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

CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT

H2020 – CREATE-IoT Project

Deliverable 05.06

Legal IoT Framework Evaluation & Final Legal IoT Framework

Revision: 1.00
Due date: 31-12-2019 (m36)
Actual submission date: 27-12-2019
Lead partner: AL

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

Summary					
No and name	**D05.06 Legal IoT Framework Evaluation & Final Legal IoT Framework**				
Status	Released	**Due**	m36	**Date**	31-12-2019
Author(s)	Arthur van der Wees (AL), Dimitra Stefanatou (AL), Prakriti Pathania (AL), Ovidiu Vermesan (SINTEF), Pasquale Annicchino (AS), Catherine Charbonnier (MI)				
Editor	Dimitra Stefanatou (AL), Prakriti Pathania (AL)				
DoW	The evaluation report, the updated Legal IoT Framework (D05.05) and a recommendation report beyond this project.				
Comments					

Document history			
Rev.	**Date**	**Author**	**Description**
0.00	04-12-2019	AL	Template, structure, initial content under Chapters 2 and 3.
0.01	06-11-2019	AL	Integration of insights from the D05.07 on Legal IoT Framework Common Event under Chapters 4, 5 and 6.
0.02	13-12-2019	AS, MI	Integration of insights Chapter 4 and Chapter 6.
0.03	13-12-2019	AL	Revision of executive summary, regulatory landscape and appendices.
0.04	16-12-2019	AL	Consolidated inputs from partners. Further work under Chapter 2 and Chapter 4.
0.05	17-12-2019	AL	Revisions under Chapter 6 and Chapter 7.
0.06	18-12-2019	SINTEF	Input under Chapter 2 and Chapter 5.
0.07	18-12-2019	AL	Revisions under Chapter 2, Chapter 4 and Chapter 7.
0.08	18-12-2019	AL	Document sent for internal review (BLU-SL, ANYSOL).
0.09	24-12-2019	AL	Review comments considered.
1.00	27-12-2019	SINTEF	Report processing and final version released.

Table of contents

1. EXECUTIVE SUMMARY

1.1 Executive Summary

Harnessing the benefits of human-centric technology in an agile and efficient manner for the Digital Single Market has been high on the agenda both, the former European Commission as well of the new Commission (2019-2024). Internet of Things is mentioned explicitly as one the critical technologies of the future, highlighting that the related opportunities should be grasped, considering the relevant safeguards, including those pertinent to ethics and safety. In this context, the present deliverable document provides an overview of the state of play concerning the applicable Legal IoT Framework as on the date of publication of this deliverable, as well as a glimpse of what is intended to be put forward in relation to "Europe fit for the Digital Age".

More, specifically, taking into account both the objectives of "Work Package 05: IoT Policy Framework – Trusted, Safe and Legal Environment for IoT" and the scope of the five Large Scale Pilots (LSPs) currently funded under the EU Large-Scale Pilots Programme, this deliverable builds on D05.05 Legal IoT Framework[1] (D05.05) that was submitted in December 2017. Under D05.05, an overview was provided of the then existing regulatory landscape relating to the creation and use of IoT in the European Union based on overarching themes such as personal data protection, cybersecurity and consumer safety. As a result, D05.05 discussed the most relevant of IoT pre-existing regulations as well as legislations the enactment of which was still in its nascent stages such the Payment Services Directive 2 (PSD2), the General Data Protection Regulation (GDPR), the Network Information Security Directive (NIS Directive). The aim of the present deliverable is to provide an up-to-date discussion of the IoT regulatory landscape and, based on the various interactions that took place with the LSPs, to put forth recommendations that may be taken on board by future LSPs projects and the IoT community of stakeholders.

To this end, the document incorporates insights gathered over the last three years as a result from interactions, directly or indirectly, with the LSPs. It encompasses key points raised in the course of the Common Event with the LSPs on Legal IoT Framework, as well as in the context of the activities of the Activity Group 5 on Security and Privacy and of the activity group on Trust in IoT. Furthermore, the present deliverable takes into account points raised by the LSPs in the context of the Privacy in IoT webinars, as well as key takeaways and recommendations captured under the "Good Practices for Personal Data Protection in Large Scale Deployment of Internet of Things", currently under publication.

[1] CREATE-IoT Project, Deliverable 5.05 Legal IoT Framework (Initial), also available at: https://european-iot-pilots.eu/wp-content/uploads/2018/02/D05_05_WP05_H2020_CREATE-IoT_Final.pdf

2. INTRODUCTION

2.1 Policy context

Harnessing the benefits of human-centric technology in an agile and efficient manner for the Digital Single Market has been high on the agenda of the, now former Commission. With the clear mission, creating "Europe fit for the Digital Age" it remains high on the agenda of the new Commission (2019-2024) as well. On several occasions the new Commission already has acknowledged the profound impact that digital technologies are having on the lives of Europeans[2] and how it has transformed the way individuals communicate, live and work.[3]

As a result, the need for establishing guidelines that cater to the new generation of human-centric technologies has been highlighted. The Commission has also recognised that embracing Europe's technological sovereignty is the need of the hour wherein investments are made in critical technologies of the future. More specifically, the Commissioner for Internal Market, Digital Single Market, Defence and Aerospace has explicitly stated that the Internet of Things and cybersecurity (amongst others) as critical technologies of the future[4]. Furthermore, he highlighted the significance of digital data and the necessity of clear criteria for data sharing in the context of Internet of Things and industry 4.0[5].

Lastly, the creation of the role of the Executive Vice-President for "a Europe fit for the digital age" clearly indicates the intention of the EU to capitalise on the enormous potential of the Digital Age[6]. To this end, the new digital services act will allow for the upgrade of the liability and safety rules on digital platforms, services and products[7], thus, in the wider context, aiming to foster trust within the Digital Single Market.

2.2 Purpose and target group

The advent of IoT has led to a paradigm shift in transforming people's lives and how organisations do business. However, the fact that the IoT creates an interconnected ecosystem also makes such individuals and organizations susceptible to potential risks, including with respect to personal data protection, liability, safety and security. To allow IoT to maximise its full potential while minimizing the risks incurred for individuals, organizations and society at large.

---

[2] Ursula von der Leyen, President-elect of the European Commission, Mission Letter to Thierry Breton, available at: https://ec.europa.eu/commission/sites/beta-political/files/president elect_von_der_leyens_mission_letter_to_thierry_breton.pdf

[3] A Union that strives for more, My agenda for Europe By candidate for President of the European Commission Ursula von der Leyen, available at: https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[4] Commitments made at the hearing of Thierry Breton, Commissioner-designate Internal Market, available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642340/IPOL_BRI(2019)642340_EN.pdf

[5] Ibid.

[6] Hearings of European Commissioners-designate, Margrethe Vestager VP: A Europe fit for the digital age, available at

[7] Ibid.

With respect to IoT, an aspect that often comes under the radar is ownership of data which varies when viewed from the perspective of personal data or of non-personal data. Interestingly, in the context of personal data, the General Data Protection Regulation refrains from making any reference to the ownership of the data but instead introduces the notion of "control" of data. As far as non-personal data is concerned, especially in the IoT ecosystem, ascertaining ownership of the data can be problematic given the multitude of actors involved in designing, manufacturing and deploying the IoT products and services. The discussion on the Trade Secrets Directive that is incorporated under the Appendices touches upon a minor part of the data ownership debate; however, even in such a situation the data in question needs to remain secret and away from accessibility of third parties. In a hyperconnected world, such a requirement can be challenging given that data travels and data can change from legal characteristics and purpose of travelling and being processed at any time.[8] That said, to answer the related questions in pragmatically, the legal discussion relates mostly to the notion of data control rather than to the idea of data ownership

In this respect, the present deliverable sheds light upon the most relevant regulations that need to be taken into account by IoT stakeholders. To this end, the deliverable is structured in a four-fold manner. Firstly, it provides a brief overview of the present-day regulatory landscape focussing predominantly on newly introduced legislations such as the Regulation on free flow of non-personal data and the Cybersecurity Act. Secondly, the deliverable captures the perspectives and insights gathered from the other Large-Scale Pilots in relation to compliance challenges during the course of the project and from the Legal IoT Framework Common Event that took place on 19 July 2019 in Brussels. Thirdly, it touches upon legislations and initiatives that are still in the pipeline and are being discussed at different levels using the evolution of the ePrivacy Regulation first published in January 2017, up until December 2019 as an illustration. Lastly, based on the overall analysis and mapping of the regulatory structure, a sample of recommendations addressed to future LSPs project and the broader IoT community.

This deliverable falls under "Task 05.03: Legal support, accountability and liability", focusing on legal support in relation to data ownership and protection, security, liability, sector-specific legislations and the exchange between IoT LSPs and other IoT initiatives on requirements for legal accompanying measures. The document builds on the regulatory framework that was discussed under D05.05 Legal IoT Framework (Initial), such the General Data Protection Regulation (GDPR) [6] and the Network Information Security Directive (NIS Directive) [7][9]. It also encompasses newly introduced legislation such as the Regulation on the free flow of non-personal data and the EU Cybersecurity Act [11] and also existing legislation that was not discussed in deliverable 5.05 such as the Radio Equipment Directive [35] and the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) [36]. The present deliverable also addresses the related proposed legislation, namely, the draft ePrivacy Regulation [9], while briefly referring to developments related to the review of the Product Liability Directive (PLD) [12]. For the sake of convenience and for reference, legislations that were captured under D05.05 such as the NIS Directive, Trade Secrets Directive, Revised Payment Services Directive have been reproduced under Chapter 9 (Appendices). Furthermore, the deliverable incorporates, to the extent relevant, insights gained in the context of the Common Event with the LSPs on Legal IoT Framework that took place in

[8] Create IoT Project, Deliverable 5.05 Legal IoT Framework (Initial), also available at: https://european-iot-pilots.eu/wp-content/uploads/2018/02/D05_05_WP05_H2020_CREATE-IoT_Final.pdf

[9] Note that the present document provides for a listing of the authors who have actually contributed to the drafting of the present document and, therefore, it does not list the names of the authors who contributed to the abovementioned deliverables that this document built upon.

summer 2019[10] addressing, among other, the relevant compliance challenges and the respective evaluation by the LSPs. Furthermore, the deliverable takes into account key findings and recommendations captured under the *"Good Practices for Personal Data Protection in Large Scale Deployment of Internet of Things".*[11]

Figure 1: Regulatory landscape 2019 & beyond.

There are, however, certain aspects of legal relevance for the IoT environment that fall outside the scope of this deliverable. For instance, the connectivity and interoperability of the IoT environment covered under the Electronic Communications Code discussed within the EU institutions fall outside the scope of Task 05.03 mentioned above. As far as the issue of net neutrality is concerned, there are no significant developments taking place at the moment at EU level;[12] hence, it is not covered under the regulatory overview produced by the discussion below. Similarly, considerations linked to the applicable law and competent jurisdiction are not linked to the aims and objectives of the present document, despite their paramount importance for the IoT environment.

2.3 Contributions of partners

This document is a consequence of the output of interdisciplinary collaboration and is the result of the partners' expertise and respective contributions. In particular, the partners involved have contributed to the present deliverable document as follows:

AL contributed to the publication of the initial Legal IoT Framework in December 2017 in line with the overarching objectives of Work Package 05 aiming at the creation of a Trusted, Safe

[10] The respective report D05.07 on Legal IoT Framework Event presenting the detailed agenda and the discussions held in the aforementioned common event was submitted European Commission Services in October 2019 and it is currently under review.

[11] CREATE-IoT Project, Good Practices for Personal Data Protection in Large Scale Deployment of Internet of Things. Lessons Learned from the European Large-Scale Pilots on Internet of Things, 2020, currently under publication.

[12] Note, however, that at the time of drafting of this document there were developments regarding net neutrality in the United States, as the US Federal Communications Commission upheld its 2017 decision to repeal the regulatory framework that aimed at ensuring a free and open internet.

and Legal Environment for IoT. For the purpose of the present deliverable, Arthur's Legal has contributed to Chapter 3 (Regulatory Landscape) by encapsulating previously existing legislation as well as newer legislations that were enacted after the initial draft was submitted such as the Regulation on the free-flow of non-personal data and the Cybersecurity Act. A brief overview of existing legislation such as the Product Liability Directive and forthcoming regulations like the ePrivacy Regulation have been provided in Chapter 5 of this deliverable. Arthur's Legal has also gleaned insights from Large Scale Pilots has been Based on Deliverable 5.07 Legal IoT Framework Common Event in Chapter 4 and put forth recommendations in Chapter 6 of the deliverable.

SINTEF worked on aligning the activities with the LSPs, the relation to other activities in the project and with the development of the trusted IoT framework that encourage the development of a robust and trusted IoT ecosystem that promotes critical capabilities, including embedded and distributed intelligence, connectivity, interoperability, privacy, security, intelligent analytics and smart data.

MI elaborated on the Trade Secrets Directive (Chapter 8) that became applicable in 2018, which is highly relevant for the industry stakeholders with a role in the IoT ecosystem. It also contributed to chapter 4 and 6.

AS provided the discussion linked to the most relevant requirements set by the GDPR linked to the scope of the LSPs and while reflecting the human-centric approach for the IoT ecosystem as embraced by Work Package 5 (Chapter 4). It also took into account the findings of the "Good Practices for Personal Data Protection in Large Scale Deployment of Internet of Things" elaborated with the LSPs and contributed to chapter 4 and 6.

BluSpecs and AnySolution have reviewed the draft of the final report to enhance its usefulness for future deployers of large scale IoT ecosystems.

2.4 Relations to other activities in the project

The topics addressed by this deliverable covers the legal support, accountability and liability activities that are relevant for the main tasks falling under the scope of the CREATE-IoT project. IoT devices collect information in different contexts and applications by involving various stakeholders and IoT platforms. Depending on the criticality of the applications (safety-critical, mission-critical, etc.), accountability, liability and legal framework are all part of the critical core issues to be addressed by the IoT ecosystems.

IoT ecosystems are heterogeneous and the actions and decisions within a specific ecosystem have far-reaching consequences. The analysis of the legal, accountability and liability provided under "WP05 – IoT Policy Framework – Trusted, Safe and Legal Environment for IoT" requires a holistic approach relevant for all LSPs, that incorporates numerous relevant perspectives, including technological, economic, consumer, customer and trade specificity.

Elements presented in this deliverable contribute to the other "WP05 – IoT Policy Framework – Trusted, Safe and Legal Environment for IoT" deliverables, and specific topics have been identified of particular importance for "WP04 – European IoT Value Chain Integration Framework" and "WP06 – IoT Interoperability and Standardisation".

Topics addressed in this deliverable are connected to the development work on the IoT Policy Framework described in "D05.01 – IoT Policy Framework" and the work on the data model described in "D05.03 – IoT Data Value Chain Model".

Recommendations related to the role of the technical and organisational aspects in the context of IoT European Large-Scale Pilots Programme provide a useful information platform to the LSPs projects to address the specific issues in their own sectorial segments and across the sectors. The

issues related to accountability, liability and legal framework affect the economic aspect of the collection and use of data in IoT and require to rethink the IoT business models linked to data use and management as well as the potential market impact of security and privacy risks associated with data economy.

The legal IoT framework is addressing the changing market dynamics, by analysing the instruments and legislations put forward, such as the General Data Protection Regulation (GDPR), the Free Flow of Non-Personal Data Regulation, as well as by updating sector-specific regulations etc., to foster the future data economy that provides equal opportunities for the market players.

The document gives an overview of the latest developments related to legislation/regulations and refers to ethics principles, rules and codes, standards/guidelines, contractual arrangements, regulations for connected devices, the networks, their security, and the data associated with the IoT devices in the context of digital economy.

This work provides the basis for an analysis of the current gaps and the necessary recommendations for legal, accountability and liability issues across IoT application domains covered by the LSPs and contributes to the development of a suitable emergence of best practices.

3. REGULATORY LANDSCAPE: STATUS

Organizations create, collect, process, derive, archive and – ideally and to the extent permitted – delete large amounts of data through IoT products, systems and services. As part of this lifecycle[13], digital data is also transmitted, exchanged and processed in different ways at a global scale. In this environment of constant change, concepts like data protection, cybersecurity and consumer safety take centre stage. This chapter highlights the most relevant legislation currently in place that regulates the IoT ecosystem, directly or indirectly, in the EU.

3.1 General Data Protection Regulation[14]

As IoT becomes more widespread, consumers and authorities demand regulatory frameworks that guarantee the protection of personal data. Protection of personal data does not only constitute a relevant issue for individuals acting in their capacity as consumers, but also for the European Single Market at large. As previously mentioned, personal data protection has been identified as one of the main obstacles for the implementation of the Digital Single Market. From this standpoint, compliance with the requirements of the GDPR[15] becomes even more important for the consortia and the afterlife of the LSPs.

It should be noted that the GDPR is not the only instrument providing for the right of personal data protection at EU level; this right is in fact enshrined in the Charter of Fundamental Rights of the EU, as well as under the Treaty of the Functioning of the EU. The discussion below takes these rights and focuses on those aspects that are considered to be of direct relevance for the LSPs in the context of the human-centric approach[16] previously promulgated.

3.1.1 Informed consent requirements

One of the major themes in GDPR compliance strategies centres on consent. Under the Data Protection Directive[17], consent was one of the grounds for lawfully processing personal data. This legal ground could be problematic when, for instance, people do not have a genuine choice as it whether to withhold it.

GDPR retains the concept of consent as a processing condition but also adds new conditions. Under the GDPR "consent" of the data subject means any "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".[18] The GDPR is more prescriptive as compared to the Directive and recital 171 of the GDPR explicitly clarifies that: "Where processing is based on consent pursuant to Directive 95/46/EC,

[13] For more information on the distinctive phases of the Personal Data Lifecycle, see, also, Deliverable 05.03 IoT Data Value Chain Model, available at: https://european-iot-pilots.eu/wp-content/uploads/2017/10/D05_03_WP05_H2020_CREATE-IoT_Final.pdf

[14] See also, Create IoT Project, Deliverable 5.05 Legal IoT Framework (Initial), also available at: https://european-iot-pilots.eu/wp-content/uploads/2018/02/D05_05_WP05_H2020_CREATE-IoT_Final.pdf

[15] D1.4 on "Privacy by design methodology & PIA" produced under SYNCHRONICITY Large Scale Pilot, expands on other requirements set forth by the GDPR. The deliverable document is available at: http://synchronicity-iot.eu/wp-content/uploads/2017/03/SynchroniCity-D1.4-M5-final.pdf

[16] Deliverable D05.01 on "IoT Policy Framework", online at: https://european-iot-pilots.eu/create-iot/deliverables/

[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[18] Article 4 (11) of GDPR.

it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation".[19] The GDPR, therefore, makes explicit the characteristic of the consent. It should be:

a) *Unambiguous* as the GDPR explicitly requires that consent should be given either through a statement or a clear affirmative action;
b) *Freely given.* This was the same under the Directive, but the GDPR clarifies that consent will not be considered freely given if: 1) the data subject has no genuine and free choice or is unable to refuse or withdraw consent without detriment;[20] 2) there is a clear imbalance between the data subject and the controller.[21] Recital 43 also clarifies that consent is presumed not to be freely given if separate consent is not allowed for different data processing operations when such separate consent would be appropriate. Article 7 (4) provides additional circumstances to take into account when evaluating consent;[22]
c) Consent must be *specific* and must, therefore, relate to specific processing operations. According to recital 32: "*Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them*".
d) Consent should be informed. According to recital 42: "*For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended*"
e) Data subjects have the right to withdraw their consent at any time and must be informed of their withdrawal right at the time of consenting.[23]

The collection of consent also has to respond to specific formal requirements. In principle, consent may be either in writing or in oral form, provided that it can be proved by the data controller, according to article 7 (1).

Consent and the entire set of associated requirements constitute, in essence, a reflection of the concept of transparency which has been, overall, significantly strengthened under the GDPR compared to how it has been embraced within the current regime defined under the Data Protection Directive. The links the concepts of consent and transparency are elaborate in detail by Article 29 Working Party that issued set of Guidelines [14] in November 2017.

3.1.2 Accountability measures: technical & organizational

The GDPR also introduces legal accountability obligations. The principle of accountability in data protection law was already codified in 1980 in the OECD Guidelines.[24] Now the principle of accountability pervades all of the primary obligations of controllers under the GDPR. Article 5(2) of the GDPR requires organisations to demonstrate compliance with the principles of the GDPR.

Article 24 of the GDPR codifies the accountability obligation by requiring the controller to "*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures*

[19] Recital 171 of GDPR.
[20] Recital 42 of GDPR.
[21] Recital 43 of GDPR.
[22] According to Article 7 (4) of GDPR: "When assessing consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of the contract".
[23] Article 7 (3) of GDPR.
[24] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), also available at: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

shall be reviewed and updated where necessary".[25] The measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. For controllers it is important to document and be able to demonstrate to authorities the proportionality of measures taken. Article 24 (3) refers to particular methods to show fulfilment of the requirements such as: "Adherence *to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller*". In general, one can argue that technical and organizational measures should follow a "risk-based" approach: the more likely and severe the risks of the processing, the more measures will be required to counteract those risks. Recital 75 provides some examples and recital 76 also distinguish between "risk" and "high risk".

The GDPR also introduces the principle of data protection by design and by default; therefore privacy protections are to be embedded in the design of business operations, processes and services. Controllers also should apply the strictest privacy settings, for example, to a product or service. Other measures worth mentioning are the need, in appropriate circumstances, of "*privacy impact assessments*" which are required if the processing is likely to result in a high risk to an individual's rights. It may also require pre-consultation with the relevant supervisory authority. It is also worth mentioning the provisions on the requirement to appoint a data protection officer under certain circumstances.

On 13 November 2019, the European Data Protection Board adopted Guidelines on Article 25: Data Protection by Design and by Default that give data controllers guidance to understand and implement the said article. The guidelines also help related actors such as data processors and technology providers create GDPR-compliant products and services that further enable data controllers to adhere to their data protection obligations. The possibility to create a certification mechanism to prove compliance with Article 25 has also been discussed in the guidelines.

3.1.3 Processing of special categories of data

In certain cases, the GDPR requires consent to be "explicit". This is, for instance, the case of sensitive data[26], profiling activities[27] or cross border data transfer[28]. Working Party 29 in a 2011 Opinion (15/2011) attempted to define "explicit consent": "in legal terms "explicit consent" is understood as having the same meaning as express consent. It encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing. Usually, explicit or express consent is given in writing with a hand-written signature. For example, explicit consent will be given when data subjects sign a consent form that clearly outlines why a data controller wishes to collect and further process personal data. Article 9 (2) sets out the circumstances in which the processing of sensitive personal data may take place. Categories of data considered to be sensitive according to Article 9 (1) are: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; data concerning health or sex life and sexual orientation; genetic data; biometric data where processed to uniquely identify a person.

The lawful bases for processing special categories of data are set out in Article 9 (2). This is, for instance, the case of health data, which is very sensitive in nature, and of particular interest for the use of big data analytics. In the case of health data, it is also worth pointing out that Article 9 (2) provides for exceptions to restrictions including where processing is necessary for various medical assessment and where the processing is required for reasons of public interest in public

[25] Article 24 of GDPR.
[26] Article 9 (2) (a) of GDPR.
[27] Article 22 (2) (c) of GDPR.
[28] Article 49 (1) (a) of GDPR.

health. Article 9 (4) of the GDPR allows Member States to maintain or impose further conditions (including limitations) to this respect.

3.2 Free Flow of Data Regulation

The European Commission's Regulation on a framework for the free flow of non-personal data (Regulation) in the EU, published in September 2017, aims, primarily, to ensure the free movement of non-personal data and to prohibit national governments from creating unjustified data localization requirements. Additionally, the European Commission believes that to fully realise the benefits and potential of the data economy, it is essential to enable public and private organisations to store and process non-personal data wherever they require to do so in the EU. To this end, the Regulation, which became applicable from 28th May 2019, ensures the availability of data to competent authorities of another Member State and puts forward the development of codes of conduct to facilitate data portability. The proposal aims ultimately at "creating legal certainty and at raising trust for cross border data storing and processing within EU" and at creating "at creating a competitive EU single market for secure, reliable and affordable cloud services" [30].

In particular, the Regulation enshrines the principle of the free movement of non-personal data into EU law with clear obligations on national governments not to restrict the location, storage or processing of non-personal data in any specific territory, unless justified on grounds of public security. EU Member States must repeal all data localisation requirements in any law, regulation or administrative provision of a general nature which are not justified by public security reasons by 30 May 2021. Any existing data localisation requirement justified on public security grounds in compliance with the principle of proportionality must be notified to the European Commission, pursuant to which the Commission will establish whether the provision is appropriate and where necessary, recommend an amendment or repeal of the provision.

Interestingly, industry is encouraged to draft self-regulatory codes of conduct providing guidelines to facilitate switching of providers and to ensure that professional users are provided with "sufficiently detailed, clear and transparent information", before a contract for data storage and processing is concluded. The regulation further requires the Commission to encourage the relevant service providers to complete the draft codes of conduct and to ensure that the said codes are implemented by 29 May 2020.

In May 2019, the Commission published a guidance to elaborate on the interaction between the GDPR and the Regulation especially concerning datasets that consist of both personal and non-personal data. The guidance is highly relevant for private businesses, especially small and medium enterprises, and other organisations that process data as a part of their business activities. [29]

3.3 Cybersecurity Act

Recognising security challenges brought about by recent IoT developments, NIS Directive was clearly the first step with a view to promoting a culture of risk management. While it merely aimed at building resilience and improving cooperation between Member States as well as introducing security requirements as legal obligations for the key economic actors it has become clear that a similar systematic approach will be necessary also from other stakeholders. This is especially with the view of an increasing number of connected devices expanding the potential cybersecurity compromise surface area. Hence, a need was felt for strong cyber resilience

[29] Note: The Guidance published by the European Commission will be further elaborated upon under D05.04 IoT Data Value Chain Model Evaluation & Final IoT Data Value Chain Model.

comprising a collective and wide-ranging approach [31]. To address this, the EC has published a Proposal for Cybersecurity Act, namely proposing objectives, tasks and organisational aspects of the European Union Agency for Network and Information Security (ENISA) and laying down a framework for the establishment of European cybersecurity certification schemes. The Act was later approved by the European Parliament in March 2019 and came into force on 27th June 2019.

As ENISA has a key role to play in strengthening EU cyber resilience and response, the EC has proposed to grant the agency a permanent mandate to facilitate a more efficient provision of support to Member states, EU institutions and businesses in key areas, including the implementation of NIS Directive. The newly passed Act puts forward an ambitious revised set of ENISA's objectives[30] including a strengthened advisory role on policy development and implementation, guaranteeing the sharing of best practices, contributing to EU-level situational awareness, as well as providing support to Member States that includes advice or technical assistance or ensuring analyses of threats and incidents. As a result, the EC has given the agency more teeth and tasked it with more responsibilities, making *the EU Cybersecurity Agency* in a relatively broad sense.

Under the Cybersecurity Act ENISA is tasked with the preparation of a candidate European cybersecurity certification scheme or to review an already existing one [32][31]. The EC has acknowledged that cybersecurity certification plays an essential role in increasing trust and security. However, at the same time, it has also argued that the growth of the EU cybersecurity market is held back by a lack of cybersecurity schemes to build higher standards into products with confidence. To address this deficiency, the EC has set up a voluntary EU cybersecurity certification framework which would lay down the procedure for the creation of EU-wide cybersecurity certification schemes, covering ICT products, services, and/or systems, which adapt the level of assurance to the use involved. The purpose of European cybersecurity certification schemes is to ensure a harmonised approach at the EU level with respect to cybersecurity certification schemes and to create a digital single market for ICT products and services. Moreover, a European cybersecurity certification framework will ensure that the ICT products, services and processes have been evaluated following specific security requirements. Such requirements concern the ability to resist, at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions of or services offered by, or accessible via those products, processes, services and systems within the meaning of the regulation.[32] To achieve this, the Regulation contains a list of specific proposed elements.[33] It is expected that complying with this provision would not only increase the level of cyber security in Member States, but would also significantly help in building customers' confidence.

3.4 Revised Payment Services Directive

3.4.1 Strong customer authentication

The rising number of internet and mobile payment transactions carried out through or using IoT devices has created new risks for customers. This is even more so due to an increased number of parties involved in the payment chain which PSD2 encourages aside from the customer, merchant and the banking institution (ASPSP), the chain now also involves third-party providers (TPPs), namely payment initiation service providers (PISPs) and account information services

[30] See Article 4 of the Cybersecurity Act.

[31] See also Ibid, Article 48 (1) of the Proposal for Cybersecurity Act.
[32] Recital 75 of the Proposal for Cybersecurity Act.
[33] Article 47 of the Proposal for Cybersecurity Act.

providers (AISPs). This new setting and the respective legal framework are ultimately expected to benefit customers. At the same time, however, the inclusion of TPPs in the payment chain and utilisation of connected IoT devices in innovative solutions introduced not only by the TPPs but also ASPSPs, has brought about numerous security challenges, including customer authentication as one of the key ones. This Section outlines the way law makers have addressed these challenges in the Directive, as they are considered very relevant with respect to IoT devices.

PSD2 recognises that the personalised security credentials used for secure customer authentication by the customer or by the PISP are usually issued by the ASPSPs.[34] As PISPs do not necessarily enter into contractual relationships with the ASPSPs, PSD2 stipulates that PISPs should be able to rely on authentication procedures provided by the ASPSPs.[35] The Directive further grants a mandate to the European Banking Authority (EBA) to draft regulatory technical standards (RTS), including standards concerning strong consumer authentication.[36]

Before discussing the RTS in some more detail, let us first consider some general authentication principles stipulated by the PSD2. The Directive requires member states to ensure that when a customer (1) accesses its payment account online, (2) initiates an electronic payment transaction, or (3) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses, strong customer authentication should apply.[37]

It defines *strong consumer authentication* as authentication based on two or more of the following elements:

i. *knowledge*, i.e. something only the customer knows (e.g. a PIN, or similar);
ii. *possession*, i.e. something only the customer has (e.g. payment card in a face-to-face context, or a smart device for a remote payment, or similar);
iii. *inherence*, i.e. something only the customer is (e.g. a fingerprint, or similar). [38]

In addition, in the case of "remote" payments, PSD2 requires strong customer authentication to include elements which dynamically link the transaction to a specific amount and a specific payee.[39]

As already indicated, PSD2 stipulates that RTS should be developed with the objective of (a) ensuring an appropriate level of security for payment service users and payment service providers, through the adoption of effective and risk-based requirements, (b) ensuring the safety of payment service users' funds and personal data, (c) securing and maintaining fair competition among all payment service providers, (d) ensuring technology and business-model neutrality, and (e) allowing for the development of user-friendly, accessible and innovative means of payment.[40] It is clear that the stated objectives set a relatively demanding threshold to be met, whereby some objectives directly compete with others. For example, the requirement of ensuring security may in some cases be directly competing with the requirement of user-friendliness. Hence, when drafting the RTS, EBA has had to carefully consider and balance the objectives [25]. Its final version was adopted by the European Commission on 27 November 2017 [26]. The RTS consists of a set of detailed provisions concerning security measures for the application of strong customer authentication.[41] These are relevant in respect of the generation of authentication

[34] Recital 30 of PSD2.
[35] Ibid.
[36] PSD2 Recitals 107 and 108, PSD2 Article 98, in consideration of Article 16 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC.
[37] Article 97 (1) of PSD2.
[38] Article 4 of PSD2.
[39] Article 97 (2) of PSD2.
[40] Article 98 (2) of PSD2.
[41] Chapter 2 of PSD2 RTS.

codes,[42] dynamic linking[43] and the requirements of the elements categorised as knowledge, possession and inherence,[44] and their independence.[45] However, at the same time, the RTS contains numerous exemptions from strong customer authentication, as per specific occurrence (use case). Amongst others, the RTS includes exemptions[46] in respect of contactless payments at the point of sale, transport and parking fares, trusted beneficiaries and recurring transactions, payments to self, and low-value transaction. If a payment service provider meets the criteria of respective provisions, they will be exempt from the strong customer authentication requirements.

An increasing number of IoT devices facilitate remote payments. Manufacturers of devices with such potential must be aware of strong authentication requirements outlined in the RTS and consider including endpoints and sensors facilitating appropriate authentication. In the beginning, manufacturers were given time until September 2019 to implement measures to ensure compliance of their devices with RTS. On 21 June 2019, the EBA gave some leeway to NCAs by allowing them to provide PSPs with "limited additional time" to implement the SCA. However, despite the EBA's announcement for a unified timeline, Member States went ahead and gave extensions ranging from 12 months to 18 months and longer. To avoid discrepancies due to different adjustment periods, on 16 October 2019, the EBA published an additional Opinion granting NCA's time till 31 December 2020 to fully comply with the SCA.[47]

In this respect it is also worth noting that although PSD2 lays down numerous specific provisions in respect of the various stakeholders concerned, it remains fairly shallow on the enforcement of these provisions. Namely, as it does not determine a specific authority in charge of enforcing the respective provisions, Member States will be able to choose an appropriate authority "to ensure effective enforcement of the provisions of national law".[48] If the respective national laws are enforced by various different authorities across Member States, a risk of fragmentation and varying interpretation of the provisions is inevitable. The EC should, therefore, play an exceptionally active role in overseeing the implementation of PSD2 and enforcement of national provisions.

3.5 Radio Equipment Directive

The Radio Equipment Directive (RED)[49] provides a regulatory framework to establish parameters that have to be met when placing radio equipment on the market and putting them into service within the European Union. Harmonized standards that include diverse aspects such as health, safety and use of radio spectrum are established under the Directive. Article 2(1) defines radio equipment as: "*electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination*." Furthermore, electromagnetic disturbance has been defined as *"any electromagnetic phenomenon which may degrade the performance of equipment; an electromagnetic disturbance may be electromagnetic noise, an unwanted signal or a change in*

[42] Article 4 of PSD2 RTS.
[43] Article 5 of PSD2 RTS.
[44] Article 6-8 of PSD2 RTS.
[45] Article 9 of PSD2 RTS.
[46] Articles 11-15 of PSD2 RTS.
[47] Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card-based payment transactions, also available at https://eba.europa.eu/file/117252/download?token=fU0jW0Dn
[48] Recital 99 of PSD2.
[49] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC

the propagation medium itself" More importantly, the Directive lays down an exhaustive list of essential requirements that have to be ensured during the designing and manufacturing phase. This includes the construction of radio equipment that supports certain features to:

- Protect personal data and privacy;
- Prevent fraud;
- Facilitate access to emergency services;
- Enable its use by users with disabilities.

Obligations of manufacturers of radio equipment are laid down in the Directive to ensure that the radio equipment is designed to meet the above-mentioned essential requirements. Distributors and importers of radio equipment, on the other hand, are required to refrain from putting products on the market which they believe do not conform to the prescribed essential requirements until the products under question are brought into conformity. Additionally, manufacturers are also required to perform conformity assessment of the radio equipment to ensure that the radio equipment meet all the requirements laid down in the directive before it is placed on the market.[50]

In August 2019, a public consultation was launched by the European Commission to obtain feedback from relevant stakeholders on the relevance of the Directive on aspects relating to 1) protection from fraud 2) protection of personal data and privacy. The consultation targeted a wide audience including manufacturers and industry associations, academics, certification bodies as well as civil society representatives and citizens.

3.6 eIDAS Regulation

The implementation of the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) was a significant step taken by the EU to build trust in the online environment. The Regulation, adopted on 24 July 2014, provides a harmonized framework to enable people and businesses of a member state to use their national electronic identification schemes (eIDs) to gain access to public services of other member states where eIDs is available. Moreover, the Regulation created an internal market for electronic Trust Services (eTS) i.e. electronic signatures, time stamps, website authentication, electronic seals etc., thereby giving them the same legal status to processes that may be paper-based.

Electronic identification offers several benefits to businesses by allowing them to verify the identity of their customers and other businesses to establish contractual relationships in an agile and seamless manner. Additionally, it enables businesses to increase their clientele by providing secure authentication methods in different EU member states. However, the implementation of eID systems for cross-border transactions between member states requires a notification step wherein a national eID system is reviewed and added to the network of eID schemes that have been recognized by other member states. Doing so ensures that eID schemes that are recognized meet the necessary security and quality requirements that are prescribed under the Regulation. This status can be revoked or suspended if the event that the scheme is breached or compromised to the extent that the reliability of the cross-border authentication of the scheme under question is impacted.

The Regulation defines "trust services" as "an electronic service typically provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates

[50] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC OJ L 153/62, art 17

for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services. Furthermore, the Regulation provides for "qualified trust service provider" where the trust service provider can establish that the services provided by them meet all the requirements stated in the Regulation. A list of the said qualified trust service providers would be made available on the European Commission's Trusted List Browser which will also be regularly audited and updated.

In September 2019, it has been pre-announced that, in line with the Better Regulation guidelines, the eIDAS Regulation will go under an evaluation process to assess its effectiveness, efficiency, relevance, coherence and EU added value. The evaluation process will include, among other, a public consultation during the first quarter of 2020, as well as a targeted stakeholder's consultation. The respective reporting to the European Parliament and to the Council is scheduled by 1 July 2020[51].

[51] See, also, eIDAS Regulation Update available at: https://www.enisa.europa.eu/events/tsforum-caday-2019/presentations/00-01-gjoen

4. INSIGHTS GAINED FROM THE LARGE-SCALE PILOTS

WP5 of CREATE-IoT project interacted in several ways with the LSPs project funded under the specific EU-IoT LSPs Programme including a series of webinars on Privacy in IoT, through the earlier stated Activity Group 5 on Security and Privacy, as well as through the series of the "Common Events with the LSPs" provided under WP5. In this context, all WP5 deliverables due in month 36 of CREATE-IoT project are largely based on the integration of insights resulting from interaction with LSPs throughout the project duration. More specifically, this chapter, focuses on the insights gained from the LSPs in the context of the D05.07 on Legal IoT Framework Event that took place in July 2019[52]. The chapter discusses the respective insights both per application domain, as well as per LSP project.

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

4.1.1 MONICA

The MONICA project collected and processed different types of personal data using various technologies such as wearables, CCTV and sound level meters. One of the important challenges for MONICA concerned the issue of “dynamic consent” or empowering the data subject to express, revoke consent in a cycle of information. To this extent, specific measures were taken to guarantee the respect of the consent of the end-user. Another concern was transparency and the transfer of information to be provided to the public. In fact, noise management and public events in wide-open spaces, also require taking safety and the customer experience into consideration. The project also had to deal with surveillance issues. MONICA considered that legal compliance in relation to the collection and processing of personal data could not be assumed to equate to compliance with ethical standards and principles. Before the testing and demonstration activities, MONICA has carried out an ethical analysis of the different surveillance and monitoring technologies to be implemented in the project.

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

4.1.2 ACTIVAGE

Due to the multidisciplinary nature of the ACTIVAGE consortium, concrete universal principles and policies of data management and also a data management strategy were initiated to cope

[52] Note that the respective workshop report D05.07 on Legal IoT Framework Event presenting the detailed agenda and the discussions held was submitted European Commission Services in October 2019 and it is currently under review.

with the diverse use cases and the broad group of stakeholders (older adults, caregivers, health and social care, professionals) involved. In particular, the governance and management of big and sensitive data (health data) brought several a. challenges b. obligations and c. requirements in alignment also to the new regulation (GDPR).

Among the main challenges were to:

- Identify, collect and group similar data among different deployment sites.
- Efficiently coordinate the effort of different Deployment Sites in alignment to GDPR requirements.
- Regulate the activities of different entities/persons involved in data collection and processing activities.

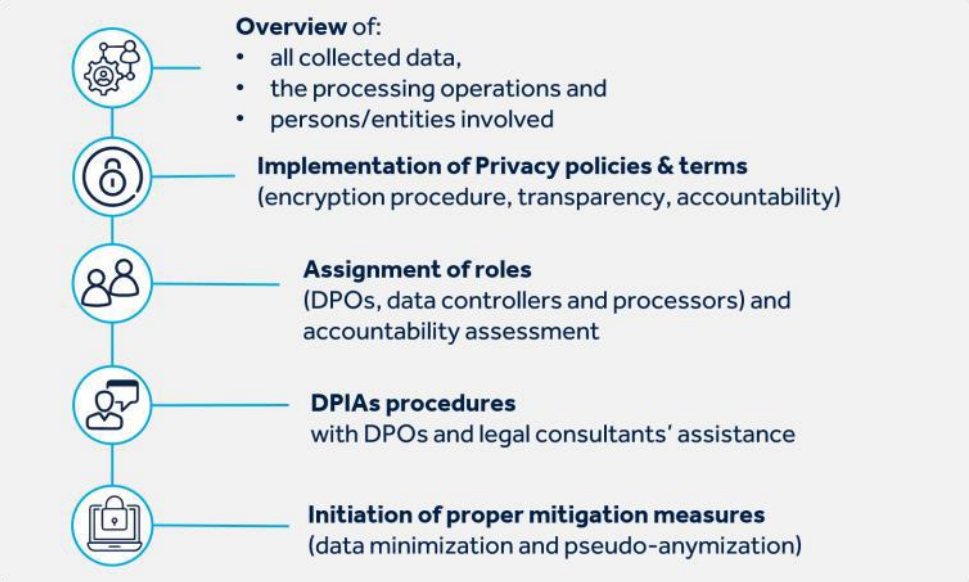

Figure 2: Technical and organizational aspects of personal data protection within the ACTIVAGE ecosystem

The ACTIVAGE consortium initiated a Security and Privacy framework based on three main principles, privacy, trust and security that have been, also been identified as key pillars of the IoT Policy Framework introduced by CREATE-IoT[53]. Aligned with these principles, proper methods and measures were applied to address the potential risk of using different kind of data (personal; health; behavioural and mobility) towards a user-centric IoT enabled system.

From the beginning of the project and in the context of the pilots' operations, each deployment site, as well as the consortium as a whole, defined a clear data management strategy where data protection and privacy issues were integrated. In particular, the protection of fundamental human rights, including, this of personal data protection were among the consortium's most significant concerns and an integral part of the whole management of the project. Nonetheless, as ACTIVAGE pilots were active before the GDPR implementation, as it came into force in May 2018, the consortium had to interpret the new requirements according to the use cases, needs and architecture, to initiate a trustworthy, reliable and widely acceptable IoT environment for end-users (elderly and caregivers). To this end, several policies, measures and activities were defined and followed with consistency to achieve GDPR compliance.

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

[53] See, also, Deliverable 05.01 IoT Policy Framework, available at: https://european-iot-pilots.eu/wp-content/uploads/2017/10/D05_01_WP05_H2020_CREATE-IoT_Final.pdf

processes. 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.

Figure 3: Common objectives and ethics requirements within the context of ACTIVAGE

4.1.3 Compliance challenges and lessons learnt in the application domain of personal wearables[54]

The table provides an overview of the key compliance challenges, to an extent discussed above, that were encountered in projects using various wearable devices in the health domain and public space.

Table 1: Data protection challenges & lessons learned in the domain of personal wearables

LSP / Domain	Challenge	Lessons Learned
MONICA / Public Space	Manage the diversity of the partnerships	Invest time to manage the combination of many cultural backgrounds
	Control several data streams that flow across several partners	Dedicate time and resources, define accountability as soon as possible
	Address governance issues: confusion of role between project Data Protection Officer and national project DPOs, suppliers versus operators.	Provide clear roles and responsibilities as early as possible
	Address operational issues: difficult to get 100% of all wearable devices back after the event.	The App must be part of the event App but this requires the event organisers' agreement.
ACTIVAGE / Health	Make sure to safeguard human rights while using large scale databases with personal sensitive health data generated from different sources	Take into account the various national data protection laws
	Accountability challenges	Implement "Privacy by Design"
	Manage user consent	Use blockchain to request/give/update permissions for accessing personal

[54] This section is largely based on material made available by the LSPs for the purpose of the above mentioned paper on Good Practices for Personal Data Protection in Large Scale Deployment of Internet of Things. Lessons Learned from the European Large-Scale Pilots on Internet of Things, 2020 (currently, under publication).

		data of the user
	Manage ethical concerns	Setup "Ethical boards" to provide ethical guidance for the project
	Address Governance issues	Need a common DPO at project-level and an interdisciplinary research team to understand law, sociology and ethics.

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

4.2.1 AUTOPILOT

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

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

The automated/autonomous vehicle and IoT policy framework offers a starting point for understanding policy's impact on autonomous vehicles applications integrated with IoT services and is intended to guide the stakeholders involved in such complex ecosystems in developing, implementing, and maintaining a coherent policy that addresses trust, security, privacy and engagement elements. In the case of automated/autonomous vehicles, user tracking may represent a common threat since the IoT platforms process the location of the cars which in turn may be later accessed by unauthorized parties to identify the location of a person. In this context, the rule of law including the legal, regulations and liability issues are of paramount importance for automated/autonomous vehicles and IoT applications that form the basis for future Internet of Vehicles (IoV) applications.

The introduction of complex autonomous vehicles, IoT and AI systems adds a new layer of complexity to attributing liability for vehicle accidents. In this context, specific legislation should define how liability is apportioned when vehicles are sold as, and drivers/owners/users expect them to be, fully autonomous. Additionally, attributing liability, fault and responsibility for insurance has to be clarified among the stakeholders involved in sophisticated autonomous vehicles, IoT and AI applications. This is because establishing the responsible stakeholder (e.g. vehicle manufacturer, manufacturer of software, network providers, service providers, owners, users, etc.) in complex autonomous vehicles, IoT and AI applications can be a difficult to establish for incidents caused by defects in the software interface between two vehicles or between a vehicle and the road, cyber-attacks on vehicles, glitches in connectivity causing the incidents, etc.

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

AUTOPILOT has used the KPMG autonomous vehicles readiness index results and the ranking of different countries around the world for 2018 and 2019 [33][34] that is based on four different

criteria: policy and legislation, technology and innovation, infrastructure and consumer acceptance to identify the gaps among the different countries in Europe.

Figure 4: Presentation of AUTOPILOT

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

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

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

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

4.2.2 IoF2020

IoF2020 focuses on the application domain of smart farming and it is the LSP project that provides for the most significant number of uses cases. Generally, the use cases of IoF2020 do not deal with personal data but in some cases, they might play a role especially when the combination of different datasets with other information or datasets could lead to the identification of the farmer.

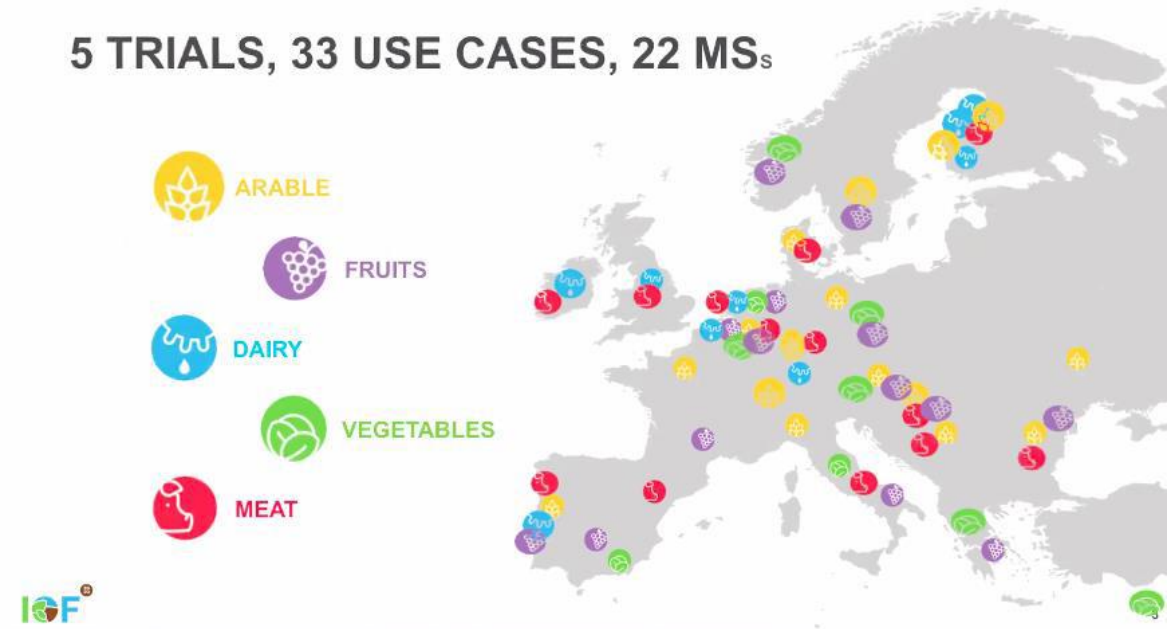

Figure 5: Overview of use cases under IoF2020

Some of the use cases faced issues related to law and regulation, however all of them managed to find solutions to overcome them. None of the use cases so far reported on barriers or serious problems related to law and regulation.

The project has worked on a specific WP dedicated to ethics. At the project level IoF2020 strongly recommends the uses cases to have good and explicit agreements on data exchange and IPR issues. In fact, the project has collected different templates and agreements which can be helpful in the use cases for the development of their technology. For this the use cases were advised to make a consortium agreement between the partners in the use case. For this, the use of the DESCA template was suggested.

The project has recognized the sensitive nature of personal and non-personal data for farmers and therefore it has tried to clarify issues since the beginning of the implementation, and it tried to build trust through the work of an ethical team.

In the meantime, the main representing organizations in agri-food (e.g. Copa-Cogeca, CEMA, IFOAM etc.) launched a code of conduct (CoC) for data exchange in agriculture. It is a set of principles to make transparent agreements on data exchange which has an important impact in the sector. Of course, when work is done in innovation context there is always an issue of "incomplete contracts" and therefore new and unforeseen issues may arise but at the project level there have been no major concerns. For instance, one issue that had to be addressed concerned the tracking of boxes that would imply automatically also the tracking of drivers carrying the boxes.

An ethical issue addressed concerned the ownership of data collected by robots that farmer was claiming. In this case it is necessary to compensate for the investment made to create the technological infrastructure to create the dataset. Finally, the project also developed a diagnostic tool that all the use-cases have to use to evaluate security.

In the annual partner event last March this CoC was promoted among the use cases, in particular the new use cases, to use this for their agreement. Because IoF2020 is a B2B project there are (so far) no privacy-related issues. Overall the project has been working to guarantee the sustainability of the use-cases after the end of the research project.

4.2.3 Compliance challenges in the application domain of moving sensors / actuators[55]

The table provides an overview of the key compliance challenges, to an extent discussed above, that were encountered in projects using various moving sensors / actuators devices.

Table 2: Overview of compliance challenges in the domain of moving sensors/actuators

LSP / Domain	Compliance Challenges
AUTOPILOT / Mobility	• Various levels of Autonomous Vehicles (AV) readiness across countries and by pillars (legislation, technology, consumer acceptance) • Cybersecurity: data vulnerabilities and multiple legislations across countries, IoT data vs human data, colossal data volume (volume of data of one automated vehicle corresponds to the amount of data generated by 2'666 human internet users) • Protecting IP, trade secrets for vehicles and technologies processing AV data • Connectivity, convergence of technology • Insurance considerations • Current level of maturity for AV is level 2 or 2.5, intending to reach level 4 • Projects to develop extensive tests to provide certification • Various challenges depending on the type of AV: autonomous cars versus autonomous trucks vs valet parking etc…
IoF2020 / Farm2Food	• Farming obey to law but because of few sensitive personal data, limited resources were devoted to data privacy in the project. Focus is on use cases. • Code of conduct for Agriculture (non-binding principles): all use cases have an agreement according to DESCA template "Building Trust" provided by the supporting unit "Ethical team" • Publishing KPIs: some negative results, meaning some KPIs not working as expected • Tracing the box implies locating the driver • The introduction of GPDR downsized the project communication newsletter/emails because it required to obtain thousands of consents.

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

4.3.1 SYNCHRONICITY

The representative from SYNCHRONICITY discussed the data management and privacy strategy adopted by the SYNCHRONICITY project. SYNCHRONICITY has developed a strategy to ensure full compliance with the highest ethical and legal standards.

The strategy has taken into account some basic principles: the user/market acceptance; the consideration of legal, financial, political and reputational risks and the applicable EU norms on privacy.

[55] This section is largely based on material made available by the LSPs for the purpose of the above-mentioned paper on Good Practices for Personal Data Protection in Large Scale Deployment of Internet of Things. Lessons Learned from the European Large-Scale Pilots on Internet of Things, 2020 (currently, under publication).

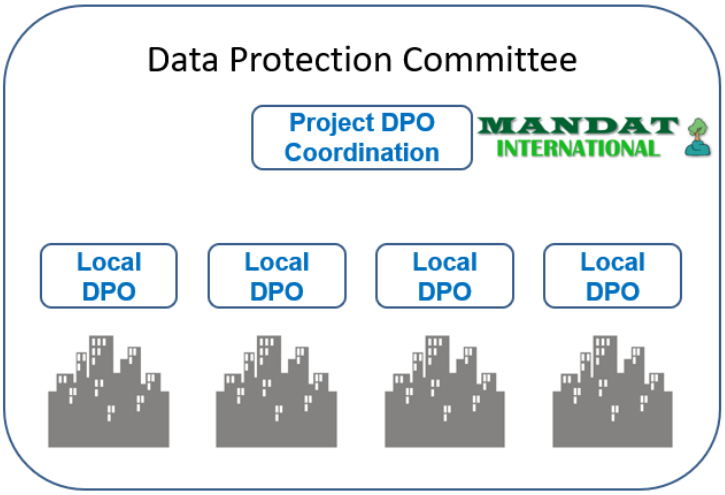

Figure 6: DPO Governance Scheme

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

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

At the DPO level:

- DPO functions and responsibilities, including data protection and GDPR compliance monitoring;
- Personal data collection identification, including data controllers and processors identification;
- Data Protection Impact Assessment (DPIA).
- At project level:
- Data Protection Policy Coordination;
- Public Information and Contact;
- Reporting and data protection issues management.

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

- GDPR is a research domain per se and there is tremendous potential for innovation;
- Take personal data protection seriously: don’t underestimate legal, financial and political risks;
- Identify and clarify DPO responsibilities;
- Continuous improvement process;
- Educate, educate, educate!

- Anticipate evolution and end-users' perceptions;
- Strong cross-fertilization potential.

4.3.2 Compliance challenges and lessons learnt in the context of smart cities[56]

The table provides an overview of the key compliance challenges, to an extent discussed above, that were encountered in SYNCHRONICITY.

Table 3: Overview of compliance challenges & lessons learned in the context of smart cities

Smart Cities Challenges	Smart Cities Lessons Learned
• Open Data & Interoperability versus Privacy & Personal Data • Risks: legal risks, financial risks, reputational & political risks, user & market acceptance • DPO coordination and distributed strategy: DPO committee with Project DPO liaising with local DPO in pilot cities • DPIA is a key requirement for Smart Cities • Audit and certification in data protection: display all city sensors and their retention policy in a Privacy App, test and get a gap analysis with the GDPR (Europrivacy.com)	• GPDR is a research domain with tremendous potential for innovation • Take personal data seriously: be aware of legal, financial, political risks • Identify the DPO responsibilities (distributed strategy) • Continuous improvement process • EDUCATE! • Be pragmatic and need-driven (focus on use cases and roll out pilots) • Identify the fears and barriers upfront • Anticipate evolution • Potential for cross-fertilisation amongst all LSP: gather all tools developed, all Best practices applied, all challenges faced and translate the research findings into business development • Establish peer-review network of local city DPO (this can survive after the project closure)

[56] This section is largely based on material made available by the LSPs for the purpose of the above-mentioned paper on Good Practices for Personal Data Protection in Large Scale Deployment of Internet of Things. Lessons Learned from the European Large-Scale Pilots on Internet of Things, 2020 (currently, under publication).

5. FORTHCOMING REGULATIONS, SOFT LAW INSTRUMENTS & OTHER INITIATIVES

While Chapter 3 highlighted the existing regulatory landscape that pertains to the IoT ecosystem, the present chapter aims at highlighting proposals for legislations and amendments to existing legislations that are still underway. It also touches upon the various measures taken by the European Commission in the form of soft law instruments or initiatives that aim to establish a general framework for the development, design and implementation of IoT.

Note, that as human-centric IoT entails taking into account the consumer perspective, one recent development in this area is the announcement for proposal for a new Digital Services Act that will upgrade the current liability and safety rules for digital platforms, services and products, therefore, completing the Digital Single Market.[57]

5.1 ePrivacy Regulation

Lawmakers in the EU have recently initiated steps with the view of updating rules relating to privacy and electronic communications and reinforcing trust and security in the Digital Single Market. Having identified areas to be addressed (including stronger protection online, more straightforward rules on cookies, and transparency on direct marketing, to name a few), the Commission released a proposal for the Regulation in January 2017. In June, this was followed by the Parliament's Committee for Civil Liberties, Justice and Home Affairs (LIBE) publishing a report with amendments to the Commission's proposal.

The resulting text strengthens privacy protection for individuals. It provides clarity regarding what legitimate grounds for processing prevail if both the GDPR and the ePrivacy Regulation apply to a processing operation and prohibits all further use of electronic communications data collected under ePrivacy rules. In addition, significantly stronger obligations including measures to ensure the confidentiality of electronic communications and implementation of safeguards to prevent tapping, listening, scanning or surveillance by anyone other the end-user concerned. Moreover, the amendments provide for an extension of the principle of confidentiality of communications to machine-to-machine communications as well as enhanced definitions of "electronic communications metadata" and "direct marketing".

On 27 October 2017, the plenary of European Parliament approved the above-mentioned report produced by LIBE Committee. The approved report will provide the basis for the negotiations with the European Council and the European Commission on the final text. It is important to stress that the legal bases for the processing of personal data remain unaltered under the text of the final report. More specifically, among others, the text prohibits any further processing of communications metadata, while – in principle – internet companies and communication providers should only be able to use data of users with their consent except for cases, of course, such as criminal law enforcement and national security[58]. In this respect, the report helps ensure that consent is genuinely freely given and requires privacy by default for software settings.

[57] A Union that strives for more, by candidate for President of the European Commission Ursula von der Leyen, available at: https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[58] In any event, note that according to Chapter 2 of Title V of the Treaty on European Union, national security remains the sole responsibility of the Member States and, thus, cannot be subject to regulation by an EU regulatory instrument applicable across all EU, such as the proposed ePrivacy Regulation.

Concerning the first draft of the ePrivacy Regulation, the definition of "electronic communication services" was rather broad as it could have been interpreted to include data transmission from one machine to another within its ambit including IoT devices. A later amendment modified this provision to distinguish between the application layer of M2M communications and the transmission layer which involves the conveyance of signals via an electronic communications network. It was clarified that the latter would be considered as an electronic communication service and not M2M communications in general. Despite the amendment, there still seems to be some ambiguity about how these terms will be interpreted.

The draft of the Regulation, which was published on 4 October 2019, provided for the addition of specific provisions as well the revision of existing ones. With respect to metadata, the draft lays down instances where metadata can be processed including cases where such processing is necessary for the purpose of calculating and billing interconnection payments, for protecting the vital interests of a natural person or where the end-user has given his or her consent. A provision to safeguard the interests of children was added allowing service providers to process electronic communications solely to identify and delete content that constitutes child pornography provided that such processing meets specific parameters.

The provision for obtaining consent in the Regulation has mostly remained the same and the recent draft continues to state that consent would be the same as provided for under the GDPR. Moreover, a ruling that was delivered on 1 October 2019 by the Court of Justice of the European Union (CJEU) gave clarity on "cookie consent" requirements under the GDPR and the current ePrivacy Directive. The Court confirmed that consent is not valid if the method of obtaining it is through pre-ticked checkboxes, thereby requiring active behaviour on the part of the user with respect to his or her consent.

After the first proposal was published in January 2017, the draft underwent several amendments including the recent amendments that were published on 4 October 2019 and later on 15 November 2019. However, as the current deliverable was being drafted, the stance of the Council of the European Union on the draft of the Regulation was rejected by the Permanent Representatives Committee of the Council of the European Union (COREPER). Failure to get the consensus of member states on topics including cookie walls, processing of electronic communications data to prevent child pornography and unsolicited commercial advertising significantly contributed to the failure of the draft regulation to gather support. The European Commission is now aiming at publishing a revised draft of the Regulation in 2020.

5.2 Product Liability Directive

As the EC has also become aware of certain possible gaps between the legal situations PLD applies to and the current challenges, it initiated an evaluation of the PLD, with particular consideration of the new technological developments.[59] As part of the assessment, the EC launched a public consultation in 2017 to assess the relevance and adequacy of the Directive in the current market and society.[60] Contributions to this consultation submitted by the end of April 2017 were subjected to EC's further in-depth analysis. This was complemented by the analysis of the responses to a targeted survey and to interviews conducted with different categories of stakeholders (e.g. producers, consumers, insurers, public authorities, civil society or technical legal experts in the domain). In addition, the Product Liability Conference was held in October 2017 to discuss the preliminary results of the evaluation of the PLD [37].

[59] See details concerning the ongoing evaluation of the PLD available online at: http://ec.europa.eu/growth/single-market/goods/free-movement-sectors/liability-defective-products/.

[60] Details available online at: http://ec.europa.eu/growth/content/public-consultation-rules-liability-producer-damage-caused-defective-product-0_en.

Interestingly, the views expressed in the course of the above-mentioned event varied. Certain participants argued that the PLD does not need to be altered as it does its job sufficiently. Their arguments, however, lacked substance as they were mainly focussed on (a) old success rates of the PLD (in relation to "regular products") and (b) the thought that the PLD covers end products, containing software, thereby ignoring the carve-outs many producers use with regard to the software components in such products and the points made above in relation to e.g. the definition of damage or the difficulties consumers encounter proving the defect. Other parties argued that any alterations to the PLD would be premature, as the area of technological changes is still moving at a fast pace and a lot of new technologies are not on the market yet. As the PLD's objective is first and foremost the protection of consumers, these arguments seem counterintuitive as it may put the risk of these aspects of (new) technologies, which are manufactured and deployed by the industry itself, on the consumers.

To this end, many other attendees of the conference acknowledged that and underlined that, in relation to current and future developments in technology, alterations need to be made in order for the PLD to remain relevant and fit for purpose in the future.

In May 2018, the European Commission published the 5th Report on the application of the PLD ("Report")[61] where it acknowledged that many of the products available in the market now were considered science fiction during the 1980s which is when the PLD was enacted. While the PLD had been successful in protecting injured persons and providing them with a legal recourse, the Report admits that due to the emergence of new technologies, concepts like "product", "defect" and "damage" have become less clear-cut.

As a result, it is the aim of the Commission to establish a reliable framework for product liability that will encourage healthy competition, innovation while also ensuring the safety of consumers. Moreover, if required the Commission will update specific provisions of the PLD including concepts like "product", "defect" and "damage."

At the same time, an Expert Group on liability and new technologies was created that consists of two configurations. One comprises of representatives of member states, civil society, industry and academia where the group assists the European Commission to evaluate the PLD keeping in mind industrial developments, existing EU and national laws and developments in the field of product liability. On the other hand, the second configuration comprises of independent academic experts and practitioners where they take a holistic overview to determine whether the current liability regime is sufficient to enable adoption of new technologies while also bolstering consumer trust and investment stability.

Another legislation that is complementary to the objectives of the Product Liability Directive is the General Product Safety Directive (GPSD)[62] that aims at ensuring that manufacturers and other related parties are only able to place products that protect the health and safety of consumers.

In order to qualify as "safe", products are required to meet the safety requirements laid down under European law or the law of the Member State where the product is being sold. Moreover, manufacturers are required to share the necessary information with consumers that will enable them to understand the inherent risks of the products in circumstances where the said risk is not evident and to also provide consumers with precautions that they can take to avoid the risks.

[61] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), also available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0246&from=EN

[62] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety

5.3 Soft Law Instruments

5.3.1 Ethics Guidelines for Trustworthy AI

After presenting an initial draft in December 2018, the High-Level Expert Group on AI published the Ethics Guidelines for Trustworthy Artificial Intelligence[63] on 8 April 2019. The Guidelines aim at promoting trustworthy AI wherein it is ensured that throughout its lifecycle, the AI system is lawful, ethical and robust. The voluntary guidelines are addressed to all stakeholders that are designing, deploying, using, implementing or being affected by AI. Chapter II of the Guidelines lay down 7 key requirements for trustworthy AI that involve systemic, human and societal aspects:

1. Human agency and oversight: AI systems should not exclude humans but rather empower them and enable them to make informed decisions by providing them with the necessary knowledge and tools to understand AI systems. Moreover, there should be mechanisms that allow human oversight such as human-in-the-loop (HITL), human-on-the-loop (HOTL), or human-in-command (HIC) approach.
2. Technical robustness and safety: AI systems should be designed in a manner to ensure that they are reliable and also can minimise unforeseeable risks and vulnerabilities. Additionally, there should be a fallback plan in place for untoward instances.
3. Privacy and data governance: Throughout the life cycle of a system, there should be sufficient safeguards in place to guarantee privacy and data protection. Integrity and quality of data should also be maintained.
4. Transparency: Decisions taken by AI systems should be documented to facilitate traceability and transparency. Such decisions may also require suitable explanations in certain circumstances.
5. Diversity, non-discrimination and fairness: Inadvertent bias can result in prejudice and discrimination and therefore, should be prevented by establishing oversight processes to comprehend and address the system´s dynamics, constraints, decisions and requirements in an integrated manner. Regardless of age, gender and abilities, AI products and services should be made usable by everyone.
6. Societal and environmental wellbeing: Some of the societal challenges that are being faced can be addressed through AI solutions for the benefit of human beings and for future generations,
7. Accountability: Procedures should be put in place to ensure responsibility and accountability for AI systems and their outcomes. Auditability of algorithms, data and design processes by external and internal auditors can further be instrumental in establishing the trustworthiness of technology.

The Guidelines further acknowledges that the potential of AI systems and its impact is not limited to certain geographical boundaries. As a result, global solutions are required that cater to the global opportunities and obstacles that are put forward while dealing with AI are required. Stakeholders were further encouraged to establish a global framework that build international consensus and uphold fundamental rights.

5.3.2 Code of Conduct on Agricultural Data Sharing

A coalition of associations representing diverse sectors of agri-food chain in the EU launched and co-signed the EU Code of Conduct on Agricultural Data Sharing (Code)[64] in April 2018. The voluntary Code establishes principles and guidelines aim at reaping the benefits of digital

[63]High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, also available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419

[64] EU Code of conduct on agricultural data sharing by contractual agreement, also available at: https://copa-cogeca.eu/img/user/files/EU%20CODE/EU_Code_2018_web_version.pdf

farming in Europe through data-driven solutions. Through contractual agreements, the Code makes it possible for parties in the agricultural industry to exchange and access relevant data fairly and transparently. The Code requires all contracts to be understandable and should clearly specific the following:

- Most relevant terms and conditions
- The purpose for which data is being exchanged, collected and stored
- Rights and obligations of parties to the contract
- Software or relevant application and information on the storage
- Verification methods for the person providing the data i.e. the data originator
- A transparent mechanism to modify the purpose of the agreement and to add future uses.

The "data originator" plays a pivotal role under the Code and is defined as "*the person or entity that can claim the exclusive right to license access to the data and control its downstream use or re-use*" i.e. the party that the data is attributed to. The explicit, express and informed permission through a contractual arrangement is a pre-requisite to collect, store and use the agricultural data for the specific purpose agreed upon in the contract by the parties. Further, unless otherwise agreed in a contract, the Code does not restrict the data originator from sharing data with other users or on other platforms. On similar lines, a "data user" is defined as "*a natural or legal person that retrieves data from the data originator or data provider under an agreement with the data originator*".

The Code states that safeguards for data protection and transparency are considered essential. The data user, pursuant to the contractual arrangement, should have a protocol on data protection safeguards to prevent unauthorised sharing with third parties. Further, it is mandated that the provisions of a contract should not be modified without the consent of the data originator.

The principle of privacy and security enshrined in the Code require data user to oversee and keep track of the data received throughout the value chain and to keep the data originator informed of the same. Moreover, a data user is accountable to the data originator for loss, theft or unauthorised access by an unauthorised third party. The Code also requires the creation of a provision to remove, destroy or return all original data if requested by the data originator,

Lastly, the Code mandates that the provision regarding liability should be clearly agreed upon and laid down in the contract. Further, it requires the data originator to guarantee that the raw data that is shared is complete and accurate to the best of their knowledge. However, the data originator cannot be held liable for any damage that results from or due to the use of the data by machines, devices or third parties.

5.4 Kick-off projects on Europe's Quantum Technologies Plan

In addition to the current proposals for new regulations on ePrivacy, the European Commission has launched an initiative of relevance, namely, the Quantum Technologies Flagship. On 28 October 2018, an announcement was made by the European Commission on the Quantum Technologies Flagship, a €1 billion initiative, which included 20 projects with a focus on four primary areas of application - quantum computing, quantum sensing and metrology, simulations, quantum cryptography, and quantum communications. The flagship aims at:

- Integrate and amplify European scientific excellence in the field of quantum research.
- Facilitate competition within European industries in quantum technologies.
- Make Europe a viable and attractive region for investments, business and innovative research in quantum technologies.[65]

[65]Quantum Technologies and the advent of the Quantum Internet in the European Union, also available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=61653

The long-term goal of the Flagship is to develop a so-called quantum web in Europe wherein quantum computers and sensors are interconnected through quantum communication networks.[66]

5.5 Relation to the state-of-the-art and progress beyond it

IoT technologies and applications are key enablers for digitising industry and can play a critical role in the foundation of Europe's future competitiveness and its digital society.

Europe represents a huge opportunity for the development of IoT applications and services as IoT is a technology that plays to Europe's strengths as one of the largest integrated markets, with a well-developed industrial sector.

In this context, a proper and efficient legal IoT framework based on best practices, including adequate sharing of non-personal machine-generated data and IoT security measures are key for the future developments of a single digital market across Europe.

The IoT legal framework has to adapt dynamically to the IoT complexities, the trend for decentralised and distributed architectures that requires adequate data sharing, data management, legal measures, while addressing in a holistic way trust, security and privacy issues.

Harmonising the application of rules across the single market, focus on of technological neutrality, developing standards across industries instead of industry-specific standards and regulations and avoid the silo approach enables the development of IoT technologies and applications across the EU economy.

[66] Quantum Technologies and the advent of the Quantum Internet in the European Union, also available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=61653

6. RECOMMENDATIONS

Based on the discussion captured in the previous chapters, set of recommendations[67] can be drawn relevant for all applications domains and, thus, for other currently ongoing and future LSPs projects covering the respective application domains.

More specifically, it was considered in this respect that:

- Human-centric IoT and the effective implementation of the existing regulations all IoT stakeholders (including end-users) should be continuously adequately informed, educated and kept up to date thereby paving the way for the development of a digital culture.
- An interdisciplinary approach and the creation of multidisciplinary teams should be a "need to have" for human centric IoT and for effectively addressing compliance challenges within IoT ecosystems.
- Considering that each LSP has gained experience with the performance of a data protection impact assessment in the respective ecosystem, this experience would be worth sharing, in particular as to how to organise in a practice a community of several stakeholders in an ecosystem in order to produce an overall data protection impact assessment[68].
- Addressing terms of appropriate governance structures, future LSPs projects should consider the appropriate DPO schemes, taking into account both the scope of the project, as well as the synthesis of the consortia.
- IoT stakeholders should put particular emphasis on how to strengthen trustworthiness in IoT ecosystems through assurance.
- IoT stakeholders should be equally vigilant with "emerging" behaviours and trends, as it is likely that those will become the modus operandi within a short frame of time.
- IoTs stakeholders should, primarily, utilize existing standards and explore the necessity for new standards that could contribute to the orchestration of IoT ecosystems. In particular, standards could contribute to the development of widely used consent dashboards.
- The need for future LSPs projects to set up DPO schemes appropriated for the scope of the projects and the synthesis of the consortia[69].
- The "regulatory sandbox"[70] concept allowing for experimentation in controlled environments under a regulator's supervision for a considerable amount of time (e.g. one or two years) should be carefully considered for IoT deployments.

Overall, in the context of the various interactions that took place between WP5 and the LSPs, it became clear in several instances that for an effective legal IoT framework, stakeholders should, also, put forward the development and utilization of soft law instruments. Such instruments (e.g. codes of conduct) could foster engagement of IoT stakeholders and further contribute to the effectiveness of hard law rules

[67] A set of recommendations focusing exclusively on the implementation of the GDPR can be found at: S. Ziegler and others (ed.), Good Practices for Personal Data Protection in Large Scale Deployment of Internet of Things. Lessons Learned from the European Large-Scale Pilots on Internet of Things, 2020 (currently, under publication).

[68] Note that SYNCHRONICITY and CREATE-IoT have contributed to ISO/IEC 27570: Privacy guidelines for smart cities (this standard is under development), which describe five ecosystem processes (governance, risk management, engineering, citizen engagement, data exchange).

[69] See, also, D05.07 on Legal IoT Framework Event, submitted European Commission Services in October 2019, currently under review.

[70] For example, for more on the concept of regulatory sandbox in the fintech sector, see, also, the "Report FinTech: Regulatory sandboxes and innovation hubs", available at: https://www.esma.europa.eu/sites/default/files/library/jc_2018_74_joint_report_on_regulatory_sandboxes_and_innovation_hubs.pdf

7. CONCLUSIONS

This deliverable expanded and enhanced the discussions captured under D05.05 on Legal IoT Framework (initial version), mainly by bringing in insights gained through the various interactions with the LSPs regarding compliance challenges and providing recommendations pertinent to the respective application domains. It, also, produced an overview of the latest regulatory developments at the EU level, as well as of other forthcoming regulations and recently launched initiatives.

More specifically and in addition to the lessons learnt per application domains discussed earlier, the resulting key findings relevant for all LSPs projects can be summarized as follows:

- rule of law has a pivotal role to play with respect to the protection of fundamental human rights across all application domains, including, in the connected public sphere;
- as opposed to the existing misconceptions, the intent of the law is to regulate the use of technology rather than creating obstacles for its development;
- with the proliferation of data in an IoT environment, the challenge that data will be used for purposes in addition or other to those originally specified becomes even more important to consider.
- the need to address ethical concerns, in addition to ensuring legal compliance has been raised by the majority of the LSPs.
- each pilot had to deal with a complex ecosystem of technologies and stakeholders, raising issues of integration and coordination;
- the use of wearable devices, especially, for events in public spaces, in reality, may turn out to be difficult, for instance, when it is expected that the same devices are to be returned to the organizers;[71]
- getting a helicopter view on personal data protection practices within the LSPs has proven to be particularly challenging, considering the large number of deployment sites and stakeholders involved across several Member States;
- although GDPR is applicable horizontally across all Member States, it does allow in certain instances for derogations at national level.
- researchers, technical experts, pilot sites managers focusing on the event safety do not necessarily share the same goals.
- more clarity is required on matters such as determining liability and identifying responsible stakeholders in the IoT ecosystem. This is especially relevant in the context of AUTOPILOT.

Overall, the interactions with the LSPs have revealed the necessity to put equal emphasis on the implementation of the appropriate technical and organizational measures (e.g. authentication mechanism, DPO governance schemes). Considering both the technical and organizational aspects is relevant not only for the effective protection of personal data but, also, for the other regulatory aims aspired, including those that are put forward under the Free Flow of Non-Personal Data Regulation that are pertinent to the achievement of the overarching objectives of the Digital Single Market.

[71] For example, this was easy for the 2019 IoT week but, most probably, quite difficult to achieve in the context of large commercial events due to the reputational risks involved.

8. REFERENCES

[1] European Commission, "Staff Working Document, Advancing the Internet of Things in Europe, Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions", 2016, online at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016SC0110&from=EN.

[2] European Commission, "Communication A Digital Single Market Strategy for Europe", 2015, online at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192.

[3] Article 29 Data Protection Working Party, "Opinion 8/2014 on the Recent Developments on the Internet of Things", 2014, online at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

[4] A. van der Wees, J. Breeuwsma and A. van Sleen, "IoT Societal Impact – Legal Considerations and Perspectives" in O. Vermesan and J. Friess (Eds.), *Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds*, ISBN: 978-87-93379-81-7, River Publishers, Gistrup, 2016, River Publishers Series in Communication, Volume 49, Chapter 7.

[5] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[6] Regulation (EU) 2016/679 of the European Parliament and of 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).

[7] 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.

[8] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

[9] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.1.2017.

[10] Regulation (EU) 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

[11] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013

[12] Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

[13] The Cloud Select Industry Group, "Cloud Service Level Agreement Standardisation Guidelines", 2014.

[14] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, 2017, online at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850.

[15] European Commission, Special Eurobarometer 460: Attitudes towards the impact of digitisation and automation on daily life, 2017, online at: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/78998.

[16] European Commission, Special Eurobarometer 464a: Europeans' attitudes towards cyber security, 2017, online at http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/79735.

[17] European Commission, "Communication from the Commission to the European Parliament and the Council "Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union", 2017, 4 October 2017, online at: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-476-F1-EN-ANNEX-1-PART-1.PDF.

[18] European Commission, "Proposed Directive on Network and Information Security – frequently asked questions", 2013, online at: http://europa.eu/rapid/press-release_MEMO-13-71_en.htm.

[19] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

[20] J. Hojnik, "Technology neutral EU law: digital goods within the traditional goods/services distinction", *International Journal of Law and Information Technology,* Oxford Academic, Volume 25, issue 1, 7 September 2016.

[21] K. Alheit, *The applicability of the EU Product Liability Directive to software,* p. 199, 200.

[22] L.A. Weber, "Bad Bytes: The Application of Strict Products Liability to Computer Software", *St John's Law Review*, Volume 66, Issue 2, 1992, number 2, p. 475 – 476.

[23] ANEC, BEUC, Consumers International, ICRT, "Securing consumer trust in the Internet of Things: Principles and recommendations 2017, 2017, p. 5 (point 5.3), online at: http://www.consumersinternational.org/media/154809/iot-principles_v2.pdf.

[24] European Commission, "Commission Staff Working Document, Impact Assessment accompanying the document Proposal for a directive of the European parliament and of the Council on payment services in the internal market and amending Directive 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC and Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions", 27 August 2013.

[25] European Banking Authority, "Final Report: Draft Regulatory Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)", 2017, online at: https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+(EBA-RTS-2017-02).pdf, Chapter 2.1, paragraph 4.

[26] European Commission, "Payment services: Consumers to benefit from safer and more innovative electronic payments", 27 November 2017, online at: http://europa.eu/rapid/press-release_IP-17-4928_en.htm.

[27] European Union Intellectual Property Office, "Protecting innovation through trade secrets and patents: Determinants for European Union firms, 2017, online at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Economics_and_Statistics_Trade_Secrets_and_Patents_Executive_Summary_en.pdf.

[28] European Commission, "Study on Trade Secrets and Confidential Business Information in the Internal Market", 2013, online at: https://ec.europa.eu/docsroom/documents/14900/attachments/1/translations/en/renditions/native.

[29] World Trade Organisation, The Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994, Section 7, Art. 39, Annex 1C to Agreement Establishing World Trade Organization.

[30] P. O'Donohue, European Commission, "Proposal for a Regulation on the Free flow of Non-personal data", 12 December 2017, online at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=49048.

[31] European Commission, "Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017, online at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:450:FIN.

[32] D. Ferrara, European Commission, "Cybersecurity Package: Highlights of key initiatives", 12 December 2017, online at: http://ec.europa.eu/information_society/newsroom/image/document/2017-51/cybersecurity_package_27C2A669-CACC-F311-8C7AF9F4BD00B2ED_49047.pdf, slide 20.

[33] Autonomous Vehicle Readiness Index: Assessing countries' openness and preparedness for autonomous vehicles, KPMG, 2018, online at: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/01/avri.pdf.

[34] Autonomous Vehicle Readiness Index: Assessing countries' openness and preparedness for autonomous vehicles, KPMG, 2018, online at: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf

[35] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC

[36] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[37] European Commission, "Minutes: Product Liability Conference", 2017, online at: https://ec.europa.eu/docsroom/documents/26661

9. APPENDICES[72]

Further information is described in related background documents.

9.1 Setting the scene

Ownership of data is a particularly critical issue for the economy and society of EU triggering questions liked to the very nature of data and the interests associated with the afforded protection. Irrespective of the different definitions and conceptual matters, data ownership forms a focal point of interest of European lawmakers. For instance, the Digital Single Market Strategy explicitly identified emerging issues on data ownership, (re)usability and access to data (including research data), and liability amongst others in relation to the Internet of Things as one of the primary triggers underlying the Free Flow of Data Initiative [2], while uncertainties linked to ownership of both personal and non-personal data have been identified as particularly relevant for the broad adoption of IoT solutions [1].

Discussions concerning data ownership are inevitably linked to the notion of data. According to EU Law, data are can be grouped into two broad categories, a separation that has been maintained both under the already adopted and proposed regulation. More specifically, the GDPR defines personal data as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[73], while Article 3(1) of the Regulation on the free flow of non-personal data [10] defines data falling under its scope as "data other than personal data" as defined under Article 4(1) of the GDPR.

Moreover, soft law instruments, also, provide definitions on the notion of data. For example, ISO/IEC 2382-1, consider data as "*a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing*", while the Cloud Service Level Agreement Standardisation Guidelines [13] define data as "*Data of any form, nature or structure, that can be created, uploaded, inserted in, collected or derived from or with cloud services and/or cloud computing, including without limitation proprietary and non-proprietary data, confidential and non-confidential data, non-personal and personal data, as well as other human readable or machine readable data.*"

The existence of varying definitions formulated under different standpoints in relation to data highlight the complexity in defining in a uniform manner the object of ownership in the first place. The emerging questions are not, of course, exhausted in the purpose of ownership, as there are other questions of legal relevance, including, "*Who owns the data or it is not feasible to retrieve the data?*" [4]

9.2 NIS Directive

With respect to the connected nature of IoT ecosystems, this section outlines the current legal framework applicable to the domains of cybersecurity, information sharing and resilience, namely from the perspective of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for high common level of security of network and

[72] The contents of the APPENDICES can, also, be found at: D05.05 Legal IoT Framework (Initial).
[73] See Article 4 (a) of GDPR.

information systems across the Union ("*NIS Directive*"). In doing so, it also aims to indicate specific challenges still to be addressed by law makers.

9.2.1 The rationale of the Directive

While almost three-quarters of Europeans believe that digital technologies have a positive impact on our economy, society and quality of life [15], a vast majority of them believe that the risk of becoming a victim of cybercrime is increasing [16]. In this regard, it is propitious that EU law makers have begun addressing the issue of cybersecurity, namely with the introduction of the NIS Directive. This directive is the first EU horizontal legislation addressing cybersecurity challenges, aiming to increase the overall level of cybersecurity resilience and cooperation in the EU and to prevent far-reaching consequences of cyber-attacks within the bloc [17]. Recognising the vital role of network and information systems and services in the society (which IoT devices and ecosystems are an inseparable part of), the Directive acknowledges that their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market [18]. In doing so, it aims to put forward measures promoting a culture of risk management and preventing or mitigating the effects of the severe incidents capable of having a significant disruptive impact on these systems and services. These can result in an impediment of the pursuit of economic activities, substantial economic loss, undermining of user confidence and major damage caused to the economy of the Union.[74]

Thus, implementation of the Directive is an essential part of the Cybersecurity package presented on 13 September 2017. Member States are therefore encouraged to take appropriate measures to ensure that the provisions and the cooperation models of the NIS Directive can provide the best possible EU-level tools to achieve a high common level of security of network and information systems across the Union [17].

9.2.2 Scope and definitions

Aiming to achieve high common level security and improve the functioning of the internal market, NIS Directive puts into place measures concerning security of *network and information systems*, encompassing a broad domain of network, infrastructure, devices as well as data.[75] By doing so, the NIS Directive takes into account all elements and stakeholders of the connected ecosystem. As IoT elements, endpoints, devices and other solutions may also form a significant part of the connected ecosystem, provisions of the Directive discussed under this Chapter are very relevant for the legal framework applicable for IoT.

To promote a culture of risk management and ensure that the most serious incidents are reported [17],[76] NIS Directive stipulates that specific security and incident notification requirements apply namely to *operators of essential services*[77] and *digital service providers*.[78] While the Directive acknowledges the importance of applicability of the rules to internet companies as well as to the operators of essential services (including internet infrastructure) [18], it recognises fundamental differences between operators of essential services and digital service providers and takes a differentiated approach in respect of the two (for further elaboration of security and incident notification requirements.

An *operator of essential services*, on the one hand, is defined as any entity which (1) provides service essential for the maintenance of critical societal and economic activities, (2) where the provision of that service depends on network and information systems; and (3) where incident

[74] Recital 2 of NIS Directive.

[75] Article 4 (1) of NIS Directive.
[76] Recital 4 of NIS Directive.
[77] Article 14 of NIS Directive.
[78] Article 16 of NIS Directive.

would have significant disruptive effects on the provision of that service. In addition, NIS Directive puts forward a list of examples of entities and industry sectors falling within the scope of the Directive, including specific entities in energy, transport, banking, financial market, health, drinking water and digital infrastructure sectors.[79]

A *digital service provider*, on the other hand, is defined as a provider of a service (normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services [19]) which is either (a) an online marketplace, (b) online search engine, or (c) a cloud computing service.[80] While the Directive clearly states that hardware manufacturers and software developers should not be considered operators of essential services, nor digital service providers,[81] it contains a relatively broad definition of *cloud computing services*, being "services allowing access to a scalable elastic pool of shareable computing resources". It also puts forward broad definitions of the respective terms "computing resources", "scalable", and "elastic pool".[82]

Given the present reasonably wide definition of *cloud computing services*, it could be argued that provisions of NIS Directive apply to a large number of providers of such services. However, with respect to the rationale of the Directive, it remains questionable whether covering the given range of cloud computing services has indeed been intended by the law makers.

It must be noted that the Directive aims to prevent the most serious incidents capable of having a significant disruptive effect on network and information systems within the EU, as these affect reliability and security of economic and social activities essential for the functioning of the internal market.

It is, however, argued that many services falling within the scope of NIS Directive definition of *cloud computing services* are used in context which does not necessarily create any risks in respect of network and information systems within the EU, nor in respect of economic and social activities essential for the functioning of the internal market.

Therefore, it is argued that the respective provisions of NIS Directive are not necessarily following the rationale of the Directive. Hence, it is suggested that applicability of the requirements of the Directive must be assessed primarily from the perspective of its rationale, rather than based on the interpretation of individual provisions.

The presented argument is highly relevant with respect to IoT legal framework. IoT devices vary substantially in their capabilities. Therefore, when assessing the applicability of the NIS Directive to their activities, organisations must consider the risk of a disruptive effect on network and information systems within the EU created by the IoT devices they engage with or rely on. Hence, an assessment should primarily be carried out with respect to the rationale.

9.2.3 The security and incident notification requirements

Aside from improving national cybersecurity capabilities, the Directive aims to build cooperation at EU level and promote a culture of risk management and increase resilience. These two objectives are addressed by identifying various relevant stakeholders and their responsibilities, as well as notification obligations for operators of essential services and digital service providers to comply with, respectively. Figure 7 illustrates the "landscape" as set out by NIS Directive, as well as relations between individual stakeholders involved.

[79] Article 4 (4) of NIS Directive. In addition, Article 5 of NIS Directive required member states to identify the operators of essential services with an establishment on their territory by 9 November 2018.
[80] Article 4 (5) of NIS Directive.
[81] Recital 50 of NIS Directive.
[82] Recital 17 of NIS Directive.

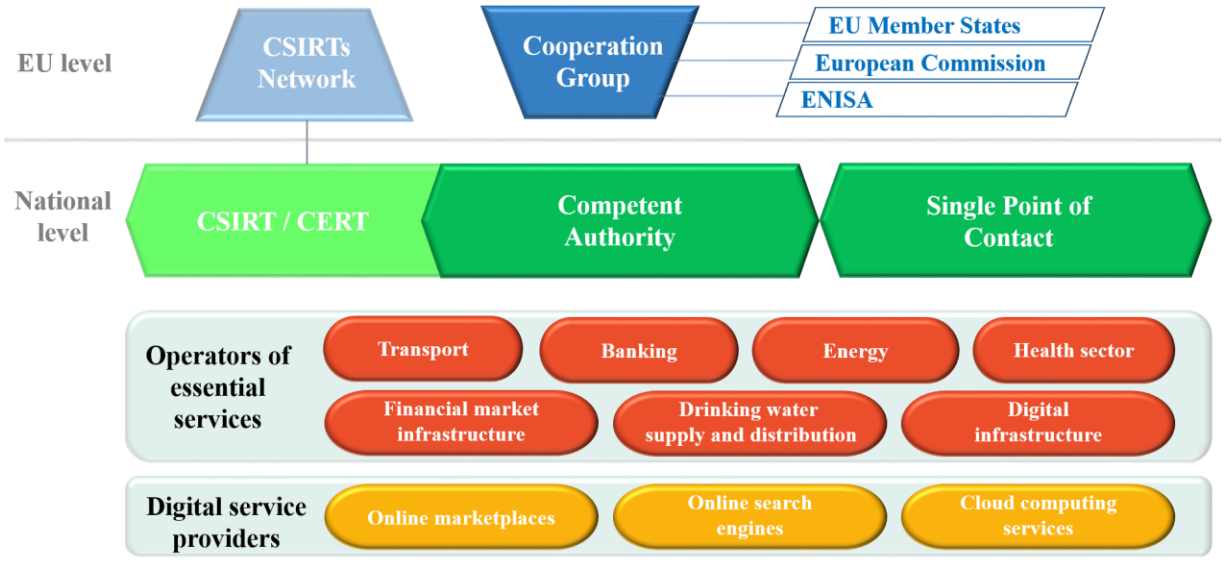

Figure 7: Overview of NIS Directive Stakeholders

To support and facilitate strategic cooperation and exchange of information among Member States, the Directive establishes the *Cooperation Group*, composed of representatives of EU member states, European Commission and European Union Agency for Network and Information Security (ENISA).[83] The Cooperation Group has various overseeing and strategic tasks including exchanging of best practices between member states and providing strategic guidance of the activities of the CSIRT's network (see below).

The Directive requires each Member State to designate one or more national *competent authorities* responsible for monitoring of the application of NIS Directive at national level.[84] In doing so, they should retain the ability to adopt national guidelines concerning the circumstances in which operators of essential services are required to notify incidents.[85]

Member States are also required to have a well-functioning *Computer Security Incident Response Teams (CSIRTs)* also known as *Computer Emergency Response Teams (CERTs)*, which may be established within the competent authority. CSIRTs (or competent authorities) should monitor incidents at national level (i.e. receive notifications of incidents), provide early warning, respond to incidents and provide dynamic risk and incident analysis.[86]

Given the importance of international cooperation on cybersecurity on EU level, CSIRTs should also be able to participate in the *CSIRTs network* established by the Directive.[87] CSIRTs network is tasked with a number of tasks and responsibilities, including the exchange of information on CSIRTs' services, operations and cooperation capabilities. As information about incidents is increasingly valuable to the general public and businesses, the secretariat of the CSIRTs network provided by ENISA is encouraged to maintain a website or to host a dedicated page on an existing website, where general information on major incidents that have occurred across the Union is made available to the general public, with a specific focus on the interests and needs of businesses.[88]

The Directive also requires each member state to designate a national *Single Point of Contact* responsible for exercising a liaison function to ensure cross-border cooperation of member state authorities with the relevant authorities in other member states, Cooperation Group and the

[83] Article 11 of NIS Directive.
[84] Article 8 (2) of NIS Directive.
[85] Article 47 of NIS Directive.
[86] Annex I, Article 2 of NIS Directive.
[87] Article 12 of NIS Directive.
[88] Recital 40 of NIS Directive.

CSIRTs.[89] National single points of contact and competent authorities should consult and cooperate with the relevant national law enforcement authorities and national data protection authorities.

Although not mentioned explicitly, it is apparent that one of the founding principles promoted throughout NIS Directive is the principle of accountability, as the provisions of the Directive, in general, require the relevant stakeholders to give regard to the overall security of the ecosystem, when applying internal policies. Also, with respect to other accountability-related legal provisions,[90] complying with the requirements stemming from this principle will present the main challenge for IoT device and service providers.

With respect to security requirements, NIS Directive requires that member states ensure that operators of essential services and digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to them.[91] The respective provisions also require that in ensuring the level of security appropriate to the risk posed the measures take into account the state of the art. With respect to the security of the network and information systems of digital service providers, the Directive requires those measures to take account of (a) the security of systems and facilities, (b) incident handling, (c) business continuity management, (d) monitoring, auditing and testing, and (e) compliance with international standards.

In addition, the Directive requires members states to ensure that operators of essential services and digital service providers take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems.[92]

Finally, NIS Directive stipulates that in the event of an incident having a significant impact on the continuity of the essential service they provide, operators of essential services shall notify the competent authority or CSIRT, together with a determination of any cross-border impact of the incident.[93] Similarly, digital service providers are obliged to notify the competent authority or CSIRT of any incident having a substantial impact on the provision of a service.[94] If necessary, the competent authority or CSIRT should use the provided notification to inform the other affected member state. Since the main task of the national single point of contact is ensuring cross-border cooperation of the given member state with other member states, the competent authority and/or CSIRT may ask the single point of contact to forward notifications to other affected member states.[95] NIS Directive also provides that the competent authority or the CSIRT may inform the public about individual incidents,[96] however, in doing so the relevant authorities or CSIRTs must carefully balance the interest of the public in being informed about threats against possible reputational and commercial damage for the operators of essential services and digital service providers reporting incidents.[97]

9.3 Revised Payment Services Directive

The widespread, accessibility and usability of the internet has enabled organisations to utilize it in the context of e-commerce, namely in offering and selling of products and services to customers. Traditionally, the handling of cashless payments has been left to banking institutions

[89] Article 8 (4) and (6) of NIS Directive.
[90] For example, please refer to Article 5 (2) of GDPR
[91] Article 14 (1) and 16 (1) of NIS Directive.
[92] Article 14 (2) and 16 (2) of NIS Directive.
[93] Article 14 of NIS Directive.
[94] Article 16 of NIS Directive.
[95] Article 14 (5) of NIS Directive.
[96] Article 14 (6) of NIS Directive.
[97] Recital 59 of NIS Directive.

which have enjoyed a unique and unrivalled position in the payment chain. However, with the emergence of connected devices and IoT ecosystems, third party organisations have been able to utilize technology and innovation in devising new ways of carrying out electronic (cashless) payments and thus compete with traditional methods of delivering financial services.

This Chapter discusses how PSD2 [5] aims to address some of the challenges brought about by these developments. As connected IoT devices and apps to a large extent enable innovative solutions introduced by third party organisations and are becoming an integral part of the payment chain, PSD2 is very relevant in the context of IoT legal framework.[98]

9.3.1 The rationale of the Directive

EU law makers have acknowledged that the solutions developed and introduced by third party organisations have fallen outside the scope of the applicable regulatory framework for the payments market [24]. This has meant that the environment of card payments and new means of payments (such as internet and mobile payments) has become inconsistent, fragmented and under-regulated.

Although customers have been able to choose which payment systems, they would use there has been very little or no guarantee that the selected third-party service would be compatible with the policies of their bank institution. In other words, there has been no guarantee that the banking institution would provide the third-party solution provider with the access to information about the customers' account balance, nor allow it to initiate payments. Hence, in some cases, customers have not been able to make effective use of the third parties' innovative payment methods, while in other cases, they have not been guaranteed safety and security of these solutions.

Recognising these challenges, PSD2 aims to create a more competitive market leading to downward convergence of costs and prices for customers, more choice and transparency of payment services for customers, and more security and trust regarding payment services.[99] It should be noted that the topics of transparency (and inclusion) and security are also key in the context of IoT. Therefore, the section below focuses on the question of transparency and inclusion of third-party providers.

9.3.2 Third-party payment services

Third-party service providers (TPPs) introduce and provide innovative payment solutions.[100] Since these are often intuitive and provide a positive user experience, TPPs' solutions positively contribute to an increased choice of products, and thus compete with traditional banks' instruments. As TPPs present a significant threat to the unique position of banking institutions, their inclusion in the Directive was possibly the most controversial aspect of the legislative negotiations.

When introducing innovative payment solutions, TPPs often make use on hardware and software equipment of IoT devices, especially smart phones and tablet computers. As these have become an integral part of the payment ecosystem, it is argued that PSD2 is very relevant for IoT legal framework.

---

[98] It should be noted that while PSD2 forms an integral part of the generally applicable legal framework, its applicability in respect of certain specific LSPs (such as IoF 2020, for example) may be limited.

[99] Recital 5 and 33 of PSD2

[100] Note that between CREATE-IoT partners there has been a lot of interest in payment mechanism that "push" payments rather than "pull payments" as is commonplace for credit card transactions. There is also interest in the potential role for block-chains for distributed ledgers as an alternative to existing settlement solutions.

This section outlines the role of TPPs, including *Payment initiation service providers* (PISPs) and *Account information service providers* (AISPs). Although both PISPs and AISPs constitute TPPs, their roles differ, as illustrated in Figure 8.

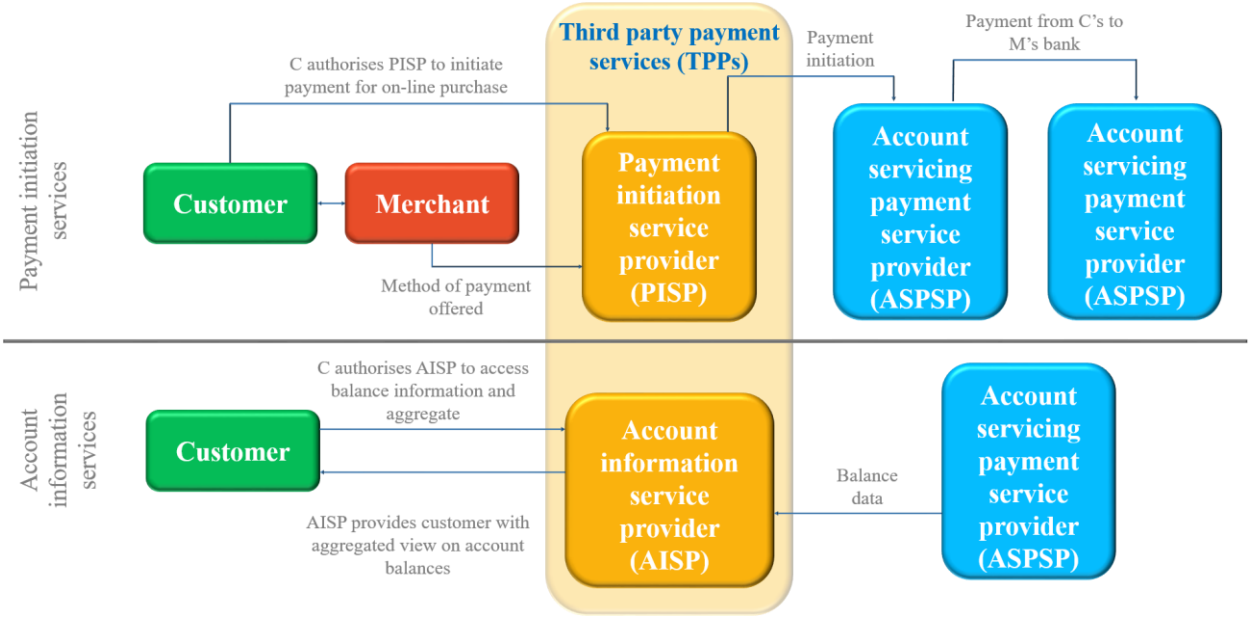

Figure 8: PSD 2 Stakeholders & Flows

In a transaction, a payer is not just sharing their personal security credentials with their bank, but also has to transmit their data through one or more third-party software providers providing the "bridging" interface through which the customer accesses their online account and transfers the payment. Therefore, the PISP acts as a *facilitator* enabling transmission of funds by populating the transaction details and confirming that the customer has sufficient funds in their account to execute the transaction.

The PISP does not handle customer funds, nor does it provide a statement of account. It will only confirm whether the customer has sufficient funds in their account to complete the transaction in question. For this to be possible, the customer must have given an explicit consent to the *Account servicing payment service provider* (ASPSP) to respond to requests from a specific PISP. The Directive prevents ASPSPs from requiring PISPs to have a contract with them as a pre-condition of the provision of the initiation service.[101] This way ASPSPs cannot force PISPs to agree to terms governing their responsibilities and liabilities when assessing user accounts.

While the PISP acts as a facilitator enabling a transmission of funds from the customer's ASPSP to the merchant's ASPSP, AISP acts as an *aggregator* of information from payment accounts maintained by other institutions (e.g. banks). As AISPs require access to those payment account to be able to perform this function, PSD2 stipulates that banks and other ASPSPs are obliged to respond to data requests from AISPs in a non-discriminatory manner.[102]

The way PSD2 approaches PISPs is a response to their rapid emergence and becoming an integral part of the connected ecosystem. In addition, the Directive recognises their potential to play an increasingly important role in the market.

However, to ensure that PISPs become a reliable part of the ecosystem, it subjects them to a level of supervision commensurate with the risk they introduce into the system. At the same time, however, PISPs are granted space to grow and propose innovative solutions by ASPSPs being prevented from putting up barriers and stifling their role, as illustrated, for example, in Figure 9.

[101] Article 66 (5) of PSD2.
[102] Article 35 of PSD2.

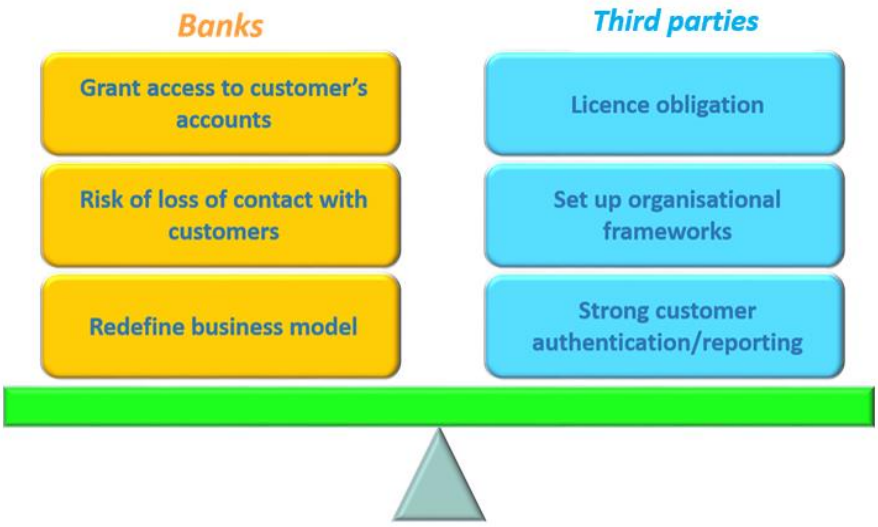

Figure 9: PSD2 – A new level playing field for banks and third party organisations

While the Directive requires banks to "takedown" some of the barriers preventing TPPs from entering the market, it provides rules and standards for PISPs to comply with. Amongst others, PISPs are required to be authorised but are subject to a reduced minimum own funds requirement.[103] They are also required to hold professional indemnity insurance of a comparable guarantee to ensure that they can meet liabilities arising in relation to their activities.[104] In addition, the Directive requires that, if a customer's payment account is being used by the customer on-line through a PISP (enabling such possibility is required by the Directive), ASPSPs must take specific steps to ensure that payments made via a PISP are handled by the ASPSP promptly and in a non-discriminatory manner.[105]

Because AISPs are TPPs, just like PISPs, some of the provisions applicable to them are similar to those applicable to PISPs. First of all, PSD2 recognises the role AISPs already play in the market and therefore the provisions are designed to allow AISPs to compete and collaborate with more traditional players.[106] Secondly, under PSD2, customers obtain a right to use AISPs in online transactions.[107] Effectively, this prevents banks and other payment institutions from thwarting the business of AISPs, as well as tying AISPs into contracts with them or forcing AISPs to adopt particular business models and practices. Finally, PSD2 provides that AISPs are expressly exempt from authorisation, but are obliged to register. Although they are not subject to regulatory capital requirements, AISPs will be required to hold professional indemnity insurance or a comparable guarantee in order to ensure that they can meet liabilities arising in relation to their activities.

9.4 Trade Secrets Directive

IoT solutions very often rely on specific innovations and technological advances which can be legally protected by a variety of intellectual property rights, such as patents or trade secrets. This is very important because recently, organisations' intellectual property has been accounting for an increasing share of their property. In the case of publicly traded companies, ownership of intellectual property also significantly increases organisations' market value. While patents have traditionally offered their owners relatively strong legal protection, European Union Intellectual

[103] Article 7 of PSD2.
[104] Article 10 of PSD2.
[105] Article 36 of PSD2.
[106] Article 67 of PSD2.
[107] Article 67 of PSD2.

Property Office has noted that "*the use of trade secrets for protecting innovations is higher that the use of patent by most types of companies, in most economic sectors, and across all Member states.*" [27]

Despite their importance from the economic as well as from the business model perspective, there had been a lack of consistent protection for innovative ideas across Europe for a long time. While only around two-thirds of Member States had specific legislation concerning the misappropriation of trade secrets, the remaining Member States, including the UK, France and the Netherlands, relied on a mixture of judicial interpretation and extra-contractual liability and traditional common law [28].

The EC has acknowledged that innovation is critical to the economies of industrialised nations. Aiming to facilitate the smooth functioning of single European market which favours innovation in the business environment, the EC has recognised that enabling business organisations protect their confidential and valuable information (i.e. trade secrets) will provide them with a competitive advantage which will allow them to turn their innovative ideas into growth and jobs, as a result. Hence, following a proposal from the EC, the European Parliament and the Council adopted the Trade Secrets Directive [8] which aims to standardise the national laws in the EU Member States against the unlawful acquisition, disclosure and use of trade secrets. The Directive entered into application on 9 June 2018.

As the topic of protection of trade secrets is relevant in respect of technological developments within IoT domain, this chapter outlines and discusses some key aspects of the new framework, including the definition of a trade secret, the notion of reasonableness as well as applicable remedies.[108]

9.4.1 Trade secrets

Although many Member States have agreed to grant protection to undisclosed information already by becoming a party to the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) [29], national implementation of the respective provision has remained considerably different across individual Member States resulting in differences in the procedure by which protection could be enforced, among others. Although Member States, in general, do facilitate protection of trade secrets, respective national frameworks vary considerably. While Sweden has been identified as the only Member State with specific legislation on trade secrets [28], the remaining Member States offer protection through other civil law sources, and in some instances under criminal law. In some countries, including Germany, Austria, Poland and Spain, trade secrets are granted protection by legislation directed to unfair competition, in labour law and in the criminal code. Italy and Portugal, on the other hand, provide protection to trade secrets through legislation directed to industrial property. The Netherlands takes a separate stance and grants protection to trade secrets by way of the law of tort [28].

TSD acknowledges the need for incentives for Europe's businesses to invest in innovation by offering a unified level of protection for confidential business information.[109] Therefore, in reducing differences among Member States the TSD harmonises the definition of trade secret following existing internationally binding standards and provides useful common definition for its application.[110] Innovations that will be particularly affected include manufacturing methods and processes; business strategies unique to a company, marketing techniques.

[108] It should be noted that while TSD forms an integral part of the generally applicable legal framework, its applicability in respect of certain specific LSPs may be limited.

[109] See also Recital 1 of TSD.

[110] According to Recital 2 of the Directive: "The differences in legal protection of trade secrets provided for by the Member States imply that trade secrets do not enjoy an equivalent level of protection throughout the Union, thus

Hence, in order to be granted protection by the TSD, the information will be considered a 'trade secret' if (1) it is secret, i.e. not generally known or readily accessible to people in the broader community than the ones who typically deal with that information, (2) it has an actual or potential commercial value because it is secret, and (3) it has been subject to *reasonable* steps under the circumstances to keep it secret.[111] It is also worth noting that "experience and skills gained by employees in the normal course of their employment", are expressly excluded from the said definition.[112]

From a methodological point of view, the TSD does not provide for a set category or definite content amounting to a trade secret; merely, it rests on a set of basic requirements.[113] The question of the actual ownership of a particular trade secret is dealt with by TSD in a similar way as in the case of other intellectual property (e.g. patents, designs, etc.): TSD provides that the person entitled to the protection of the trade secret is not only the person who lawfully controls a trade secret, but also their licensee or contractual partner.[114] In this respect, the TSD also contains provisions concerning lawful and unlawful acquisition, use and disclosure of trade secrets.[115]

It is worth emphasising that the TSD is likely to provide an additional layer of protection for innovations of numerous organisations, including CREATE-IoT LSP consortia. While Art. 2 can be seen as providing sufficient guidance in respect of the *quality of secret* and *commercial value*, it offers very little guidance on the requirement of *reasonable steps to keep it secret*. It is likely that the assessment of *reasonableness*[116] will be further developed by case law. However, it can be claimed that this requirement is not always taken seriously by international businesses. Therefore, it is advisable that organisations (including CREATE-IoT LSP consortia) introduce measures to show "reasonable steps" are in place to protect processes, formulas, recipes, manuals, software and data at all levels. This may include revision of security management, appropriate marking of documents, as well as ensuring suitable contractual confidentiality and security obligations.

9.4.2 Remedies

In accordance with the legal framework provided by TSD, Member States will have to provide measures, procedures and solutions necessary to ensure the availability of civil redress against the illegal acquisition, use and disclosure of trade secrets.[117] TSD offers a wide range of solutions for enforcing trade secret rights against infringers, while ensuring proportionality between the violation and the sanction.[118] Available remedies include provisional and precautionary measure,[119] final injunctions as well as corrective measures.[120]

Namely, if a trade secret is used, copied or disclosed without permission by someone who has acquired it unlawfully, broken an agreement that limits its use, or breached a confidentiality agreement (such as a Non-Disclosure Agreement), the remedies may include[121] (i) injunctions to prevent further use or disclosure of the information, (ii) court orders prohibiting infringing goods

leading to fragmentation of the internal market in this area and a weakening of the overall deterrent effect of the relevant rules".

[111] Article 2 (1) of TSD.
[112] Recital 14 of TSD.
[113] Article 2 of TSD.
[114] Article 2 (2) of TSD.
[115] Article 3 and Article 4 of TSD.
[116] C.f. requirement of *appropriateness* under GDPR.
[117] Article 6 of TSD.
[118] Article 7 of TSD.
[119] Article 10 and 11 of TSD.
[120] Article 12 to 15 of TSD.
[121] Article 10 to 15 of TSD.

from being produced, marketed, sold, stored, imported or exported, (iii) seizure or delivery up of infringing goods (including imported goods) to stop them being circulated in the market, (iv) delivery up of electronic information, even where it is part of a larger file or materials, (v) court orders compelling product recalls, (vi) orders requiring alteration to the products, so that infringing characteristics are removed, including software and electronic data such as customer databases, (vii) destruction of infringing goods, and (viii) publication of judgements in appropriate cases. In addition, the infringing party may be ordered to pay damages fees.

9.5 Product Liability Directive

Together with personal data protection, consumers' safety presents one of the main challenges of recent IoT developments, as identified by EC, among others [1]. In general, the domain of consumer protection is regulated by the Product Liability Directive (PLD) [12], which is also applicable in respect of IoT products, unless specific sectorial regulations apply

Despite the resulting consumer benefits arising within the IoT environment in rendering, for example, consumer lives more comfortable (such as in the case of remotely operated domestic appliances, for example), sustainable (e.g. smart meters) or safer (e.g. autonomous cars), there is a series associated risks. For example, there is an increased likelihood that third parties' access IoT devices and services illicitly to tamper with them and intentionally cause nuisance or harm to the consumer or that the harm suffered by consumers has a domino effect in society at large. Under this perspective, questions such as who actually caused the damage or who is ultimately liable for the damage become quite complicated to answer convinvingly.

The discussion below outlines the main challenges posed by the concepts embedded in the current PLD in relation to IoT. In doing so, it also puts forward specific amendments to the framework ensuring its applicability to IoT and guaranteeing appropriate levels of consumers' protection in this context.

9.5.1 Outdated definitions of Product, Defect and Damage

The definition of Product

IoT ecosystems are extensive and consist of a range of elements, including not only hardware devices and their parts, but also software therein and networks facilitating communication between them. As Article 2 of the PLD clearly states that the PLD only covers movables, (hence only tangible goods), its applicability in respect of a range of IoT products is relatively uncertain. If interpreted in respect of IoT, the said provision may result in only being applicable to tangible hardware elements. Hence, it may follow that consumers are not offered an adequate level of legal protection with respect to other intangible elements forming an equally essential part of the IoT ecosystem. However, due to the complex nature of many IoT devices, it is argued that determining what aspects fall within and outside the scope of PLD would be reasonably difficult. Ultimately, such situation is not desired from the perspective of legal certainty.

Reflecting upon this fact, it has to be noted that in the context of today's consumer market, *tangibility* is no longer a justified requirement to condition products upon, as can be illustrated through the example of software.

The reasoning of the European Court of Justice for choosing the quality of tangibility to describe the products which would fall within the scope of the PLD can be explained as follows.

As services consist of an activity, often resulting from a specific skill or knowledge,[122] the services themselves and their outcomes are difficult to describe objectively. Therefore,

[122] Case C-137/9, *Josemans v. Burgemeester van Maastricht*, 16 December 2010 , para. 48, 49.

warranties are normally not provided in relation to services or only in ambiguous wording such as "*the services will be provided in a good and professional way*" or "*on a best effort basis*".

Contrary thereto, tangible products can be perceived and as such, their material(s), functionalities and other qualities can be described objectively. As a result, specific warranties regarding quality, functionality and other characteristics can be given. Clearly, this makes products more compatible for any fixed product liability framework, such as the one laid down in the PLD.

This is where the condition of tangibility unintendedly excavates the intended effects of the PLD. In particular, it is a well-known fact that software developers and vendors consciously describe their software and the provision thereof as a service, to exempt themselves from product liability. This approach is seen as unacceptable as software can, just like tangible products and in contrast to services, often be described in detail, which *does* make it possible to make certain warranties in relation to its functionalities, capacities and interoperability.[123] In addition to this, the provision of software often cannot really be described as an activity. Once the program is available its availability and quality will not be dependent on its repetitive provision by a particular person to each separate user; each party simply receives a copy of or has access to *the same* software [20].[124]

The abovementioned is also confirmed by both the essential nature test and the dominant thrust analysis, which have been used in the Anglo-American context to assess whether software must be seen/treated as a product or a service. According to those theories, the software must be seen as a product if the essence of the contract concerns the delivery of a product, hence, is focussed on the functionalities of the software instead of the skills of the software developer. This seems to be often so in case of "standard" software, developed for a larger audience, which is not tailored [21][22].

The definition of Defect

Even if software is not seen as a product, the current definition of *defectiveness* in the Directive would still be problematic, because it focusses on the safety which a person (meaning the audience at large) is entitled to *expect* from a product.

First of all, because consumer demand has been and is nurtured and steered by software developers and vendors for decades, the expectation of quality in relation to software of the average consumer is relatively low. Consumers have been taught that software will always contain certain flaws and risks which will eventually (hopefully) be eliminated through available updates and patches. Moreover, they are steered to prefer (cheap) flawed software with new functionalities and features over safe(r) software, which is often more expensive and takes a longer time to market.

Secondly, due to a constant information asymmetry, partially sustained by the industry itself, and complexity of many software products and IoT devices, it is difficult for a consumer to decide whether such product or device is actually functioning as promised.[125]

Thirdly, the capability of IoT devices to act autonomously makes it very hard to describe or foresee what kind of safety level they have, let alone what type of safety level people are entitled to expect [23].

[123] This is to an extent also acknowledged in Directive 2011/83/EU on consumer rights of 25 October 2011. According to Recital 19 thereof, contracts by means of which intangible software is supplied, should neither be classified as contracts of services, nor as contracts of sale. In addition, these contracts have to comply with several information conditions, such as the provision of a description of the functionalities of the software. See also [23]

[124] The fact that this may lead to the conclusion that software is a product rather that a service, was also acknowledged in Case C-128/11, *UsedSoft v. Oracle*, 3 July 2012, paras. 45 *et seq* and 73 *et seq*.

[125] In fact, the Dutch Consumer Authority initiated a (now pending) law suit against Samsung in relation to information asymmetry regarding updates.

Usually, these questions will be (partially) answered through the assessment of the functionalities and features of a product. However, in the case of autonomous products, this might not be sufficient or too complex because the manner of execution of such functionalities and features can depend on decisions autonomously made by the device itself or by other (unforeseen) third parties and/or devices which are unpredictable to a certain extent. Answering these questions will become even harder, in case a device has a self-learning or adaptive ability, as it may then also be unpredictable what kind of functionalities and features a IoT device has and/or may have in the future.

The definition of Damage

Finally, the challenge to be addressed in respect of the current definition of *damage* is, most importantly, that it focusses on damage caused by death, injury or damage to any other item of property other than the product itself, for as much as EUR 500. Damage in relation to defective software and IoT devices is however, mostly financial.[126] However, the estimate of damages resulting from incidents occurring in hyper-connected environments is highly challenging, also, for courts, as this is linked to the harm[127] caused, which is briefly touched upon later in relation to the cloud environment under the analysis to follow.

Furthermore, the definition is based upon the presumption that damage to the product itself does not have to be recoverable under the Directive itself, as this type of damage can be taken care of by contractual clauses and contract law. This presumption clearly cannot apply in relation to software and IoT devices, as the complementary value of contract clauses in these markets is null. In general, software developers and vendors have a stable market position, which often results in standard contracts wherein consumer rights and warranties are limited to a bare minimum and other clauses further excavate the position of the consumer.[128] Taking into account the critical role software and IoT devices play and will play in our daily lives, this is unacceptable.

9.5.2 The principle of strict liability

The principle of strict liability is one of the most important features of the PLD, as it limits the burden of proof on the consumer to a bare minimum. As emphasized above, this is quintessential in a market such as the one assessed here, where one cannot count on the complementary function of contract clauses and contract law [22]. Unfortunately, because of the characteristics of IoT devices, this anticipated effect of the principle of strict liability is minimized.

First of all, it can be expected that the burden of proof as described in Article 4 of the PLD, is still too heavy for the consumer. This is so because the IoT can generally be defined as a highly complex supply chain which links an unlimited number of different things to each other, while they operate through different infrastructures in different supply chain layers.

Assuming the consumer is positioned entirely downstream of this supply chain it is evident that, before an IoT device is even delivered to him, its assembly and functioning depend on the vast upstream multi-dimensional web of different hardware and software components and on one or more digital networks, all provided by different parties.

Furthermore, IoT devices, on their own account, can be also defined as highly complex value chains, linking different hardware and software components together, communicating with one

[126] For example, consider loss of or unauthorized disclosure of data and the question of how will that damage be qualified and quantified.

[127] Note that the perceptions associated to harm vary across common law and civil law jurisdictions.

[128] Consider clauses limiting the time to raise a complaint, clauses which give a very broad meaning to force majeure, unilaterally changeable clauses, exclusion of assets such as data from warranties and liabilities, poor service levels, difficult to read clauses, difficult complaint processes, no contact details provided or accessible, poor communication through third party support desks.

or more networks and other devices. As a result, a consumer not always has a good and complete understanding of what a device does, how it works and more importantly, what *more* a device *can* do and how it *then* works. This lack of insights might result in a situation where damage is caused, but the consumer does not even know-how and by what.

In both cases, this generally means: the more parties involved, the harder it will be to trace down and prove (a) the defect (and optionally, its cause) and (b) a causal relationship between the defect and the damage suffered.

Secondly, the State-of-the-art exoneration in Article 7 (e) could undermine the principle of strict liability. This exoneration has been a topic of discussion for a long time, also in relation to "regular" standalone products, as some authorities believe that the risks of new innovations should be borne by the parties producing them as they are the ones (a) with the most knowledge about the product and its risks and (b) who capitalize the innovation.

In addition, the State-of-the-art level can be misused, as it can, to a certain extent, be determined and held at a certain level by the industry itself through fenced of R&D activities. Namely, as the results of these activities are not available to competitors or any other party in the market, they can very well not form part of the State-of-the-art level. In this case, Article 7 (e) would apply, which can give companies immunity when they use these results.

A third clause which may cause problems in relation to the principle of strict liability is Article 8 (2), as the responsibility for the quality of the software often is gradually shifted to the consumer to a certain extent, by obliging the consumer to timely download/deploy updates and patches.

Lastly, another clause which could unjustly limit the principle of strict liability could be seen in Article 11. Although a limitation period of ten years sounds very reasonable, it is still designed for non-connected products which have a certain quality which slowly diminishes due to wear and tear.[129] In contrast thereto, software and IoT devices characterize themselves through the ability to change and improve through the years with the help of updates and other solutions, which cycle can go on perpetually. In that context, the question is whether the period of ten years is still reasonable or whether it is actually too short.

[129] The occurrence of newer, better products is already dealt with in article 6 (2) of PLD.