sustainable food value chain. With the help of IoT technologies, higher yields and better-quality produce is within reach. Pesticide and fertilizer use would drop, and the overall efficiency would be optimized. IoT technologies also enable better traceability of food, leading to increased food safety.

IoF2020 is part of Horizon 2020 Industrial Leadership and supported by the European Commission with a budget of EUR 30 million. The aim of IoF2020 was to build a lasting innovation ecosystem that fosters the uptake of IoT technologies. For this purpose, key stakeholders along the food value chain were involved in IoF2020 together with technology service providers, software companies and academic research institutions.

Nineteen use cases were organized around five sectors (arable, dairy, fruits, meat and vegetables) develop, test and demonstrate IoT technologies in an operational farm environment all over Europe. More information is available at https://www.iof2020.eu/.

Monica

The MONICA project was a large-scale demonstration of new and existing IoT applications for a smarter living. The demonstration involved six major cities in Europe: Lyon, Bonn, Leeds, Turin, Copenhagen and Hamburg.

The focus was on one of the key aspects of European society: the cultural performances in open-air settings which create challenges in terms of crowd safety, security and noise pollution.

To demonstrate how these challenges could be met through the use of technology, MONICA developed, deployed and demonstrated three IoT ecosystems on security, acoustics and innovation, addressing real user needs. Within these systems, several applications have been deployed, using IoT-enabled devices such as smart wristbands, video cameras, loudspeakers and mobile phones.

One strand of applications addressed the challenge of managing public security and safety at open-air settings where large crowds gather. These included concerts, carnivals, sporting events and other city manifestations. The second strand demonstrated a number of acoustics applications, controlling and reducing the emission of unwanted noise to the neighbouring communities. In addition, some of the applications invited the citizens to engage in the creation of solutions which enable better adaption of open-air events to city living.

The third strand of applications enabled developers and service providers to integrate the MONICA platform with other smart city systems. Additionally, MONICA shared open data, inviting entrepreneurs to develop new innovative applications for a smarter living. To support the multiple applications, MONICA deployed a secure, cloud-based platform which wirelessly connects and handles devices used at the events. Furthermore, the platform consists of components which could analyze data and detect critical incidents, thereby supporting operators in making decisions. Since the platform have been based on open standards and architectures and could support multiple applications, it could be used by other cities and in other settings.

The individual pilot sites mixed and matched applications according to their specific needs showing the flexibility of the MONICA platform. More information is available at https://www.monica-project.eu/.

SynchroniCity - Delivering an IoT enabled Digital Single Market for Europe and Beyond

SynchroniCity ambitioned at delivering a Single Digital City Market for Europe by piloting its foundations at scale in 11 reference zones: 8 European cities and 3 more worldwide cities-connecting 34 partners from 11 countries over 4 continents. Building upon a mature European knowledge base derived from previous initiatives (such as OASC, FIWARE, FIRE, and EIP-SCC) and including partners with leading roles in standardization bodies (e.g. at ITU, ETSI, IEEE, OMA and IETF), SynchroniCity has researched and developed a harmonized ecosystem for IoT-enabled smart city solutions, where IoT device manufacturers, system integrators and solution providers can innovate and openly compete. With an already emerging foundation, SynchroniCity has developed a reference architecture for the envisioned IoT-enabled city marketplace with identified interoperability points and interfaces and data models for different verticals. It leveraged co-creation processes, integration of legacy platforms and IoT devices for urban services, enablers for data discovery, access and licensing lowering the barriers for participation on the market. SynchroniCity has piloted these foundations in the reference zones together with a set of citizen-centered, business and citizens involved, linked directly to the global market. SynchroniCity ambitioned to serve as lighthouse initiative inspiring others to join the established ecosystem and contribute to a global marketplace. SynchroniCity took an inclusive approach to grow the ecosystem by inviting business and cities to join through an open call, allowing them to participate in the pioneering marketplace enabling a second wave of successful pilots. More information is available at https://synchronicity-iot.eu/.

2.3 Coordinated and Support Actions

The five LSPs were complemented and supported by two complementary Coordination and Support Actions:

Create-IoT

Create-IoT stands for “Cross Fertilization through Alignment, Synchronization and Exchanges for IoT”. Its aim is to 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. This requires synchronization and alignment on strategic and operational terms through frequent, multi-directional exchanges between the various activities under the IoT Focus Areas (FAs). It also requires cross-fertilization of the various IoT LSPs for technological and validation issues of common interest across the various application domains and use cases.

CREATE-IoT aligns activities with the Alliance for Internet of Things Innovation (AIOTI). It will coordinate and support the upcoming LSPs in sustaining the ecosystems developed during these projects through mapping the pilot architecture approaches, and addresses interoperability and standards approaches at both technical and semantic level. It focuses on object connectivity, protocols, data formats, privacy, security, trusted IoT and open APIs and will share the road-mapping with international initiatives.

The project fosters the exchange on requirements for legal accompanying measures, development of common methodologies and KPI for design. It promotes testing and validation, success and impact measurement, federation of pilot activities and transfer to other pilot areas. It facilitates access for IoT entrepreneurs/API developers/makers, SMEs, including combination of ICT & Art. CREATE-IoT builds on strong connection with the initiatives of member states and others. The project transfers learning points to the broader IoT policy framework including contractual PPPs (e.g. Big Data, Factories of the Future, 5G-infrstructure), Joint Technology Initiatives (e.g. ECSEL), European Innovation Partnerships (e.g. on Smart Cities), as well as to other FAs (e.g. on Autonomous transport). It maintains a coordinated working relationship with U4Iot, a center on RRI-SSH. More information is available at https://european-iot-pilots.eu/create-iot/.

U4IoT

U4IoT stands for “User Engagement for Large Scale Pilots in the Internet of Things”. It brings together 9 partners from 5 European countries.

The objective of the project is to develop a toolkit for LSPs end-user engagement and adoption, including online resources, privacy-compliant crowdsourcing tools, guidelines, an innovative privacy game for personal data protection risk assessment and awareness and online training modules.

The partners provide direct support to mobilize end-user engagement with co-creative workshops and meetups, training, Living Labs support and an online pool of experts to address LSPs specific questions.

The project analyses societal, ethical and ecological issues and adoption barriers related to the pilots with end-users. 4UIoT makes recommendations for tackling IoT adoption barriers, including educational needs, sustainability models for LSPs and future IoT pilots’ deployment in Europe.

The activities include supported communication, knowledge sharing and dissemination with an online portal, as well as an interactive knowledge base gathering the lessons learned, FAQs, tools, solutions and end-user feedback. More information is available at https://u4iot.eu/.

3. Common (cross-domain) Privacy by Design and by Default Approach for Internet of Things Deployments

This chapter focuses on the role of the technical and organizational measures with respect to the implementation of the overarching data protection principles in practice, as envisioned under the GDPR. To this end, in view of putting emphasis on the necessity for a proactive approach for a human-centric IoT, the following discussion expands on certain novelties of the GDPR, namely, the DPIA, the role of the DPO and of the security measures.

3.1 Accountability Principle

Accountability is a fundamental principle on which the GDPR is built. It implies that data controllers need to be proactive and organized about their approach to data protection and they must be able to provide evidence of the steps they have undertaken to guarantee their compliance. Data controllers must also put in place appropriate technical and organizational measures in order to implement data protection principles and to safeguard individuals' rights.

3.2 Data Protection by Design and by Default

One of the important changes resulting from the GDPR is the principles of 'data protection by design' and 'data protection by default'. These two principles place controllers under the obligation to ensure data protection is taken into account since the conception of new data processing activities. It requires to minimize data collection and processing to what is effectively needed and justified to achieve the legitimate purpose. Controllers must take appropriate technical and organizational measures to implement data protection principles in an effective manner, ensuring that default settings guarantee that personal data is processed only if absolutely necessary for the specific processing purpose, in accordance with Article 25(1)(2) of the GDPR. In essence, the two key principles can be described as follows:

> **Data protection by design**: aims at addressing and mitigating the risks of a data processing activity for the rights and freedoms of the natural persons since the conception and the determination of the means of a data processing. Data protection must, therefore, be built into a data processing since the very beginning of its life cycle.
>
> **Data protection by default**: aims at ensuring that by default *"only personal data which are necessary for each specific purpose of the processing are processed."* [1] It applies to four dimensions: minimizing the amount of collected personal data, minimizing the processing itself, minimizing the retention period, and minimizing access to the data. Additionally, personal data provided by the user to enable a product's optimal use should only be kept for the amount of time necessary to provide the product or service.[2]

The obligations of Article 25 of the GDPR has a direct impact on the design process of innovative technologies, as well as on the design of specific deployment plans in pilots. It requires that researchers and engineers address the regulatory requirements at a very early stage. This has been a key challenge for the LSPs which are deployed in diverse and heterogeneous ecosystems. Each use case required particular measures to comply with the privacy by design and by default requirements. This diversity is also related to different risks specific to each LSP. These differences are also reflected in the diversity of privacy enablers that the LSPs have produced to foster their privacy compliance and guarantee an appropriate level of protection of fundamental rights.

[1] Art. 25 GDPR.

[2] For a detailed analysis see EDPS, *Preliminary Opinion on privacy by design* (5/2018).

3.3 Data Subject Rights

Data subjects' rights are one of the key areas of change under the GDPR. From 25th May 2018, data subjects can evoke a greater set of rights against businesses and organizations that process their personal data. For this purpose, a data subject is considered to be a living, identifiable individual to whom personal data relates.

Under the GDPR, individuals can exercise the following rights:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object to processing
- the rights in relation to automated decision making and profiling

LSPs have produced specific tools to support data subjects in the exercise of their rights. A clear example, with the possibility of implementation also in other ecosystems, is the Privacy App produced by Synchronicity that guarantees a mapping of IoT devices in a smart city ecosystem and the possibility for the data subject to contact the responsible DPO of the city. MONICA has developed a set of procedures for how data subjects can exercise their rights and how the project will meet those rights. The procedures are available as online and paper-based documents and may also be carried out as an online process or paper-based process as part of the e-inclusion principles in the project.

3.4 Data Minimization

The principle of data minimization is an indispensable part of the 'ethics by design' and 'by default' concept[3]. This ethically and legally oriented framework has been implemented properly by the LSPs' controllers. According to Article 5(1)(c) of the GDPR, personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Therefore, according to this minimization principle, data controllers should identify the minimum amount of personal data needed to achieve their goals. According to the accountability principle, data controllers should be able to demonstrate that they only collect and hold the personal data needed.

Data controllers must ensure that the personal data they are processing are:

- adequate: sufficient to fulfil the stated purpose;
- relevant: as they should have a rational link to the purpose;
- limited to what is necessary: they should not hold more data than those needed for the stated purpose.

Examples of the application of this principle can be found in the actions undertaken by IoF2020 where personal data of farmers not necessary for research purposes have not been collected, therefore, fully respecting the principle of minimization.

[3] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf

Data Retention Period Limitation

Storage limitation is a fundamental principle implying that data should not be kept longer than necessary. According to Article 5(1)(e) of the GDPR, personal data should be "*(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')"*.

This principle is closely linked to data minimization and accuracy. Storage period has to be defined based on the different types of data as the GDPR does not specify specific time limits. Too long data retention period may result in a lack of lawful basis for retention. The different LSPs have dealt with this issue in their Data Management Plans by specifying clear limits to the data retention period for each kind of datasets they have dealt with. The data retention policy must subsequently be implemented under the surveillance of the DPO of each Data Controller.

3.5 Clarifying Data Controllers' and Processors' Responsibilities

Compliance with the GDPR is a formal responsibility of data controllers and processors. However, in a networked world or in complex IoT ecosystems, it is becoming more complex to identify and specify clear roles as far as data protection is concerned. For instance, websites and mobile applications integrate third-party services for user analytics, behavioral targeting, etc. In the public sector, government or cities build infrastructure to share data efficiently with different institutions. Therefore, the question arises who is responsible for observing data protection obligations in such networked service to guarantee an "effective and complete" protection, as emphasized by the European Court of Justice.

Large scale deployment tends to involve diverse stakeholders who may act as data controllers, co-controllers and/or processors. It may create some grey areas regarding formal responsibilities.

Clarifying who is the Formal Data Controller

In practice, clarifying who is the data controller or, in some cases, who are the joint controllers can be complex as many organizations may be involved and do not necessarily have a clear overview of data flows and data governance taking place in separated units. A key requirement is to clarify who are the formal data controllers and processors, in order to ensure that the legal accountability is understood.

For instance, in the context of Synchronicity, it appeared quite clearly that the de facto data controllers were the cities themselves. They are the one who control what data are collected and for what purpose. At the same time, the project had a collective responsibility to ensure that its research activities were complying with the regulation too.

Data Protection Coordination – Mezzanine Model

While several data controllers may be involved, coordination among them at the project level has to be ensured and guaranteed.

This is what Synchronicity experienced by setting up a Data Protection Committee (DPC) gathering the Data Protection Officers (DPO) of each smart city chaired by a Project Data Protection Coordinator (PDPC) at the project level.

By law, the cities remain the formal data controllers of the data processing under their control and they are directly accountable for it. However, the establishment of the DPC enables close coordination and sharing of experience to ensure that the project as a whole complies with the regulation, as well as to identify and mitigate potential risks that may impact the partners.

Such mezzanine model was successfully experimented by Synchronicity with a clear distribution of responsibilities and proactive collaboration among DPOs. It contributed to developing mutual support and exchange of experience. Another key element was related to the alignment of the interpretation of the new regulation. The possibility to discuss diverging understanding and interpretations enabled the DPOs to learn from each other and to converge towards a common policy at a project level.

The roles and responsibilities have been distributed as follow:

At City 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)

At Project Level

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

The following Figure illustrates the Mezzanine model adopted by Synchronicity.

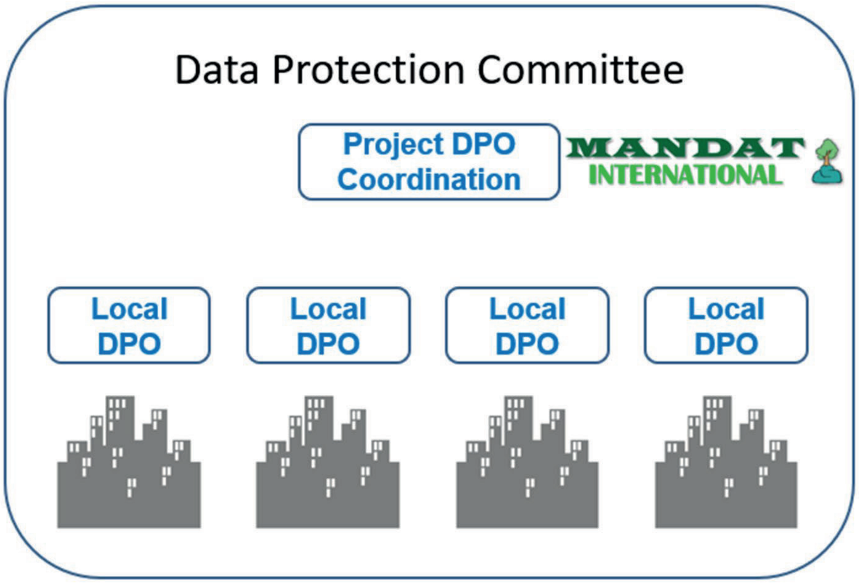


Figure 3: Data Protection Committee of Synchronicity.

3.6 Data Protection Requirements for IoT LSP Open Calls

Open calls overall, aim to complement and/or improve the use cases and the technologies used in terms of primary research. Ethical issues of the secondary use remain more or less the same. However, additional privacy concerns may be raised in respect to secondary data use with regard to specific conditions that potentially could be valid as specific services that the open callers may initiate in the existing platforms or services.

Therefore, in order to identify the potential ethical and legal concerns of open calls, stakeholders (open callers) have to define initially which data and to what extent data are planned to be exploited, elaborated and, in general, be used, and to introduce specific guidelines for data re-use and safeguard. Open callers should set up an ethical framework in the context of data processing according to EU data law requirements.

For instance, data subjects that are planned to be recruited in another research with other purposes should have expressed their consent to this participation in terms of the primary research. In case this is invalid, updated consent forms should be prepared and signed by the participants.

Furthermore, in terms of these guidelines, the techniques that will be used should be also defined. The re-negotiation of consent forms and of the Data Processing Impact Assessment (DPIA) documentation are among the key forms.

Consistency to ethical standards defined and strictly followed in the original research has to be kept in terms of the extension of the project technologies. Within ACTIVAGE, the use of new technologies had been justified in updated project documentation in order to ensure that the processing is fair to the data subjects. More specifically, the conditions of primary research had been checked and the further analysis of primary research exploitation by third parties had been studied extensively both from the legal and the ethical perspective.

3.7 End-user Engagement

Privacy concerns from individuals' perspectives are related to collection, IoT device, collected data storage and use of collected data. This underlines the social and legal aspects of privacy within the IoT and requires the inclusion of users affected in such discussions. Successful policies surface from a deep understanding of the context they intend to regulate and contributions to policy-making should be developed using a bottom-up framework. Contextual privacy within the IoT should take into account the concerns from those individuals involved, not only the end-users but also those who are affected. Thus, in LSPs, it is crucial to consider the role of these concerns in developing governance for empowering and enabling IoT, as motivated by previous literature.

The U4IoT project has provided a set of guidelines to be used by the LSPs in order to ensure full compliance with the GDPR in the form of a serious game called "privacy games". It is meant to help the LSP stakeholders to learn the fundamental principles of data protection, to raise awareness on the main risks related to data protection with IoT deployments, translating complex legal norms into clear and easily understandable principles. In this regard, all end-users, ranging from the IoT LSP beneficiaries to individuals and citizens can learn and gain knowledge about GDPR. The game is meant to be easily understandable, enjoyable and educative, covering the IoT privacy risks and all main definitions and principles of the GDPR. It follows a clear iterative methodology of game design, playtests, analysis and improvements. The game has been disseminated through privacy seminars, LSP events, game festivals and more.

4. Addressing Domain-specific Data Protection Requirements

4.1 Ageing Well, Assisted Living and e-Health

Technology advancements and computational intelligence currently enable the handling of big health data according to large scale heterogeneous data sources, which could provide a positive impact in the domains of prevention, diagnosis and therapeutic methods. However, these novelties also raise challenges for transparency and accountability as EU laws set up legislations for data processing and, in particular, for health data as sensitive data. In terms of LSPs, the problem was that apart from laws, practical guidelines and assessment procedures also had to be implemented, following the ethical by design principle.

Transparency was also a key principle in the use of ICT and IoT. To strictly follow it, the consortium had to ensure the security and privacy of both the hardcopy information and the electronically recorded and stored personal health data. Moreover, the principle of transparency had to be enabled according to the work of healthcare professionals and the security of sensitive data during the whole lifecycle. Among the innovations of the ACTIVAGE project was the combination of IoT technologies with e-Health solutions in one single integrated IT system.

To formulate a trustworthy environment, ACTIVAGE consortium initiated a Security and Privacy framework based on three main principles: privacy, trust and security. Aligned with these principles, proper methods and measures were applied to address the potential risk of using diverse data (personal, health, behavioural and mobility data) towards a user-centric IoT enabled system, as shown in Figure 4:

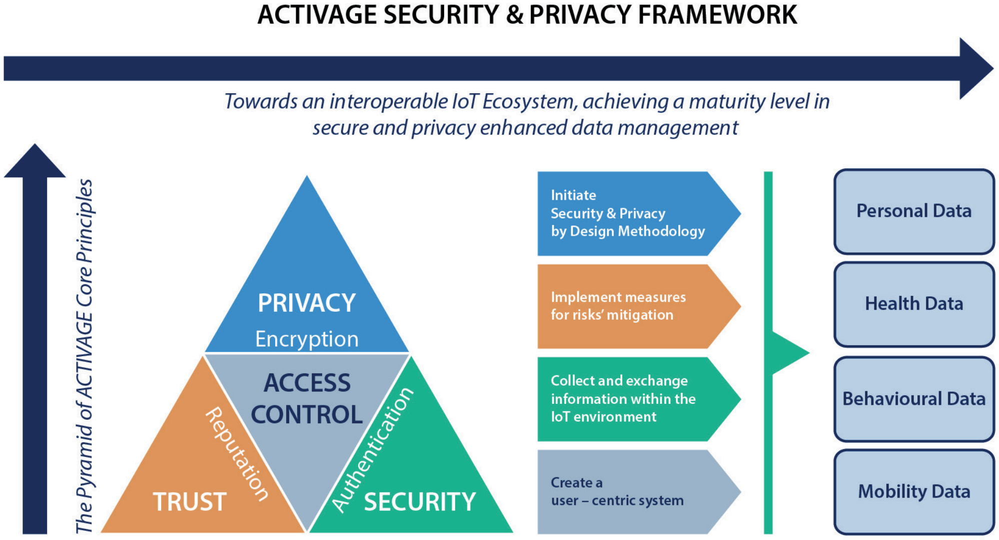

ACTIVAGE SECURITY & PRIVACY FRAMEWORK
Towards an interoperable IoT Ecosystem, achieving a maturity level in secure and privacy enhanced data management
The Pyramid of ACTIVAGE Core Principles
PRIVACY
Encryption
ACCESS CONTROL
Reputation
Authentication
TRUST
SECURITY
Initiate Security & Privacy by Design Methodology
Implement measures for risks' mitigation
Collect and exchange information within the IoT environment
Create a user – centric system
Personal Data
Health Data
Behavioural Data
Mobility Data

Figure 4: ACTIVAGE Security and Privacy Framework.

Despite personal and sensitive (health) data management brings opportunities such as improved quality of life and healthcare, critical challenges of security and privacy also arise. These considerations to data management and handling were initially addressed. Additionally, challenges were identified, and corresponding requirements were set up in respect to the data subjects' rights. Therefore, the ACTIVAGE consortium had to balance not only the ethical and legal principles and guidelines but the access to health data, along with the fundamental rights of data subjects to privacy protection. The project partners utilized proper methods for the systematic monitoring of the mechanisms of accountability and transparency. Controllers had to ensure that the processors comply with data protection regulations. Access authorization was set as a safety measure for data handling so only authorized persons (i.e. doctors, healthcare personnel, psychologists) could have access to patients' databases.

In most of the DSs, elderly people and end users in general did not possess adequate skills to understand electronic data processing. The lack of awareness among data subjects thus raised concerns about the viability of any regulatory model based on individual self-determination and consent, even when applying the DPIA model.

For risk mitigation, the ACTIVAGE practices included a request to technicians, researchers and developers to work closely with the Policy, Legal and Gender Board (PLGB) and follow its guidelines. In recent months, most of the PLGB Board (and ethics coordinators within ACTIVAGE) have been focused on complying with the GDPR requirements.

In order to systematically coordinate data management, to cope with data collection, storage and processing though different devices and to address a diverse target population (e.g. older people, formal/informal careers, patients) ACTIVAGE executed a Security and privacy risk assessment and used the results to define a data management strategy and a plan to organize such data. To successfully manage this plan both at Deployment Site and project levels, the ACTIVAGE consortium had to organize data processing internally and externally.

The following activities have been planned:

At project level:

- Set up the ethical board of the project and collaborate with experts to coordinate ethical and legal activities properly;
- Define and strictly follow the project action plan according to ethics activities;
- Assign and coordinate the responsible roles undertaken by consortium members in an effective manner;
- Monitor and assess the effectiveness of data management in consistency with ethical values' safeguarding;
- Set up a technical taskforce specific to security and privacy ensuring that the technology deployed upholds the ethical and legal standards;

At deployment site level:

- Data type identification and corresponding risks;
- Identification and description of data flow and the data processed;
- Cybersecurity assessment of employed technologies.

Security and Privacy were guided by two approaches: (1) the technological approach for the large scare deployment of smart, interconnected objects, and (2) the societal approach for the IoT enabled smart environments for older people allowing the collection of personal data. As the ACTIVAGE pilots involved more than 7000 users, the main concern of the consortium was to build trustworthiness in IoT considering the sensitivity of the services and data handled.

To this end, the consortium conducted a risk and privacy impact analysis at each deployment site, aligned with the privacy and cybersecurity objectives and requirements and the project level. These analyses were performed by using the STRIDE methodology to identify security risks at four IoT domains (device, gateway, cloud and application) and the DREAD threat mitigation methodology to provide proper risk management for the identified threats. A critical element was to provide a security cartography assessment for each deployment site, IoT domain and severity type.

To be consistent with the Security and Privacy framework, the interpretation and harmonization with the GDPR were highly important. According to Article 25 and the related recitals 28, 29 and 78 of the GDPR, controllers and processors have to implement Privacy Enhancing Technologies (PETs) to eliminate or reduce personal data, or to prevent unnecessary data processing, in line with the core ethical principle of data protection by design. Aligned with these requirements, ACTIVAGE implemented a number of organizational and technical measures (e.g. pseudonymization) to enable the effectiveness of privacy principles and data minimization and to safeguard data subjects' rights.

4.2 Connected Vehicles

Automotive is a very specific environment with many unique problems related to security and privacy. The devices and especially the vehicles are usually highly valuable assets requiring high protection and detailed access log containing information about who accessed which function or for which purpose. For instance, this data may be used in case of incident resolution. In the case of vehicles, it also needs to be considered that they are heavy machinery able to cause damage and threaten lives meaning that detailed information about incidents may be necessary for legal resolution of accidents. The information must be detailed enough to allow resolution of liability for the damage with enough measures to ensure non-repudiation of the personnel, as well as protection against forging. From this point of view, privacy may be inherently less important than in the case of other environments. On the contrary, the fact the vehicles are connected to IoT platform and provide almost real-time information about their location, surroundings and, in rare cases, also live video stream means that the whole IoT platform may be considered as a potential privacy threat not only to participants directly connected to the platform but also to all persons coincidentally walking by IoT sensors. User personal information is entering the system at specific points and as such, it is usually not necessary for the system to function. A user may be the owner of the car or he may be using one of the services offered by the platform such as car sharing. While in the first case the identity is permanent and is liable to legal matters (obligations for car registration), the latter case means that the service needs to know user identity in case of an incident, but this does not necessarily have to be permanent. The system should be able to eventually resolve user identity, but only in the case of need and under very specific controlled conditions. It should not be able to have an overview of user actions but only the possibility to request real-life identity resolution.

The system may pose a very specific privacy threat: user tracking. The fact the IoT platform processes position information of the cars, the information may be persisted and even made accessible to external entities via offered services creates a threat that someone may track the position of a selected car and when combined with information obtained from different sources to resolve it to a position of a person. This tracking may occur in real-time but may also allow reconstruction of a person’s behavior over the whole data retention period.

The collateral information collected by the platform can be a specific threat. The platform sensors may collect various information from their environment and the information may potentially contain personal information such as video with people crossing the road, Bluetooth and Wi-Fi beacons of mobile handsets or other IoT devices. This information is very difficult to classify and should be treated as potentially sensitive. This leads to a strong requirement that the platform should not collect or store raw information and the sensors should sanitize the information prior to sending it to the platform.

The information handling and storage are subject to GDPR regulation and must be correctly managed. It should be noted that the information collected and stored by the IoT platform may have an added value for the platform operator, it may be processed and the results utilized directly by the operator to improve the services, the results may be used by automotive partners or even raw data may be offered to other companies such as insurance or transport companies. The information sharing is one of the most sensitive topics, and recent cases of information misuse by social networks will only increase user awareness and caution. If the information sharing must be done with the prior consent of the user and the data sold should be anonymized. In a special case when data may be provided with personal information such as driving information delivered to insurance company in exchange for benefit of lower insurance fee. In that case, a contract between all the parties must be established and the user should be aware of the information scope of the transfer.

Privacy of the IoT automotive platforms may be one of the enablers of business exploitation and affects both user acceptance and legal establishment of the service.

4.3 Smart Agriculture

Generally, the use cases of IoF2020 do not deal with sensitive personal data but direct and indirect personal data might play a role.

Identifiable

An identifiable natural person – in the case of smart farming a farmer - is one who can be identified, directly or indirectly, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of that natural person.

In practice, these also include all data which are or can be assigned to a person in any kind of way. For example, the telephone, credit card or personnel number of a person, account data, number plate, appearance, customer number or address are all personal data.

Indirectly identifying

Indirectly identifying personal data can be:

1. A combination of non-personal data can be indirectly identifying e.g.:
   - Shoe size + general location --> only 1 person with size 48 at the Subway.
   - Eye color + course --> only 1 person with green eyes in the Food Law course.
2. Indirectly identifying by using all the means likely reasonably to be used by a person to identify the said person' e.g.:
   - Google Search.
   - Combining available datasets.

Data on how much a farm machine has sown, harvested and where are generally not considered as personal data. Or satellite data of parcels are also not considered as personal data.

Other examples of possibly indirectly identifiable data include the observation data that are provided by the farmer through the use of a service (e.g. a smartphone app) or a device (e.g. a wearable sensor) or generated by operating a tractor or machine that has a built-in GPS. A tractor used by a farmer during harvesting also says something about the farmer.

Combining those anonymous datasets with other information or datasets could lead to the identification of the farmer, especially that in the EU, many farms are one-man businesses (sole holder holdings). Therefore, IoF2020 had to adopt a strategy for privacy compliance.

Furthermore, a dedicated work package on ethics has empirically investigated what stakeholders identify as sensitive data and what kind of protection they would prefer if any. Based on these findings, the consortium intends to form a guideline for responsible data stewardship to complement the codes of conduct that have already been shaped.

4.5 Smart Cities

Smart Cities are complex environments where diverse data are collected and processed. As IoT are usually deployed in public space, the risk to collect personal data at scale is high. The diversity of the data processing leads to a high level of complexity, with diverse data processors and sometimes controllers and joint-controllers.

A common issue occurs when the municipal administration and the State level administration have overlapping competences on a same territory. The question of data transfer from one administration to another may raise complex issues.

Another specificity of data processing in smart cities is the complexity generated by the multi-stakeholder's nature of a city environment. The Municipality must take into account diverse and competing interests. For instance, citizens may be more interested in creating new kindergartens than deploying IoT technologies.

The personal data protection dimension is particularly important in smart cities environment. The medias and the European public opinion are quite sensitive and reluctant to let public administration intruding in their privacy. The monitoring of public space is a complex and politically sensitive topic. This is also connected to a specific risk that has been identified in the context of smart city LSPs: the political risk. Beyond the need to ensure that technology is understood and accepted by the citizens, municipal authorities are also concerned not to deploy technologies that could appear as an attempt to monitor and control the citizens.

Synchronicity, as a research project, has developed a strategy in order to ensure full compliance with the highest ethical and legal standards. The strategy has focused a lot on strict and proactive compliance with the GDPR in order to reduce the legal, financial, political and reputational risks.

An important step was achieved by clarifying the roles and responsibilities in each city (or reference zone) and by establishing the Data Protection Committee chaired by one of the partners: Mandat International (see section 3.5). Each City DPOs remained in charge and responsible for the data collection in its respective city. The City DPOs were in charge of implementing appropriate safeguards to protect the processed data in their reference zone and to ensure compliance with the GDPR.

The Data Protection Committee has defined the data protection policy, facilitated the coordination among the different DPOs, served as public information and contact point, working on reporting and data protection issue management. A specific task of the Data Protection Committee has been the development of a clear Data Management Plan at project level, in order to specify a common data protection policy.

The project used the Data Protection Committee to assess the risks of the pilots on the rights of the data subjects. To this extent, a specific data protection impact assessment (DPIA) methodology has been developed to specifically address the risks related to smart city projects. This DPIA has been designed to serve as an important accountability tool. It does not only foster the compliance of data controllers with the obligations set by the applicable data protection law, but it also serves to demonstrate that appropriate measures have been taken to ensure compliance with it.

Synchronicity took advantage of the Europrivacy (www.europrivacy.org): a certification scheme developed by another European research project for assessing GDPR compliance of IoT deployments in smart cities. It applied the scheme in the context of one of the smart cities and also contributed to enrich this certification scheme with complementary specific requirements related to GDPR compliance of smart cities.

Finally, the project developed a specific application, Privacy App (www.privacyapp.info) in order to enable the municipalities to inform their citizens about the IoT deployments.

4.4 Wearables

The MONICA project collected and processed different types of personal data using different technologies such as wearables, CCTV and sound level meters. There are five different types of wearables employed in MONICA demonstrations, four of which were used by event staff and/or authorities and one which was offered to the audiences at the demonstration event: Crowd wristbands, Staff wristbands, Smart glasses, LoTrack GNSS-based staff locators, and RIOT-LoRaWAN-GPS staff trackers.[4]

The purpose of using wearables in the project was to improve crowd monitoring and staff coordination in cases of security or safety incidents during an event (e.g. knowing the precise location of a staff member handling or involved in an incident, support/additional staff members can be guided/sent to the precise location more efficiently). Wearables may be used in combination with other monitoring technologies, thus, requiring extra careful analysis of the implications and requirements related to data protection and privacy.

The five different types of wearables all collect positioning data that is displayed in real-time at the Common Operational Picture (COP) system installed in a secure control room on the pilot location. The COP must, therefore, be included in the discussion of wearables in the context of the GDPR and general data protection and privacy issues.

The COP provides professional operators knowledge to make informed decisions on the environment and crowd control. As the COP shows the geo-position of a wearable that, in case of staff wearables, is matched to a pseudonym (usually registration ID) of the bearer, it contains indirectly identifiable personal data. Therefore, wristbands equipped with COP were distributed anonymously and it was ensured that the geo-positioning could not be used to identify data subjects.

A distinction was made between personal data collected automatically (i.e. through sensors and devices such as wearables) and manually (i.e. through surveys in connection with impact assessment activities). The former requires careful consideration of the data subjects' rights and data protection issues. Therefore, MONICA has developed consent forms to specify what type, how much, why and when data is collected. The consent form was collected form all staff members testing wearables during the project demonstration. Nonetheless, for crowd wearables as they had been distributed anonymously, it was not feasible to collect informed consent via the traditional form. Instead, the privacy policy was embedded in the event app describing data subjects' rights and how to exercise them.

MONICA considered the collection and processing of personal data from both legal and ethical perspective as compliance with legal requirements cannot be assumed to comply with ethical standards and principles. Therefore, obtaining informed consent from data subjects does not automatically redeem data controllers and/or processors from handling personal data in an ethical manner. The process of obtaining informed consent is equally important; if the data subject is afraid of the negative consequences of not signing the consent form, it implies the unethicality of processing. Therefore, MONICA identified a clear guideline on how to obtain informed consent freely and voluntarily from staff members.

Prior to the testing and demonstration activities, MONICA had carried out an ethical analysis of the different surveillance and monitoring technologies to be implemented in the project. In line with the analysis, a set of protocols, guidelines and an ethics checklist had been developed to ensure that all activities are ethically sound. The purpose of these tools was to help partners and pilots to identify their obligations, as well as ethical and legal requirements. Thus, the Ethical Manager of the project focused on using these tools to actively support the project's development ensuring compliance with the regulatory requirements. MONICA wanted to ensure that tools were not used by developers to restrict, criticize or reject their work.

[4] The technical specification of the MONICA wearables is available in D3.2 IoT Enabled Devices and Wearables 2

Surprisingly, the tools have been valuable in supporting the communication between developers and pilots on issues related to data management and data protection.

To document the project's compliance with data protection and privacy regulations, annual compliance and monitoring reports have been compiled for all MONICA pilots. These reports contain a summary of the DMPs, a completed Ethics Checklist per type of personal data collected, the Data Privacy Impact Assessment and, if applicable, an Incidental Findings report, a Non-compliance Corrective Actions report and a description of any ethical concerns raised by a partner or a data subject and how such concerns have been handled. The annual compliance monitoring reports have been reviewed and approved by the project Ethical Board. The project's Ethical Board consists of a Chair (the project's Data Security Manager), the Ethical Manager, representatives from the six pilots, and two external experts. Through its annual meetings on discussing ethical issues and regulatory requirements, the Ethical Board has specified recommendations to improve data management, as well as data protection and privacy of the project.

In addition to data privacy and protection requirements, the use of wearables in the project has been subject to compliance with local radio-spectrum and health and safety regulations. It also required briefing of the involved authorities prior to the event. Moreover, the installation of the solution required full cooperation and commitment of the event production management and crew as it involved visible presence and adjustments to event decoration, infrastructure and other structural changes.

Finally, for each event, the Data Management Plans and the DPIA had to be signed by the DMP-responsible and the pilot representative. Additionally, the Data Protection Acknowledgement had to be signed by all relevant partners involved in the collecting and processing data prior to the event demonstration.

5. Data Protection Enablers and Tools

For the purpose of the discussion captured in this document, an ‘enabler’ is defined as a technology or tool which enables data controllers to achieve the compliance with data protection norms or standards.

5.1 Data Privacy Impact Assessment (DPIA) and Risk Assessment

Big data and privacy are key factors that LSPs must continuously take into account. The impact of technologies, especially those based on IoT, will be unstoppable. Its effect in many fields can be incredibly beneficial. Nevertheless, there are also dark areas to which we must pay attention. Without clear regulation, the problems will multiply.

In the case of the LSPs, ACTIVAGE has offered a good opportunity to explore not only the standard levels of security or compliance with regulations on data protection but also provided a perspective to work transversally on ethical aspects in the technological dimension. The ACTIVAGE project copes with large-scale databases with personal information and, therefore, a privacy methodology had to be defined for risk analysis with regard to the IoT system. This methodology has been followed by ACTIVAGE to highlight proper recommendations for the ACTIVAGE IoT system towards the minimization of potential threats in relation to data processing. Thus, DPIA was set up as mandatory for all the entities participating in the project.

The security risk analysis and DPIAs performance of the ACTIVAGE project and all of its DS enabled the process of risks’ identification and corresponding solutions to IoT security enhancement alongside with the privacy activities to GDPR compliance. The ACTIVAGE AIOTES framework also implemented privacy and security components but privacy recommendations determine the security of the whole IoT system. In addition, an overview of GDPR issues has been carried out to identify the concrete legal obligations of entities/persons that they should comply with in relation to pilots’ operational needs at the DS level.

Synchronicity developed a specific Data Protection Impact Assessment (DPIA) framework which has helped cities involved in the project to identify their privacy risks. It has been offered to the DPO of the different reference zones as an enabler useful to map their risks and to identify mitigation measures. The Smart City DPIA has been structured and made available as an Excel file to be completed by each and every participating city.

5.2 Data Protection Game

Ensuring basic compliance with the GDPR already requires specific knowledge and understanding. Applying the GDPR to a research project or to a large scale IoT deployment is even more challenging.

In the context of U4IoT, Archimede Solutions developed an *ad hoc* serious game on data protection. It takes the form of a set of cards with questions and answers encompassing the various obligations of the GDPR. It includes questions related to each one of the application domains of the 5 LSPs, as well as generic and domain-agnostic questions. It has been developed with the objective to raise awareness of professionals involved in IoT deployments. It enables researchers, engineers and Data Protection Officers to test their knowledge of the GDPR in an entertaining and effective manner.

The serious game has been used as a basis to the development of a formal certification scheme for assessing the qualifications of Data Protection Officers at national level.

More information: www.dataprotectiongame.com

5.3 Privacy App

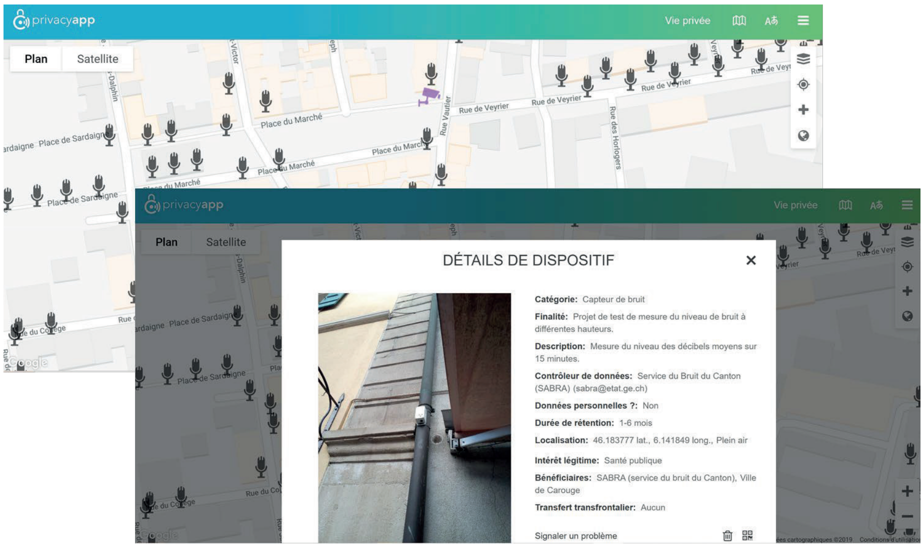
An important challenge and obligation for smart cities are to inform data subjects, such as citizens and visitors about the data processing performed in their public spaces. Synchronicity's DPO Coordinator (Mandat International) developed a privacy application that has been made available to all participating cities.

The Privacy App enables citizens to access clear information on the IoT deployed in their city, including on the data controller and data retention policy. It provides an innovative concept and model to engage citizens and public administration to work hands in hands ensuring a transparent and privacy by design model of smart cities and IoT deployments. The application combines data protection expertise together with a crowdsourcing mechanism to inform citizens on privacy compliance in smart city deployments.

The privacy app enables smart cities to inform the public on IoT devices installed in the public environment and enable crowd-sourced monitoring and identification of IoT devices deployed in the public space, as well as mutualization of information on such devices. Moderators can complement the information on identified devices. The moderators can be data controllers or smart cities themselves.

The application has been designed according to the GDPR. At the top of the application management, there is a platform administrator and a personal data protection officer. This application can be deployed on the smartphone of each citizen interested to contribute to his smart city. The operation is quite simple: the citizen sees an IoT device in the street and opens the application on his smartphone.

More information: www.privacyapp.info



DÉTAILS DE DISPOSITIF

Catégorie: Capteur de bruit

Finalité: Projet de test de mesure du niveau de bruit à différentes hauteurs.

Description: Mesure du niveau des décibels moyens sur 15 minutes.

Contrôleur de données: Service du Bruit du Canton (SABRA) (sabra@etat.ge.ch)

Données personnelles ?: Non

Durée de rétention: 1-6 mois

Localisation: 46.183777 lat., 6.141849 long., Plein air

Intérêt légitime: Santé publique

Bénéficiaires: SABRA (service du bruit du Canton), Ville de Carouge

Transfert transfrontalier: Aucun

Signaler un problème

Figure 5: Privacy App access to data protection information in smart cities.

5.4 EuroPrivacy – GDPR Gap Analysis and Certification

The GDPR includes over 70 references to certification. Synchronicity took advantage of the EuroPrivacy Certification Scheme developed by the Privacy Flag H2020 European research project to perform gap analysis and to ensure compliance of IoT deployments with the GDPR.

EuroPrivacy provides a well-defined and efficient methodology to perform a systematic and comprehensive evaluation of GDPR compliance. The EuroPrivacy methodology has been developed to encompass emerging technologies, including Internet of Things, data analytics and artificial intelligence. It covers a vast set of data processing, stretching from products, services, processes to information management systems. Moreover, it is easily combinable with ISO 27001 certifications and extendable to complementary domain specific and national obligations. It enables to combine a single certification the GDPR requirements with complementary national obligations such as the Swiss federal act on data protection or other non-EU regulations on data protections.

In the context of Synchronicity, the Europrivacy certification scheme has been further extended and adapted to better cover smart city specific requirements in terms of GDPR compliance. It was successfully applied and validated with real IoT deployments in the LSP.

More information: www.europrivacy.com

5.5 Privacy Pact

Another relevant tool to be mentioned is Privacy Pact. As previously mentioned, the LSPs are involving European research partners as well as non-EU based research partners. Data processors located outside of the European Union territory must commit to respect the GDPR when processing data coming from the EU. Such commitment may be complicated to formalize across diverse jurisdictions.

In order to facilitate cross-border collaboration and data transfer, the H2020 project Privacy Flag developed an online commitment tool enabling any data processor located outside of the European Union to voluntarily commit to respect the GDPR obligations. It enables partners to demonstrate that they are contractually bound to respect the GDPR rules and the associated data subject rights.

More information: www.privacypact.com

5.6 Trusted Framework for Connected Vehicles

Within the context of Autopilot, four frameworks have been created and recommended for the usage of Autonomous Vehicles augmented by IoT: A Policy Framework, a Security Framework, a Privacy Framework, and an Engagement Framework. These frameworks contribute to trust-building necessary to operate and use Connected Autonomous Vehicles.

The Privacy Framework embeds principles and mechanisms to minimize the privacy breach risks while using connected autonomous vehicles augmented by IoT, as illustrated in the following Figure 6.

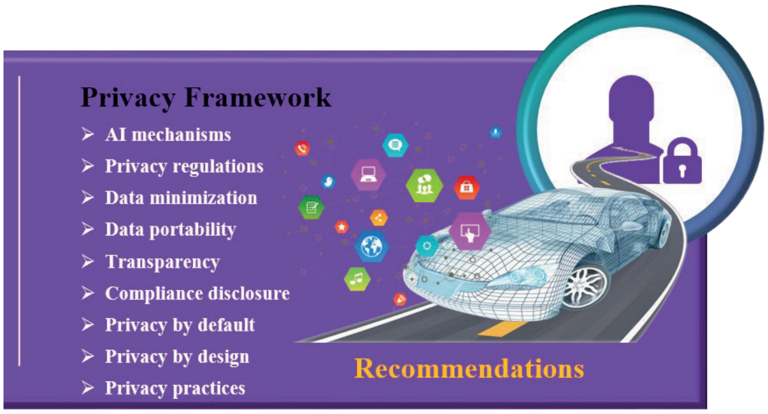


Figure 6: Privacy Framework.

The key consideration is to center the approach on the user and focus in predominance on the data protection by design, transparency and data minimization.

With regards to the “Privacy by Design”, Autopilot adopted the adaptive principles of Dr. Cavoukian (see bibliography):

- Principle 1: Proactively Prevent Privacy Invasive IoT Events;
- Principle 2: Ensure IoT Privacy by Default;
- Principle 3: Embed Privacy Enhancing Capabilities into IoT Service Design and Device Architecture;
- Principle 4: Adopt a Stakeholder Approach to IoT Privacy for Full Functionality, Positive Sum Outcome;
- Principle 5: Provide Full Lifecycle Protection of IoT Data for End-To-End Security and Privacy;
- Principle 6: Opt for a Verification Based Trust Approach to IoT;
- Principle 7: Consider Users at the Core of IoT Services.

In addition to privacy, particular attention has been devoted to security. The key enabling factors for Privacy in AUTOPILOT are:

- Security;
- Strong authentication to services;
- Data pseudonymization and anonymization;
- Identity derivation and anonymous authentication techniques;
- Translation of information between the solution layers and segregation of duties.

From a technological point of view, AUTOPILOT Security and Privacy architecture closely follows the ETSI Intelligent Transport System (ITS) standard augmented by IoT. In this architecture, there are a number of security interfaces that allows security services to be provided at different levels. In fact, security in an autonomous driving IoT system is more than just information security as assets are not just data and IT infrastructure, and also as securing a distributed network of devices present different challenges.

Following this consideration, the Industrial Automation Control Systems (IACS) standards, such as the ISA/IEC 62443, are useful to provide guidance for some parts of the systems and offer good approach in which security is analyzed in a context where a failure can have very high costs both in terms of human lives and money. Protecting against risks should be at the product component level guided by ISA 62443 – 4 – 1 and 62442 – 4 – 2 requirements. Even if AUTOPILOT is not designed as an IACS, it is able to use it when analyzing requirements.

As required by the risk analysis procedure described in ISA IEC 62443 – 2 – 3, the AUTOPILOT system, or the System Under Consideration (SUC) has been divided into three main zones to identify and predict several risks and corresponding countermeasures:

1. In-vehicle network;
2. V2X and IoT network of connected devices;
3. Cloud IoT platform.

The in-vehicle-IoT-network provides interconnection of car devices. This is the most critical zone of the system that requires a high-security level. It is also possible to foresee a security perimeter around the safety-critical sub-zone, the one connected with to the AD decision-taking devices. On the other hand, all the devices connected to the In-vehicle-IoT-Platform are outside the perimeter and thus are potentially vulnerable.

The IoT & V2X zone covers the medium-range communications between the vehicle and its close surroundings: vehicles can send heartbeat-like localization signals using CAM and on-event-messages using DENM, both defined in C-ITS. The IoT Cloud Platform collects and exploits data from IoT peripheral devices and provides back control/navigation/optimization data to peripheral devices. The mitigations for the identified risks have been mapped to System Level Requirements so that the Security Level Capability (SL-C) of the overall system can be derived by following the requirements in that part of the standard. The use of the ISA IEC 62443 has been beneficial in both providing grounded guidance to the risk analysis process and in deriving results and mitigations that can be easily tested, understood and compared.

5.6 Other Privacy Enhancing Technologies (PETs)

The ACTIVAGE project has offered the opportunity to adopt proper technologies for data management and data sharing dealing with the privacy of data.

In particular, technical mitigation measures have been utilized in order to increase the security of processing, PETs as encryption and pseudonymization have been adapted and applied to avoid data linkage and disrespect of data subjects' rights. More specifically, encryption algorithms as BCRypt, SHA256withRSA, SSL/TLS and TDE have been used along with secure channels (e.g. https, token, VPN connections, etc.). Moreover, anonymization of personal data through a surrogate key and limited access to this key was considered as a safe technique for data protection.

One of the key enablers for privacy in ACTIVAGE is the use of Semantic Services. The underlying technology (Semantic Service Interoperability Layer – SSIL) makes the definition of abstract services using semantic technologies possible. These services could then be implemented by different entities participating in the framework, and then located and invoked later when needed, independently of their implementation or interface. This is an effective way to define data subjects' rights by the means of technological services and make such services available to users or data processors.

Within ACTIVAGE, extended research has been conducted in respect to cutting edge technologies for privacy protection as Blockchain that could be used in healthcare domains, as well as in IoT smart home environments with an enormous impact. It is because it reduces the time for patient information access, enabling interoperability and improving the quality of data, also eliminating maintenance costs.

As it has been mentioned, ACTIVAGE paid special attention to GDPR compliance and technologies. As Blockchain is built on distributed architecture, it does not demand multiple levels of authentication while digitizing data and ensuring patients' privacy connection to enable privacy, security and trust through a decentralized repository for users' identification. It also acts as a valuable tool towards the consistency of the requirement of the new regulation.

However, among the main concerns were to ensure that a) personal data should not be stored on the Blockchain and that b) the cryptography technique should be used to give to the end-user the "right to be forgotten". Blockchain technology can enable the connectivity of IoT devices, ensuring safe and reliable data processing avoiding the risk of data breach. Each IoT device which is registered in the Blockchain has a unique ID that will solely identify this device in the universal namespace.

- BaaS Web UI (The Blockchain-as-a-Service (BaaS) Web UI): a web front-end for functionalities access provided by the Blockchain network implemented within myAirCoach H2020 project;
- Middleware API: The Middleware API supports the communication between the ACTIVAGE Monitoring Platform and the Blockchain network.

6. Standardization of Data Protection and Security for IoT

Privacy and privacy by design are recent concerns, therefore, only a few standards are published. On the other hand, a wealth of standards related to data protection are being developed in various Standards Development Organizations, such as ISO, IEC, ETSI, ITU, IET, IEEE. Annex II includes an illustrative and unexhaustive list of data protection related standards.

Standards tend to be developed in several directions, including:

- Terminology;
- Technology and mechanisms;
- Methodologies;
- Principles, policies and guidelines.

The LSPs have directly contributed to several standardization processes.

Create-IoT contribute to several standardization tracks at ISO and ITU, while Synchronicity contributed to several standardization processes at the ITU and ETSI. Some key contributions to be noted include:

- The International Telecommunication Union, with a focus on:
    - The ITU-T Study Group 20 on the Internet of Things and smart cities, where Synchronicity initiated a new recommendation to standardize the Open API for IoT Data in Smart Cities (Y.API4IOT), including data protection requirements.
    - The ITU-T Focus Groups on Data Processing and Management to support IoT and Smart Cities & Communities (FG-DPM) where Synchronicity partners have actively contributed to write the *“Framework for security, privacy, risk and governance in data processing and management.”* (Technical Report D4.1), addressing the concerns related to data security, privacy and risk for data processing and management in IoT and Smart Cities and Communities.
- The ETSI, with the contribution to the ETSI ISG for cross-cutting Context Information Management and ETSI STF 566.

A key conclusion from the standardization efforts lies in the need to integrate data protection by design as a common requirement across all relevant standards for the IoT.

Finally, it is to be noted that EDPS started in 2016 is an initiative to create a privacy engineering community called IPEN (Internet Privacy Engineering Network)[5]. The LSPs and CSAs have liaised with this initiative.

[5] https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en

7. Guidelines for GDPR Compliant IoT Deployment

The LSPs have contributed to develop a shared knowledge that has been enriched by the various partners. After three years of research, test and validation in diverse application domains, the research community has identified several guidelines that can be useful for future projects. These guidelines are intended to be refined and iteratively complemented by future research projects and large-scale pilots.

1. **Perform a preliminary data protection impact assessment** before collecting any data with new technologies. Ensure that you address and mitigate the identified risks.

2. **Minimize personal data collection**, including by adapting the granularity of the data and by processing the data at the edge. Consider data minimization and data protection by design as an opportunity to save costs and to increase the scalability of the system to be deployed. This is a way to leverage the approach to build trust within the organization and towards the different stakeholders.

3. **Minimize personal data transfer** by prioritizing onsite (pre-)processing, edge computing and local storage. Decentralized data processing can contribute to enhance both data protection and scalability of the system.

4. **Minimize data storage and retention time**, which will also save you infrastructure costs.

5. **Maximize the use of anonymization and pseudonymisation techniques.**

6. **Ensure that the data processing is lawful** and that the amount of personal data collected is proportionate to the legitimate purpose of the data processing.

7. **Clarify who are the data controllers and processors** involved in the deployment and identify their respective Data Protection Officers. Establish adequate coordination mechanisms and regular communication among the DPOs and clarify their respective responsibilities.

8. **Designate a Data Protection Officer** at the level of the pilot in charge of monitoring the IoT deployment compliance with data protection regulations.

9. **Ensure that the Data Protection Officer can be easily contacted through the website** of the pilot.

10. **Formalize your data protection policy** in a clear document and communicate it to all involved stakeholders and employees.

11. **Organize regular communication and training activities on data protection** for all those involved in the processing of personal data. Serious games can be used to build capacity and enhance compliance with the GDPR (i.e. dataprotectiongame.com).

12. **Write a Data Management Plan** that specifies what data are collected for what purpose, who can access them, how long they are stored, etc.

13. **Secure your IoT Network** physically and logically, and use end-to-end encryption such as IPSec in tunnel mode when using the Internet in IPv6.

14. **Each IoT mote should be protected by a unique and distinct password** and never use a default password provided by the manufacturer.

15. **Define and implement a clear access right policy** that minimizes access to the processed personal data. The personal data should be accessible only to those who have a legitimate need to access them.

16. **Adopt and enforce a strict policy and procedure for updating the firmware** of the IoT Motes whenever vulnerabilities are identified.

17. **Establish procedures to comply with the data subjects' rights**.

18. **Exchange and collaborate with other DPOs** and organize peer reviews.

19. **Use external certification of compliance** with data protection regulation as a mean to reduce liability and to increase trust and transparency with end-users.

20. **Identify any cross-border data transfer** of personal data and check if they are lawful.

21. **Clearly inform and communicate the purpose for data collection**, the categories of data processed, who has access and how long the data will be stored online through online applications (i.e. privacyapp.info).

22. **Take advantage of online commitment tools** to ensure that all partners located in other jurisdictions are committed to respect the same level of data protection (i.e. privacypact.com).

8. Future Research Needs and Challenges

As new challenges approach, the work done within the LSPs program can also offer useful insights for future research to the IoT community. To this extent, the LSPs have identified different research needs and challenges to be addressed:

Multi-stakeholder Collaboration with Manufacturers and Solutions Providers

There is still a lot to research in relation to end-user adoption and validation of the IoT technologies. There is a need to better analyze and understand the interactions among the various stakeholders to guarantee and enhance privacy by design in IoT deployments. It will require an increased collaboration between manufacturers and providers of IoT solutions with the end-users, to align their solutions much more closely to the cybersecurity requirements and to the expectations and needs of the end-users.

IoT Security by Design

The IoT technology is pervasive and will have a huge impact in many application domains. It will constitute an unprecedented surface of risk of hacking in a globally interconnected environment where personal data are collected from a multitude of devices. It raises concerns about the privacy and data security implications. Privacy concerns mainly refer to the lack of transparency in respect to data processing and are critical to define who has access to data and what the purpose of data processing in each case is. One thing to be kept in mind is that good security practices are of fundamental importance and what has to be known all along the value chain is that along all the stakeholders has to be the raise awareness about security. New models of security by design for IoT in multitenant environment should be researched.

IoT, Artificial Intelligence and Data Analytics

The emergence of Artificial Intelligence coupled to Big Data raises a whole set of questions on the frontier between personal data and non-personal data. The potential to combine and analyze diverse datasets may allow the identification of personal profiles and the generation of personal data out of non-personal data. The consent management of such border line data will be a challenge to research, in order to prevent unlawful profiling, tracking, surveillance or automated decision-making.

Interaction between Data Protection, Privacy and Ethics

The notions of Data Protection, Privacy, and Ethics seem to converge. However, they rely on distinct grounds. It is on purpose that the GDPR does not use the term “Privacy” and refers instead to personal data protection. While these two concepts are defined in laws, the ethics has different foundations. All of them are influenced by and interacting with the societal and cultural environment. The interaction between these notions requires further research to pave the way towards a global framework of data protection.

IoT Responsibility and Liability

IoT technologies will be more and more pervasive, and will progressively provide a growing support to human beings by assuming decision to adapt the environment to the end-user needs. It will certainly change the perception of citizens on IoT. IoT devices are expected to become smarter and smarter. They will progressively take autonomous decisions and interact with our daily life. Autonomous vehicles, eHealth and smart homes will raise questions on the legal responsibility and liability of decisions taken by distributed smart nodes.

A Real Human-centric IoT

The challenge to enable a human-centered IoT will pass through a real assessment of the impact of this technology not only in the privacy domain but also in a wider context. The research should associate end-user representatives to address the ethical and privacy implications associated to the Next Generation Internet of Things. New technologies should align with end-user expectations and requirements, including datab orotection by design. This is key to support worldwide adoption of IoT technologies.

9. Conclusion

The Horizon 2020 European research programme offered five Large Scale Pilots and two Coordinated & Support Actions the opportunity to demonstrate how compliance with personal data protection regulations can be applied in the Internet of Things. To illustrate IoT compliance with the GDPR, the objective of these Guidelines was to share the experiences of the five LSPs through an overview of developed methodologies, strategies and enablers.

Implementing privacy by design and by default was not an easy task. Such increased collection of data raises issues of trust and authentication in data subjects, leaving them concerned about whether data is used for the intended purposes only. This is particularly true, as we have seen in the context of ACTIVAGE, in the case of vulnerable groups. Each LSP operates in a different ecosystem and their use cases needed specific measures, producing various enablers to guarantee an appropriate level of protection of personal data. The interaction between IoT, the rule of law and the management of legal issues had to be addressed. Through examining common privacy approaches and domain-specific data protection requirements, each LSP brought their own perspective and solution, sharing the most relevant lessons learned. Without adopting a generic privacy by design approach, full compliance with the existing regulatory framework is impossible.

For the future, we suggest exploring those research needs and challenges, such as security practices, human centric IoT, etc., that were identified by the project partners while sharing their own insights. Although the work done by LSPs increased both the horizontal and vertical know-how of protecting rights and privacy in an increasingly connected world, the generalizability and applicability of both cross-domain and domain specific approaches needs to be explored.

10. Links and references

Useful Links

LSP-related Projects Websites

- Activage: https://www.activageproject.eu
- Autopilot: https://autopilot-project.eu
- Create-IoT: https://european-iot-pilots.eu/create-iot
- IoF 2020: https://www.iof2020.eu
- Monica: https://www.monica-project.eu
- Synchronicity: https://synchronicity-iot.eu
- U4IoT: https://u4iot.eu

Tools and Resources

- EuroPrivacy GDPR Gap Analysis and Certification: https://www.europrivacy.com
- Privacy App: https://www.privacyapp.info
- Privacy Pact: https://www.privacypact.com
- Serious Game on Data Protection: https://www.dataprotectiongame.com

Normative References

- Regulation 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector (Directive on privacy and electronic communications) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union https://eur-lex.europa.eu/eli/dir/2016/1148/oj
- Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

Other Web References

- https://www.dogtownmedia.com/is-there-a-right-way-to-build-a-smart-city/
- https://www.smart-industry.net/interview-with-iot-inventor-kevin-ashton-iot-is-driven-by-the-users/
- https://www.sap.com/trends/internet-of-things.html
- https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-privacy-by-design-and-by-default.html#

Bibliographical references

Books

Cavoukian, Ann, and Claudiu Popa. *Embedding Privacy into What's next: Privacy by Design for the Internet of Things*. Ryerson University Privacy & Big Data Institute, 2016. https://www.ryerson.ca/content/dam/pbdce/papers/Privacy-by-Design-for-the-Internet-of-Things.pdf.

Hoepman, Jaap-Henk. "Privacy Design Strategies." In *9th IFIP International Information Security Conference (SEC)*, Nora Cuppens-Boulahia, Frederic Cuppens, Sushil Jajodia, Anas Abou El Kalam, and Thierry Sans (Eds.). IFIP Advances in Information and Communication Technology, Vol. 428. Springer Berlin Heidelber, 446–59, 2014.

Lévy-Bencheton, Cédric, and Eleni Darra. *Cyber Security and Resilience of Intelligent Public Transport*. European Union Agency for Network and Information Security (ENISA), 2015.

Vermesan, Ovidiu, and Bacquet Joël. Next Generation Internet of Things: Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation. River Publishers, 2018.

Ziegler, Sébastien. Internet of Things Security and Data Protection. Springer, 2019.

Ziegler, Sebastien, and Pacheco Ana Maria, Evequoz Emilia. "The Impact of the European General Data Protection Regulation (GDPR) on Future Data Business Models: Towards a New Paradigm and Business Opportunities", in Digital Business Models, Palgrave Macmillan, 2019

Deliverables

Van der Wees, Arthur, Dimitra Stefanatou, Jiri Svorc, Marieke van den Ham, Ovidiu Vermesan, Pasquale Annicchino, Sebastien Ziegler, Lucio Scudiero. *D.05.05: Legal IoT Framework*. CREATE-IoT, 2017.
https://european-iot-pilots.eu/wp-content/uploads/2018/02/D05_05_WP05_H2020_CREATE-IoT_Final.pdf

Ziegler, Sébastien, Ana Maria Pacheco, Lucio Scudiero, and Pasquale Annicchino. *Guidelines and Game for Privacy and Personal Data Protection in LSPs*. U4IoT, 2019. https://u4iot.eu/pdf/U4IoT_PrivacY_Guidelines-Part_1_of_D1.3.pdf.

Articles

Chung, Jane, George Demiris, and Hilaire J. Thompson. "Ethical Considerations Regarding the Use of Smart Home Technologies for Older Adults: An Integrative Review." *Annual Review of Nursing Research* 34, no. 1 (2016): 155–81.

Julisch, Klaus. "GDPR-Privacy by Design and by Default." Deloitte Switzerland, January 3, 2018. https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-privacy-by-design-and-by-default.html#.

Mantelero, Alessandro. "Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection." *Computer Law & Security Review* 32(2), (2016): 238–55.

Padyab, Ali, and Anna Ståhlbröst. "Exploring the dimensions of individual privacy concerns in relation to the Internet of Things use situations." *Digital Policy, Regulation and Governance* 20(6), (2018): 528-544.

Tzafestas, Spyros G. "Ethics and Law in the Internet of Things World." *Smart Cities* (34)1, (2018): 98–120.

Ziegeldorf, Jan Henrik, Oscar Garcia Morchon, and Klaus Wehrle. "Privacy in the Internet of Things: Threats and Challenges". *Security and Communication Networks*, 7(12), (2014): 2728-2742.

Privacy-by-design framework for assessing internet of things applications and platforms. In *Proceedings of the 6th International Conference on the Internet of Things* (pp. 83-92). ACM.3. Perera, C., McCormick, C., Bandara, A. K., Price, B. A., & Nuseibeh, B. (2016, November).

Other

Cavoukian, Ann. “Privacy by Design” (2019). https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

“European Large-Scale Pilots Programme.” https://european-iot-pilots.eu/.

Perera, Charith, Ciaran McCormick, Arosha K. Bandara, Blaine A. Price, and Bashar Nuseibeh. “Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms,” 83–92. Stuttgart, Germany, November 2016.

Annexes

Annex I – Overall LSPs and CSAs results

A document on privacy is one amongst several joint activities developed by the LSPs. The Figure 7 on next page briefly lists them:

- Architecture commonalities:
    - LSPs and CSAs have produced recommendations for commonalities on architecture;
    - LSPs and CSAs have contributed to AIOTI work on high-level architecture;
    - LSPs and CSAs have contributed to ISO/IEC 30141 IoT reference architecture 2nd edition. This work will continue during the 2nd wave of LSP;
    - LSPs and CSAs have contributed to ISO/IEC JTC1 AG8 work for a common approach to reference architecture. This work will continue during the 2nd wave of LSP.
- Interoperability commonalities:
    - LSPs and CSAs have produced recommendations for minimum interoperability mechanisms, published by OASC;
    - LSPs and CSAs have contributed to technical reports produced by ITU-T focus group on data processing management;
    - LSPs and CSAs have contributed to two AIOTI white papers on semantic interoperability;
    - LSPs and CSAs have contributed to ISO.IEC 21823-3 IoT semantic interoperability. This work will continue during the 2nd wave of LSP to include more results from SAREF work.
- Use case commonalities:
    - LSPs and CSAs have contributed to the publication of use cases in a repository (www.iot-catalogue.com);
    - LSPs and CSAs from the 2nd wave will contribute new use cases;
    - LSPs and CSAs will contribute to the adoption of a common repository of use cases at standardization level (IEC).
- Privacy commonalities:
    - LSPs and CSAs have contributed to the publication of this Guideline;
    - LSPs and CSAs have contributed to an IoT policy framework;
    - LSPs and CSAs have contributed to technical reports produced by ITU-T focus group on data processing management, with one focusing on privacy (D4.1);
    - LSPs and CSAs have contributed to three ongoing standards: ISO/IEC 27570 Privacy guidelines for smart cities, ISO 31700: Privacy-by-design for consumer goods and services, ISO/IEC 27030: Security and privacy guidelines for IoT. This work will continue during the 2nd wave.

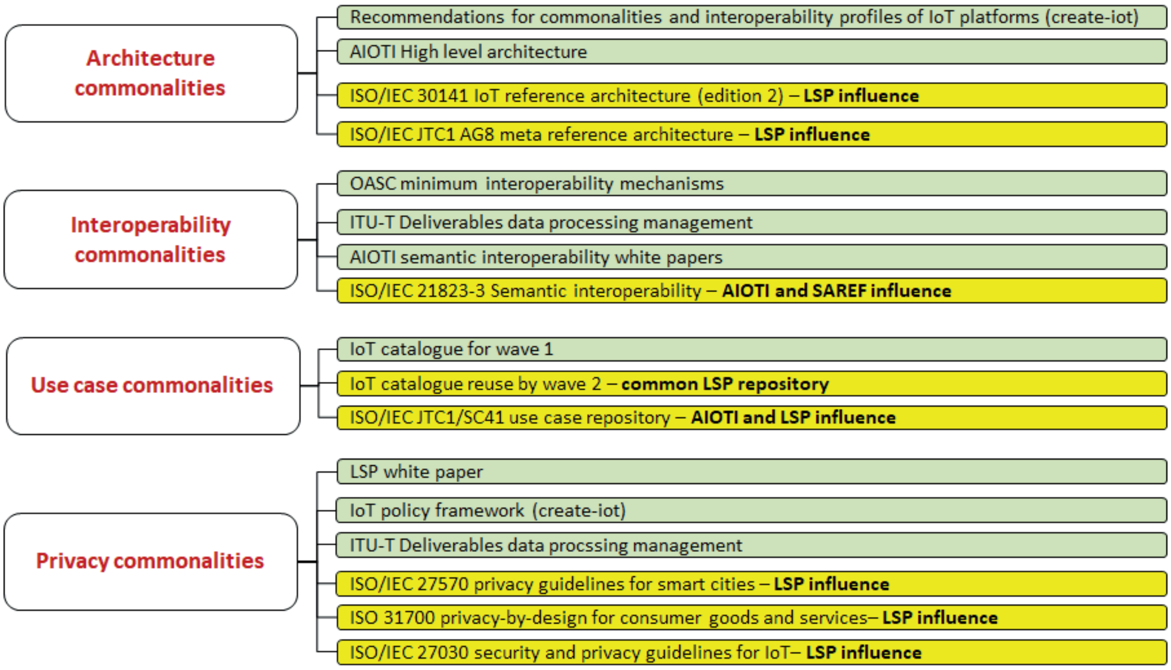

Architecture commonalities
Recommendations for commonalities and interoperability profiles of IoT platforms (create-iot)
AIOTI High level architecture
ISO/IEC 30141 IoT reference architecture (edition 2) – **LSP influence**
ISO/IEC JTC1 AG8 meta reference architecture – **LSP influence**
Interoperability commonalities
OASC minimum interoperability mechanisms
ITU-T Deliverables data processing management
AIOTI semantic interoperability white papers
ISO/IEC 21823-3 Semantic interoperability – **AIOTI and SAREF influence**
Use case commonalities
IoT catalogue for wave 1
IoT catalogue reuse by wave 2 – **common LSP repository**
ISO/IEC JTC1/SC41 use case repository – **AIOTI and LSP influence**
Privacy commonalities
LSP white paper
IoT policy framework (create-iot)
ITU-T Deliverables data procssing management
ISO/IEC 27570 privacy guidelines for smart cities – **LSP influence**
ISO 31700 privacy-by-design for consumer goods and services– **LSP influence**
ISO/IEC 27030 security and privacy guidelines for IoT– **LSP influence**

Figure 7: Large scale pilots common results
(in green results, in yellow, work to be continued).

Annex II – Examples of Data Protection Related Standards

The following table highlights some standard development works that have been directly influenced by the LSPs and CSAs activities.

Category	Reference	Description	Availability
Technical	ITU Y.API4IOT	Open data application programming interface (API) for IoT data in smart cities and communities	Under development
Technical	Y.Sup.Pot_API4 IOT	Features of application programming interface (API) for IoT data in smart cities and communities	Under development
Technical	Y.Sup.AI4IoT	Unlocking Internet of Things with Artificial Intelligence	Under development
Technical and policy	ITU FG-DPM TR D4.1	Framework for security, privacy, risk and governance in data processing and management	Published
Technical and policy	ITU FG-DPM TR D2.1	Data Processing and Management Framework for IoT and Smart Cities and Communities	Published
Technical and policy	ITU FG-DPM TR D0.1	Data Processing and Management for IoT and Smart Cities and Communities: Vocabulary	Published
Principles	ISO 37100	Consumer protection: privacy-by-design for consumer goods and services	Under development
Organization level practice	ISO/IEC 27550	Privacy engineering for system life cycle processes	Published (2019)
Organization level practice	ISO/IEC 27556	User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences	Under development
Ecosystem level practice	ISO/IEC 20547-4	Big data security and privacy	Under development
Ecosystem level practice	ISO/IEC 27030	Security and privacy guidelines for IoT	Under development
Ecosystem level practice	ISO/IEC 27570	Privacy guidelines for smart cities	Under development
Ecosystem level practice	ISO/IEC 23751	Data sharing agreements	Under development
Technical and policy	ETSI 561	Smart cities and communities: standardization to meet citizen and consumer requirements	Under development
Technical and policy	ETSI	Standardization of Sustainable & Efficient ICT	Under development

CREATE-IoT

U4IoT

ACTIVAGE
PROJECT

AUTOPILOT

IOF 2020

MONICA

SYNCHRONICITY

PERSONAL DATA PROTECTION

FOR INTERNET OF THINGS DEPLOYMENTS:

LESSONS LEARNED FROM THE EUROPEAN
LARGE-SCALE PILOTS OF INTERNET OF THINGS

The present report has been published in the context of the Create-IoT project, in collaboration with the five European Large-Scale Pilots on the Internet of Things. It has received funding from the European Union and Switzerland through the Horizon 2020 research and innovation programme under grant agreement No 732929.