CREATE-IoT

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

European Large-Scale Pilots Programme

CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT

H2020 – CREATE-IoT Project

Deliverable 05.05

Legal IoT Framework (Initial)

Revision : 1.0
Due date : 31-12-2017 (m12)
Actual submission date : 29-12-2017
Lead partner : AL

European Commission

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

Summary					
No and name	**D05.05: Legal IoT Framework (Initial)**				
Status	Released	**Due**	m12	**Date**	31-12-2017
Authors	Arthur van der Wees (AL), Dimitra Stefanatou (AL), Jiri Svorc (AL), Marieke van den Ham (AL), Ovidiu Vermesan (SINTEF), Pasquale Annicchino (MI), Sebastien Ziegler (MI), Lucio Scudiero (AS)				
Editors	Arthur van der Wees (AL), Jiri Svorc (AL)				
DoW	The present document constitutes the initial report describing the main regulatory and other legal ingredients of Internet of Things (IoT), large-scale pilots (LSPs) and similar IoT ecosystems, falling under Task 05.03: Legal support, accountability and liability. The task focuses 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. This task will cover the issues of product liability, safety, security, net neutrality and (other) horizontal or vertical specific risks and compliance matters and liabilities.				
Comments					

Document history			
Rev.	**Date**	**Author**	**Description**
0.00	17-11-2017	AL	Template
0.01	24-11-2017	AL	Initial input under Chapters 5 and 6
0.02	28-11-2017	AL	Initial input under Chapters 3 and 9
0.03	01-12-2017	AL	Initial input under Chapters 7 and 2
0.04	08-12-2017	AL	Input under Introduction and editing Chapters 5, 6, 7
0.05	12-12-2017	AS, MI	Input under Chapters 4 and 8
0.06	14-12-2017	AL	Editing Introduction and Chapter 6
0.07	18-12-2017	AL	Editing Chapter 1 (Executive Summary) and Chapter 8
0.08	18-12-2017	SINTEF	Input for Section 2.3 and update illustrations
0.09	29-12-2017	AL	Editing Chapter 11 and addressing reviewer's comments
1.00	29-12-2017	SINTEF	Final version

Table of contents

1. EXECUTIVE SUMMARY

Taking into account both the objectives of "Work Package 05: IoT Policy Framework – Trusted, Safe and Legal Environment for IoT" as well as the scope of the five large-scale pilots (LSPs) projects currently funded by EC under the IoT European Large-Scale Pilots Programme [1], the present document forms the initial report producing an overview of the relevant generally applicable regulatory frameworks and legislation relevant for the IoT ecosystem under EU law.

Despite the indisputable benefits of IoT for individuals and society at large with respect to quality of life in general, hyper-connectivity entails a great deal of risks, thus, rendering issues of paramount importance within the rule of law, such as the attribution of liabilities, for example. In this context and bearing in mind the wide range of stakeholders present and participating in IoT ecosystems, the discussion presented in this document expands on certain regulatory aspects associated to (1) the protection of individuals acting under multiple personas (e.g. data subjects, consumers), (2) the protection of interests of organizations (e.g. trade secrets), (3) the protection of things and (4) the protection of infrastructure at a moment of transition of EU law.

In particular, the discussion focuses on specific requirements emerging from the General Data Protection Regulation (GDPR), Network Information Security Directive (NIS Directive), the second Payment Services Directive (PSD2), and the Trade Secrets Directive (TSD) that will become applicable in the course of 2018, as well as Product Liability Directive (PLD) currently under revision by the European Commission. Moreover, the discussion takes into consideration a number of legislative instruments currently worked on and negotiated by policy-makers, yet to take effect, namely the proposals for ePrivacy Regulation, the Regulation on a framework for the free flow of non-personal data in the EU, and the Cybersecurity Act. It is worth noting that although the outlined legal frameworks can be perceived as relevant for all LSPs, the degree of their relevance per individual LSP project may vary. For instance, the issue of protection of personal information and trade secrets is significantly more relevant for certain LSPs compared to others.

It can be argued that the outlined panorama of generally applicable legal frameworks relevant for all LSPs reflects the IoT regulatory ecosystem that is being created at the moment. Among others, the discussion shows that the existing EU legislation is being inevitably challenged by IoT (such as in the case of PLD), while the actual effectiveness of the forthcoming rules (e.g. GDPR) remains unknown. In addition, it is argued that contract law on its own cannot be relied upon in governing the emerging relationships between IoT stakeholders in a harmonized manner across EU Member States that allows stakeholders to reap the benefits of the Digital Single Market. The Legal IoT Framework discussed within the present deliverable document will be further developed and refined under the final deliverable version, namely under "D05.06 on Legal IoT Framework Evaluation and Final Legal IoT Framework" due in December 2019.

2. INTRODUCTION

2.1 Purpose and target group

IoT has facilitated the world's increasing digitisation and interconnectedness at an unprecedented pace. Naturally, this phenomenon brings about numerous innovative, societal and economic advantages, including more responsive services, shorter feedback loops, remote fixes, greater convenience, decision making support, better allocation of resources, verification of behaviour, for example for insurance purposes, or the remote control of services [1]. However, the fact that the internet enables the connection and communication between various elements and endpoints of the connected ecosystem also accounts for a great deal of potential risks which are just as significant, notably in the domains of liability, security, and data protection. Thus, these developments have created a series of challenges for regulators and policy makers to address in achieving the creation of an innovative yet user-centric environment. For instance, it must not be overlooked that the connected ecosystem has enabled an effective deployment of cyber-attacks[1] aiming to compromise proper functioning of network infrastructures and connected IoT devices, as well as facilitating personal data breach incidents.

The regulation of technological developments is at the heart of political and regulatory developments at global scale.[2] Some authorities take a firm position on the matter stating that "*[w]e are now in a position in the digital age where technology has outstripped our legal framework.*"[3] Similarly, it has been stated in Europe that "*[w]e need a single rule book for the Internet of Things in Europe, capable to properly address new challenges raised by the technology. This includes data protection, safety and liability rules, including the emerging issues of data ownership, rules on access and re-use of non-personal data in an industrial context, just to mention a few.*"[4]

Numerous authorities have also identified and validated numerous legal risks and challenges posed by IoT developments.

Among others, the European Commission (EC) has started addressing questions of safety and liability in relation to IoT, possible obstacles to data flow and access to data, and users' privacy and data protection [3]. At the same time, the EC has been dealing with policy-related issues such as the risk of national fragmentation [4],[5] industrial fragmentation [3],[6] the risk of being

[1] See also discussion under Deliverable 05.01 on "IoT Policy Framework", online at: https://european-iot-pilots.eu/wp-content/uploads/2017/10/D05_01_WP05_H2020_CREATE-IoT_Final.pdf

[2] Ibid.

[3] Navy Adm. Mike Rogers, commander of U.S. Cyber Command and director of the National Security Agency speaking at Aspen Security Forum on 22 July 2017; https://www.defense.gov/News/Article/Article/1255194/pace-of-change-complicates-signals-intelligence-world-nsa-chief-says/

[4] Gunther Oettinger, Keynote Speech at the Closing Plenary session of Net Futures 2016, Brussels, available at: https://ec.europa.eu/commission/commissioners/2014-2019/oettinger/announcements/keynote-speech-closing-plenary-session-net-futures-2016-brussels_en

[5] European Commission, "A Digital Single Market for Europe", 2015 [4]: "The scale provided by a DSM is also important for the deployment of high-speed infrastructure to enable advanced digital services and the development and adoption of new technologies in Europe, such as the Internet of Things, big data analytics or cloud computing. Companies may refrain from investing in the deployment of these technologies if they have to use different costly specifications or have to invest in new infrastructure (e.g. cloud based data centres), as regards the transfer of data or cross-border service delivery, making it unprofitable to innovate".

locked in into proprietary ecosystems [3] and the lack of common standards and interoperability.[7] [8]

Given its position of a European independent personal data protection advisor, the Article 29 Working Party (A29 WP) has also voiced its opinion [5] concerning specifically privacy and security challenges posed by the IoT. The A29 WP has mainly been concerned with the lack of control and information asymmetry, quality of the user's consent, interferences derived from data and repurposing of original processing, intrusive bringing out of behaviour patterns and profiling, and limitations on the possibility to remain anonymous when using services.

In addition, while providing a list of examples of digital security incidents with physical consequences, the significance of security and privacy risks in relation to the IoT has recently also been noted [6] by the Organisation for Economic Co-operation and Development (OECD). In particular, the OECD has emphasised the challenges of comprehensive data collection, inference and the loss of control, transparency and purpose of data collection, raising individual awareness and promoting responsible use by organisations, and accountability and privacy risk management.

In this context, where existing legal and regulatory frameworks are being exposed to the complexity of the IoT, the potential of Digital Economy and the resulting benefits for the Digital Single Market (DSM) cannot be fully harvested. Moreover, Eurostat has identified numerous significant blocking factors hampering DSM; while identifying *security*, *personal data protection* and *compliance* as considerable blocking factors, EuroStat has identified organisations' and consumers' *insufficient knowledge* as the main blocking factor [7][8].

Aspiring to contribute to the increased awareness of legal issues related to DSM the present deliverable sheds light on the complex legal landscape underlying the creation and use of IoT across EU market. To this end and bearing in mind the overarching objectives of "Work Package 05: IoT Policy Framework - Trusted, Safe and Legal Environment for IoT", this deliverable document 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. Thus, it expands on concepts holding a key role within rule of law discussed under the lens of the currently adopted EU legislation, including the Payment Services Directive 2 (PSD2) [9], the General Data Protection Regulation (GDPR) [10], the Network Information Security Directive (NIS Directive) [11] and the Trade Secrets Directive (TSD) [12] that have all entered into force and will become applicable in the course of 2018. The present deliverable document, also, touches upon the related proposed legislation, namely, the draft ePrivacy Regulation [13], the draft proposal Regulation on a framework for the free flow of non-personal data in the EU [14], the Cybersecurity Act [15], while briefly referring to developments related to the review of the Product Liability Directive (PLD) [16]. The entire set of the adopted and presented relevant legislation is captured by Figure 1 below.

---

[6] Areas of application we see today for IoT include but are not limited to: multi-modal mobility and smart road infrastructure, smart agriculture and food traceability, smart assisted living and wellbeing, smart manufacturing, energy management at home and in buildings, worker safety, environmental monitoring and management, load-aware power generation and demand response, smart living environment, smart public safety, smart design, open platforms for the audio-visual industry.

[7] See also "AIOTI Recommendations for future collaborative work in the context of the Internet of Things Focus Area in Horizon 2020", online at: https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020.

[8] See also "Standards and Architecture for the IoT. A path for convergence? Main outputs from the Workshop on IoT Standardisation and Architecture", online at: https://ec.europa.eu/digital-single-market/en/news/standards-and-architecture-iot-path-convergence-main-outputs-workshop-iot-standardisation-and.

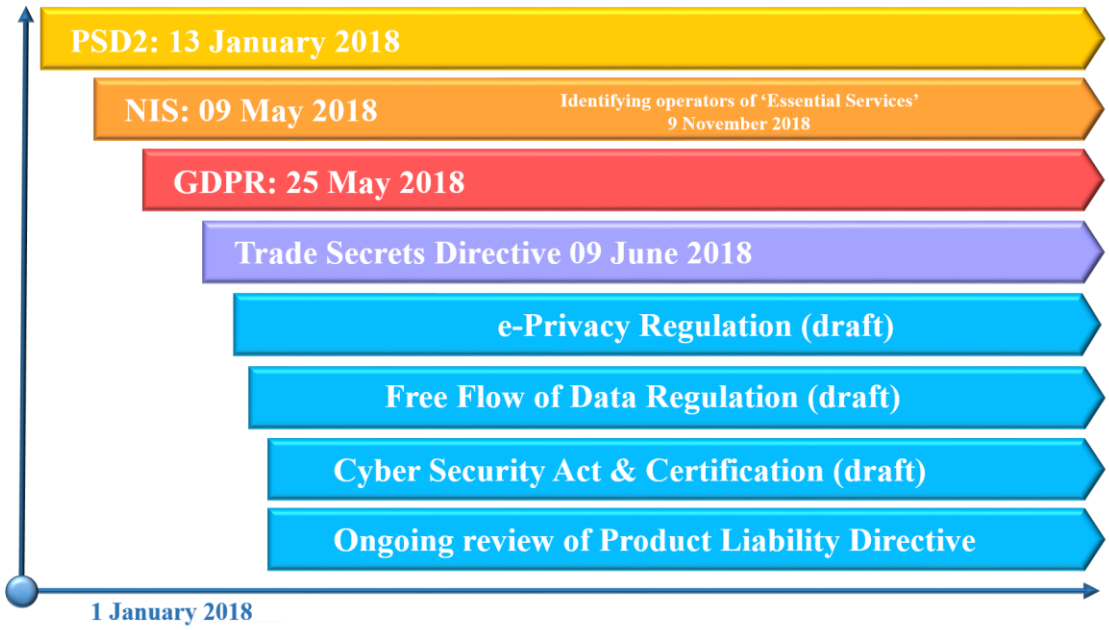

Figure 1: From 2018, Digital and Data become highly regulated domains

It should be noted that this document forms the initial report expanding on the main ingredients of the Legal IoT Framework and it will be further developed, elaborated upon and refined under the final deliverable version, namely, "D05.06 on Legal IoT Framework", which is due in December 2019 (month 36). Based on progress made in the course of the negotiation process within the EU institutions, the above stated instruments currently at the stage of legislative proposals will be further discussed under the final deliverable version.

By discussing the general legal frameworks relevant for all LSPs, the present document outlines the responsibilities of the various IoT stakeholders, as identified under "D05.01 on IoT Policy Framework"[9] regarding i) the protection of individuals acting under multiple personas (e.g. data subjects, consumers), ii) the protection of interests of organizations (e.g. trade secrets), iii) the protection of things and iv) the protection of infrastructure, as articulated under the general regulation applicable for all LSPs.

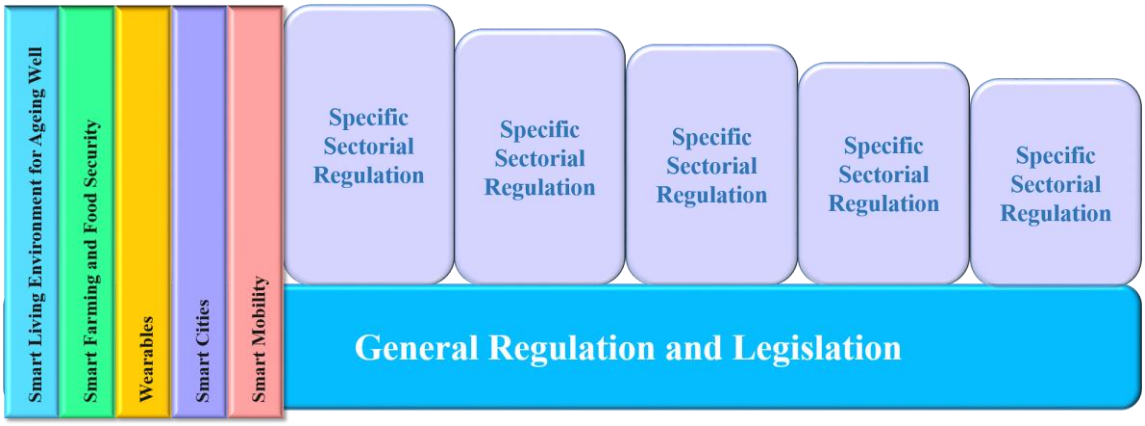

Figure 2: The mandatory domains of Rule of Law

There are, however, certain key 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

[9] See also discussion under Deliverable 05.01 on "IoT Policy Framework", online at: https://european-iot-pilots.eu/wp-content/uploads/2017/10/D05_01_WP05_H2020_CREATE-IoT_Final.pdf

institutions fall outside the scope of the above-mentioned Task 05.03. As far as the issue of net neutrality is concerned, there are no significant developments taking place at the moment at EU level,[10] 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.

Moreover, as illustrated in Figure 3, and same as it was the case for the other two deliverable documents produced so far under Work Package 5, namely, deliverable "D05.01 on IoT Policy Framework" and "D05.03 on IoT Data Value Chain Model"[11], the present document forms the outcome of the multidisciplinary expertise within the CREATE-IoT consortium. It is targeted not only at the CREATE-IoT consortium and the consortia of the five LSPs, but also at the broader community of IoT stakeholders.

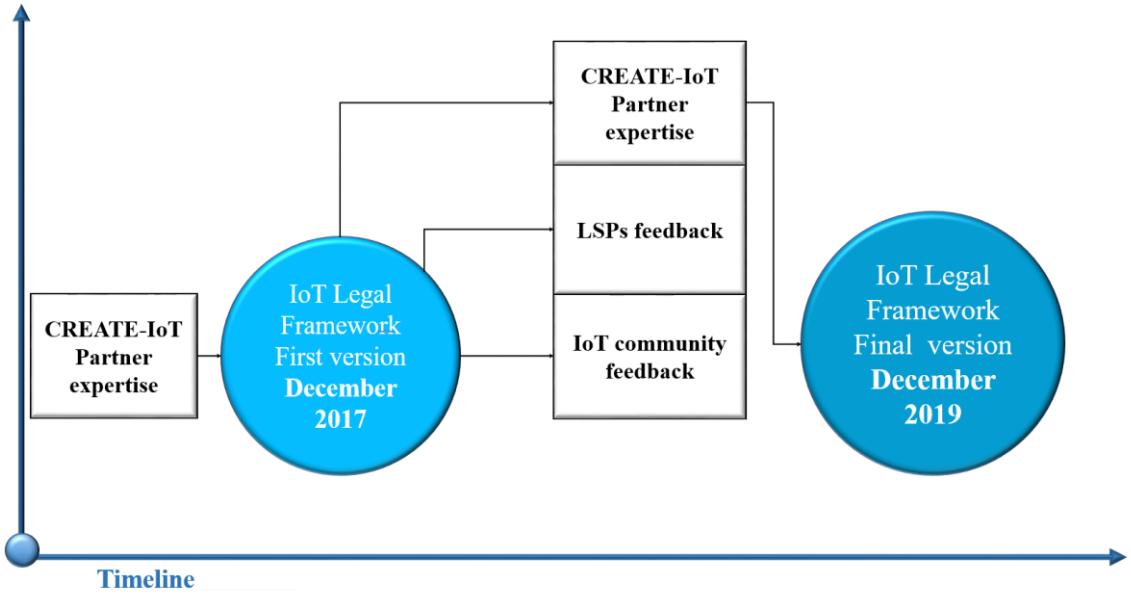

Figure 3: Relevance of Legal IoT Framework for various stakeholders

Furthermore, the work captured in the present deliverable partly links to the tasks associated with the role of "Activity Group 5 on Security and Privacy" (AG05) composed of project partners of CREATE-IoT Project, as well as of partners representing the above mentioned five LSPs. AG05 is open for all consortium partners of each of the five LSPs and two coordination and support action projects within the IoT European Large-Scale Pilots Program. In this context, it is aimed that questions raised by the participating LSPs within AG05 in the course of CREATE-IoT project will be taken into account to the extent they relate to general legislation and, thus, are relevant for all LSPs under the final version of the present deliverable.

2.2 Contributions of partners

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

[10] Note, however, that at the time of drafting of this document there are developments regarding net neutrality in the United States, as the US Federal Communications Commission voted in favour of repealing the current regulatory framework that aimed at ensuring a free and open internet.

[11] 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

AL contributed to the development of an IoT Policy framework in line with the overarching objectives of Work Package 05 aiming at the creation of a Trusted, Safe and Legal Environment for IoT. Due to AL long-term experience in the field of technology law and related aspects, AL has been ideally positioned to lead, co-author as well as edit the present deliverable. In addition, AL has contributed by providing a thorough analysis and evaluation of legal frameworks relevant to the topics of Data control (Chapter 3), Cybersecurity and Resilience (Chapter 5), Consumers' safety (Chapter 6), Customer data (Chapter 7) and Chapter 9 providing a brief overview of Upcoming Regulation. It is emphasised that AL actively participates in discussions with the relevant policy-makers as well as consumer associations and has therefore been able to take into consideration their respective perspectives and concerns.

SINTEF worked on analysing the link with Nordic countries' legal initiatives in the area of IoT and aligned the activities with the LSPs and the relations to other activities in the project. At the same time, it has been able to align the activities 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) to be applicable in the course of 2018, which is highly relevant for the industry stakeholders with a role in the IoT ecosystem.

AS provided the discussion linked to the most relevant requirements set by the GDPR linked to scope of the LSPs and, while reflecting the human centric approach for the IoT ecosystem as embraced by Work Package 5 (Chapter 4).

Note that it is intended that the rest of the partners taking part with limited resources in the abovementioned Task 05.03, namely, GTO and TL, make use of the available resources for the effort required in view of the final version of this deliverable due in December 2019.

2.3 Relations to other activities in the project

The task addressing this delivery focuses 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 topics addressed by the legal support, accountability and liability activities are relevant for the main tasks falling under the scope of CREATE-IoT project. IoT devices collect information in different contexts and applications by involving different stakeholders and IoT platforms. Depending on criticality of the applications (safety critical, mission critical, etc.), accountability, liability and legal framework are part of the important 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, economical, 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 legal support, accountability and liability in the context of IoT European Large-Scale Pilots Programme provide a useful information platform to the LSPs projects in order 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 rethinking 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.

This work provides the basis for an analysis of the current gaps and the needed recommendations for legal, accountability and liability issues across IoT applications domains covered by the IoT European large-scale pilot projects, and contributes to the development of suitable emergence of best practices.

3. DATA CONTROL: AN ISSUE OF HORIZONTAL RELEVANCE

Through IoT products, systems and services, organizations create, collect, process, derive, archive and – ideally and to the extent permitted – delete large amounts of data. As part of this lifecycle[12] composed of different stages of processing, digital data is also transmitted, exchanged and processed in different ways at global scale. In this flux environment concepts like data ownership are highly relevant yet challenged as not being appropriate to capture the reality of data processing, while – conversely – other concepts linked, for instance, to data control, access, use and digital rights management have been gaining attention and – to an extent- embraced as preferable solutions [8].

In this context, the chapter below first sets the scene by giving an overview of the main considerations associated to ownership of data both personal and non-personal. Second, it briefly discusses the shortcomings of the existing ownership related legislation at EU level. Third, it touches upon the role of contracts and on the potential benefits resulting from the upcoming legislation. Note that although data ownership is not being addressed under a dedicated regulatory instrument, it forms rather an underlying issue relevant for all LSPs that it is gaining prominence due to the increasingly growing flows of data and the value assigned to data per se [8].

3.1 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 main triggers underlying the Free Flow of Data Initiative [4], while uncertainties linked to ownership of both personal and non-personal data have been identified as particularly relevant for the wide adoption of IoT solutions [3].

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, 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"[13], while the draft Regulation on the free flow of non-personal data [14] defines data falling under its scope as "data other than personal data"[14].

[12] 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

[13] See Article 4 (a) of GDPR.

[14] See Article 3 (a) of the Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union.

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 [17] 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 object of ownership, as there are other questions of legal relevance, including, "*Who owns the data or it is not feasible to retrieve the data?*" [8]

3.2 The regulatory challenges

The questions on data ownership regarding personal data obviously differ from those concerning data ownership with respect to non-personal data.

As far as personal data are concerned, it could be argued that data, in essence, form an aspect of selfhood and, thus, ownership would presume some sort of alienation between the individual an and the information linked to him/her. It is not, therefore, obvious that "ownership" when being understood as a form of property status, can be conceived as such in relation to personal data. Notably, the General Data Protection Regulation abstains from any reference to the notion of ownership embracing, instead, the concept of control.

As far as non-personal data are concerned data ownership -especially in the IoT environment- legitimately raise the question on how to assign ownership when there is a complex chain of actors involved in the delivery of products and/or services and when there is, also, big amount of machine generated data produced. It becomes, thus, even more unclear to determine the entity owning the machine generated data or whether the concept of ownership remains in this case relevant at all.

Overall, ownership of digital data in general is basically not possible. The current framework of copyright regulations is not particularly designed for digital assets including data, while the redesign thereof in the early 90s regarding software (Directive 91/250/EEC) has not proved to be a transparent framework that resolves discussions and disputes on ownership as well. The Database Directive (96/9/EC) [18] dating from 1996 also has lost its effectiveness, as the major requirement for protection thereunder is a substantial investment to build the relevant database, where such databases nowadays can be built and used for a fraction of the cost. The threshold to be eligible for protection thereunder is not met anymore, and lowing the threshold would even increase and not resolve the discussion on data ownership either.

Nevertheless, certain scholars claim that the Court of Justice of the European Union (CJEU) paved the ground for a discussion on ownership in intangible assets in its *UsedSoft* judgment issued on 3 July 2012 (case C-128/11). The decision implies that there is a specific ownership right assigned to intangible goods, including software downloaded from the internet. Despite the value of such decision, the questions concerning ownership of data still remain.

3.3 Bridging the gaps

In the absence of a satisfactory answer on the topic of data ownership by the already implemented regulatory frameworks, valuable assistance is being provided by contract law.

From the customers and users perspective, the existing awareness, expertise and transparency of both such customers, users as well as vendor level as well as policy makers and authority level is generally not sufficient to provide actors in the data value chain with trust, predictability and legal certainty requiring in reality that each actor is in the position to assess, make informed decision and have reasonable access and use of IoT and related services [8].

The role of contracts, especially, with respect to transparency could become particularly critical in the context of the changing regulatory landscape to be further sketched by the discussion to follow. Nevertheless, actual contractual practices are highly diverse per product, cloud deployment model and service model as well per vendor and the (envisioned or actual) use of the customer and users thereof. In this context, actual contractual practices endorsed by IoT stakeholders may in reality create obstacles to data use, access, and in certain cases create data lock-in effects as well.

Furthermore, building on cloud computing technology the asymmetry of powers between cloud service providers and cloud customers is, also, reflected upon the relationships deployed within the IoT ecosystem; vendors may, therefore, have a completely different opinion on or perception of data ownership than its customers and users, whether being SMEs or not, which has an impact on the related contractual practices.

The upcoming Trade Secret Directive (COM/2013/0813) that is being adopted and will be discussed later under this deliverable document, may resolve a minor part of the data ownership discussion, but in such case the protected data thereunder needs to remain secret and not generally known or readily accessible to third parties. In hyper-connected ecosystems where data travels and data can change from legal characteristics and purpose of travelling and being processed at any time, this will be quite challenging. Owning data is just very difficult, as one would like, or need to, share such data, have it processed and transferred. On the other hand, domain names and related domain name rights have been designed by law not to use the concept of ownership; it uses the concept of holdership of a domain name, which has proven to work quite well.

Overall, having a discussion on data control, instead, of data ownership would be a way to address certain of the questions raised in a pragmatic manner.

4. DATA PROCESSING AND DATA PROTECTION

As the IoT becomes more widespread consumers and authorities demand regulatory frameworks that ensure the protection of personal data. Protection of personal data does not only constitute a relevant issue for individuals, possibly, acting in their capacity as consumers, but also for European Single Market at large. As previously mentioned, Personal data protection has been identified as one of the main blockers 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; on the contrary, it is established under the Charter of Fundamental Rights of the EU, as well as under the Treaty of the Functioning of the EU. The discussion below focuses on those aspects that are considered to be of direct relevance for the LSPs in the context of the human centric approach put forward under Deliverable D05.01 on "IoT Policy Framework"[16], which was due in September 2017.

4.1 Informed consent requirements

One of the major aspects on GDPR compliance strategies concerns consent. Consent is already, under the Directive, 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 to withhold it. The GDPR retains the concepts 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".[17] 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, 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".[18] 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;[19] 2) there is a clear imbalance between the data subject and the controller.[20] Recital 43 also clarifies that

[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] Article 4 (11) of GDPR.

[18] Recital 171 of GDPR.

[19] Recital 42 of GDPR.

[20] Recital 43 of GDPR.

consent is presumed not to be freely given if separate consents are not allowed for different data processing operations when such separate consents would be appropriate. Article 7 (4) provides additional circumstances to take into account when evaluating consent;[21]

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.[22]

The collection of consent also has to respond to certain 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 [19] at the moment that the present deliverable document is being drafted.

4.2 Accountability measures: technical and organizational

The GDPR also introduces legal accountability obligations. The principle of accountability in data protection law was already codified in 1908 in the OECD Guidelines. 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 shall be reviewed and updated where necessary*".[23] 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 will 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

[21] 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".

[22] Article 7 (3) of GDPR.

[23] Article 24 of GDPR.

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.

4.3 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[24], profiling activities[25] or cross border data transfer[26]. 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 worth also noticing that Article 9 (2) provides for exceptions to restrictions including where processing is necessary for various medical assessment and where the processing is necessary for reasons of public interest in public health. Article 9 (4) of the GDPR allows Member States to maintain or impose further conditions (including limitations) to this respect.

[24] Article 9 (2) (a) of GDPR.

[25] Article 22 (2) (c) of GDPR.

[26] Article 49 (1) (a) of GDPR.

5. CYBERSECURITY AND RESILIENCE

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

5.1 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 [20], a vast majority of them believe that the risk of becoming a victim of cybercrime is increasing [21]. In this regard, it is propitious that EU law makers have begun addressing the issue of cybersecurity, namely with the introduction of 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 [22]. Recognising the important 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 [23].[27] In doing so, it aims to put forward measures promoting a culture of risk management and preventing or mitigating the effects of the most serious incidents capable of having a significant disruptive effect 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.[28]

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 [22].

5.2 Scope and definitions

Aiming to achieve high common level security and improve functioning of the internal market, NIS Directive puts into place measures concerning security of *network and information systems*, encompassing a wide domain of network, infrastructure, devices as well as data.[29] By doing so, 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.

[27] Recital 1 of NIS Directive.

[28] Recital 2 of NIS Directive.

[29] Article 4 (1) of NIS Directive.

To promote a culture of risk management and ensure that the most serious incidents are reported [22],[30] NIS Directive stipulates that specific security and incident notification requirements apply namely to *operators of essential services*[31] and *digital service providers*.[32] 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) [23], 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, please refer to Section 5.3).

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 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.[33]

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 [24]) which is either (a) an online marketplace, (b) online search engine, or (c) a cloud computing service.[34] While the Directive clearly states that hardware manufacturers and software developers should not be considered operators of essential services, nor digital service providers,[35] it contains a fairly 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'.[36]

Given the present fairly 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 in accordance with rationale of the Directive. Hence, it is suggested that applicability of the provisions of the Directive must be assessed primarily from the perspective of its rationale, rather than based on interpretation of individual provisions.

---

[30] Recital 4 of NIS Directive.

[31] Article 14 of NIS Directive.

[32] Article 16 of NIS Directive.

[33] Article 4 (4) of NIS Directive. In addition, Article 5 of NIS Directive stipulates that by 9 November 2018, member states should identify the operators of essential services with an establishment on their territory.

[34] Article 4 (5) of NIS Directive.

[35] Recital 50 of NIS Directive.

[36] Recital 17 of NIS Directive.

The presented argument is highly relevant with respect to IoT legal framework. IoT devices vary substantially in their capabilities. Therefore, when assessing applicability of NIS Directive to their activities, organisations must consider the risk of 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, as discussed in Section 5.1.

5.3 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 4 illustrates the "landscape" as set out by NIS Directive, as well as relations between individual stakeholders involved.

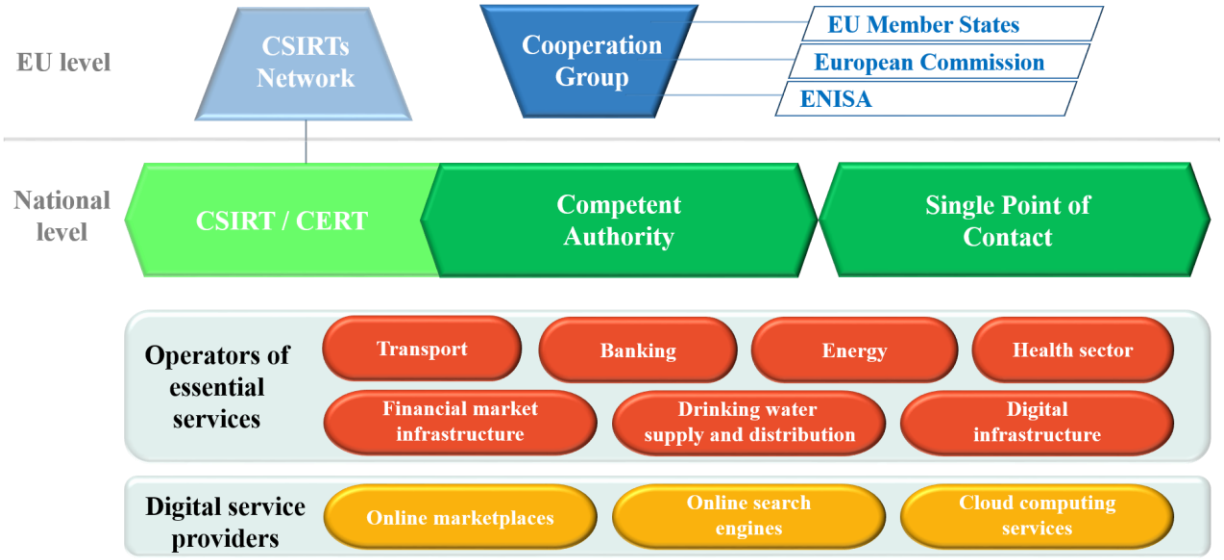

Figure 4: Overview of NIS Directive Stakeholders

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).[37] 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.[38] 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.[39]

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)

[37] Article 11 of NIS Directive.

[38] Article 8 (2) of NIS Directive.

[39] Article 47 of NIS Directive.

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.[40]

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.[41] 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.[42]

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 CSIRTs.[43] 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,[44] 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.[45] 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.[46]

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

[40] Annex I, Article 2 of NIS Directive.

[41] Article 12 of NIS Directive.

[42] Recital 40 of NIS Directive.

[43] Article 8 (4) and (6) of NIS Directive.

[44] For example, please refer to Article 5 (2) of GDPR

[45] Article 14 (1) and 16 (1) of NIS Directive.

[46] Article 14 (2) and 16 (2) of NIS Directive.

incident.[47] In a similar manner, 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.[48] 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.[49] NIS Directive also provides that the competent authority or the CSIRT may inform the public about individual incidents,[50] however, in doing so the competent 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.[51]

[47] Article 14 of NIS Directive.

[48] Article 16 of NIS Directive.

[49] Article 14 (5) of NIS Directive.

[50] Article 14 (6) of NIS Directive.

[51] Recital 59 of NIS Directive.

6. CONSUMERS' SAFETY

Together with personal data protection, consumers' safety presents one of the main challenges of recent IoT developments, as identified by EC, among others [3]. In general, the domain of consumer protection is regulated by the Product Liability Directive (PLD) [16], 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 in order 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 in a convincing manner.

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.

6.1 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 fairly 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 adequate level of legal protection with repsect to other intanginble elements forming an equally essential part of the IoT ecosystem. However, due to the complex nature of many IoT devices, it is argued that detemining what aspects fall within and outside the scope of PLD would be fairly 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 chosing 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 certain skill or knowledge,[52] the services themselves and their outcomes are difficult to describe objectively. Therefore, 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

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

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 tangibilty 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 serivces, often be described in detail, which *does* make it possible to make certain warranties in relation to its functionalities, capacities and interoperability.[53] 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 is not dependent on its repetetive provision by a certain person to each separate user; each party simply receives a copy of or has access to *the same* software [25].[54]

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, 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 developper. This seems to be often so in case of 'standard' software, developped for a larger audience, which is not tailored [26][27].

The definition of Defect

Even if software would be 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, due to the fact that 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.[55]

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 kind of safety level people are entitled to expect [28].

Normally, 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,

[53] 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 [28]

[54] 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*.

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

as it may then even 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.[56] 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[57] 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 very strong 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.[58] Taking into account the important role software and IoT devices play and will play in our daily lives, this is unacceptable.

6.2 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 [27]. 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 completely downstream of this supply chain it is very clear 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 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 the situation where damage is caused, but the consumer does not even know how and by what.

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

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

[58] 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.

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) 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 are of the opinion 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 research and development 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 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.[59] 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.

6.3 Paving the way forward

As the EC has also become aware of certain possible gaps between the legal situations PLD is applicable to and the current challenges, it initiated an evaluation of the PLD, with a particular consideration of the new technological developments.[60] As part of the evaluation, the EC launched a public consultation in 2017 to assess the relevance and adequacy of the Directive in the current market and society.[61] 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, Product Liability Conference was held in October 2017 to discuss the preliminary results of the evaluation of the PLD [30].

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

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

[60] 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/.

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

any alterations to the PLD would be premature, as the area of technological changes is still moving at a fast pace and a lot new technologies are not on the market yet. As the PLD's objective is first and foremost the protection of consumers, these arguments cannot be taken seriously. It is unacceptable to put the risks of these aspects of (new) technologies, which are for 100% in the hands of industry itself, upon 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.

7. CUSTOMER DATA

The widespread, accessibility and usability of 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 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 [9] 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.[62]

7.1 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 applicable regulatory framework for the payments market [31]. 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 chosen 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.[63] It should be noted that the topics of transparency (and inclusion) and security are also key in the context of IoT. Therefore, they are discussed in this Chapter: Section 7.2 focuses on the question of transparency and inclusion of third party providers, while Section 7.3 discusses the Directive's strong customer authentication requirements (i.e. security).

7.2 Third party payment services

Third party service providers (TPPs) introduce and provide innovative payment solutions.[64] 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'

[62] 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.

[63] Recital 5 and 33 of PSD2

[64] 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.

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.

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 5.

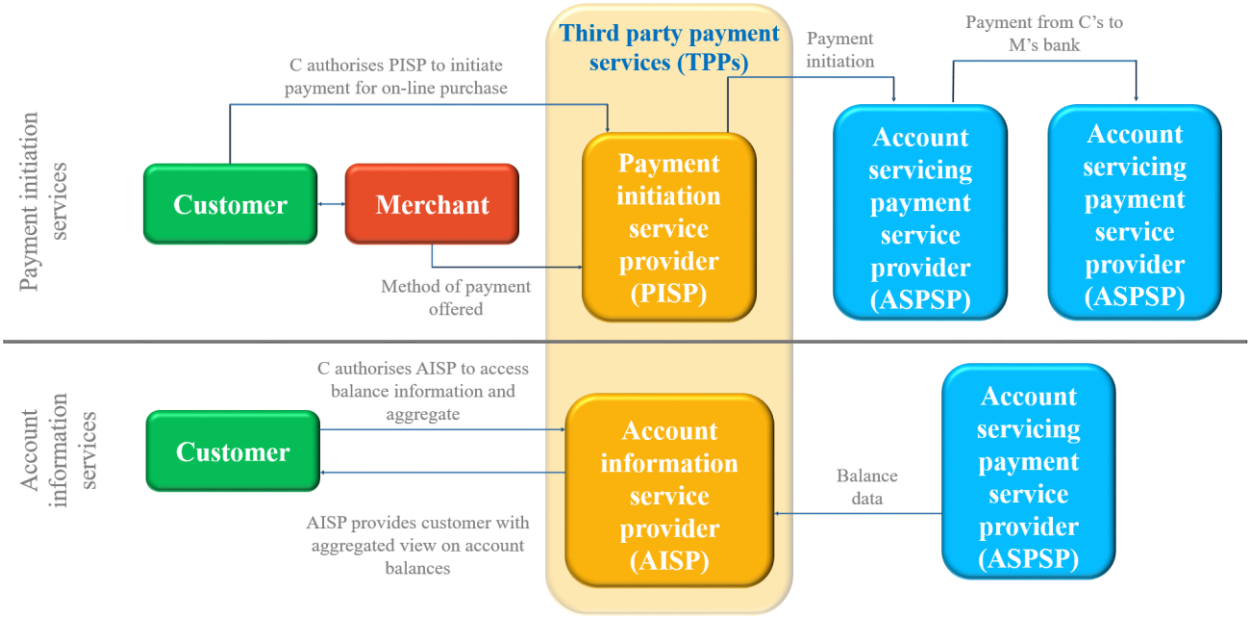

Figure 5: PSD 2 Stakeholdrs and Flows

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 transmits 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 provision of the initiation service.[65] This way ASPSPs cannot force PISPs to agree 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 accounts

[65] Article 66 (5) of PSD2.

in order 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.[66]

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 introduce innovative solutions by ASPSPs being prevented from putting up barriers and stifling their role, as illustrated, for example, in Figure 6.

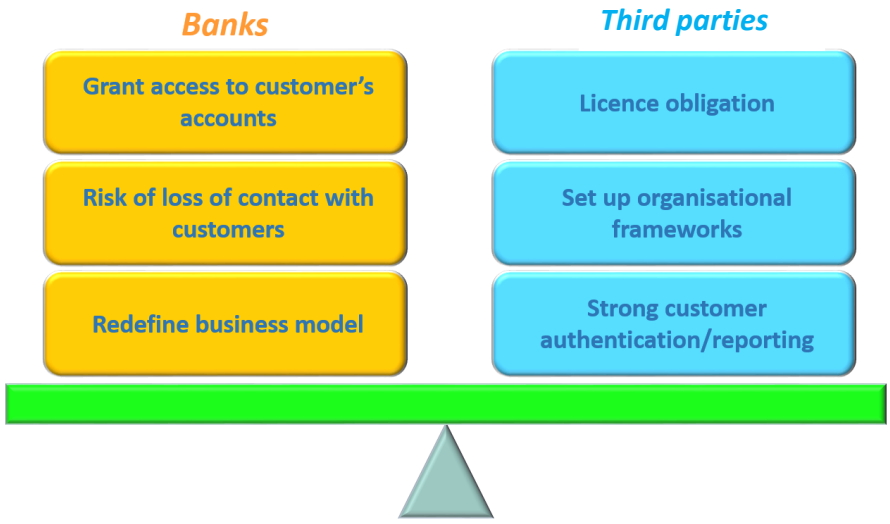

Figure 6: PSD2 – A new level playing field for banks and third party organisations

While the Directive requires banks to "take down" 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.[67] They are also required to hold professional indemnity insurance of a comparable guarantee in order to ensure that they are able to meet liabilities arising in relation to their activities.[68] 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.[69]

Because AISPs are TPPs, just like PISPs, some of the provisions applicable to them are similar to those applicable to PISPs. First, 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.[70] Secondly, under PSD2, customers obtain a right to use AISPs in online transactions.[71] 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

[66] Article 35 of PSD2.

[67] Article 7 of PSD2.

[68] Article 10 of PSD2.

[69] Article 36 of PSD2.

[70] Article 67 of PSD2.

[71] Article 67 of PSD2.

exempt from authorisation, but are obliged to register. Although they are not subject to regulatory capital requirements, AISPs will be obliged to hold professional indemnity insurance or a comparable guarantee to ensure that they are able to meet liabilities arising in relation to their activities.

7.3 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: as discussed in Section 7.2, aside from the customer, merchant and the banking institution (ASPSP), the chain now also involves TPPs, namely PISPs and AISPs. This new setting and the respective legal framework is 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.[72] 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.[73] The Directive further grants a mandate to the European Banking Authority (EBA) to draft regulatory technical standards (RTS), including standards concerning strong consumer authentication.[74]

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.[75] 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). [76]

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.[77]

---

[72] Recital 30 of PSD2.

[73] Ibid.

[74] 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.

[75] Article 97 (1) of PSD2.

[76] Article 4 of PSD2.

[77] Article 97 (2) of PSD2.

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.[78] 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 [32]. Its final version was adopted by the European Commission on 27 November 2017 [33].

The RTS consists of a set of detailed provisions concerning security measures for the application of strong customer authentication.[79] These are relevant in respect of the generation of authentication codes,[80] dynamic linking[81] and the requirements of the elements categorised as knowledge, possession and inherence,[82] and their independence.[83] However, at the same time, the RTS contains numerous exemptions from strong customer authentication, as per specific occurrence (use case). Amongst others, the RTS contains exemptions[84] in respect of contactless payments at 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 criteria of respective provisions, they will be exempt from the strong customer authentication requirements.

An increasing number of IoT devices facilitate remote payments. It is important that manufacturers of devices with such potential are aware of strong authentication requirements outlined in the RTS and consider including endpoints and sensors facilitating appropriate authentication. Manufacturers have until September 2019 to implement measures to ensure compliance of their devices with RTS.

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 enforcement of these provisions. Namely, as it does not determine a specific authority in charge of enforcement of respective provisions, Member States will be able to select an appropriate authority "to ensure effective enforcement of the provisions of national law".[85] 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. EC should therefore play an exceptionally active role in overseeing the implementation of PSD2 and enforcement of national provisions.

[78] Article 98 (2) of PSD2.

[79] Chapter 2 of PSD2 RTS.

[80] Article 4 of PSD2 RTS.

[81] Article 5 of PSD2 RTS.

[82] Article 6-8 of PSD2 RTS.

[83] Article 9 of PSD2 RTS.

[84] Articles 11-15 of PSD2 RTS.

[85] Recital 99 of PSD2.

8. TRADE SECRETS

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 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 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.*" [34]

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 [35].

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 to 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 [12] which aims to standardise the national laws in EU Member States against the unlawful acquisition, disclosure and use of trade secrets. The Directive will enter 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.[86]

8.1 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) [36], 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 [35], 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

[86] 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.

Netherlands takes a separate stance and grants protection to trade secrets by way of the law of tort [35].

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.[87] 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.[88] Innovations that will be particularly affected include manufacturing methods and processes; business strategies unique to a company, marketing techniques.

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 a wider 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.[89] 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.[90]

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.[91] 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.[92] In this respect, the TSD also contains provisions concerning lawful and unlawful acquisition, use and disclosure of trade secrets.[93]

It is worth emphasising that the TSD is likely to provide an additional layer of protection for innovations of numerous organisations, including CREATE-IoT and LSPs 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*[94] 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 and the LSPs 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.

[87] See also Recital 1 of TSD.

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

[89] Article 2 (1) of TSD.

[90] Recital 14 of TSD.

[91] Article 2 of TSD.

[92] Article 2 (2) of TSD.

[93] Article 3 and Article 4 of TSD.

[94] C.f. requirement of *appropriateness* under GDPR.

8.2 Remedies

In accordance with the legal framework provided by TSD, Member States will have to provide measures, procedures and remedies necessary to ensure the availability of civil redress against the illegal acquisition, use and disclosure of trade secrets.[95] TSD offers a wide range of remedies for enforcing trade secret rights against infringers, while ensuring proportionality between the violation and the sanction.[96] Available remedies include provisional and precautionary measure,[97] final injunctions as well as corrective measures.[98]

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[99] (i) injunctions to prevent further use or disclosure of the information, (ii) court orders prohibiting infringing goods 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.

[95] Article 6 of TSD.

[96] Article 7 of TSD.

[97] Article 10 and 11 of TSD.

[98] Article 12 to 15 of TSD.

[99] Article 10 to 15 of TSD.

9. UPCOMING REGULATION

Aside of the set of the already adopted acts either already applicable for decades (e.g. PLD) or enforced and are to become applicable in the course of 2018, there are also a set of proposed acts of high relevance for the IoT ecosystem and, thus, for the five IoT European LSPs projects, namely, the draft regulation on free flow of non-personal data, the Cybersecurity Package and the draft ePrivacy Regulation**.** According to the ordinary legislative process provided under EU law, these acts are currently being subject to the trilateral negotiation between the Council, the European Parliament and the Commission.

The discussion below aims merely at touching upon certain aspects of the proposed acts and give an indication of the respective timeline. Taking into account the progress made and depending, of course, on any outcomes reached in the meantime, the instruments below will be further discussed under "D05.06 on Legal IoT Framework Evaluation and Final Legal IoT Framework" due in December 2019.

9.1 The proposed Regulation on the free flow of data

The European Commission's proposal for a Regulation on a framework for the free flow of non-personal data 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. To this end, the proposal 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" [37].

In particular, the draft 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 which are not justified by public security reasons within a year from the adoption of this Regulation. Any new data localisation requirement justified on public security grounds must be notified to the European Commission, while details of all approved data localisation rules must be made publicly available.

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 above-mentioned codes of conduct will be subject for review by the Commission two years after the start of the application of the proposed Regulation, while the Regulation shall apply six months after its publication.

More specifically, as far as the time of adoption of this proposal and the planning of the related developments are concerned, Commission has recently made provided additional information in a concise manner. In particular, Commission aims that the proposed draft is adopted by the Parliament and the Council by June 2018 and becoming applicable as of December 2018. The code of conduct provided under the proposal linked to data portability and switching of cloud service providers is intended to enter into force in December 2019 and be reviewed by the Commission in December 2020 [38].

9.2 The proposed 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 (see Chapter 5), it has become clear that a similar systematic approach to will be necessary also from other stakeholders. This is especially with the view of an increasing number of connected devices expanding the potential cyber security compromise surface area. Hence, strong cyber resilience comprising a collective and wide-ranging approach is needed [39]. To address this, the EC has published a Proposal for Cybersecurity Act [15], 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.

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 more efficient provision of support to Member states, EU institutions and businesses in key areas, including the implementation of NIS Directive. The proposal puts forward an ambitious revised set of ENISA's objectives[100] including strengthened advisory role on policy development and implementation, ensuring sharing of best practices, contributing to EU-level situational awareness, as well as providing support to Member States consisting of providing advice or technical assistance, or ensuring analyses of threats and incidents. As a result, the EC is proposing to task the agency with more responsibilities, making *the EU Cybersecurity Agency* in a relatively wide sense.

Under the proposed Cybersecurity Act, ENISA would also be tasked with the preparation of a candidate European cybersecurity certification scheme [41][101]. The EC has acknowledged that cyber security certification plays an essential role in increasing trust and security. However, at the same time it has argued that growth of EU cyber security market is held back by lack of cybersecurity schemes to build higher standards into products with confidence. To address this deficiency, the EC has proposed to set up a voluntary EU cybersecurity certification framework which would lay down the procedure for the creation of EU-wide cybersecurity certification schemes, covering products, services, and/or systems, which adapt the level of assurance to the use involved. The purpose of European cybersecurity certification schemes should be to ensure that ICT products and services certified under such a scheme comply with specified 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 proposed regulation.[102] To achieve this, the proposal contains a list of specific proposed elements.[103] 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.

[100] See Article 4 of the Proposal for Cybersecurity Act.

[101] See also Ibid, Article 44 (1) of the Proposal for Cybersecurity Act.

[102] Recital 55 of the Proposal for Cybersecurity Act.

[103] Article 47 of the Proposal for Cybersecurity Act.

9.3 The proposed 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, simpler 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 for privacy by default are proposed, including end-to-end encryption (with no backdoors) proposed as a security default measure for ensuring confidentiality of communications. Finally, 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[104]. In this respect, the report helps ensure that consent is genuinely freely given and requires privacy by default for software settings.

[104] 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.

10. CONCLUSIONS

This deliverable document has presented a vivid discussion consisting of a plethora of facts and arguments illustrating the amount and variety of developments as well as risks posed by IoT. In doing so it has demonstrated that the extent of the phenomenon of IoT is remarkable, cross-cutting and stretching across a range of diverse fields and disciplines. This, in its own, is a sufficient reason why special care needs to be taken when devising any legal framework addressing specific challenges posed by IoT that can be relevant for organizations and/or individuals.

Instead of providing a lengthy analysis potentially constrained by a limited number of regulatory acts, this document has thoroughly analysed the variety of current and forthcoming applicable legal frameworks that are relevant for all LSPs. The approach adopted has demonstrated the evolving nature of the regulatory ecosystem aiming to map the IoT ecosystem. The Legal IoT Framework is indeed composed of distinctive ingredients some of which seem to have expired, while others not yet having matured to specific flavours being added to the European market and society. For example, at the time of its drafting in 1976 and its implementation in 1985, the PLD appeared to be a future-proof solution ensuring adequate protection of consumers from defective products, yet failing to address legal liability for defective software, services and data. Naturally, the current PLD cannot be expected to sufficiently address the risks consumers face when using IoT devices. As far as the impact of the adopted yet not applicable legislation is concerned, its actual impact, though, looking quiet promising, remains unknown. The elaborations that led to the adoption of the GDPR had started in 2011 focusing on platforms and social media, without aiming at that point to address cloud, edge and IoT. Nevertheless, the principle-based nature of the GDPR allows to presume that data protection related matters will be sufficiently addressed under the new regime.

From a legal viewpoint, the challenge with respect to IoT largely relates to the proliferation of harm and the attribution of liabilities underlying all texts discussed. Incorrect or incomplete data may be created or deducted by a particular IoT device and subsequently transferred to or exchanged with other IoT devices, causing a potential domino effect of harm suffered by individual consumers and society at large, also, due to incorrect decisions taken on the basis of those incorrect or incomplete data. This is a consequence of the dependence of IoT on cloud computing technology leading to the so-called cloud harm. [42][43]

In this context, the resulting uncertainty in this changing regulatory landscape highlights the role of stakeholders' accountable conduct by committing to social norms, best practices and other soft law instruments, also discussed under the above referred "D05.01 on IoT Policy Framework". It is not coincidental – and certainly linked to the objectives of the DSM – that the entire set of currently proposed legal acts have the form of a "regulation" and of a "directive" promising higher degree of harmonization across Member States, also especially vis-à-vis contract law that is not harmonized across EU jurisdictions.[105]

Furthermore, even if the earlier discussed acts currently at the stage of proposal are ultimately adopted, such development will not constitute a guarantee in absolute as the challenge will be then transferred at the level of implementation. The laws discussed are meant, of course, to have complementary functions (e.g. the GDPR regulating flows of personal data while the draft proposal on the free flow of non-personal data regulating the flows of non-personal data) and

[105] See, also, the discussion on contracts included under "D05.01 on IoT Policy Framework" available at: https://european-iot-pilots.eu/wp-content/uploads/2017/10/D05_01_WP05_H2020_CREATE-IoT_Final.pdf and under "D05.03 on 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

further deploy synergies (e.g. the proposed Cybersecurity Act and the draft proposal on free flow of non-personal data). However, it is inevitable that the interoperability of those frameworks will pose challenges in practice, also for enforcement authorities. Despite mostly presented as challenges, these developments could actually function as an enabler – even from a business perspective – creating an opportunity for organisations acting in their capacity as IoT stakeholders to demonstrate their social corporate responsibility by willing to run the extra mile and commit to soft regulation, potentially, mitigating the uncertainties resulting from strict rules.

11. REFERENCES

[1] IoT European Large-Scale Pilots Programme, online at: https://european-iot-pilots.eu/

[2] Consumers International, “Testing Our Trust: Consumers and the Internet of Things”, 2017, pp. 3, online at: http://www.consumersinternational.org/media/154746/iot2017review-2nded.pdf.

[3] 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.

[4] 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.

[5] 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.

[6] Organisation for Economic Co-operation and Development, “The Internet of Things: Seizing the benefits and addressing the challenges”, 2016, online at: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP%282015%293/FINAL&docLanguage=En.

[7] Eurostat, European Commission, “News Release”, 9 December 2014.

[8] 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.

[9] 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.

[10] 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).

[11] 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.

[12] 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.

[13] 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.

[14] Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, 13.9.2017.

[15] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), 13.9.2017.

[16] 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.
[17] The Cloud Select Industry Group, "Cloud Service Level Agreement Standardisation Guidelines", 2014.
[18] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
[19] 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.
[20] 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.
[21] 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.
[22] 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.
[23] 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.
[24] 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.
[25] 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.
[26] K. Alheit, *The applicability of the EU Product Liability Directive to software,* p. 199, 200.
[27] 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.
[28] 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.
[29] European Commission, "Brief factual summary on the results of the public consultation on the rules on producer liability for damage caused by a defective product", 2017, online at: http://ec.europa.eu/docsroom/documents/23471.
[30] European Commission, "Minutes: Product Liability Conference", 2017, online at: https://ec.europa.eu/docsroom/documents/26661.
[31] 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.
[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] P. O'Donohue, European Commission, "The way forward", 12 December 2017, online at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=49050.

[39] 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.

[40] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act')", 2017, online at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN.

[41] 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.

[42] European Parliament, Directorate General for Internal Policies, "Cloud Computing: Study", 2012, online at: http://www.europarl.europa.eu/document/activities/cont/201205/20120531ATT46111/20120531ATT46111EN.pdf.

[43] D. Stefanatou, R. Leenes, M. G. Jaatun, V. Tountopoulos, C. Frøystad, A. S. de Oliveira, L. D. Corte, C. Reed, E. Kosta, R. Alnemr, B. Dziminski, K. Stuurman, C. Cuijpers, M. Schellekens, A. C. Specchia, N. C. Gleeson, A. Garaga, B. Newell, "Cloud Accountability Project: D-4.4 Remediation guidelines and tools, 2015, online at: http://cloudaccountability.eu/sites/default/files/D44.4%20Remediation%20guidelines%20and%20tools_0.pdf.