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

CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT

H2020 – CREATE-IoT Project

Deliverable 05.01

IoT Policy Framework

Revision : 1.0
Due date : 30-09-2017 (m09)
Actual submission date : 12-10-2017
Lead partner : AL

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

Summary					
No and name	**D05.01 IoT Policy Framework**				
Status	<Released >	**Due**	m09	**Date**	30-09-2017
Author(s)	Ovidiu Vermesan (SINTEF), Roy Bahr (SINTEF), Alberto Crespo (ATOS), Javier Valino (ATOS), Ross Armit Little (ATOS), Ronald Maandonks (PHILIPS), Arthur van der Wees (AL), Dimitra Stefanatou (AL), Jiri Svorc (AL), Andrea van Sleen (AL), Antonio Kung (TL), Tanya Suarez (BLU), Sebastien Ziegler (MI), Lucio Scudiero (AS).				
Editor	Ovidiu Vermesan, Dimitra Stefanatou				
DoW	The document provides an IoT policy framework to address issues of horizontal nature and common interest (i.e. privacy, end-to-end security, societal, ethical aspects and legal issues) in a coordinated and consolidated manner across the IoT activities and pilots. The work focuses on setup a trusted environment for IoT applications and provide further development and exploitation of mechanisms towards trusted, safe, secure and legal best practices and a potential label ("Trusted IoT"). In this context, issues such as IoT Life Cycle, trust definitions, common understanding, and common durable adoption reference model are covered. This deliverable is the first out of the two deliverables provided under the previously mentioned task. The second deliverable is due in December 2019.				
Comments					

Document history			
Rev.	**Date**	**Author**	**Description**
0.1	13-07-2017	AL	Template/Initial version. General information and structure.
0.2	24-08-2017	AS, MI SINTEF	Input to Sections 3.3 and 4.4
0.3	29-08-2017	AL	Integration of input provided by Philips via email. Editing & further input by AL
0.4	05-09-2017	AL	Editing (and further work under sections 1, 2 and 3)
0.5	06-09-2017	AL, TL, SINTEF	Section 3.1,3.2 and 4
0.6	07-09-2017	AL	Integration of all input.
0.7	12-09-2017	AL, SINTEF	Document alignment with the input provided by SINTEF.
0.8	19-09-2017	ATOS	Incorporation of contribution by ATOS.
0.9	28-09-2017	FE, BLU	Reviewing of the document
1.0	12-10-2017	SINTEF	Approved and submitted document

Table of contents

1. EXECUTIVE SUMMARY

The IoT Policy Framework presents a conceptual structure that aims to organise and clarify the collective principles, functions, definitions, requirements and practices, created through the technical expertise of stakeholders within the IoT European Large-Scale Pilots Programme stakeholders through a process and organised methodology within this active stakeholder community. Taking into account the existing approaches and other related developments within EU and beyond, the IoT Policy Framework presented below brings together the distinctive IoT trust, engagement, privacy and security frameworks in a coherent and integrated manner. This IoT Policy Framework aims at ultimately providing the solid and pragmatic basis for a human centric approach relevant for the different set of relationships linked to the IoT environment, including Business to Consumers (B2C), Business to Business (B2B) and hybrid models like Business to Business to Consumer (B2B2C). The present approach takes equally into account consumer/user and industry trust through hardened IoT solutions in order to encourage industry innovation, stimulate adoption and, as a result, enhance participation in the IoT marketplace.

The proposed IoT policy framework is built upon a holistic approach that integrates society and human centred approaches with user, technology, information and knowledge centred approaches. To this end, the high-level principles that underlie the proposal of such a framework involve the use of proactive and preventative methods and link to the identification of policy items of key importance, such as the embedding of privacy and security into architecture and design, the IoT device lifecycle and the protection of user privacy, also, against the implications inferred due to the use of the IoT cognitive components.

The IoT Trust Framework provides for the collective principles and underlying structure that exhibit the trustworthiness, dependability and privacy for IoT solutions into an integrated manner. The framework integrates the concepts of availability, reliability, safety, security resilience, privacy and sustainability best practices, it embraces "privacy and security by design" as a model for an implementable IoT code of conduct and engagement. The IoT trust framework needs to consider trust semantics, metrics, models, IoT platforms, trusted IoT network computing, operating systems, software and applications, while addressing the trust in mobile, wireless communications and risk and reputation management.

In the context of the overarching human-centred approach adopted, the discussion expands on the creation of an IoT Engagement Framework producing the need for stakeholder engagement in ethics, rules, guidelines and standards for an effective IoT Policy Framework that would safeguard a sustainable and safe IoT environment in the long term. To this end, the analysis points at the emerging regulatory and contractual relationships relevant for the Large-Scale Pilots (LSPs) and highlights the challenges for engagement and compliance at this time of significant changes in the European regulatory arena.

Moreover, starting from the user-centred point-of-view and taking into account the General Data Protection Regulation (GDPR), the IoT Privacy Framework focuses on key aspects of European Data Protection law, addressing, more specifically, the principles of data protection by design and data minimization. Note that a more in-depth discussion linking to a privacy framework for IoT will be provided under the forthcoming deliverables falling within the scope of "Task 05.03: Legal support, accountability and liability".

Furthermore, the IoT Security Framework is based upon a methodology for evidence gathering to ensure the user/customer industry derives suitable IoT security mechanisms and practices which are appropriate for the IoT applications domain and solutions in various sectors. It also paves the way forward by indicating best practices and choices in design, features, implementation, testing, configuration and maintenance, as well as a dedicated methodology for facilitating compliance by design within the changing regulatory landscape. The IoT security framework needs to consider IoT security policy, model, architecture, security of complex parallel, distributed IoT systems and

mobile and wireless communications, while addressing authentication, authorization, and accounting.

The IoT privacy framework addresses the policy issues on privacy for IoT parallel, distributed systems, cloud/pervasive/edge computing environments, mobile and wireless communications with reference to the IoT privacy in network deployment and management. In this context, the IoT privacy framework, is constitutive component of the broader IoT Policy framework discussed in this deliverable. Taking into account the nature of privacy as a fundamental human right[1] and in view of best surfacing the human centred nature of the privacy framework per se –being part of the overarching human centred IoT Policy Framework proposed, the analysis proposed in this document starts by using as a benchmark point of reference the user centred concerns associated with privacy.

Overall, the IoT Policy Framework is intended to help IoT European Large-Scale Pilots Programme stakeholders make informed decisions through a robust methodology and evidence gathering process. The evidence gathered during the process can be used to demonstrate conformity with best practice to consumers and other IoT stakeholders. The IoT Policy Framework discussed here within will be further developed and refined under the final deliverable version due in December 2019.

[1] Articles 7 and 8 of the Charter of Fundamental Rights of the European Union http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

2. INTRODUCTION

2.1 Purpose and target group

There are multiple definitions available for the Internet of Things (IoT); the European research community, for instance, defines IoT as "a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network" [52],while at the same time, the International Telecommunication Union and, more specifically, the Standardization Sector (ITU-T) has defined IoT as , "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" [51]. Taking both these definitions into account, it becomes apparent that through identification, data capture, processing and communication capabilities, IoT maximises the use of physical objects (things) to offer services for a wide variety of applications, whilst at the same time it is important to ensure the fundamental rights for individuals and society at large. It therefore is argued that IoT, in its widest sense, forms a materialization of a vision which is based on the exploitation of knowledge thus creating a series of technological and societal implications which calls for responsible interventions.

In the last few years, the IoT has gained widespread detrimental attention due to the extensive occurrences of IoT security related incidents affecting devices that are commonly used on a daily basis; fitness watches, thermostats, printers, refrigerators. These devices were brought to the centre of the discussions taking place worldwide, as examples that were poorly secured were targeted by malicious actors for various malign purposes. More specifically, due to the fact that IoT devices are sensing/actuating and processing units (in the future including intelligent, cognitive devices, autonomous systems and robotic things) connected to a network, and have operating systems with the ability to perform quite complex computational operations, they create opportunities for exploitation by malicious actors. Those malicious actors may take advantage of the absence of sufficient security measures in place, as certain IoT devices, for instance, do not require passwords at all, while others are sold to consumers with default passwords that many users do not change.

Nevertheless, the development of IoT applications and smart devices at the edge of the network is increasing and the rapid prototyping and "rush-to-market" strategies are creating the right circumstances for increasing the volume of possible incidents.

It is the value of using IoT devices and applications per se that increases the motivation of malicious actors to act. The extensive dependence on undependability of IoT devices entails a series of consequences that may create an unwelcome and growing impact on everyday life of individuals, on economies as well as on national security.

In response to the increasingly growing risks and associated impacts, regulators across the globe have started taking action in order to address specifically the IoT ecosystem. For example, a bill was recently introduced in the Senate of the United States[2] to provide minimum cybersecurity operational standards for internet-connected devices purchased by Federal agencies. The bill promises to incentivise malicious actors to expose vulnerabilities in flawed devices and prohibit vendors from selling devices with unchangeable passwords, or with known vulnerabilities, while at the same time providing legal ground to encourage vendors to ensure that their internet-connected equipment is patchable i.e. able to be protected retrospectively through updates in the firmware and software. The proposed regulatory instrument is largely consistent with an ongoing

[2] Note that the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'' published in September 2017 explicitly addresses the risks associated to connected devices.

multi-stakeholder effort led by the National Telecommunications and Information Administration (NTIA) aimed at developing voluntary security standards for Internet-connected devices.

Key elements of the proposed legislation relate to the setting of IoT security standards building on vendor compliance and commitment to provide, amongst others, for IoT devices to be patchable and that IoT devices do not contain hard-coded passwords. However, this particular instrument does not provide for any direct enforcement mechanisms for vendors of IoT devices aside from the threat of disqualification from federal contracting opportunities. It is proposed that these requirements are, however, limited to contractors participating in the federal procurement market and that other consumer devices are exempted from such requirements.

In the light of the associated developments, creating an IoT Policy Framework that would address trust, engagement, privacy and security in an appropriate manner for individuals and society is essential for the sustainability and trustworthiness of IoT ecosystems within EU and beyond.

Building on the existing definitions and approaches adopted within the EU and beyond [1][2][3],[3] highlighting, also, privacy and trust among other issues relating to IoT from an ethical point of view [4], this deliverable document builds a policy framework appropriate for the IoT environment[4]. It produces a synthesis of the related principles, functions, definitions, requirements and practices identified, as well as the technical expertise of the partners within the IoT European Large-Scale Pilots Programme. The IoT Policy Framework to be addressed under this analysis is composed of distinct components, namely, the trust framework, the engagement framework, the privacy framework and the security framework prioritized and structured in way that further reveals the underlying human centred approach.

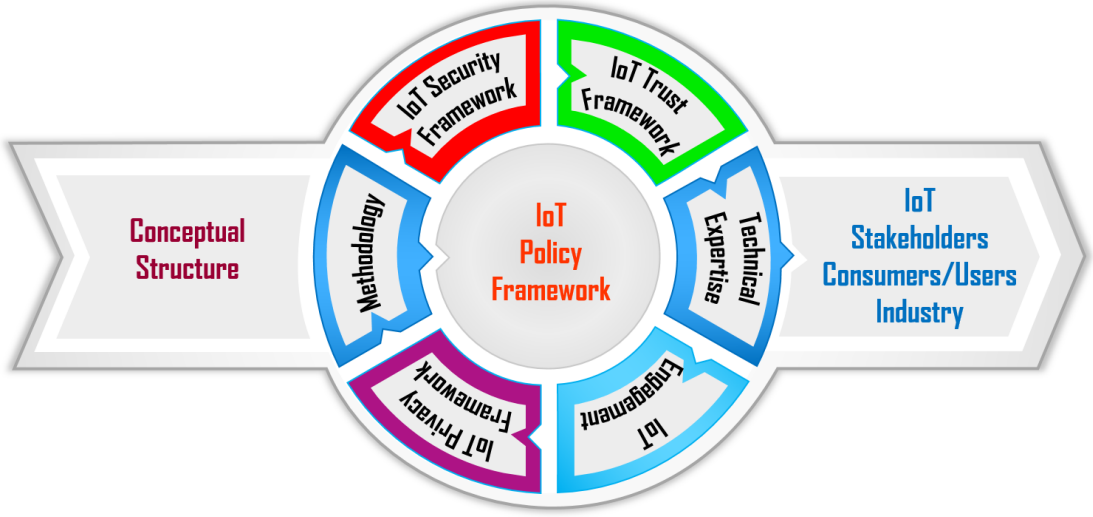


Figure 1: IoT Policy framework aims and target group

In particular, the IoT Trust Framework provides an underlying structure and a set of principles that manifest trustworthiness, dependability and privacy for IoT solutions in an integrated manner. This framework integrates the concepts of availability, reliability, safety, security resilience, privacy and sustainability best practices, embracing "privacy and security by design" as a model for an implementable IoT code of conduct and engagement.

[3] An in-depth discussion of the existing approaches falls outside the aims of the present deliverable; a more elaborated discussion, though, will be provided –to a certain extent- under the final deliverable due in December 2019.

[4] Note that there are multiple definitions on the notion of framework per se. For instance, the framework is defined as "a *basic structure underlying* secure human centric IoT systems'' or as "*a system of rules, ideas, or beliefs that is used to plan or decide something".* See, also, https://en.oxforddictionaries.com/definition/framework and http://dictionary.cambridge.org/dictionary/english/framework

In view of the ultimately aim of a human centred approach, a key pillar of the present deliverable document, the discussion expands on the creation of an IoT Engagement Framework producing the need for stakeholders' engagement to ethics, rules, guidelines and standards for an effective IoT Policy Framework that would safeguard a sustainable and safe IoT environment in the long run. To this end, the analysis points to emerging regulatory and contractual relationships relevant for the Large-Scale Pilots (LSPs) and highlights the challenges for engagement and compliance at this time of significant changes in the European regulatory arena. Note that stakeholders' engagement in relevant soft law instruments (e.g. best practices, standards and guidelines), is what underlies the aforementioned bill currently discussed in the US, while, also, being reflected in European instruments including the General Data Protection Regulation (GDPR) and the proposal of the Free Flow of Non-Personal Data [61] that both strengthen the role of soft regulation.

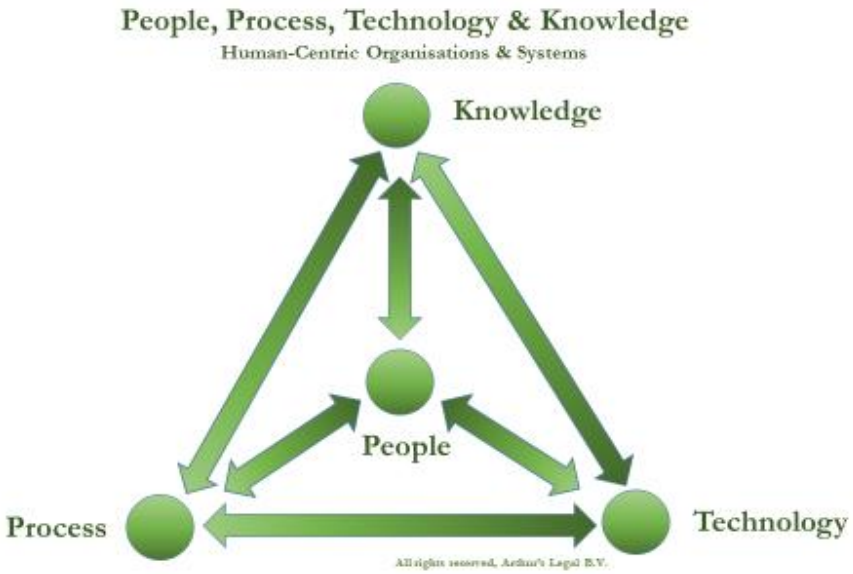


Figure 2: IoT consisting of People, Process, Technology & Knowledge

Moreover, starting from the user centred concerns and taking into account GDPR, the IoT Privacy Framework focuses on key aspects of the European Data Protection law, addressing, more specifically, the principles of data protection by design and data minimization. A principle based approach with respect to privacy would give stakeholders room and freedom, with respect to the appropriate means to employ, in order to achieve the level of protection aspired to by the Regulator; for example, commitment to standards may be an appropriate behaviour for companies to demonstrate compliance with the data protection rules in the context of Business to Business relationships, while the endorsement of best practices could be an appropriate means to build individuals trust in the context of the Business to Consumers relationships. Note that a more in-depth discussion linking to a privacy framework for IoT will be provided under the forthcoming deliverables falling within the scope of "Task 05.03: Legal support, accountability and liability".

The IoT Security Framework proposed in this document is based upon a methodology for evidence gathering to ensure the user/customer industry derive suitable IoT security mechanisms and practices which are appropriate within the IoT applications domain and solutions in various sectors. It, also, paves the way forward by indicating best practices and choices in design, features, implementation, testing, configuration and maintenance as well as a dedicated methodology for facilitating compliance by design within the changing regulatory landscape.

The particular traits of the concepts to be discussed, namely, trust, security, privacy, engagement, are reflected in the structure of the entire document, as well as in the structure of the dedicated chapters. More specifically, and in the context of the human centred approach adopted, the more theoretical discussion on the trust framework precedes the discussion on privacy and security.

Similarly, the discussion on the privacy framework has as a benchmark the user centred concerns linking to privacy.

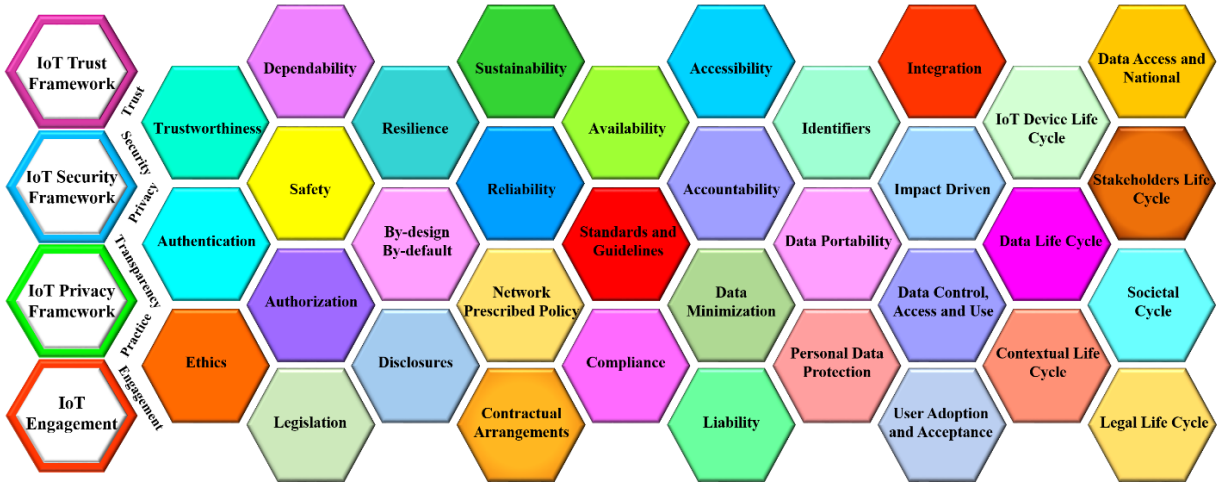


Figure 3:Constitutive elements of the IoT Policy framework

The above mentioned conceptual framework follows-on from the dynamic interactions amongst the community of stakeholders active within the CREATE-IoT consortium and the Large-Scale Pilots. These interactions reveal a series of relevant items that will be partly addressed under this deliverable, as well as within the forthcoming deliverables due under "Work Package 05: IoT Policy Framework - Trusted, Safe and Legal Environment for IoT".

Figure 3 captures the entire set of items that emerged so far in the discussions, as well as from the literature review of the existing frameworks, while providing an illustration of the multidisciplinary expertise of consortium partners.

Note that an initial set of the associated definitions deriving from the applicable regulatory instruments is available as an annex of this deliverable, while the overarching set of definitions relevant across the CREATE-IoT project is incorporated under "D02.01 IoT LSP handbook".

Overall, the IoT Policy Framework aims to serve as the initial, yet robust, governance model for the broader IoT environment and, more specifically, for the five (5) Large Scale Pilots (LSPs) supported by CREATE-IoT.

Taking into account, also, the composition of the consortia involved, the present deliverable will provide immediate assistance to consortium partners in making informed decisions affecting consumer choices and industrial practices.

This deliverable document falls under "Task 05.01: Policy framework and trusted IoT environment". It forms the initial report expanding on the main ingredients of the IoT Policy Framework. The final deliverable document[5], due in December 2019, will produce an updated version of the IoT Policy Framework presented here while also expanding upon the societal aspects involved.[6]

2.2 Contributions of partners

This document forms the output of interdisciplinary collaboration, as the result of partner's expertise and respective contributions.

[5] D05.02 IoT Policy Framework Evaluation & Final IoT Policy Framework: The evaluation report as well as an updated IoT Policy Framework (D05.01) and a recommendation report beyond the project, due in month December 2019 (month 36).

[6] The societal aspects involve–among other- critical aspects such as the potential rejection by end users –including citizens-driven by lack of trust. This is considered to be a roadblock to market uptake, given that the IoT applications impact on the lived environment.

AL contributes 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. To this end, Arthur's Legal expanded on the development of an appropriate engagement framework that can afford additional guarantees towards a sustainable and human centred IoT. Arthur's Legal, also, contributed to the discussion of the Privacy Framework incorporating the appropriate principles for the effective protection of personal information, which constitute background information of key significance. Furthermore, Arthur's Legal produced a customized set of high-level official and validated security principles and requirements by using a unique State-of-the-Art Security in IoT (SOTA) methodology, taking into account the changing regulatory landscape.

AS contributes by exploring the potential for a IoT Trusted Label from different viewpoints. In this deliverable the perspective of businesses which can be exposed to conflicting obligations under current privacy and security public policies is dealt with, particularly in the light of the obligations arising from the application of both Regulation EU/679/2016 on the protection of personal data (hereinafter "GDPR") and Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (hereinafter "NIS Directive''). By illustrating the scene of regulatory compliance, it becomes apparent that if compliance to strict rules per se is quite complex, then IoT stakeholders' commitment to other norms and values – including ethics and soft regulation- constitute a highly complex matter. More broadly, AS also closely follows the development of standardization initiatives in support of European privacy and security policies, besides being active in the field of privacy certification of IoT deployments under the GDPR, through the EuroPrivacy European Certification scheme, which has been developed by the Privacy Flag European research project.

ATOS contributed to the IoT Privacy Framework (a constitutive part of the IoT Policy Framework) with an analysis of the major types of relations between security and privacy concepts, exemplifying their differences and also their complementarity in the context of IoT. Based on ATOS extensive experience with privacy and security by design methodologies, the fundamentals are given of a principle-based approach to security and privacy, suitable to operationalize such principles in a privacy engineering framework for IoT systems and subsystems to cover comprehensively their entire lifecycle."

BLU provided valuable insights for the development of a human cantered IoT Policy Framework that were extensively taken into account for the creation of the policy framework approach presented. In particular, they contributed to the discussion on trust and engagement, especially, relevant from an end-user's standpoint.

MI contributed to the discussion relating to the user – centred concerns associated to privacy and, thus, highlighted the significance of the Privacy Framework, as a key component for a human centred IoT Policy Framework

SINTEF contributes to the development of a European and global policy 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 and security, intelligent analytics and smart data. The work is focused on building an IoT policy framework based on a holistic approach that integrates society and human centred approaches with user, technology, information and knowledge centred approaches. The framework includes end to end IoT trust, security, privacy and engagement and addresses among many issues elements such as authentication, authorization, communication network monitoring/enforcing, neutrality policy, security, privacy, trustworthiness at the technology, platforms and user engagement. The principle of security and privacy by design are applied. SINTEF contributes to 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 and security, intelligent analytics and smart data.

TL contributed to the creation of a security framework, as a constitutive part of the broader IoT Policy framework, detailing further the associated key components that having been considered appropriate to serve in practice a human centred IoT Policy Framework. To this end, the analysis used as a benchmark point of reference the approach of human centred computing putting forward a synthesis of human and computing systems that embrace human centred design, encourage interactions between individuals and aim at users' empowerment.

2.3 Relations to other activities in the project

The work on creating an IoT policy framework linked with IoT Governance that is addressing the issues of horizontal nature and topics of common interest (i.e. privacy, security, safety, societal, ethical aspects and legal issues) is done in a coordinated and consolidated manner across the IoT activities and pilots to maximise the output and impact of IoT technologies and applications across various domains. The framework focuses on (personal) data protection, security, safety, liability and net neutrality with a cross-domain IoT approach as part of the Digital Single Market strategy. Issues such as trust, privacy by design and security by design are part of the framework to support the adoption and compliance of IoT strategies in LSPs, start-ups, early-stage companies, SMEs, large companies and other organisations across sectors. The focus is on the technology and solutions providers side as well as the policy makers. The work is interrelated to other activities in the IoT European Large-Scale Pilots Programme dedicated to the definition of the framework and to the creation of a related framework environment. The latter will involve engaging LSPs in using it. This will also allow for the evaluation of criteria such as sustainability of IoT developments, easy accessibility, IoT technology adoption, and seamless integration of IoT technologies in various applications and industrial sectors.

Due to its scope relating to the creation of a conceptual framework for IoT Policy, the discussion captured in this document relates to all LSPs and the CREATE-IoT Project Work Packages that are at the fore front of user centred concerns and industry related considerations.

In particular, the policy impact work performed is directly linked to WP01 " Coordination and Support to the IoT Focus Area", WP03 "Creation, Innovation and Adoption", WP04 "European IoT Value Chain Integration Framework" as well as to WP06 "IoT Interoperability and Standardization". As far as user acceptance is concerned, this will be influenced in a direct and indirect manner: a) firstly, by enabling end users to understand how their data is stored, accessed and used and to what end, b) secondly, by providing clarity on that data for other stakeholders who are able to use the IoT pilots to develop further value-added goods and services, and c) thirdly, the move to open systems, that are modular and can be modified by the user. The basic principle underlying the aforementioned WP03, concerning creation, innovation and adoption, suggest that for IoT innovation, creation and adoption to flourish different skills, knowledge, resources, business models, and "cultural domain" background are required. This, of course, cannot lead any further, in the absence of the "sparkle in the machine", namely, stakeholders' engagement to a responsible behaviour in line with a human centred approach for IoT. Furthermore, the work captured in the present deliverable relates to the work being performed by CREATE-IoT concerning the integration of an IoT value chain framework for the EU, in the sense that the integration of such a framework cannot be achieved without the creation of a solid IoT governance framework providing for security and, ultimately, creating trust within the Digital Single Market, as discussed by the present document.

Moreover, the work captured in the present deliverable 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 (5) LSPs. By addressing the main horizontal yet hyper-connected domains of Trusted IoT, Privacy, Security & Legal

Frameworks, the aim of AG05 is to render these domains, generally seen as barriers or problems, into main components of the solution. AG05 considers that one of the ways to convert these domains into enablers for IoT and the use and sustainable uptake of IoT, is to first start with transparency: demystifying IoT and these domains, understanding what those domains are about from the ground up, and come to workable and understandable yet multi-layered frameworks that addresses these domains where relevant in each LSP. AG05 has been open for all consortium partners of each of the five (5) LSPs and two (2) coordination and support action projects within the IoT European Large-Scale Pilots Program to attend, participate in, learn and contribute to. Note that it is in the context of AG05 that the requests to give priority to security and engagement when building a policy framework for IoT were formulated.

In the broader context, the present deliverable due to its content and aims aspired is, of course, related in a direct or indirect manner to all current and future activities of CREATE-IoT Project.

3. THE IOT TRUST FRAMEWORK

Taking into account the complexities of trust as well as it high relevance for "Work Package 05: IoT Policy Framework - Trusted, Safe and Legal Environment for IoT," this section will first give an overview of the various interpretations assigned to trust and the meaning it obtains under the different perspective examined (namely, the socio-economical and the business perspective). Second, it identifies the trust component and, finally, it proposes a trust framework.

Figure 4: IoT Trust Framework

Overall, the IoT Trust Framework provides collective principles and underlying structure that exhibit the trustworthiness, dependability and privacy for IoT solutions into an integrated manner. The framework integrates the concepts of availability, reliability, safety, security resilience, privacy and sustainability best practices, embracing "privacy and security by design" as a model for an implementable IoT code of conduct and engagement.

3.1 Trust: A chameleon concept

The notion of trust constitutes a highly complex concept used across disciplines and assigned with various interpretations. The societal, human, user, technological, information, and knowledge - centred trust perspective, as well as the interdisciplinary discourse of social and economic life have generated a debate surrounding the concept of trust. This debate has emerged across various scientific and research domains, such as the social sciences [13], philosophy [14], political science [15], social anthropology [16], transaction cost economics [17], art and design [8] [10], sociology [19], economic sociology [20], computer science [21], the IoT [22] and cloud computing [23].

No definition of trust is complete; what is more, the existing definitions differ both between and within disciplines. The diversity of notions and concepts reveals a 'degree of confusion and ambiguity that plagues current definitions of trust' [11]. The range of definitions creates challenges in working with formalised models of computational trust for assisting the decision-making of human and artificial entities (sensor/actuator nodes, intelligent/cognitive instruments, robotic devices, etc.). Since the digital transformation of society is moving the issue into the mainstream of economic and technological disruption, socio-economic and technological notions of trust both need to be addressed holistically.

The trust concept is used in various contexts and with different meanings. Although its importance is widely recognised, trust is a complex notion about which no definitive consensus exists in the scientific literature. A primary problem with many approaches towards the definition of trust is that they do not lend themselves to the establishment of metrics and evaluation methodologies. Moreover, the satisfaction of trust requirements relates strictly to identity management and access control issues.

Online trust is a customer's willingness. It enables accepting an online transaction according to their positive and negative expectations regarding future online shopping behaviour [28]. Trust is

the willingness of a party to be vulnerable to the action of another party, based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party [29]. There is an attitude of confident expectation that one's vulnerabilities will not be exploited in an online situation of risk [30]. The trusting agent has a belief in the trusted agent's willingness and capability to deliver a quality of service in a given context and in a given timeslot [31].

According to [33], trust can be decomposed in device trust, entity trust and data trust. Device trust is a challenge, since *a priori* trust in devices cannot always be established (e.g. due to high dynamics and cross main relations). Hence, approaches such as trusted computing [34] and computational trust [35] are required to establish device trust. Every entity may assess trust in a device differently.

IoT architectures have to deal with its different perspectives of trust entity, while trust in the IoT applications and deployments refer to the expected behaviour of the participants, such as persons or services.

Device trust can be established via trusted computing and mapping different approaches to device trust is claimed to be more challenging and still in the experimental phase. The authors argue that data trust occurs in a twofold manner in the IoT. First, trusted data may be derived from untrusted sources by aggregation. Second, IoT services themselves can create data for which trust assessment is required.

As far as IoT is concerned, the complexity of the interactions involved calls for an approach to trust at a high level, end-to-end, at each architectural layer and at the interfaces, M2M (Machine-to-Machine), H2M (Human-to-Machine), H2H (Human-to-Human), M2H (Machine-to-Human), M2I (Machine-to-Infrastructure), and M2E (Machine-to-Environment).

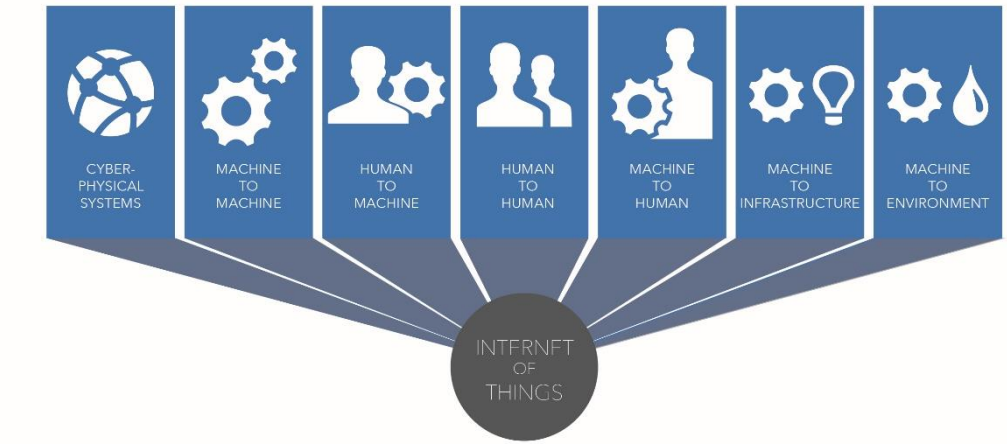


Figure 5: IoT interactions

In the IoT the complexity of interactions requires addressing the trust at the high-level, end-to-end, at each architectural layer and at the interfaces, M2M (Machine-to-Machine), H2M (Human-to-Machine), H2H (Human-to-Human), M2H (Machine-to-Human), M2I (Machine-to-Infrastructure), and M2E (Machine-to-Environment).

3.2 Social-Economical Perspective of Trust

Trust is recognised as an important element in negotiations and transactions in the economic and political arena. It is acknowledged that, 'the advantage to mankind of being able to trust one another penetrates into every crevice and cranny of human life' [12].

The reason for analysing trust from an economic perspective stems from the recent popularisation of the argument that trust enhances economic efficiency under certain conditions. This hypothesis can be traced back to [12], who emphasises that trust can reduce the transaction costs of enforcing

honest behaviour and that situations in which an absence of trust causes inefficiency are of equal, if not more, concern.

There is a distinction between the attribute of trust and the behaviour of trust [24]. Different types of trust are identified according to their role: commercial, problem solving, informational, knowledge or identity [25], based on the area of use: behavioural, business or technology [26] and from different perspectives on trust: individual, societal or relationship [27].

In [37], a method was proposed to explore the different meanings of trust and strategies that can be used to determine whether something is trustworthy and the proposed model for trust that takes people, devices and their connections into consideration. This model uses *a priori* and *a posteriori* trust to provide an indication of how much a user can trust or distrust the information provided by things. This trust indicator can inform users' decisions on whether to use a device or service or not.
Virtually every commercial transaction has an element of trust within itself, as does any transaction conducted over a period of time. It can be plausibly argued that much of the economic backwardness in the world can be explained by a lack of mutual confidence. The absence of trust may be particularly prevalent in numerous developing and transition economics in which economic transactions are viewed as exploitative, rather than mutually beneficial.

3.3 Business Perspective of Trust

Trust in IoT is an indispensable prerequisite for the growth of IoT business. This growth of IOT business is further subject to a series of adoption factors relevant for trust. In particular, as far as providers are concerned, their reputation is of key importance for the response of IoT users. Similarly, trust entails users' psychological feeling about the adoption. In a broader scale, trust from a business perspective involves user's perceptions as shaped by the social environment. Furthermore, on a more concrete basis, trust in the business context, primarily, links to the product's characteristics and the risks occurring through its mere use.

Figure 6: IoT Trust balance

Strategies, products and services to enhance trust can be evaluated along different dimensions, while different implications on trust and privacy address the *whom (participant element), where (dimension, area, boundaries), when (publication, release), who (investor, stakeholder paying) and how much (cost).*

Understanding the different dimensions is important in developing rules, guidelines and policies for evaluating, monitoring, comparing and developing different approaches and products to deal with specific trust-enhancement goals.

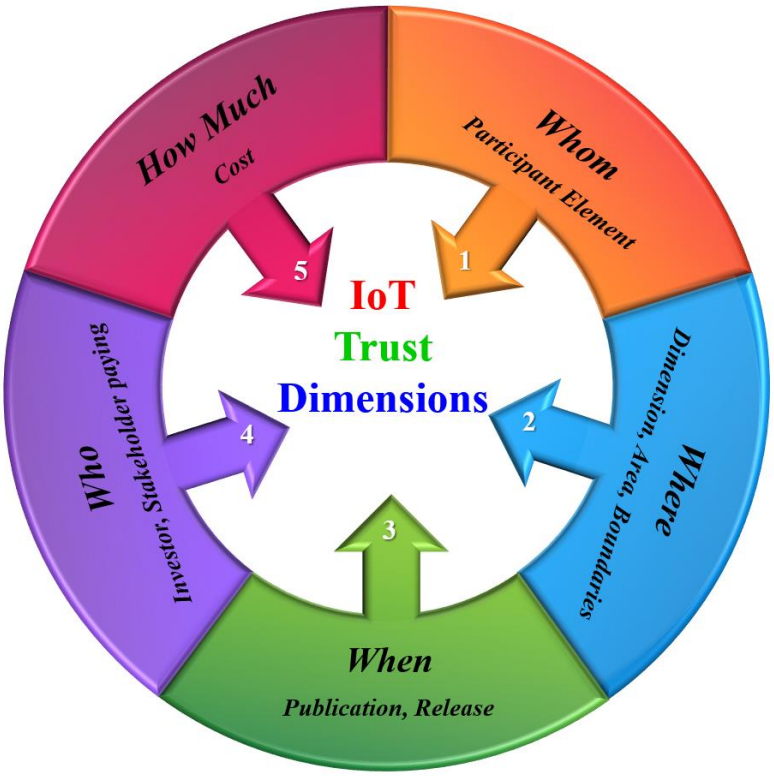


Figure 7: IoT Trust dimensions

The 'whom' is represented by the participant element (human, thing, software agent) covered by a particular approach to trust enhancement. 'Where' is represented by the area or dimension that refers to the boundaries for the trust-enhancing mechanisms. 'When' is addressed by the publication of the legislation or other trust- enhancing approach to be made available or released. 'Who' is represented by the one to be charged for the trust-enhancing product or service and 'how much' is represented by the cost to be charged to obtain a trust-enhancing product or service, such as certification.

3.4 Trust Components

Designing for trust requires the identification of elements and mechanisms of trust that can be embedded in a system. Defining trust as the intersection of privacy, security and reliability can enable or simplify the identification of trust as embedded in a technical design, such as in IoT systems. Since trust assumptions are built in when data collection is enabled or coordination is made feasible, trust can be built into systems, even those without security.

Trust is an element with multiple dimensions combining, for example, privacy, security reliability, availability, and integrity with human and machine behaviour. In this context, there is a need for greater understanding of how individuals interact with machines and how machines/things interact with other machines/things with respect to the extension of trust.

Trust is a function of privacy, while security reliability, availability, and integrity are operational elements based on risks, rather than user perception of risk, and focused on the existence of risk (Boolean), rather than quantifying the risk (deterministic or stochastic). Privacy is a measure of the tendency to share information (tendency is based on the risk of secondary use of information rather than a psychological sensitivity to information exposure). It is the right to act without observations and it applies to people. The connection between privacy and autonomous things is an evolving theme.

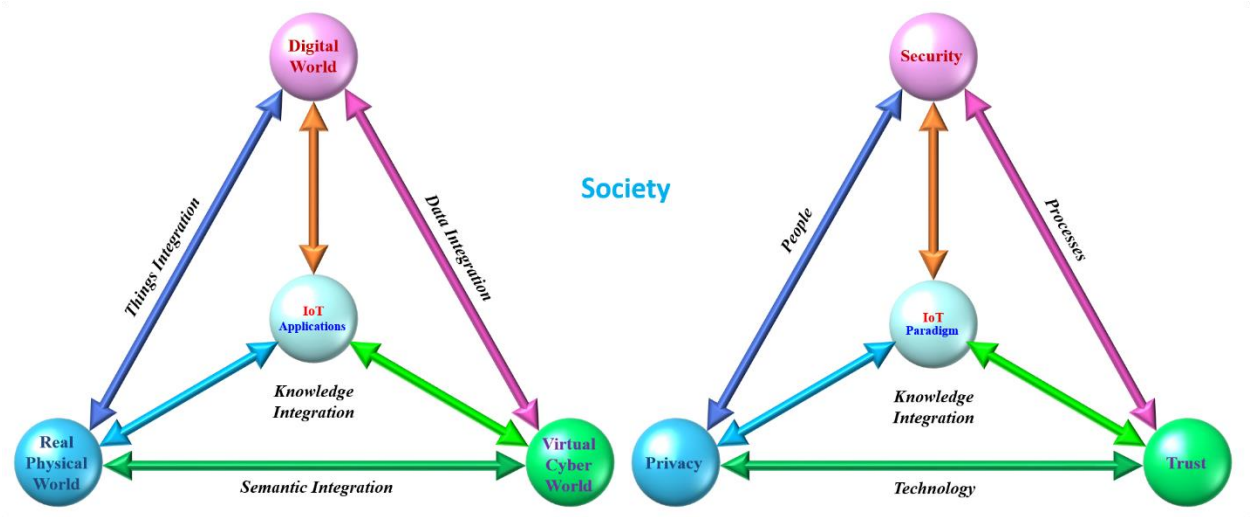


Figure 8: Trust as part of the IoT physical, digital, virtual and cyber convergence

Although confidentiality is an element of both security and privacy, this commonality does not make them the same. Confidentiality allows a person/thing to communicate to another without eavesdroppers and, in general, the control of information enabled by security does not imply privacy. Security enables the control of digital information, while social, organisational and technological (i.e. autonomous, cognitive, artificial intelligence systems) forces determine who exercises the power of that control. Privacy requires that a person/thing be able to control information about his-/her-/itself. Security provides the ability to generate privacy in a specific case (as with the confidentiality of communication), or the capacity for cryptography, which is the art of hiding information. Security can be considered to provide anonymity when the information that is hidden is identifying information. Anonymity is a technical guarantee of privacy.

Trust implies secure endpoints and it requires that security mechanisms do not affect survivability. The Internet Protocol is distributed and exhibits graceful degradation, which means that any computer/thing/device can connect to a network without altering the access of others. The loss of one computer/thing/device should not affect those who are not using its services. The ability of any network, the Internet or an intranet, to degrade gracefully rather than suffering catastrophic failure is a critical component in survivability. Both security systems and the lack of security systems enable denial of service attacks. Security systems that are computationally intensive or intolerant of user input make it more likely for a user to experience a lack of reliability.

The trust mechanisms in today's IoT are based on all-or-nothing trust relationships. A network resource request is not trusted before authentication and after authentication, it is granted the full credentials of the corresponding user. Executable content from within a protected network is completely trusted, but content from outside the firewall is strictly disallowed. Once established, a network connection has equal priority with all other network connections on the system. These all-or-nothing trust relationships fail to match the expectations of users and the needs of next generation network applications. Since users undermine simplified trust models to meet their own complex resource-sharing needs, this mismatch promotes security breaches among users.

Although the firewall model of trust is very simple for use in distinguishing secure sources of executable content, there is a need for distributed trust modes that allow distinctions to be made in the trustworthiness of network entities. Security in today's Internet is focused on a centralised model where strong security requires a firewall. The firewall is a barrier, but once it has been compromised, the entire network that it protects is compromised, making the firewall a single point of failure. The tunnelling example demonstrates how this centralised approach can allow a single breach of security to compromise the security of an entire protected IoT network.

Figure 9: IoT Trust components

Design for trust requires enumerating the social assumptions and examining how those assumptions can function to put some user of the system at risk. To understand and design trust systems requires acknowledgement of the social, human and autonomous/cognitive elements.

From an information and communication technology perspective, trust actually refers to trust measurement capabilities and –similarly- privacy actually refers data protection capabilities. This definition mirrors trust assessment approaches, such as recommendation and reputation systems, which calculate the trustworthiness of one subject to match it against the need for trust of another subject.

3.5 IoT Trust Framework

The IoT is bridging the virtual, digital, physical worlds and mobile networks need to scale to match the demands of billions of things, while the processing capabilities require addressing the information provided by the "digital shadow" of these real things. This need focusing on the developments in the virtual world and the physical world for solving the challenges of IoT applications. In the virtual world, network virtualization, software-defined hardware/networks, device management platforms, edge computing and data processing/analytics are developing fast

and urgency to be endeavoured as enabling technologies for IoT. Connecting the virtual, digital, physical worlds generates knowledge through IoT applications and platforms, while addressing security, privacy and trust issues across these dimensions.

Smart IoT applications modify the way people interact with the intelligent spaces (called also cyber-spaces), from how remotely control appliances at home to how the care for patients or elderly persons is perform. The massive deployment of IoT devices represents a tremendous economic impact and at the same time offers multiple opportunities. IoT's potential is underexploited, the physical and intelligent are largely disconnected, requiring a lot of manual effort to find, integrate, and use information in a meaningful way. IoT and its advances in intelligent spaces advances can be categorised along with the key technologies at the core of the Internet.

Ensuring the security, reliability, resilience, and stability of Internet applications and services is critical to promoting the concept of trusted IoT based on the features and security provided of the devices at various levels of the digital value chain.

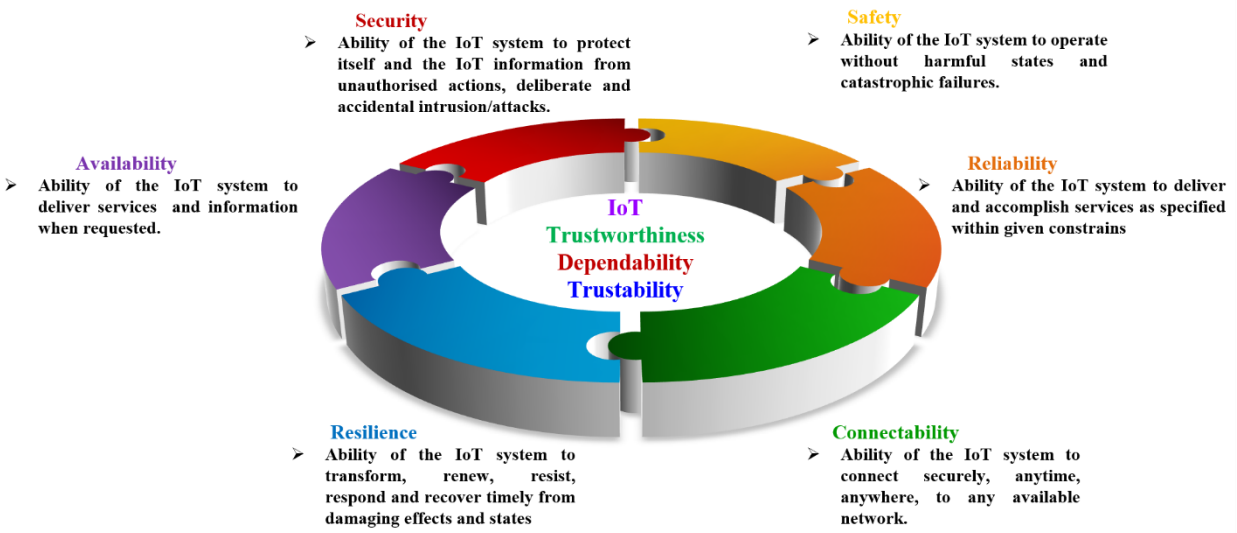


Figure 10: IoT complex interlinked concepts of trustworthiness, dependability and trustability

Security needs to be designed into IoT solutions from the concept phase and integrated at the hardware level, the firmware level, the software level and the service level. IoT applications need to embed mechanisms to continuously monitor security and stay ahead of the threats posed by interactions with other IoT applications and environments. Trust is based on the ability to maintain the security of the IoT system and the ability to protect application/customer information, as well as being able to respond to unintended security or privacy breaches. In the IoT, it is important to drive security, privacy, data protection and trust across the whole IoT ecosystem and no company can "do it alone" in the IoT space; success will require organizations to partner, value chains to be created and ecosystems to flourish. Yet, as IoT users start to bring more players, service providers and third-party suppliers into their value chain, tech firms and IoT solutions providers will face increasing pressure to demonstrate their security capabilities [52].

A layered IoT architecture is proposed for a trust management control mechanism [50]. The IoT infrastructure is decomposed into three layers: sensor, core and application. Each layer is controlled by a specific trust management under the following purposes: self-organisation, routing and multi-service, respectively. The final decision-making is executed by the service requester (i.e. the user) according to the collected trust information and the requester policy. A formal semantics-based and fuzzy set theory are used to realise the trust mechanism.

The distinction between trust and the related concepts of trustworthiness, confidence and the act of entrusting something to someone are extremely important. Uncertainty and vulnerability are two of the core elements in trust relations. In addressing issues of trust, actors select strategies that

reduce uncertainty or decrease vulnerability, depending on the particular context in which the issues emerge. Mechanisms for reducing vulnerability in the face of increased contact with unknown things include enforceable contracts, insurance schemes, etc. The characteristics of different types of trust relations include faith, confidence, legal trust and trust/distrust.

Since it is a sign of a more usual quality known to be correlated with trustworthiness (for example, same group, class, family, or same source), identity 'signals' trustworthiness in many cases.

Works in [38] and [39] focus on trust level assessment of IoT entities. These authors assume that most smart objects are human-carried or human-related devices, so they are frequently exposed to public areas and communicate through wireless, and are consequently vulnerable to malicious attacks. Smart objects have heterogeneous features and need to work together cooperatively. Since users are friends among themselves (i.e. friendship), users own the devices (i.e. ownership) and the devices belong to some communities (i.e. community), the social relationships considered include friendship, ownership and community. Malicious nodes directed towards breaking the basic functionality of IoT through trust related attacks include self-promoting and bad- and good-mouthing. The trust management protocol for IoT proposed in [38] is distributed, encounter- and activity-based: two nodes that come in contact with each other or are involved in a mutual interaction can rate each other directly and exchange trust evaluations about the other nodes; therefore, they perform an indirect rating, which seems like a recommendation. The reference parameters to trust evaluation include honesty, cooperativeness and community-interest. Such a dynamic trust management protocol is capable of adaptively adjusting the best trust parameter setting in response to dynamically changing environments to maximise application performance.

4. THE IOT ENGAGEMENT FRAMEWORK

The present chapter discusses the IoT Engagement[7] Framework, a constitutive component of the overarching IoT Policy Framework. In particular, first, the chapter gives an overview of the related engagement mechanisms; second, it depicts the regulatory and contractual relationships between the five Large Scale Pilots (LSPs) and the CREATE-IoT stakeholders and, third, it gives an overview of the challenges for compliance – and engagement – at this moment of change of the European regulatory scene. In the context of the present analysis engagement is defined as follows: "engagement refers to commitment and endorsement of norms and values through concrete practices". Note that an extensive discussion of the associated concepts will be provided under the forthcoming deliverable document falling under "Task 05.03: Legal support, accountability and liability".

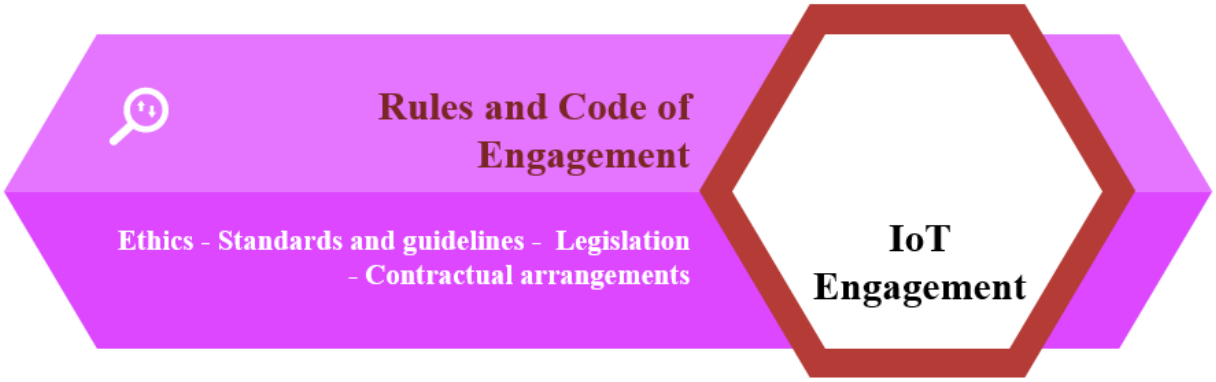


Figure 11: IoT IoT engagement framework[8]

4.1 The engagement mechanisms

The section gives an overview of the benchmark points of reference for the entire spectrum of IoT stakeholders ensuring engagement in an appropriate manner for the IoT environment. The figure below captures the stepping stones of engagement, meaning, Ethics, Standards and Guidelines, Legislation and Contractual Arrangements. It has been noted that much ink has been spilt in by scholars dealing with the above-mentioned concepts – the discussion below expands on them to the extent necessary for the purpose and audience of the present deliverable. However, a more in-depth discussion – from a legal standpoint – will be elaborated under "D05.05 Legal IoT Framework" and "D05.06 Legal IoT Framework Evaluation & Final Legal IoT Framework" due in December 2017 and December 2019 respectively.

As far as the notion of Ethics is concerned, this is assigned with fundamental importance, as engagement to ethics is what – in essence – underlies engagement to the rest of the items identified. The notion of Ethics per se is vast including a series of different kinds of Ethics[9] identified. The most relevant categories of Ethics for the IoT Environment are the "Business Ethics" and "Digital Ethics."

Business Ethics and, more specifically, Corporate Social Responsibility are highly relevant for the IoT environment. Corporate Social Responsibility is, in general, understood as actions performed by businesses that i) are not dictated by law and ii) aim at benefiting entities other than a business

[7] Note that the current version of the Code of IoT Engagement is annexed at the end of this deliverable.

[8] Please, note that in the context of this chapter the terms "regulation" and "legislation" are used interchangeably.

[9] See, for instance, Stanford Encyclopaedia of Philosophy, available at: https://plato.stanford.edu/search/search?page=1&query=Ethics&prepend=None

corporation. Business Ethics, in this sense, are highly relevant for IoT due to its' impact on society at large.

Furthermore, digital ethics are found at the heart of the discussions at EU level concerning data protection matters. The European Data Protection Supervisor urges "the EU and also those responsible internationally, to promote an ethical dimension in future technologies to retain the value of human dignity and prevent individuals being reduced to mere data subjects."[10] In this respect, IoT is considered to be one of the main technological trends, triggering concerns of ethical nature as, for instance, the likelihood of discrimination and the use of IoT devices in the health insurance sector.[11]

Standardization and Guidelines constitute forms of soft regulation that are quite commonly attempting to provide for technical matters and, more broadly, for the behaviour for organizations active in the domain of technologies, such as Cloud Computing. Soft law instruments such as the ones mentioned above do emerge from the original engagement of stakeholders, which –in most case- fades away later on, leading later on basically to them not being adopted in practice by the relevant stakeholders. Moreover, the effectiveness of soft law measures - as mentioned above - may vary due to a number of reasons. In any event, the common denominator of all these soft law instruments of is the potential lack of "real effectiveness" due to their voluntary nature and the related absence of redress mechanisms.

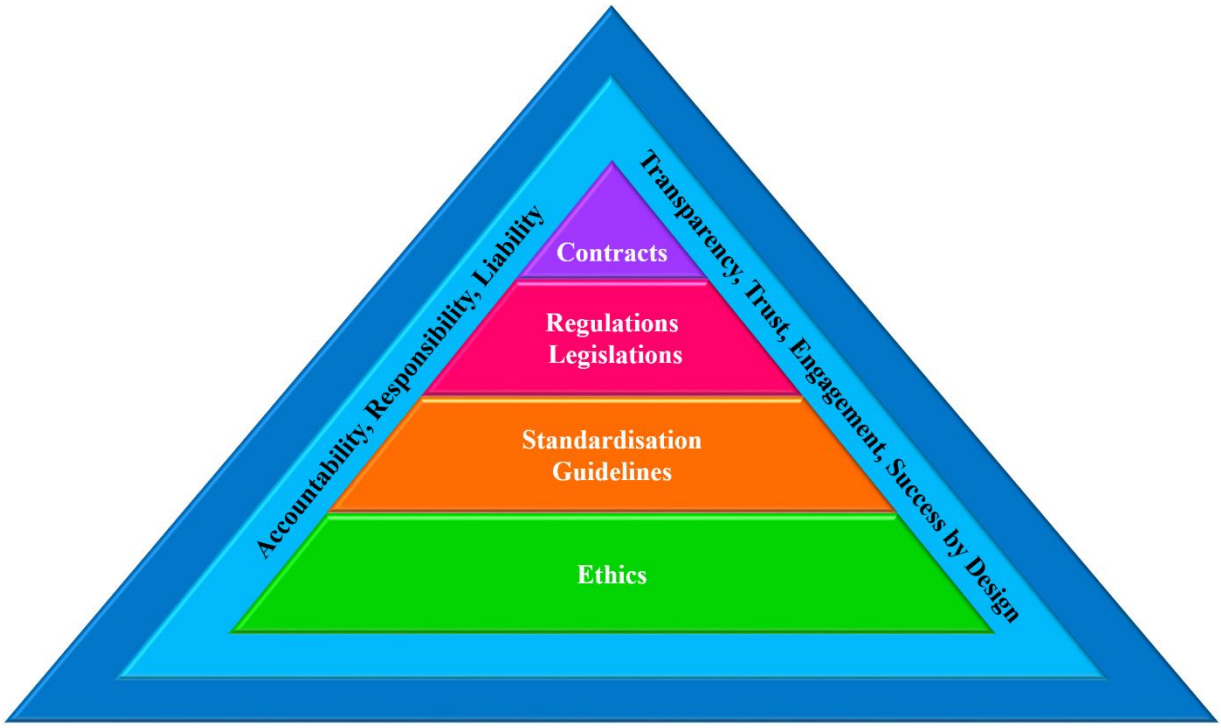


Figure 12: The hierarchy of engagement mechanisms

As opposed to Ethics and Soft Law instruments, Regulation and Legislation in essence impose stakeholders' engagement due to their mandatory nature. Interestingly, though, engagement in this case should not be mistaken as an equivalent to compliance, but rather as a safeguard for effective protection of all interests involved. Engagement in this case calls the entities assigned with the relevant responsibilities to go beyond the "mere box ticking" exercise of compliance and take all necessary action required in the context of responsible governance. Note that the regulatory texts applicable in the IoT environment will be discussed in detail under the above-mentioned

[10] See, also, https://edps.europa.eu/data-protection/our-work/ethics_en

[11] European Data Protection Supervisor, "Opinion 4/2015 Towards a new digital ethics Data, dignity and technology", available at: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf

deliverables falling within the scope of "Task 05.03: Legal support, accountability and liability"; an overview of those is currently provided under section 4.3, as well as under the Annex.

"Contracts can be defined as any legally binding agreement. The agreement gives rise to obligations to perform the promises made to the other party or parties to the contract, which are enforced and/or recognized by the law. The agreement is formed through an offer and acceptance between two or more consenting parties. If those agreements meet the requirements set in the context of each jurisdiction, which make them legally binding, they are contracts. Contracts specify what it is provided by national laws and/or provide, of course, for aspects not covered by the regulator. In any event, contracts cannot provide against what it stipulated by law (e.g. European Directives, national implementing laws)."[12] Note that there are differences between common law (e.g. UK, USA) and civil law jurisdictions (e.g. France, Germany) as to what it is precisely required in order for a contract to be valid. This discussion, though, falls out of the aims of the present deliverable.

The aforementioned engagement mechanisms form the implementing system of engagement within the IoT environment aiming – ultimately – at ensuring – among other noble goals – transparency, trust and accountability within the community of the IoT stakeholders. Nevertheless, it should be noted that first two engagement mechanisms identified, namely, one the one hand Ethics and, on the other hand, Standardization and Guidelines form an initial "testbed" of engagement, in the sense, that they cannot be enforced by authorities, thus, surfacing in a clear manner IoT stakeholders' "real" engagement to implement them.

4.2 The regulatory & contractual relationships within LSPs

Both state imposed law and contracts govern relationships between entities that can either be natural persons (e.g. acting in their capacity as consumers) or legal entities (e.g. companies or public-sector organizations). State imposed law, naturally, leaves no room for negotiation to the entities falling within its scope, while – as opposed to state imposed regulation – contracts emerge from a negotiation process between the parties willing themselves to enter into a legal relationship. State imposed regulation and contracts form law assigning rights and responsibilities to the regulated entities and can be, therefore, enforced by courts.

As it will be further explained below, the aforementioned Code of IoT Engagement mirrors the earlier discussion and actually stems from it. In particular, the Code of IoT Engagement is applicable to each and every entity wishing to become part of the community active within the Large-Scale Pilots (LSPs) and Coordination and Support Activities (CSAs) of the European Large-Scale Pilots Programme. Note that it is of great significance for stakeholders not only to identify themselves within those domains, but also to recognise in timely manner who are the other stakeholders that they may engage with in the future.

In particular, the IoT stakeholders include without limitation the following "entities" listed in detail below in random order:

- Society and environment
- Users
- Users
- Customers
- Non-users
- Data brokers

[12] Cloud Accountability project, ""D-4.3, Guidelines and tools for cloud contracts, available at: http://www.a4cloud.eu/sites/default/files/D44.3%20Guidelines%20and%20tools%20for%20could%20contracts_0.pdf

- Data providers
- Service providers
- Software providers
- Hardware providers
- Infrastructure providers
- Machines, interfaces and user-interfaces
- Universities and other knowledge institutions
- Standardisation development organisations
- Policy makers: governments, municipalities and others
- Authorities, law enforcement and intelligence services

Note that for the sake of this discussion, the notion of entities is being used "lato sensu", thus, including references to environment and society at large. In order to better depict the emerging relationships, the figure below groups the aforementioned entities into wider groups as follows:

Figure 13: Code of IoT Engagement

In particular, the figure above captures how various stakeholders within the IoT Engagement Zone relate to each other. The figure illustrates the nature of relationships between the LSPs/CSAs and individual Consortium Partners. At the same time, it also visualises the nature of relationships between the LSPs/CSAs and parties that are no part of an LSP or CSA consortium (i.e. Third-Party

Partners). To complete the picture, relationships between the Consortium Partners and Third-Party Partners, as well as between various Third-Party Partners are also accounted for.

As mentioned above, the Code of IoT Engagement is applicable to each and every entity wishing to become part of the community active within the LSPs and/or CSAs. Hence, it applies naturally to all relationships between the LSPs/CSAs and Consortium Partners, on top of other contractual and statutory obligations. In a similar way, the Code of IoT engagement supplements the contractual and statutory regime established between the LSPs/CSAs and the Third-Party Partners. However, while it is desired that Third Party Partners act and cooperate with LSPs/CSAs in accordance with the established ethical principles, often there is no direct contractual relationship between the individual LSP/CSA and the Third-Party Partner to ensure such compliance. Thus, the overarching and universally applicable Code of IoT Engagement serves to ensure compliance with ethical standards within the Zone, regardless or the relationship with the LSP or CSA.

4.3 The challenges of engagement

IoT stakeholders engagement constitutes a quite complex objective as it presumes organizational awareness, development of an organizational cultures that ensures the translation of norms and values into concrete practices, as well as, the investment of the necessary resources; the latter holds particularly true, as even mere compliance with strict rules can be costly, taking into account the expertise and the time required.

The section below touches upon the associated complexities for organizations by producing an overview of the difficulties relating to security that organizations will soon encounter in view of the upcoming legislation at EU level (e.g. GDPR, ePrivacy) and the conflicts with the existing standards. Note that an extensive discussion of the relevant difficulties will be provided under the deliverables falling within the scope of "Task 05.03: Legal support, accountability and liability".

4.3.1 Setting the scene

Organizations in Europe will face regulatory complexity related to security in that they may be subject to the combined application of different legislative items regulating security obligations in the IoT domain.

The regulatory framework for security in the IoT domain consists of:

a) 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 GDPR)
b) 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 ("NIS Directive")
c) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("Directive on privacy and electronic communications" or "ePrivacy Directive")

Here below the main provisions of each of the mentioned legislative act will be analysed in greater detail.

a) Key GDPR security provisions

- It applies to any organization, whether private or public, that processes personal data
- It imposes the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk
- It applies to data controllers and data processors alike

- It requires data controllers and data processors to enter into data processing agreements detailing the list of security requirements and obligations that the parties commit to respect;
- Data Controllers must notify supervisory authority of a security incident affecting personal data within 72 hours of becoming aware if feasible
- Individuals must be notified where an incident could cause serious harm
- Data Processors have the duty to notify data controllers "without undue delay"

b) Key NIS Directive security provisions

- It applies only to **Operators of essential services** and **digital services providers**

Operators of essential services are defined as private businesses or public entities with an important role for the society and economy.

Under the NIS Directive, identified operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority.

The **security measures** include:

- Preventing risks: Technical and organisational measures that are appropriate and proportionate to the risk.
- Ensuring security of network and information systems: The measures should ensure a level of security of network and information systems appropriate to the risks.
- Handling incidents: The measures should prevent and minimize the impact of incidents on the IT systems used to provide the services

Operators of essential services shall notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide, regardless of whether they affect personal data.

The Directives covers **digital service providers ("DSPs")** too. They are identified as:

- Online marketplaces (which allow businesses to set up shops on the marketplace in order to make their products and services available online)
- Cloud computing services
- Search engines

DSPs are under the obligation to implement security measures such as:

- Preventing risks: Technical and organisational measures that are appropriate and proportionate to the risk.
- Ensuring security of network and information systems: The measures should ensure a level of security of network and information systems appropriate to the risks.
- Handling incidents: The measures should prevent and minimize the impact of incidents on the IT systems used to provide the services.

The security measures taken by DSPs should also take into account some specific factors, to be further specified in a Commission implementing due at the time that the current deliverable is being drafted. Note that all developments of significant importance will be discussed under the deliverables falling under the scope of "Task 05.03: Legal support, accountability and liability''.

- Security of systems and facilities
- Incident handling
- Business continuity management
- Monitoring, auditing and testing
- Compliance with international standards
- DSPs are also under obligation to notify security incidents the national supervisory authorities. Yet, differently from what is required to operators of essential services, they can take into account more criteria before performing the notification, such as:

- Number of users affected *(common with operators of essential services)*
- Duration of incident *(common with operators of essential services)*
- Geographic spread *(common with operators of essential services)*
- The extent of the disruption of the service
- The impact on economic and societal activities

The rationale behind this difference in the provisions applicable to DSPs is that they shall be subject to a *light-touch set of rules.*

c) Key ePrivacy Directive provisions

- The security provisions of the ePrivacy Directive apply to providers of a publicly available electronic communications service and to provider of the public communications network.
- They must take appropriate technical and organisational measures to safeguard security of their services (…) Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.
- In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.
- In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.
- When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

The ePrivacy Directive is currently under revision by the EU legislator; it will be replaced by a Regulation which will be aligned with the GDPR. A key aspect of the reform will likely be the extension of the ePrivacy norms from traditional voice, text and email services to: (i) "over the top" service providers; (ii) M2M communications (i.e. IoT technology); and (iii) probably all services with an electronic communications element.

4.3.2 Consequences on the IoT operators

For the obliquity and wide potential of IoT deployments, IoT service providers may be subject to concurring security obligations under different sources of legislation.

In their capacity as data controllers or data processors, they may be subject to the GPDR and, once the reform of the ePrivacy Directive Is passed into EU law, to the new ePrivacy regime too.

Given that IoT services may be part either of services provided by operators of essential services or by DSPs, IoT may be also caught by the rules of the NIS Directive. A case by case analysis is therefore needed to appraise to which legal regime they shall abide under the NIS Directive.

When this is the case, for example, IoT services providers will be subject to two concurring regimes as for what regards the notification of security breaches. They will have to be certainly notified to the relevant national authorities under the NIS Directive, and also the Data Protection Authorities if the breaches affect personal data.

The level of security to be provided will also vary depending on the qualification of the IoT service providers. Under both the GDPR and the NIS Directive, the concerned operators have to adopt security measures which are "*appropriate and proportionate to the risk*". Even so, risks will have to appraised and mapped differently, and therefore security measures applied under the GDPR and the NIS Directive may overlap to some extent, but not entirely.

5. THE IOT PRIVACY FRAMEWORK

This chapter produces an overview of the IoT privacy framework, being a constitutive component of the broader IoT Policy framework discussed under the present deliverable. Taking into account the nature of privacy as a fundamental human right[13] and in view of best surfacing the human centred nature of the privacy framework per se –being part of the overarching human centred IoT Policy Framework proposed, the analysis below starts by using as a benchmark point of reference the user centred concerns associated with privacy. It further touches upon the basic requirements of European Data Protection Law (e.g. principle of data minimization, privacy by design etc.) that will be extensively discussed under the forthcoming deliverables due under "Task 05.03: Legal support, accountability and liability". Note that for the sake of the present discussion, the concepts of privacy and data protection are being used interchangeably.

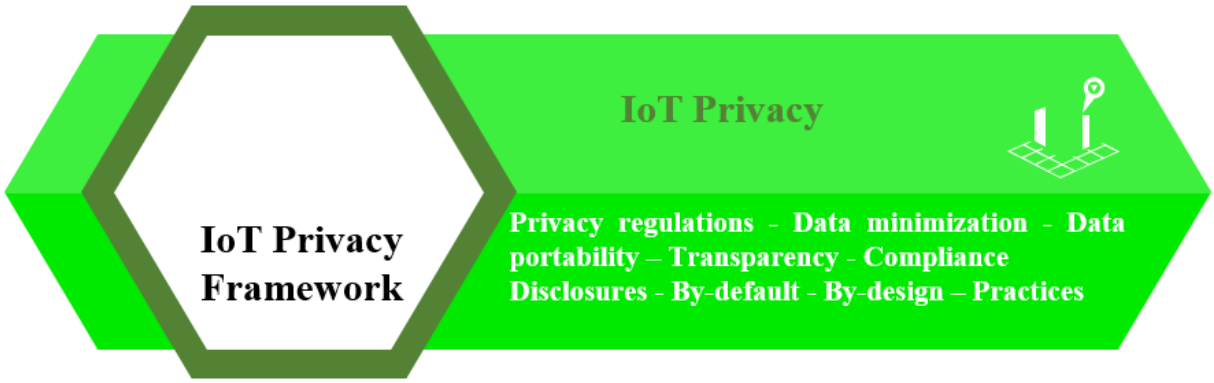


Figure 14: IoT Privacy framework[14]

5.1 The panorama of user centred concerns

Sensors, mobile phones, wearable objects, RFID tags, cameras, middleware components, have a common feature: they are all points of entrance of data, often personal data. As the players of the IoT landscape heavily leverage on personal data to deliver services and increase consumers' welfare, personal data protection and security are key elements in the "value creation chain" of IoT.

In this regard, IoT does not necessarily pose new challenges; it – however – makes traditional challenges escalate and multiply. For example, data subject's control on personal data becomes more difficult due to the dispersed number of data sources and entities processing personal data; as the chain of providers of IoT services stretches, allocation of responsibilities and enforcement of data protection law become more complex than before; and the same can be said with regards to compliance to the principles of purpose limitation and data minimisation. Plus, it is not easy to identify in each case what the viable legal ground for personal data processing is. The data subject's consent is not always a reliable one; in some cases – especially in the Smart Cities domain – Union or Member State law may constitute the legal basis for personal data processing through IoT deployments.

There is therefore an underlying relation between the need of privacy and the consequential need of trust in the IoT architectures handling our personal data, which renders necessary to make the IoT trustworthy and the data processing operations taking place therein transparent.

[13] Articles 7 and 8 of the Charter of Fundamental Rights of the European Union http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

[14] The concepts mentioned in the figure relate to the GDPR, discussed –to an extent- under the present chapter, though, they are not all of them addressed separately.

The need for privacy can thus be categorized around the following subcategories:

1. **Identity Privacy**: The need of privacy for information that can identify a person.
2. **Location Privacy**: The need of privacy for information that can identify a person's location, since the location is in itself a personal data which can reveal further personal data, e.g. points of interest
3. **Footprint Privacy**: The need of privacy for all personal data leaked unintentionally, e.g. Preferred language [40]. To these subcategories a further one should be added:
4. **Dynamic Privacy**: The need to keep control on the processes of profiling, inferencing and automated decision making started from the collected personal data, which can be further categorized in:
    a. **Device Trust**: Need to interact with reliable devices.
    b. **Processing Trust**: Need to interact with correct and meaningful data.
    c. **Connection Trust**: Requirement to exchange the right data with the right service providers and nobody else
    d. **System Trust**: Desire to leverage a dependable overall system. This can be achieved by providing as much transparency of the system as possible [40].

According to an elaboration made by IoT-EPI, the relation between privacy and trust in IoT can be defined with Figure 15 below:

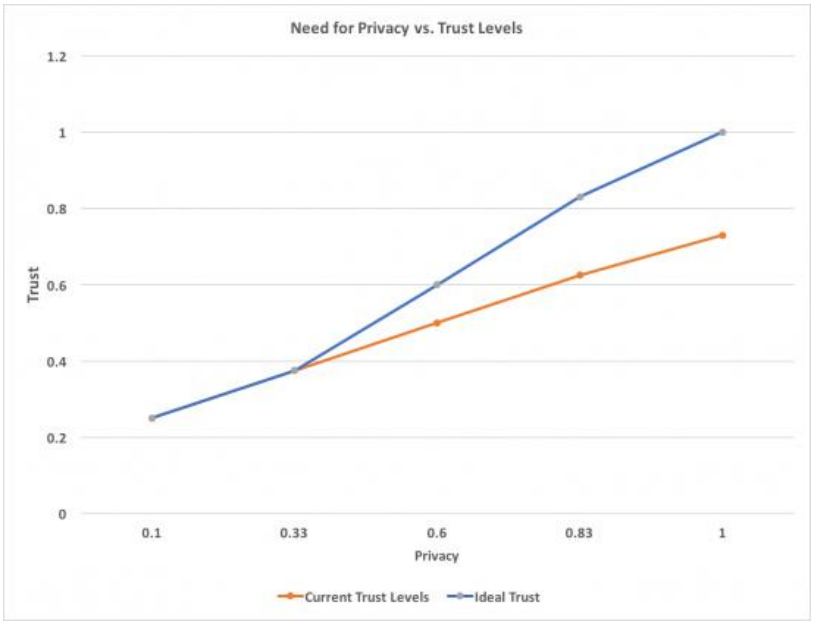


Figure 15: Relation between privacy and trust

This graph represents the required trust levels given a certain need for privacy. There we see, that even when the need for privacy is at a maximum, at 1, the required trust level towards a service / architecture is below 0.75.

Such a mismatch is due to the fact that for users it is impossible to trust a service / architecture 100% since there are too many unknown factors in the current state of things. An individual sharing personal data usually does not have a complete understanding of how the architecture is built up, about how security measures are realised or how trustworthy potentially involved third parties are. The graph also implies that that the user is not able to trust the service at the expected level in relation to his privacy needs – leaving room for improvement on the side of IoT device and

software vendors. IoT-EPI researchers have therefore included an "Ideal Trust" line in Figure 15 to indicate the user trust levels that vendors should be striving towards.[15]

The biggest challenge for IoT is therefore to fill this information asymmetry with users by means of technical and organisational user-friendly solutions.

One idea could be to deploy a **solution which measures the level of trustworthiness of a service using the traffic light metaphor**. Alternatively, a more elaborate dashboard could be used to give the user an overview of trust values and make adequate suggestions about which services to use [41].

Yet in some different contexts, like in the smart cities domain, users should be involved when carrying out **Privacy Impact Assessments** on the envisaged smart city initiative.

In fact, According to Article 35 (9) of Regulation 679/2016 on the processing of personal data (GDPR) "*Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations*".

This can be done through:

Open Consultation of users (citizens/data subjects)

Meetings or workshops with the data subjects' representatives

Other measures aimed at tackling trust and privacy issues of users could be:

- Anonymizing as much as possible; alternatively, personal data should at least be pseudonymized;
- Setting a clear retention and portability policy for personal data processed by IoT services;
- Informing users on the envisaged data processing operations, as well as on the stakeholders involved, by means of dashboards.

Furthermore, Create-IoT will leverage on several data protection related resources and tools that are developed by European research projects to strengthen user's acceptance, including:

1) Serious game on data protection for IoT

U4IoT is currently developing a serious game on IoT and data protection. The game will be used to raise awareness and educate the various stakeholders on the risks and obligations related to data protection when deploying IoT.

2) Privacy by Design Crowdsourcing Application

The IoT Lab European research project (www.iotlab.eu) developed a privacy by design smartphone application to perform crowdsourcing and collect end-user feedbacks in IoT testbeds, while ensuring a complete respect and protection of their personal data. The IoT Lab application is being redesigned by the U4IoT European research project in order to more specifically address the needs of the various IoT Large-Scale Pilots (LSPs). This new app is likely to be used and tested for collecting anonymized end-user feedbacks on Synchronicity IoT deployments.

3) EuroPrivacy Certification

The Privacy Flag European research project has contributed to the development of a European Certification Scheme on personal data protection named EuroPrivacy (www.europrivacy.org). EuroPrivacy will be used in the context of the City of Carouge (one of the Synchronicity reference zones).

[15] "The need for Privacy and its relation to Trust in the Internet of Things", http://iot-epi.eu/2017/08/10/privacy-and-trust-in-iot/.

4) European Privacy Portal

One of the partners of the Privacy Flag European research project has developed a European Privacy Portal (www.privacyportal.eu) that will be used to promote the Synchronicity privacy enablers.

5.2 Data Protection by Design: the overarching privacy principle

The Directive 95/46 – widely known as the Data Protection Directive – and the GDPR introduce a set of principles that should underlie the processing of personal information under EU Law. Those include principles such as the principle of data minimization[16] and the principle of purpose specification.[17] This section, though, puts emphasis on the principle of "Privacy by Design" that constitutes a newly introduced principle under Article 25 of the GDPR.

In particular, it has been argued that in order to implement a sound data protection approach within IoT, the key is to adhere privacy-by-design in advance [56]. Taking into account the aforementioned regulatory instruments and the associated challenges identified within the IoT environment, the basic set of principles for privacy-by design- are captured in the figure below:

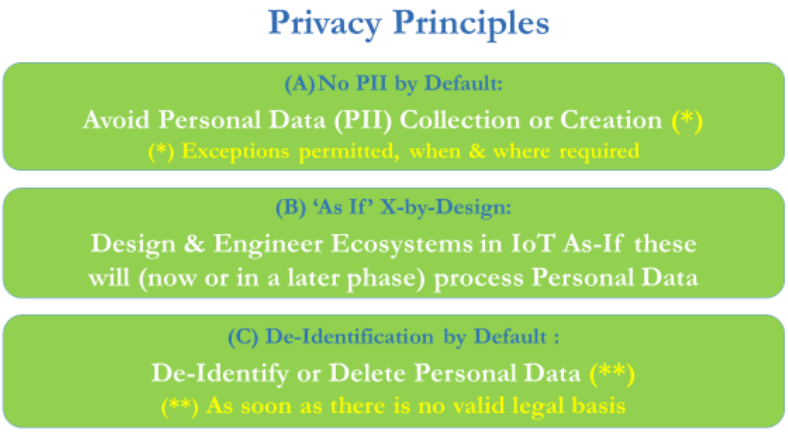


Figure 16: Privacy Principles

In particular:

- *No personal data by default* implies refraining from any collection or creation of personal data by default, except for cases where such collection or creation is legally required and to the exact extent required.
- *'As-If' X-by-Design* refers to the requirement that ecosystems are designed and engineered as-if these will process personal data at an immediate and/or later stage.
- *De-Identification by Default* refers to the de-identification, sanitization or deletion of personal data as soon as the legal basis for keeping such data ceases.
- *Data Minimization by Default* stipulates that personal data shall only be processed where, when and to the extent required; otherwise this data shall be deleted or de-identified.
- *Encryption by Default* refers to the requirement to encrypt personal data by default, while capturing both digital rights and digital rights management.

Note that the aforementioned set of principles will be further discussed under the final version of the present deliverables due in December 2019, as well as under the forthcoming deliverables

[16] The principle of "data minimization" means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it. See, also, https://edps.europa.eu/node/3099#data_minimization

[17] See also Article 5 (1) (b) of the Data Protection Directive and the General Data Protection Regulation (GDPR).

falling under the scope of "W05: IoT Policy Framework - Trusted, Safe and Legal Environment for IoT".

5.3 The close interconnection between privacy and security

The concepts of security and privacy, while exhibiting a complex and nuanced mesh of interrelationships, which includes touch points and areas of overlap, are different. A common misconception consists in the identification of confidentiality (one of the key constitutive concepts or goals of the information security triad, see definition given in ISO/IEC 27000:2009 [42]) with privacy. Several classical security techniques can be instrumental in enhancing privacy and personal data protection[18]. For example, data encryption cryptographic algorithms, hashing functions/digital signatures, and server mirroring (combined with effective identity and access management solutions that protect from unauthorized access and use) can help to ensure confidentiality, integrity and availability of personally identifying information. Proxy re-encryption, malleable signatures or homomorphic encryption are examples of newer security approaches to secure sharing or processing in untrusted environments of such data.

While security techniques are indeed relevant to support data protection and privacy, they do not guarantee per se the principles of privacy[19]. For instance, an e-Commerce transaction may be secured with https protocol but fail to apply the principle of data minimisation or, in the context of IoT, a device may be collecting and/or storing more data than is needed to provide a service e.g. relying on raw data rather than aggregated data[20]. Furthermore, some approaches to security which could be justified in some contexts as necessary, can nonetheless be detrimental to privacy goals and principles, for instance security checks (in particular body scanners) or boarding checks in airports (no anonymity allowed), or design choices e.g. use of stable identifiers in wearable things, may limit data subjects' possibilities to remain anonymous[21]. Thus, depending on a number of complex socio-ethical and even political factors in the specific contexts of application, security and privacy goals may be aligned or at different degrees of conflict. This relates to the notion of privacy being a fundamental right protected in Articles 7 and 8 of the Charter of Fundamental Rights of the EU[22], but not an absolute value inasmuch as context determines if and how it should be applied [43]. In fact, restrictions are contemplated as well to the application of data protection principles and data subjects rights in the General Data Protection Regulation[23] e.g. "when necessary and proportionate in a democratic society to safeguard: national security, defence, public security, the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties […]".

In order to classify the possible relations between security and privacy we can consider the **four world views** proposed by Wolfgang Hofkirchner [44]: reductionism, projectionism, dualism and dialectic. A suitable representation of them, along orthogonal axes, is provided in the figure below,

[18] The General Data Protection Regulation establishes the obligation for data controllers and processors to provide a description of the technical and organisational measures needs in the record of processing activities (Art. 30), and this is also a key element of Data Protection Impact Assessments (Art. 35, paragraph 6 (d)), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=ES

[19] See https://www.w3.org/P3P/mobile-privacy-ws/papers/zks.html

[20] See pp, 19, 23 of Article 29 Data Protection Working Party, WP223, Opinion 8/2014 on the on Recent Developments on the Internet of Things, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[21] Ibid., p.8.

[22] Charter of Fundamental Rights of the European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

[23] See Art. 23, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

where horizontal axis reflects a zero-sum or mutually exclusive trading-off of security vs privacy while the vertical axis considers alternative possibilities in the security-privacy relation:

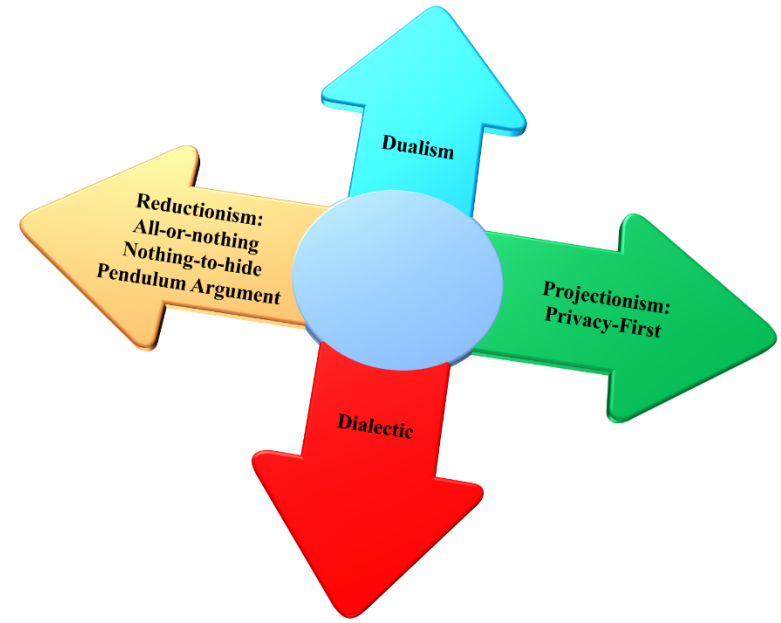


Figure 17: Relationship Privacy-Security

In the **reductionist** approach, security dominates privacy, that is, deprivation of rights to personal data protection i.e. indiscriminate surveillance, is justified on the grounds that well-behaving individuals should have "nothing to hide", that security is mutually exclusive of privacy in a zero-sum trade-off ("all or nothing") or that in times of crisis it is necessary to sacrifice or restrict human rights ("pendulum" argument). At the opposite end, the **projectionist** approach values privacy as an absolute good which must be preserved at the expense of security and even the common good of society. In the **dualistic** approach, security and privacy are seen as completely autonomous variables and is often related to the views on privacy by design advocated by former Ontario's Information and Privacy Commissioner Ann Cavoukian where privacy enhancing technologies can maximize both privacy and security. Finally, the **dialectical** approach tries to address, from human security concept that takes into account a broader view of the elements that cause instability and conflict in our global world, trying to address root causes of problems affecting common people and moving away from simplistic solutions based on technologies and law & order policies[24].

As an integrally constitutive part of the IoT Security Framework we propose, there is clear need to consider a **principle-based approach to security and privacy**. In this respect, in addition to data protection principles and security principles and measures explicitly mentioned in the GDPR (Arts. 5-11 and 32)[25], we consider standard ISO 29100[26], which defines a privacy framework provides a set of concepts (actors and roles, interactions, recognizing Personally Identifiable Information, privacy safeguarding requirements, privacy policies; and privacy controls) and a set of privacy principles: consent and choice, purpose legitimacy and specification, collection limitation, data minimization, use, retention and disclosure limitation, accuracy and quality, openness, transparency and notice, individual participation and access, accountability, information

[24] Please see a more complete discussion of the four views in pp.4-8 of Research Paper #6, Privacy and Security in Europe, Fuchs C., The Privacy & Security Research Paper Series, PACT Project, May 2013

[25] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=ES

[26] International Organization for Standardization (ISO), Information technology – Security techniques – Privacy framework, ISO/IEC 29100:2011, First edition, Geneva, 15 Dec 2011.

security, privacy compliance. As proposed in paper "A Privacy Engineering Framework for the Internet of Things"[27], additional principles should be added from an engineering viewpoint to this framework towards transforming it into a **privacy engineering framework** suitable to address the lifecycle of privacy controls and policies, with due consideration of privacy engineering principles and safeguards, actors' roles in the engineering process, use of common privacy engineering terms, among others[28]. The additional engineering principles described in this paper include the integration of risk management, compliance, goal-orientation (in requirements phase), data and process oriented design strategies, comprehensive lifecycle support as well as privacy-related objectives (unlink ability, transparency and intervenability)[29].

Further to this, a **privacy and security by design engineering methodology** is needed in order to make the above-mentioned principles from the privacy engineering framework operational in IoT systems and subsystems. For instance, the FP7 PRIPARE project[30] proposed a methodology[31] combining privacy risk analysis with a goal-oriented elicitation of operational requirements, integrates architecture-related decisions with PETs and privacy controls as a result of the design process and can be applied to cover entire IoT systems and subsystems (in the latter case focused on enabling features for building privacy control at integration time) engineering lifecycle, integrating with different mainstream development technologies.

[27] See pp. 24-25, Kung A. et al. (2017) A Privacy Engineering Framework for the Internet of Things. In: Leenes R., van Brakel R., Gutwirth S., De Hert P. (eds) Data Protection and Privacy: (In)visibilities and Infrastructures. Law, Governance and Technology Series, vol 36. Springer, Cham, https://link.springer.com/chapter/10.1007/978-3-319-50796-5_7/fulltext.html

[28] Ibid, p. 6

[29] Ibid. p. 24

[30] http://cordis.europa.eu/project/rcn/110590_en.html

[31] See http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf

6. THE IOT SECURITY FRAMEWORK

This chapter expands on the creation of an appropriate security framework for a human centred IoT. To this end, the analysis focuses on "secure systems", which –in the context- of the discussion below refer to the systems that are currently found in the "*state of being free from danger or threat* [32], or systems which are *not likely to fail or be lost*.[33]"

Taking into account that human centred computing is often defined as the study of systems mixing human and computing systems involving human interactions, human centred design, and human empowerment, the analysis to follow focuses on human centred IoT systems.[34]

Note that the term security is used as an overarching term that subsumes other terms, including ICT security. Instead of the term security framework, we have also considered using the term dependability framework.

Due to the strong domain connotation of the term "dependability[35]", though, referring to fault tolerant systems or safety critical systems, the term "security" was considered most appropriate.

The construction of the framework is based on the following approach: security, dependability and privacy properties must be applied throughout the lifecycle processes of IoT systems. This includes impact assessment (when risks are assessed) and design of controls (when risks are mitigated).

The obtained security framework also includes the necessary assurance of the processes to allows for trust.

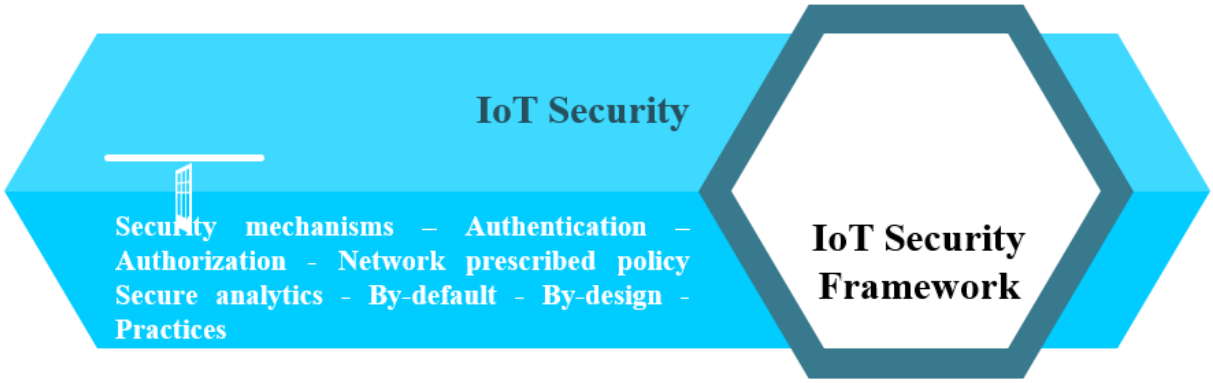


Figure 18: IoT Security Framework

6.1 Objectives of framework

As showed in Figure 19, the IoT security framework has to take into account the following elements:

- Ensuring IoT security mechanisms
- Ensuring IoT data protection
- Ensuring IoT system resilience
- Providing IoT system/application trust

[32] https://en.oxforddictionaries.com/definition/security
[33] http://dictionary.cambridge.org/dictionary/english/security
[34] The Cambridge dictionary states that *human centred* is an adjective used to describe systems that are *designed to work in ways that people can easily understand and learn. See, also,* http://dictionary.cambridge.org/dictionary/english/human-centered
[35] Dependability is the *ability to deliver a service that can justifiably be trusted*. Another definition of dependability is the *ability to avoid service failures that are more frequent and more severe than is acceptable.*

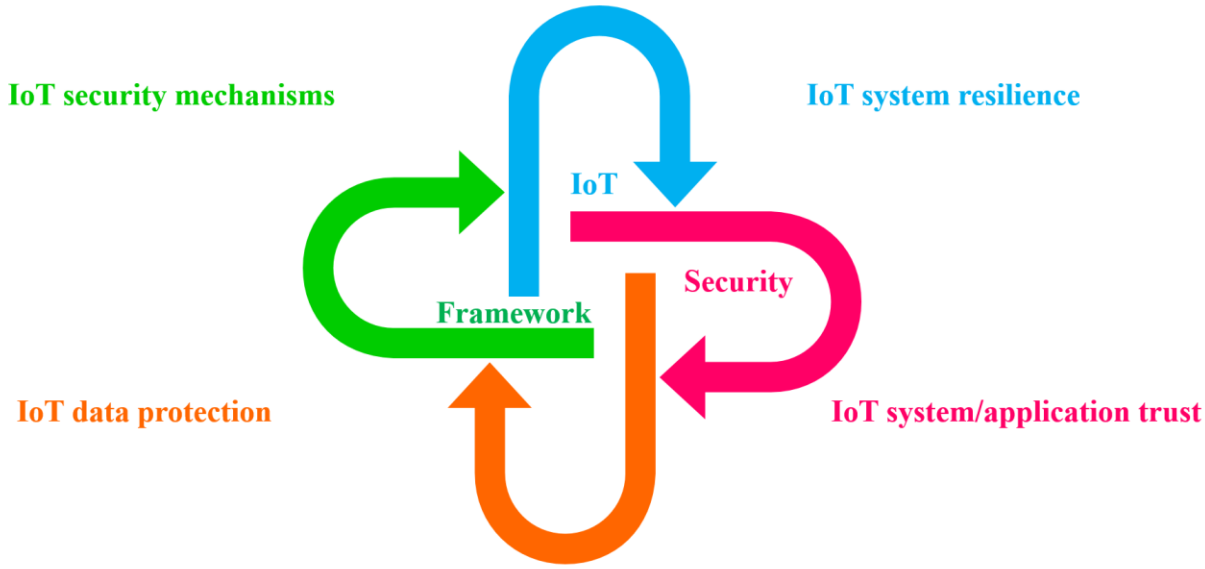


Figure 19: Key Objectives of a Security Framework for a human Centred IoT

Figure 20 shows the relationship between the key objectives: data protection and resilience are the two pillar objectives concerning dependability in IoT systems, while trust is associated with the accepted level of dependence.

Figure 20: Trust - Accepted dependence

6.1 Security, Dependability and Privacy Properties

The following properties have been proposed for security, privacy and dependability.

- Properties for security are often based on the established CIA triad of confidentiality, integrity, and availability:
  - Confidentiality ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes. Examples of measures for achieving or enhancing confidentiality include protected transmission of collected data, protected access with suitable authentication schemes, protected processing of data, and protected storage.

- Integrity ensures the accuracy and completeness of data over its entire life cycle. Examples of measures for achieving or enhancing integrity include schemes such as digital signatures.
- Availability ensures accessibility and usability upon demand by an authorized entity. Examples of measures for achieving or enhancing availability include preventing service disruptions due to power outages, hardware failures, or security denial of service attacks using schemes such as redundant systems.

- Properties for dependability are often based on the landmark paper published in 2004 combining security and dependability [45]:
  - The CIA triad (Confidentiality, Integrity, Availability)
  - Reliability, defined as continuity of correct service
  - Safety defined as the absence of catastrophic consequences on the user(s) and the environment
  - Maintainability defined as the ability to undergo modifications and repairs
- Three properties have been defined for privacy [46], unlink ability, transparency, intervenability. They are presented as the extension of the security triad:
  - Unlink ability ensures that a use may make multiple uses of resources or services without others being able to link these uses together. The objective of unlink ability is to minimize the risk to privacy created by the potential linking of separate sets of personal data, for instance a customer uses two different accounts for navigation and for telephone calls.
  - Transparency ensures that an adequate level of clarity of the processes is reached so that the measures taken during the lifecycle for security and privacy can be understood and reconstructed at any time. Transparency covers the entire system life cycle. Transparency allows stakeholder to reconstruct and improve the legal, technical and organisational setting in case it is needed, for instance when there is a security or privacy breach.
  - Intervenability ensures that relevant partners can intervene in security and privacy operations. The objective of intervenability is to provide the possibility for parties involved in any privacy-relevant data processing to interfere with the ongoing or planned data processing. This can possibly involve the application of corrective measures and counterbalances where necessary, for instance requesting for data erasure, withdraw consent.

6.2 Life Cycle Processes for Security, Dependability, Privacy

In order to meet the objectives of the security framework, a number of processes must be integrated as showed in Figure 21 must:

- Impact assessment (focus is on risk analysis activities)
- Controls (focus is on the measures)
- Assurance (focus is on activities that are aimed in raising confidence).

We have singled out these processes, because:

- They are the pillar processes to achieve data protection, resilience, trust,
- They will involve substantial development and organisation resources,
- They will affect profoundly the design, deployment and operation of IoT systems.

In particular**, Security, dependability and privacy impact assessment in life cycle** analyses the effect of vulnerabilities concerning data protection, resilience and trust in IoT systems:

A data protection impact assessment corresponds to the analysis of risks concerning data protection (e.g. unauthorised personal data processing), their consequences (e.g. privacy breach) and their mitigations (e.g. minimizing data collection),

A resilience impact assessment corresponds to the analysis of risks concerning ICT security (e.g. denial of service of the electricity grid), their consequences (e.g. essential services not available) and their mitigations (e.g. incident response measures),

A trust impact assessment corresponds to the analysis of risks concerning trust vulnerabilities (e.g. lack of transparency at the governance level), their consequences (e.g. lack of trust on some applications/solutions/stakeholders) and their mitigations (e.g. providing an information desk for citizens, setting up a citizen engagement process). This is a higher-level assessment that is not widely promoted, nor defined.

Security, dependability and privacy controls in life cycle corresponds to a focus on organisational and technical measures for security, dependability and privacy in the life cycle of IoT systems:

The integration of data protection corresponds to privacy-by-design (e.g. the definition of ISO/IEC 27550 privacy engineering) and to data protection by design and data protection by default as stated in the GDPR.

The integration of resilience corresponds to cybersecurity (e.g. the NIST cybersecurity framework[36], or the NIST publication on systems security engineering[37]), with definition of phases such as Identify, Protect, Detect, Respond, Recover.

The integration of trust corresponds to trust-by-design (e.g. transparency capabilities, empowerment capabilities, accountability practice). It can be argued that trust-by-design integrates data protection and resilience. For instance, data protection compliance could require data controllers to keep a registry of all personal data processing activities.

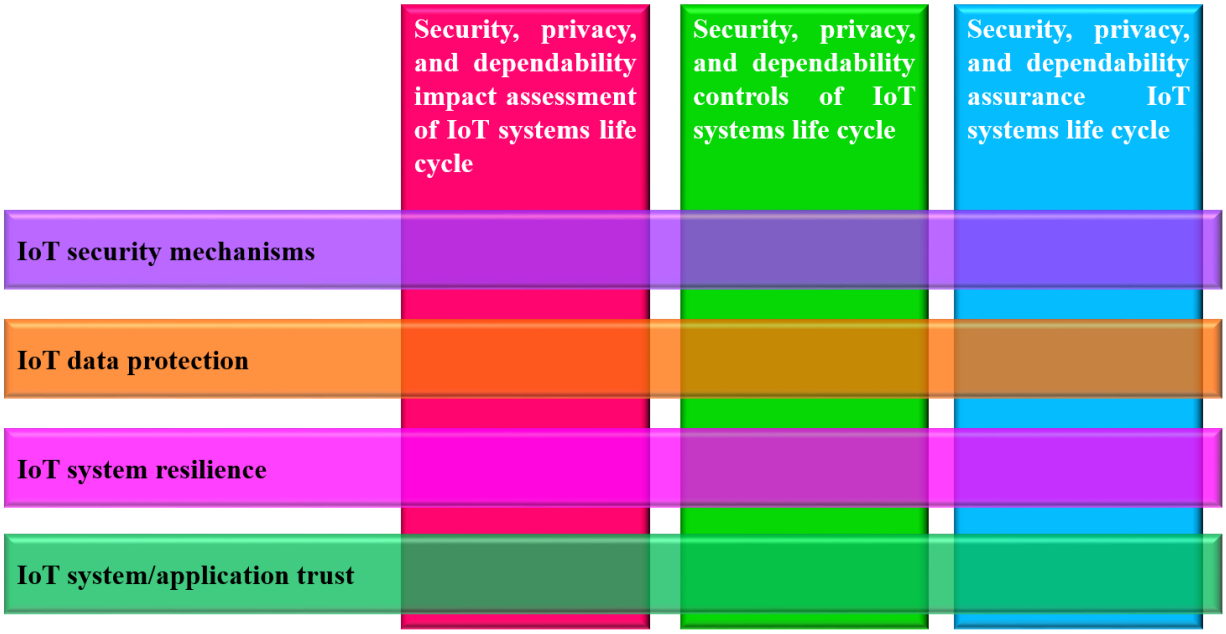


Figure 21: Lifecycle processes for security, dependability and privacy

Security, dependability and privacy assurance in life cycle corresponds to processes to ensure that IoT systems meet a defined level of data protection, resilience and trust:

Data protection assurance corresponds to the activities that will help demonstrate that a given level of data protection is reached. This can involve privacy impact assessment audits, privacy

[36] https://www.nist.gov/cyberframework

[37] http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf

engineering audits, interoperability verification activities (e.g. user expresses privacy preferences, which must be shared by multiple application providers), or certification activities[38].

Resilience assurance corresponds to the activities that will help demonstrate that a given level of resilience is reached. This can involve security assurance and audits and certification (e.g. common criteria evaluation). Resilience depends on the services. For instance, resilience of essential services (e.g. finance, electricity) will necessitate more stringent levels.

Trust assurance corresponds to the activities that will help demonstrate that a given level of trust is reached. This can involve transparency assurance activities (e.g. verifying that a citizen privacy breaches complain is properly handled, or verifying that a registry of personal data processing activities is compliant with GDPR).

Assurance refers to processes that are largely influenced by policies from data protection authorities (for data protection and GDPR compliance) and national security centres (for resilience and the NIS directive). Note that at the moment that this document is being drafted European Commission released an EU Cybersecurity Legislative Package consisting of several Communications and Reports, as well as a proposal for a new ENISA Regulation. These developments will be addressed under D05.05 Legal IoT Framework due in December 2017.

6.3 Organisations and roles in the processes

IoT systems involve a complex ecosystem of stakeholders. This is because many such systems are systems of systems. For instance, autonomous vehicles are systems that are integrated in a higher transport system infrastructure.

It is therefore important to provide a categorisation of the main roles in the ecosystems, as individual organisations specialised in a given role will use the security framework in IoT from different viewpoints.

Figure 22 shows an example of categorisation:

- Suppliers provide the technologies and components that will be integrated in an IoT system. Such suppliers have one main objective: meeting the needs of a market. When it comes to the security framework in IoT, these suppliers are expected to provide capabilities that will be useful to meet the requirements associated with trust, data protection and resilience, for instance a storage system could include access right management capabilities.
- Integrators select suppliers' products and integrate them in order to deliver an IoT application. The integrators play a key role in selecting and developing properly the capabilities underlying the security framework in IoT
- Operators are responsible for the deployment, maintenance or removal of IoT applications. Hence, they are responsible for the provision of the right level of trust, data protection and resilience.
- Authorities provide an overall governance. This governance can be limited to regulation supervision (e.g. consumer market applications), or it could involve significant responsibilities (e.g. smart city applications).

The observance of the security framework in a IoT systems is made difficult by:

- Multiple levels of stakeholders (e.g. data controllers and data processors concerning data protection),
- Multiple supply chains (e.g. electric vehicles involve the smart grid supply chain, the automotive supply chain, and the ICT supply chain);

[38] This will be depending on policies. For instance, it is a general practice that safety oriented application are subject to certification schemes.

- Multiple interoperability requirements (e.g. an application can access similar devices)
- Multiple system lifecycles (e.g. integrating new systems with legacy systems).

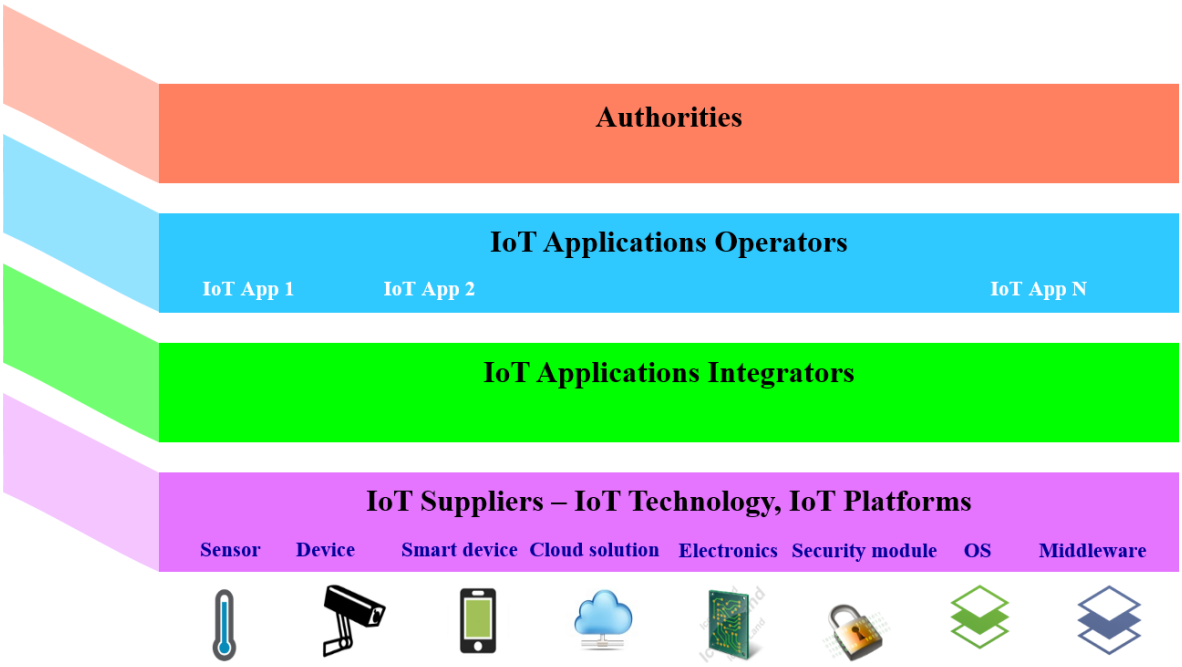


Figure 22: Organisations and roles in the Secure Framework for IoT

Consequently, it is necessary to optimise the positioning of each individual stakeholders, suppliers, integrators, operators and authorities with respect to the security framework:

- Key components: trust, data protection, resilience
- Associated processes: impact assessment, control design and assurance

6.4 Integrating organisation and roles in IoT Architectures

The security framework points out the importance of organisations and roles in the security framework. This emphasis is also visible in current standardisation initiatives:

- On IoT standards
  - The current standard being developed on an IoT reference architecture (ISO 30141 integrates a so-called usage view. The current version (January 2017) defines the following roles: IoT service provider, IoT service developer and IoT-user.
  - Current discussions which will lead to the creation of a new standard on security and privacy guidelines for the IoT is likely to take a lifecycle viewpoint[39].
- On big data standards
  - The current standard being developed on a big data reference architecture (ISO 20547-part 3) defines the following roles: data provider, big data framework provider, big data service partner, big data application provider, big data consumer.
  - The current standard being developed on big data security and privacy (ISO 20547 part 4) defines the following roles: big data security and privacy planner, big data security and

[39] The following phases are proposed by the Japanese contribution: establish policy, identify risks, apply secure design basics, apply network controls, maintain security.

privacy manager, big data security and privacy implementer, big data security and privacy operator, big data security and privacy auditor[40].

- On smart city standards
  - The current standard being developed on smart city business process framework (ISO 30145-1) defines a specific process on safety, security and resilience which follows the following principles
    - Holistic approach
    - Aggregation data from multiple sources to manage safety, security and resilience
    - Elaboration of deployment of data privacy standards
    - Separation between critical and non-critical services of the city so that services can be engineered accordingly
    - disaster recovery plans that are regularly tested

This is also visible in current research initiatives. For instance, the CTI French SystemX project on cybersecurity for intelligent transport is currently investigating a common ITS architecture, identifying three types of isolation: certified/non- certified isolation, safety/non safety isolation, critical/non critical isolation.

6.5 The main security domains of IoT

Figure 10 shows how IoT systems can be decomposed into different segments.

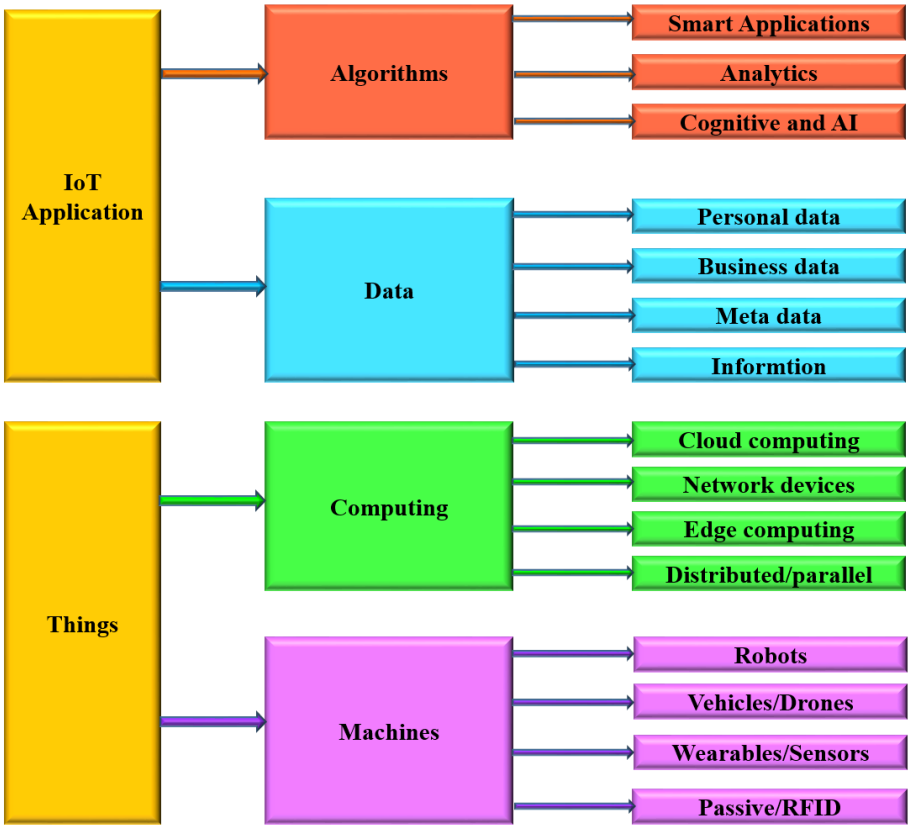


Figure 23: Security Domains of IoT

The segments address several areas as explained below:

- The vision is that there are IoT applications which take advantage of features provide by things.

[40] E.g. the manager typically focusses on impact assessment, and institutional and life cycle integration. The auditor focuses on assurance.

- IoT applications consist of algorithms and data. Examples of algorithms are smart applications, analytics. Examples of data are personal data, business data and meta data.
- Things consist of computing facilities and machines. Examples of computing facilities are cloud computing, network devices, edge computing. Examples of machines are robots, vehicles, drones, wearables, sensors.

The rationale for defining security domains is to provide a taxonomy to allow for comprehensive risk analysis (for trust, data protection and resilience). Figure 23 provides another categorisation for complex systems such as vehicles, drones or rail systems: perception means, communication channels, embedded devices, on-board storage and shared services.

6.6 Applicable State-of-the-Art Security in IoT Principles

Taking into account the significance of an IoT Security Framework for an effective IoT Policy Framework discussed earlier under this deliverable document, this section depicts what actually happens at an organizational level in relation to security and proposes SOTA Methodology as the way forward.

Setting the scene

Rather than investing heavily in ensuring highly secure solutions, organizations often take the 'Build-Fast Fix-Later' route when deploying new products. In most cases these devices suffer from symptoms of premature connectivity and do not contribute to creating a secure and trusted environment.

For this reason, many organizations are currently faced with a challenge of having to advance from a stage of low-cost hygiene: in order to bring legacy systems to 'X-by-Design' state (where 'X' includes security, compliance, (personal) data protection, convenience, etc.) and become hyper-compliant organizations need to find appropriate ways of achieving state-of-the-art cyber resilience, which may include any combination of retrofitting, redesigning or designing from the very beginning. In short, if one cannot afford to ensure proper security, then one should cannot afford to connect.

The regulatory instruments discussed previously under this document applicable as of 2018, namely, the GDPR and the Directive on Security of Network and Information Systems (NIS Directive). require all organizations around the world doing business in the European Union – so, including organizations from the United States – to comply. Although many organizations have recently taken steps and implemented organizational and technical measures in order to seek and obtain compliance and assurance regarding various international information security standards, such as the ISO 27000 series, with the recently adopted user centred GDPR, just being compliant to international or other standards is not enough anymore and would actually mean regulatory non-compliance.

The SOTA Methodology

The State-of-the-Art ('SOTA') Security methodology presented below aims to facilitate organizations' compliance by design with these legal developments.

The SOTA methodology -relevant for both public and private organizations- recognizes that every IoT ecosystem consists of core a stack of layers and dimensions (including, among others, the user, data, application and infrastructure). It is created on the basis of thorough examination and reviewing of numerous relevant standards, guidelines, best practices, frameworks and other resources developed and made publicly available by various stakeholders, including the U.S. Department of Homeland Security, National Institute of Standards and Technology and other organizations. The subsequent systemizing and segmenting have resulted in identification of almost 400 unique security principles which have been plotted against the appropriate layers and dimensions. The relevance of individual principles to stakeholders varies with respect to context,

i.e. the stakeholder's role in the ecosystem and domain. Based on a couple of simple criteria, an individual stakeholder can utilize the methodology and use it as a tool to produce a set of relevant and applicable principles to ensure state-of-the-art cyber security.

In particular, State-of-the-Art security of IoT ecosystems is essential for achieving high-level security as well as sustainability and durability of these ecosystems. Recognising this fact, SOTA Methodology provides the organization using this methodology with customised set of high-level official and validated security principles and requirements. It does so using a using a unique *State-of-the-Art Security in IoT* (SOTA) methodology.

It has been recognized that IoT ecosystems consist of the following layers (numbers 3, 4, 5 and 7 below) and dimensions (numbers 1, 2 and 6 below) where dimensions may be relevant in one, more or all layers:

1. User/Human factor
2. Data
3. Service
4. Software/Application
5. Hardware
6. Authentication
7. Architecture/Network

When determining and implementing applicable SOTA principles, an organisation should carefully assess these principles while taking account of every individual layer and dimension. Especially, organizations should approach both security and privacy from the "by design" perspective, requiring IoT devices to take security- and privacy-related requirements into consideration already at the stage of their early design. On the one hand, by doing so, an organisation will be able to demonstrate that it is a mature, aware, accountable and relevant market player, and thus establish the desired level of trust with its partners and customers. On the other hand, many of the presented principles are reflected in mandatory legal requirements contained in new tech-related laws applicable as of 2018 (including the General Data Protection Regulation and the Directive on Security of Network and Information Systems).

The relevance of SOTA principles is based on the organisation's answers to the set of questions mentioned below. These have been found relevant and selected from a repository of almost 400 unique and individual principles identified in numerous sufficiently mature standards, guidelines, best practices, frameworks and other resources published by various governments, government agencies, state bodies, industry associations, international organizations and other relevant stakeholders. The resources have been carefully analysed, semantically and taxonomically unified, and segmented against the above stated layers and dimensions. Finally, their relevance in respect of the stakeholders' context has been assessed to enable the production of this resulting set of principles.

The SOTA paradigm

The set of SOTA principles outlined above is based on the role and context of an organisation within the IoT ecosystem. This is done based on answers to the following four categories of questions listed below:

1. Identification:

Which LSP do you identify yourself in?

i. ACTIVAGE
ii. IoF2020
iii. MONICA
iv. SYNCHRONICITY
v. AUTOPILOT

2. Persona:

In what context does your persona act?

i. Demand side *[tick the box]*
   a. End-user
   b. Customer
   c. BOTH

ii. Provider *[tick the box]*
   a. Data
   b. Services
   c. Software
   d. Hardware
   e. Network
   f. ALL

3. Data:

What data classes are you involved in?

i. Non-Personal data
ii. Personal data
iii. Sensitive data
iv. Classified data
v. Trade Secrets & IPR
vi. ALL

4. Data Life Cycle:

Which data life cycle phases are most relevant for you?

i. Obtain / Collect
ii. Create / Derive
iii. Use
iv. Store
v. Share / Disclose
vi. Archive
vii. Destroy / Delete
viii. ALL

Applicable Guidelines

Based on specific answers provided to four questions above, this Section consists of the set of SOTA principles applicable to the respective scenario.

Please note that for purposes of this demonstration, this document only identifies the selection of relevant principles from a total of 52 principles identified reports of two workshops organised in 2016 and 2017 by the European Commission and the Alliance for Internet of Things Innovation [48], [49].

1. User/Human factor

1.1. **Basic principles:**

1.1.1. *Human centred approach:* Security and privacy should be universally applied to all users.

1.1.2. *Privacy by design:* Privacy of users must be embedded into the design of business processes, technologies, operations and information architectures. Each service or business process designed to use personal data must take all the necessary security requirements into consideration at the initial stages of

their developments. Privacy must be embedded into the design of business processes, technologies, operations and information architectures.

1.1.3. *Privacy by default:* The strictest privacy settings and mechanisms must automatically apply once a user acquires a new product or service; no manual change to the privacy settings should be required on the part of the user.

1.1.4. *Decoupling multiple identities:* It should be easy to decouple multiple personae of the users from one another.

1.2. **User's awareness and control:**

1.2.1. *Transparency of data processing:* The service provider should empower users to know what the devices are doing and what personal data they are sharing and why, even if it concerns M2M communications and transactions.

1.2.2. *Transparency of privacy policy:* The service provider should ensure that the user is and remains clear and aware of privacy issues, choices it makes and possible consequences thereof.

1.3. **Handling of personal data:**

1.3.1. *Non-discriminatory practices:* The service provider should ensure non-discriminatory practices against users and businesses on the basis of information derived from IoT deployments (e.g. within smart cities).

1.3.2. *Manufacturer-implemented parametrization:* By design, the user should be able to configure and manage rights for accessing data controlled by them based on the assessment where (in its lifecycle) the device comes into contact with personal data, creates/derives (new) personal data, or otherwise processes personal data, while keeping in my mind the contextuality of purposes and use, as well as multi-purpose Things and IoT ecosystems.

2. Data

2.1. **Data segmentation and classification:** According to the Cloud Service Level Agreement Standardisation Guidelines published by the European Commission, "data" implies "data of any form, nature or structure, 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." Service providers should ensure segmentation and classification of data, that is contextualising data with respect to its purpose, risk and impact, and persona. Data classification enables processing of data with respect to the description of different classes of data. For instance, regarding personal data, data should be segmented according to the multiple personae each user has, and the related protection – including fundamental and consumer rights – it has.

2.2. **Indication of purpose:** The service provider should indicate the purpose of data collection and ensure that personal data is collected for that specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes.

2.3. **Consent:** Based on the particulars provided by the data controller to the user, the user should express an informed and unambiguous consent per contextual processing of personal data (which data for which use). No data should be collected and processed without this consent.

2.4. **Data minimisation:** The less data an actor can access, the less risk there is of a security breach. If data is minimised based on a specific purpose, there is less chance that the actor will breach trust (and the law). Data minimisation starts with only requesting, collecting, obtaining, deriving and processing personal data to the extent necessary (need-to- know principle). The data provider should observe the principle of data minimisation, i.e. (i) only collect personal data whose collection the user has consented

to, and (ii) erase personal data from whenever they are stored as soon as they are no longer necessary.

2.5. **De-identification:** The service provider should design and apply and de identification capabilities so personal data is de identified as soon as legally possible.

2.6. **Data control:** User should have the possibility to opt-out, right to their data, portability of their data, communication platform to control data access and to ensure security and privacy, and the overall securing of personal data processed, also in the context of related systems and devices.

2.7. **Data access:** The service provider should make it possible to technically regulate access to data to define who can use it for what purpose, and how that can be made transparent, and subsequently measured and monitored (relevant in e.g. connected automobiles domain).

2.8. **Data ownership:** The service provider should clarify the principles of ownership of user's data.

2.9. **Data management/Data stewardship:** The service provider should apply a process to manage data of users not only as a business necessity but also on behalf of the individuals themselves. The service providers should apply an ethical approach to data handling.

2.10. **Data isolation:** Functional separation of datasets and databases should be in place.

2.11. **Security of personal data:** The service provider should obey by the principles of data availability, integrity, confidentiality, transparency, unlinkability/isolation and intervenability.

2.12. **Encryption:**

2.12.1. *Encryption by default:* Encryption should be applied at all stages of handling data, including in communication, storage od data at rest, storage of keys, identification, access, as well as for secure boot process.

2.12.2. *Encryption at the application layer:* Data should be encrypted on the application layer. End-to-End security, cryptographic principles and key management are extremely important and should be carefully described.

2.12.3. *Standardisation:* All aspects of cryptographic principles and key management should be carefully described.

2.13. **Compliance with data protection legislation:** Any service provider should be accountable for regulatory, contractual and ethical compliance.

2.14. **Accountability:** Any service provider should be accountable for regulatory, contractual and ethical compliance, as well as for any misuse of collected personal data. If data is compromised, disclosed, accessed or lost, clear statement by vendors, data controllers and data processors on impact is another prerequisite.

2.15. **Risk impact assessment by design:** The service provider should carry out an assessment of the risk of data being compromised, disclosed, accessed or lost. Likewise, an assessment of the consequences from regulatory, contractual and ethical perspective should be carried out.

2.15.1. *Accountability:* Any service provider should be accountable for regulatory, contractual and ethical compliance.

3. Services

3.1. **Metrics:** The service provider should engage dynamic trust key performance indicators and metrics on security, privacy, safety, resilience, reliability and the like.

3.2. **Life time protection:** Give security, safety and privacy protection over the full life time.

3.3. **Single point of contact:** The service provider should provide a single point of contact for personal data protection and privacy.

3.4. **Support:** End of support: Where the current practice is about 12 to 15 years, the end of life cycle and the related support is prerequisite. Questions to be addressed are: what happens if a services agreement is lawfully terminated, is there an update possibility, when will updating and upgrading become limited, and who is accountable for the risk of not updating IoT devices and systems.

4. Software/Application

4.1. **Security by default:** The service provider should ensure that the most secure, proven, well understood and securely updateable setting are indispensable before starting operations and during IoT life time.

4.2. **Updatability:**

4.2.1. *Secure updates:* Trusted and transparent updates should only be provided by authorised parties, not by malicious actors.

4.2.2. *Frequency of updates:* Software providers should ensure regular updates and upgrades during the device lifetime.

4.3. **Accountability and liability:** Manufacturers must be accountable and liable as they have or should have total control of the entire design, manufacturing and software development lifecycle; to execute third-party software the manufacturer should set the rules to ensure that the software is compliant with them.

4.4. **Third-party libraries:** Software developers should put rules in place for maintaining, updates and checking for vulnerabilities of third-party libraries.

5. Hardware

5.1. **Security principles:**

5.1.1. *High-level baseline:* High level baseline should be applied when safety is at stake or critical infrastructure or national safety can be materially impacted.

5.1.2. *Safe and secure interactions:* Manufacturers have to implement and validate safety principles, separately from security principles.

5.1.3. *Security rationale:* Manufacturers should be required to provide explanation of implemented security measures related to expected security risks from any designer of IoT device, auditable by independent third party.

5.1.4. *Security evaluation:* Manufacturers should specify precisely capabilities of device of a particular type. This could help to manage liability and evolutivity on system level.

5.1.5. *Security levels:* The industry should make use of the security scale 0 – 4 fit to the market understanding.

5.1.6. *Sustainability:* Manufacturers should ensure that connected devices as well as any IoT component as defined above are durable and maintained as per its purpose, context and respective life cycle.

5.1.7. *'As-if' by design:* The devices and ecosystems must be engineered as if these will (now or in a later phase) process personal data.

5.1.8. *Assurance:* Component and system suppliers need to be prepared for security monitoring and system maintenance over the entire life cycle and need to provide end of life guarantees for vulnerabilities notifications, updates, patches and support.

5.2. **Certification and Labelling:**

5.2.1. *Certification:* Device manufacturers should test devices and make use of existing, proven certifications recognized as state-of-the-art based on assessed risk level. Additional introduction of a classification system to certify devices for use in particular use case scenarios depending on the level of risk should be encouraged.

5.2.2. *Trusted IoT label:* Labels such as the 'Energy efficiency label' of appliances should give a baseline requirement of protection based on the level of

assurances and robustness, and should be used to classify individual IoT devices.

5.3. **Secure Performance and Functionality:**

5.3.1. *Defined functions:* Manufacturers should ensure that IoT devices are only able to perform documented functions, particular for the device/service.

5.3.2. *Secure interface points:* Manufacturers should identify and secure interface points also to reduce the risk of security breach.

6. Authentication

6.1. **Authentication of identities among themselves:** In the context of communication of various applications, authentication of identities should be open to all technologies and applications.

6.2. **Identity protection by design:** Decoupling personal identity of a user from device identity should be possible.

6.3. **Transparent roles:** The service provider should ensure clear allocation and identification of roles, including who is data controller, co-controller, processor, co-processor, and so forth.

7. Infrastructure/Network

7.1. **Architecture & Ecosystem:**

7.1.1. *Interoperability:* Stakeholders should aim at achieving interoperability of components and communication protocols. Manufacturers should aim at creating interoperable devices.

7.2. **Knowledge sharing:**

7.2.1. *Monitor and respond:* Stakeholders should ensure continuous monitoring and improvement of relevant IoT ecosystems, including clear metrics and measurements.

7.2.2. *Information sharing platforms:* Stakeholders should be active in sharing information about incidents/potential vulnerabilities with each other.

Other items

1. **Independent privacy and security audits:** Organizations of certain size and public bodies should mandatorily carry out third party privacy and security audits.
2. **Harmonised industry approach:** Stakeholders should participate in standardisation efforts of the functional and security assurance requirements through common harmonised industry approach. This should ensure that devices are designed, manufactured and assembled with clear understanding of what means what, and to what extent there is consensus in the related complex value chain and ecosystems. At the same time, the goals of data protection such as limiting the scope of data processing to the necessary level should be promoted, as well as data segmentation, mapping, categorisation, purpose limitation, data isolation, and data control and data access of personal data are seen as prerequisite elements.
3. **Reduce impact of national regulations:** Stakeholders should actively participate in harmonisation efforts to reduce the impact of different national regulations.
4. **Taxonomy:** The basic taxonomy does not need to be perfect, but sufficiently workable. Definitions established as prerequisite include *data*, *personal data*, *data controllers and other actors*, *the personal data life cycle*, *IoT ecosystems* and the *physical* and *virtual "Things".*

It should be noted that due to the nature of the subject, the applicable set of relevant SOTA principles is likely to develop over time taking into account additional resources reflecting developments in the IoT domain as they become publicly available. While the repository of SOTA principles will be regularly reviewed and kept up to date, it is essential that every organisation refers to this methodology periodically in order to obtain an up-to-date customised overview of principles to ensure that its security measures are state-of-the-art and hyper-compliant.

Note that a more extensive discussion of the SOTA methodology will be incorporated under the final report, "D05.02 IoT Policy Framework Evaluation & Final IoT Policy Framework" due in December 2019.

7. CONCLUDING REMARKS

The Internet of Things has become a highly relevant domain encompassing a vast number of devices, processes and services that are playing an important role in people's lives. However, IoT technologies and applications expose us to a wider number of challenges, including policy and governance, some of which are already present nowadays, i.e. unification of the rules pertaining to the protection of personal data within the EU. Other policy challenges are arising in conjunction with the development and deployment of other new technologies such as 5G, smart data, cybersecurity, autonomous systems or artificial intelligence. IoT systems need to be progressively integrated with the complex systems of practically all large vertical domains; Industry, Manufacturing, Robotics, Aeronautics, Intelligent Transport Systems, Maritime, Smart Living, eHealth, Farm and Food, Energy, Buildings, Environment, Cities.

In this context, it is apparent that the journey on the road to the 'Internet of Everything' is going to take time to complete. On this journey, the role of IoT standardisation in the emergence of IoT on a largescale will be key. One of its major challenges is to help break the silos and support the integration of new, currently unforeseen, cross domain, federated applications based on open, interoperable solutions. In breaking the silos, it is essential that engagement and the cooperation of relevant stakeholders is encouraged and supported, and that sufficient resources are devoted to creating a culture within this broader community. Finally, it is essential that any and all further developments are made from the human centred perspective, i.e. with the user and their needs and expectations in mind.

To this end, the analysis elaborated under the present deliverable has considered numerous frameworks relevant for the IoT Policy Framework. Under its respective sections, it has thoroughly considered the concepts of *trust*, *engagement*, *privacy* and *security*. Respectively, the deliverable has analysed the components of IoT trust, engagement frameworks applicable to every entity wishing to become a part of the community, data protection and privacy under the GDPR as well as the importance of applying a methodology of state-of-the-art security requirements. These individual domains develop a multi-layered, cross-cutting, multidisciplinary and integrated approach, and together they form a part of the high-level IoT architecture. Moreover, the analysis expands on engagement, aiming to ensure the effectiveness of the frameworks by focusing on the behaviour of the IoT stakeholders. The effectiveness of those interoperable frameworks is of key importance for the fostering of industry innovation as well as for the motivation of adoption and wide participation in the IoT marketplace. Also, based on the assumption that security and privacy are assigned with complementing functions, the IoT Privacy Framework points at the relevant principles and requirements for privacy under EU law, in light of the forthcoming development, especially, of the GDPR to be applicable as of the 25th of May 2018. Finally, the IoT Security Framework Security puts forward a human centred, yet pragmatic approach for building a trustworthy and sustainable IoT ecosystem, while also presenting a methodology based on the state of the art security principles.

Overall and taking account of the concrete requests raised by partners with a leading role within the consortia of the IoT European large-scale pilot projects, this deliverable achieves the navigation of the main components of the policy framework for a trusted IoT environment. It enables the partners to implement those components in practice and to facilitate them through the implementation stage. The IoT policy framework has provided for issues of horizontal nature and common interest to ultimately create a trusted, safe and, – essentially, – legally compliant environment for IoT as well as paving the ground for the goal of a human- centred approach to be developed and refined under the final deliverable version due in December 2019.

8. REFERENCES

[1] Developing a Framework to Improve Critical Infrastructure Cybersecurity, NIST 2013.

[2] O. Vermesan and J. Bacquet (Eds.). Cognitive Hyperconnected Digital Transformation Internet of Things Intelligence Evolution, ISBN: 978-87-93609-10-5, River Publishers, Gistrup, 2017.

[3] Strategic Principles for Securing the Internet of Things (IoT), Version 1.0, 2016, U.S. Department of Homeland Security.

[4] Europe's policy options for a dynamic and trustworthy development of the Internet of Things, Final Report (D7) 2013, Prepared for the European Commission, DG Communications Networks, Content and Technology (CONNECT).

[5] Senate of United States, ''Internet of Things (IoT) Cybersecurity Improvement Act of https://www.scribd.com/document/355269230/Internet-of-Things-Cybersecurity-Improvement-Act-of-2017

[6] Technology Assessment – Internet of Things Status and implications of an increasingly connected world, United States Government Accountability Office, Center for Science, Technology, and Engineering, online at https://www.gao.gov/assets/690/684590.pdf

[7] Digital Transformation of Industries: Digital Enterprise, World Economic Forum White Paper, 2016 online at: http://reports.weforum.org/digital-transformation-of-industries/wp-content/blogs.dir/94/mp/files/pages/files/digital-enterprise-narrative-final-january-2016.pdf

[8] Digital transformation of industry, Roland Berger Report, 2015, online at: https://www.rolandberger.com/publications/publication_pdf/roland_berger_digital_transformation_of_industry_20150315.pdf

[9] O. Vermesan, R. Bahr, A. Gluhak, F. Boesenberg et., al., IoT Business Models Framework, UNIFY-IoT Report, 2016, online at: http://www.internet-of-things-research.eu/pdf/D02_01_WP02_H2020_UNIFY-IoT_Final.pdf

[10] D. Hemment, J. Bletcher, and S. Coulson, Art, creativity and civic participation in IoT and Smart City innovation through 'Open Prototyping'. In Proceedings of the Creativity World Forum 2017. Aarhus, Denmark. November 1-2, 2017.

[11] C., Castelfranchi and R., Falcone, Trust Theory: A Socio-Cognitive and Computational Model. Wiley Series in Agent Technology. John Wiley & Sons Ltd., Chichester, 2010.

[12] J.S., Mill, Principles of Political Economy, London: Longmans, 1891, pp. 68.

[13] R. Swedberg, "Economic sociology: past and present", Current Sociology, Vol 35 No 1: 1-221, 1987, pp. 131.

[14] B., Williams, "Formal structures and social reality" in D. Gambetta (ed) Trust: Making and Breaking Cooperative Relations, Oxford: Basil Blackwell: 1988, pp. 3-13.

[15] J. Dunn, "Trust and political agency" in D. Gambetta (ed) Trust: Making and Breaking Cooperative Relations, Oxford: Basil Blackwell: 1988, pp. 73-93.

[16] K., Hart, 1988, "Kinship, contract, and trust: the economic organization of migrants in an African city slum" in D. Gambetta (ed.) Trust: Making and Breaking Cooperative Relations, Oxford: Basil Blackwell.

[17] O. Williamson, "Calculativeness, trust, and economic organization", Journal of Law and Economics, Vol 36 No 2, 1993, pp. 453-486.

[18] P. Dasgupta, "Trust as a commodity" in D. Gambetta (ed.), Trust: Making and Breaking Cooperative Relations, Oxford: Basil Blackwell, 1988, pp. 49-72.

[19] N. Luhmann, 1988, "Familiarity, confidence, trust, problems and alternatives", in D. Gambetta (ed), Trust: Making and Breaking Cooperative Relations, Oxford: Basil Blackwell.

[20] M., Granovetter, 1985, "Economic action and social structure: the problem of embeddedness, American Journal of Sociology, Vol 91: 481-510.

[21] J. Sabater and C. Sierra, "Review on computational trust and reputation models," Artif. Intell. Rev., vol. 24, pp. 33–60, September 2005.

[22] F. Bao and I. Chen, “Trust management for the internet of things and its application to service composition,” in 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012, San Francisco, CA, USA, June 25-28, 2012. IEEE Computer Society, 2012, pp. 1–6, online at: http://dx.doi.org/10.1109/WoWMoM.2012.6263792.
[23] K. M. Khan and Q. M. Malluhi, “Establishing trust in cloud computing,” IT Professional, vol. 12, no. 5, pp. 20–27, 2010.
[24] P. Pettit, “The Cunning of Trust”, Philosophy and Public Affairs 24, 1995, pp. 202-225.
[25] B. Misztal, Trust in Modern Societies, Polity Press, Cambridge MA, 1996.
[26] A. McCullagh, “E-commerce: A Matter of Trust”, in Proceedings of the 1998 Information Industry Outlook Conference,1998.
[27] A. Kini, and J. Choobineh, “Trust in Electronic Commerce: Definition and Theoretical Considerations”, in W. Blanning, and D. King, (eds.), Proceedings of the 31 Annual Hawaii Conference on System Sciences, volume IV, IEEE Computer Society, 1998.
[28] K. Kimery and M. McCard, "Third-party assurances: Mapping the road to trust in e-retailing," Journal of Information Technology Theory and Application, vol. 4, no. 2, pp. 63-82, 2002.
[29] R. Mayer, J. Davis and F. Schoorman, "An integrative model of organizational trust," The Academy of Management Review, vol. 20, no. 3, pp. 709-734, 1995.
[30] C. Corritore, B. Kracher and S. Wiedenbeck, "On-line trust: concepts, evolving themes, a model," Int.J. Human- Computer Studies, vol. 58, no. 6, pp. 737-758, 2003.
[31] E. Chang, T. Dillon and F. Hussain, "Trust and reputation relationships in service-oriented environments," ICITA 2005. Third International Conference on Information Technology and Applications, vol. 1, pp. 4-14, 2005.
[32] L. Buttyan and J. Hubaux, Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing, New York, NY, USA: Cambridge University Press, 2007.
[33] J. Daubert, A. Wiesmaier and P. Kikiras, "A review on privacy and trust in IoT," in In IoT/CPS-Security Workshop, IEEE International Conference on Communications, ICC 2015, London, 2015.
[34] I. Alexander and W. Sean, "Protecting client privacy with trusted computing at the ser," in IEEE Security and Privacy, 2005.
[35] J. Audun, I. Roslan an B Colin, "A survey of trust and reputation systems for online service provision," Decision Support Systems, Vol. 43, No. 2, pp. 618-644, 2007.
[36] V. Gligor nd J. Wing, "Towards a theory of trust in networks of humans and computers," in the 19th international workshop on security protocols, LNCS, 2011, UK, April 2012, LNCS 7622, Springer Verlag.
[37] W. Leister and T. Schulz, "Ideas for a Trust Indicator in the Internet of Things," in Th First International Conference on Smart Systems, Devices and Technologies, 2012.
[38] F. Bao, I. Chen, Dynamic trust management for internet of things applications, in: Proceedings of the 2012 International Workshop on Self-Aware Internet of Things, Self-IoT "12, USA, San Jose, 2012, pp. 1–6.
[39] F. Bao, I. Chen, Trust management for the internet of things and its application to service composition, in: 13th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012, San Francisco, CA, United States, 2012, pp. 1–6.
[40] Daubert, Jorg, Alexander Wiesmaier, and Panayotis Kikiras. A View on Privacy & Trust in IoT. Tech. AGT International, Germany, Telecooperation Group, Technical University of Darmstadt, Web. <https://www.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_TK/filesDownload/Published_Papers/joerg15privacytrust.pdf>.

[41] Leister, Wolfgang, and Trenton Schulz. Ideas for a Trust Indicator in the Internet of Things. Tech. IARIA, 27 May 2012. Web. <https://www.thinkmind.org/index.php?view=article&articleid=smart_2012_2_10_40043>
[42] ISO/IEC 27000:2009 (E). (2009). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC.
[43] Nissenbaum, Helen. 2010. Privacy in context. Standford, CA: Stanford University Press.
[44] Hofkirchner, Wolfgang, 2010. Twenty questions about a unified theory of information. Litchfield Park, AZ: Emergent Publications.
[45] A. Avizienis, J.C. Laprie, B. Randell, and C. Landwehr, Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on dependable and secure computing, vol.1, n°1, Jan-March 2004.
[46] Marit Hansen, Meiko Jensen, Martin Rost: "Protection Goals for Engineering Privacy"; in 2015 International Workshop on Privacy Engineering (IWPE). http://ieee-security.org/TC/SPW2015/IWPE/2.pdf.
[47] European Commission. AIOTI. Report on Workshop on Security & Privacy in IoT. <http://www.theinternetofthings.eu/sites/default/files/docs/final_report_20170113_v0.1_clean.pdf>.
[48] AIOTI. Report on Workshop on Security and Privacy in the Hyper-Connected World. <https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf>.
[49] M. Nitti, R. Girau, L. Atzori, A. Iera, G. Morabito, A subjective model for trustworthiness evaluation in the social internet of things, in: 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications, PIMRC, Australia, Sydney, 2012, pp. 18–23.
[50] L. Gu, J. Wang, B.B. Sun, Trust management mechanism for internet of things, China Commun. 11 (2) (2014) 148–156].
[51] International Telecommunication Union – ITU-T Y.2060 - (06/2012) – Next Generation Networks – Frameworks and functional architecture models – Overview of the Internet of things
[52] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, et al., "Internet of Things Strategic Research Agenda", Chapter 2 in Internet of Things – Global Technological and Societal Trends, River Publishers, 2011, ISBN 978-87-92329-67-7.
[53] KPMG - security and the IoT ecosystem, online at https://www.kpmg.com/BE/en/IssuesAndInsights/ArticlesPublications/Documents/security-and-the-iot-ecosystem.pdf.
[54] Is the Internet of Things Too Big to Protect? Not if IoT Applications Are Protected!, online at https://securityintelligence.com/is-the-internet-of-things-too-big-to-protect-not-if-iot-applications-are-protected/.
[55] O. Vermesan, P. Friess, P. Guillemin, H. Sundmaeker, et al. Internet of Things Strategic Research and Innovation Agenda. O. Vermesan and P. Friess, Eds. *Internet of Things Applications - From Research and Innovation to Market Deployment*. Alborg, Denmark: The River Publishers, ISBN: 978-87-93102-94-1, 2014, pp. 7-142.
[56] O. Vermesan and J. Bacquet (Eds.). Cognitive Hyperconnected Digital Transformation Internet of Things Intelligence Evolution, ISBN: 978-87-93609-10-5, River Publishers, Gistrup, 2017.
[57] Developing a Framework to Improve Critical Infrastructure Cybersecurity, NIST 2013.
[58] Europe's policy options for a dynamic and trustworthy development of the Internet of Things, Final Report (D7) 2013.
[59] Prepared for the European Commission, DG Communications Networks, Content and Technology (CONNECT).
[60] Strategic Principles for Securing the Internet of Things (IoT), Version 1.0, 2016, U.S. Department of Homeland Security.

[61] European Commission COM(2017) 495 final 2017/0228 (COD), 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, 2017, online at: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-495-F1-EN-MAIN-PART-1.PDF

9. ANNEXES

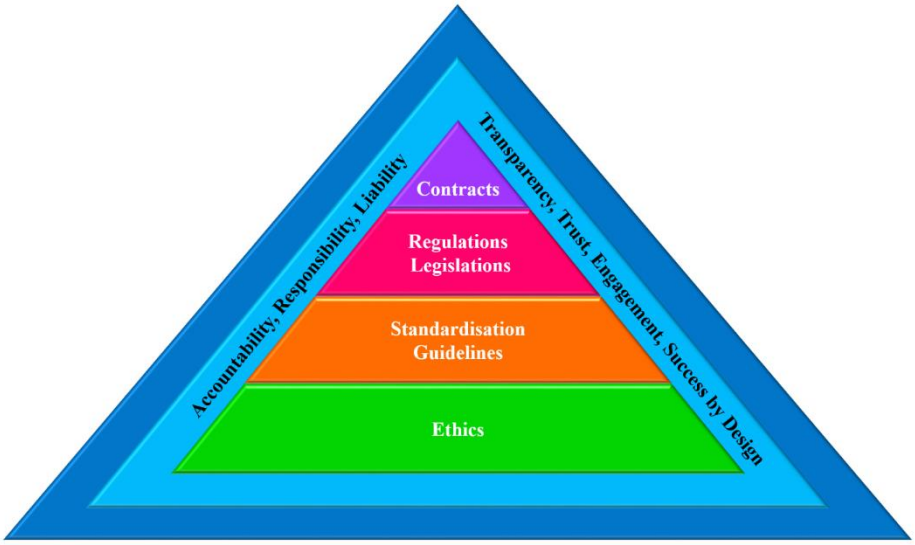
Code of IoT Engagement [*preliminary draft version*]

1. WHY THIS CODE?

Imagine you want to be part of a sports team, a musical ensemble, an innovation hub, a rural or urban area or even a country. With that, you want to become part of a certain community, each with its particular habits, codes and rules. These are meant to set the expectations of the members of such community straight, and meanwhile protect the interests of each of them separately, the community as a whole, as well as society and its environment within the community is operating.

Welcome to the world of IoT and the European Large-Scale Pilots Programme, where you and your community can be part of, connect with new people, things and other opportunities, engage, test, try, pivot, iterate, hyper-connect, calibrate, collaborate, mature, mitigate risks, optimize results and succeed. We call this Success by Design.

In order to organise this, and – again – to set the expectations straight and aim to avoid discussions and conflicts, we need to play by some rules. The framework of those rules are in this Code of IoT Engagement.



In the era of the technological galloping – which we embrace but also try to understand and where necessary organise and mitigate risk and negative impacts – we are all experiencing, human knowledge and experience on given concepts are challenged. In the Internet of Things era, the very essence of the notion of knowledge and experience is challenged.

Bearing in mind this very interesting challenge and its vast amount of various opportunities, this Code of IoT Engagement is meant to navigate, enable and facilitate pleasant, fair, reasonable, highly-ethical and successful engagement between you and the relevant members and domains of the communities and IoT ecosystems within the European Large-Scale Pilots Programme.

This code will demystify engagement in the IoT context and shed light on the very grounds of this engagement.

2. WHO IS WHO?

This Code of IoT Engagements ('Code') is applicable to each and every one – and everything – that in anyway wish to become part of any part of a community, ecosystem within the vast

domains of the Large-Scale Pilots (LSPs) and Coordination and Support Activities (CSAs) of the European Large-Scale Pilots Programme. It is not only good to understand who you are within those domains but also who the other stakeholders maybe you will or may engage with.

These include, without limitation the following stakeholders, in random order:

a. **Society and environment**
b. **Users**
c. **Users**
d. **Customers**
e. **Non-users**
f. **Data brokers**
g. **Data providers**
h. **Service providers**
i. **Software providers**
j. **Hardware providers**
k. **Infrastructure providers**
l. **Machines, interfaces and user-interfaces**
m. **Universities and other knowledge institutions**
n. **Standardisation development organisations**
o. **Policy makers: governments, municipalities and others**
p. **Authorities, law enforcement and intelligence services**

The figure below illustrates how these stakeholders relate to each other, where for instance parties that are not part of a LSP or CSA consortium are indicated as Third-Party Partners or Third-Party Suppliers. They engage with a specific LSP or CSA consortium partner though this Code and with that are engaged with them within the European Large-Scale Pilots Programme.

3. DECLARATION OF ADHERENCE

I hereby declare that I adhere to the Code of IoT Engagement.

4. BACKGROUND INFORMATION

The latest technological developments have surfaced in an unprecedented manner the insufficiencies of the existing laws to tackle with a series of matters of paramount significance both for individuals and society at large. The expansion of the internet of things, the galloping of artificial intelligence, the widespread use of drones, are merely an indicative list of examples triggering questions around human autonomy, the extent of human decision making or even the scope of fundamental human rights. Taking into account those concerns, the present document produced by CREATE-IoT project discusses how the ongoing European large-scale pilots programme can be legally compliant, while meeting the criteria of an ethical assessment as set forth by the European Commission[41].

Naturally, the development of technology and responding to the needs of the future dynamic IoT systems, which is at the core of CREATE-IoT large scale pilots (LSPs), has to be carried out in compliance with statutory (legal) requirements. However, since legal compliance may in some instances fall short of observing core ethical principles, supplementary ethical requirements have to be provided in this code of IoT engagement.

Overall, though, LSPs are expected to comply with a complex set of requirements stemming from different sources, as illustrated in the figure below:

This set of requirements create a load of obligations for the LSPs that may vary significantly depending on the exact role of each organisation with a role within the IoT LSP consortium. Bearing in mind this complexity, the present code of IoT engagement will demystify the scene aiming to ensure that each LSP as a whole, as well as, each organization being part of each LSP is compliant with the relevant set of rules dictating their responsibilities under law and ethics.

Based on this code of IoT engagement LSPs will be in the position to assess themselves what is permissible and what is not with respect to privacy and security in the IoT environment.

Distinction between code of ethics and code of conduct; distinctive elements of the concept – and a value- of a Code of an IoT Engagement.

5. LIFECYCLE THINKING

IoT is a dynamic living system, not static, therefore, allowing for an approach on the basis of separate lifecycles

IoT Device/Product Life Cycle: What does the life cycle entails, how long needs and can a device/product remain connected to an IoT ecosystem in a secure, safe and compliant manner, what can the user/customer expect, and how is both the device/product as well as the user/customer able to keep up to date with (at least) the state of practice?

Stakeholders Life Cycle: What stakeholders are involved regarding an IoT device/product and in a relevant IoT ecosystem, what if the dynamics thereof changes, who is accountable for what part of the ecosystem, how to keep the stakeholders up to date, and what happens if there is an incident of any kind within the IoT ecosystem?

Data Life Cycle: What data is collected, created or otherwise concerned, what is its classification, can it be segmented, minimised and isolated, what if it has multiple classifications

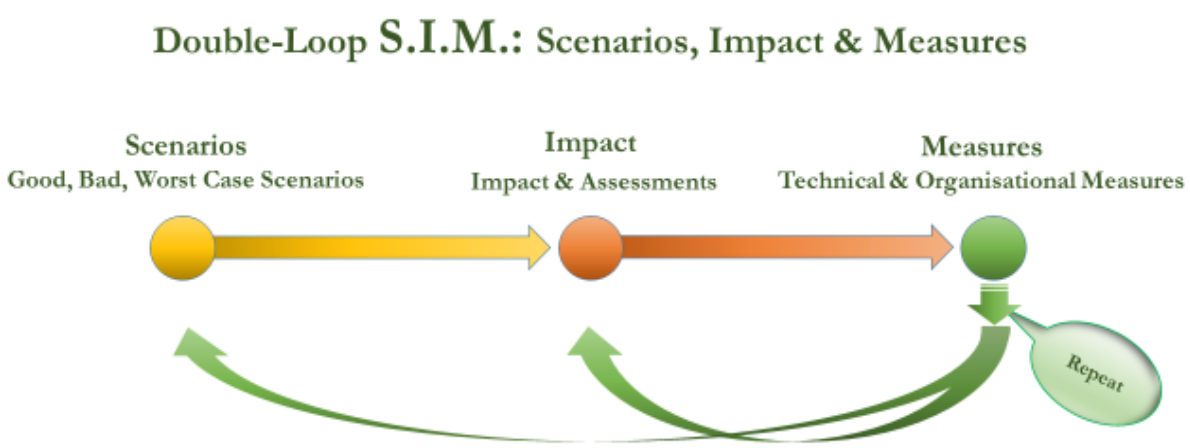
[41] H2020 Programme Guidance 'How to complete your ethics self-assessment', available at: http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

and what if the classification changes, how controls the data, for what purposes is one entitled to process the data, what meta data and derived data is generated during the data life cycle, and what does data deletion mean?

Contextual Life Cycle: In what context is a device/product/ecosystem used, as what persona is a stakeholder involved and in what context is data used in an IoT ecosystem, what if the context thereof changes, who is accountable in what context, how to make stakeholders aware of changes in best practices, rights and obligations when the context changes, and how to secure the rights and obligations of the relevant other stakeholders?

Legal Life Cycle: As a person or legal entity, with whom do you want to engage? And if so, how to assess, prepare, negotiate, contract, execute, operate, update, amend, escalate and terminate such engagement (a.k.a. legal relationship)?

Double Looping



6. APPLICABLE REGULATION

6.1. 2012/C 326/02: Charter of Fundamental Rights of the European Union

6.1.1. *Article 1 – Human dignity:* Human dignity is inviolable. It must be respected and protected.

6.1.2. *Article 7 – Respect for private and family life:* Everyone has the right to respect for his or her private and family life, home and communications.

6.1.3. *Article 8 – Protection of personal data:* (1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority.

6.1.4. *Article 21 – Non-discrimination:* Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

6.2. Regulation (EU) 2016/679: General Data Protection Regulation

6.2.1. *Article 5 – Principles relating to processing of personal data*

6.2.2. *Article 9 – Processing of special categories of personal data*

6.3. **Directive (EU) 2016/1148: NIS Directive**

6.3.1. *Article 2 – Processing of personal data*

6.4. **Directive 2002/58/EC: e-Privacy Directive**

6.4.1. *Article 4 – Security:* (1) The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented. (2) In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

6.4.2. *Article 5 – Confidentiality of the communications:* (1) Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). (...) (3) Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. (...)

6.4.3. *Article 6 – Traffic data:* (1) Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1). (...) (3) For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time. (4) The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3. (...)

6.4.4. *Article 7 – Itemised billing:* (1) Subscribers shall have the right to receive non-itemised bills. (...)

6.4.5. *Article 9 – Location data other than traffic data:* (1) Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision

of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time. (2) Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication. (3) Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

6.4.6. *Article 12 – Directories of subscribers:* Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory. (...)

6.5. **Regulation (EU) No 1291/2013: Establishing Horizon 2020**

6.5.1. *Article 16: Gender equality*

6.5.2. *Article 18: Open access*

6.5.3. *Article 19: Ethical principles*: Particular attention shall be paid to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure high levels of human health protection.

6.6. **H2020 Programme Guidance: How to complete your ethics self-assessment**

6.7. **Council Regulation (EC) No 338/97: Protection of species of wild fauna and flora**

6.8. **Directive 2009/41/EC: Contained use of genetically modified micro-organisms:** The Directive concerns Members States' obligation to take appropriate steps to avoid adverse effects on human health and the environment which might arise from the contained use of GMMs.

6.9. **Directive 2006/25/EC: Minimum health and safety requirements of workers**

6.10. **Regulation No 428/2009: Handling dual-use items**

7. ACCOUNTABILITY

Who is responsible for the enforcement of this code?

8. CONSEQUENCES OF NON-ADHERENCE & NON-COMPIANCE

What happens in case of non-compliance?Are there remedies in place?

9. APPENDICES

APPENDIX I- ETHICAL PRINCIPLES

This Section presents the ethical principles to be observed by all participants taking part in CREATE-IoT LSPs. Reference to Article Human dignity is inviolable. It must be respected and protected.'

- Article 1,EU Charter of Fundamental Rights

To ensure consistency and clarity, some key general ethical principles are summarised in points a. to i. below:

a. **Human dignity** is inviolable. It must be respected and protected.

b. Any practices engaged must adhere to the principles of **freedom**, **security and justice economic and social progress**, and to the **well-being of natural persons**.

c. **Discriminatory practices** and discriminatory treatment must be avoided.

d. Special care must be taken in cases of **minors, special groups and vulnerable individuals**.

e. **Personal data** remains ownership of individuals and may not be collected and/or handled without a freely given, specific, informed and unambiguous consent. Protection of natural persons in relation to the processing of personal data remains a fundamental right, however, not an absolute right. Data subject's right of access to personal data as well as right to be forgotten must be observed.

f. **Transparency:** Data subjects must be informed about the types and volume of data to be stored as well as about any transmission of their data to third parties. The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used.

g. **Accountability:** It must be possible to establish what an entity did at any point in the past and how.

h. **Technological neutrality:** These ethical principles apply universally, regardless of technology, technological means of carrying out a (research) project or technological means of handling personal data.

i. **Ethics board** or **ethics advisor** must be appointed which includes relevant independent expertise to monitor, endorse and oversee the implementation of ethical concerns in any project.

Sections 9.1 to 9.3 outline numerous domain-specific ethical principles:

9.1. **Personal data[42]:**

9.1.1. *Ownership:* Personal data remains ownership of the data subject.

9.1.2. *Collection only with consent:* Personal data can only be collected from consenting data subjects. They possess independent capacity to clearly understand what the process entails and agree to it. Consent must be informed as well as explicit and affirmative, i.e. expressed through a clear agreement to stated terms. Personal data will not be collected from a non-consenting data subject.

9.1.3. *Obtaining consent:* Consents have to be handled through the user interface allowing the data subjects to agree the transmission and storage of sensitive data.

[42] Relevant for ACTIVAGE, SYNCHRONICITY, MONICA and AUTOPILOT. Source: GDPR.

The consent legal text must be customized for each country where the controller is seeking consent from data subjects, with respect to applicable local legislation.

9.1.4. *Notification:* Data subjects must be notified that their data is being collected and about how this data will be disclosed and used. This notice must be provided in and easily located and readily accessible format.

9.1.5. *Justification for collection:* Justification must be given in case of collection and/or processing of personal sensitive data.

9.1.6. *Purpose specification and limitation:* The consent text included in the interface should specify which data will be stored, who it will be transmitted to and for which purpose. Personal data may only be collected for the specified purpose and not further processed in a way incompatible with the stated purpose.

9.1.7. *Terms and definitions:* Data subjects should know with whom they are contracting, if the contract involves sharing with third parties, partners, business partners, the controller's partners, or affiliates. Controllers should clearly explain the following definitions in a consistent manner in all of their respective agreements: (1) data; (2) third party; (3) partner; (4) business partner; (5) controller's partners; (6) affiliate; (7) data account holder; (8) original data subject data. If these definitions are not used, the controller should define each alternative term in the contract and privacy policy. Controllers should strive to use clear language for their terms, conditions and agreements.

9.1.8. *Information on procedures:* Detailed information must be provided on the procedures that will be implemented for data collection, storage, protection, retention, transfer, and destruction or re-use and confirmation that they comply with national and EU legislation.

9.1.9. *Information on informed consent:* Detailed information on the informed consent procedures that will be implemented in regard to the collection, storage and protection of personal data must be submitted on request.

9.1.10. *Consent forms and information sheets:* Templates of the informed consent forms and information sheet must be submitted on request.

9.1.11. *Public availability of data:* A controller using public available personal data must explicitly confirm that the data used is publicly available.

9.1.12. *Unnecessary collection:* A controller must clarify which personal data will be collected from data subjects and confirm that they will avoid and prevent any unnecessary collection and use of data.

9.1.13. *Sensitive data, genetic information, tracking:* If the (research) activity involves the collection or processing of sensitive personal data (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction), genetic information or tracking of participants, the necessary notification or authorization for processing of this data must be obtained (if required).

9.1.14. *Anonymity:* The anonymous participation of citizens to the proceeding shall be enabled for those countries whose legislation explicitly defines this right.

9.1.15. *Minimization:* Only the amount of personal data needed for the operational purposes of the project should be collected.

9.1.16. *Transparency:* Data subjects must be informed about the type and volume of data to be stored, how it will be transmitted, at what locations and for which purposes must be openly communicated to all participants within and outside a consortium, including consenting participants volunteering their private data.

Data subjects must also be informed about how they can contact the controller with inquiries or complaints, the types of third parties to which the controllers disclose the data and options the controller offers for limiting use and disclosure. Controllers' principles, policies and practices should be transparent and fully consistent with the terms and conditions in their legal contracts. A controller should not change the contract with the data subject without their agreement.

9.1.17. *No data sharing by default:* By default, personal data is not automatically shared. Data sharing and diffusion only applies to data for which consent has been given, and in accordance with the diffusion terms expressed by the consent.

9.1.18. *Data retention, availability and erasure:* Personal data cannot be stored longer than needed for specific and clearly defined purposes, and must be in a format that allows its erasure or anonymization. Each controller should provide for the removal, secure destruction and return of original data subject's data from the data subject's account upon the request of the data subject or after a pre-agreed period of time. The controller should include a requirement that data subjects have access to the data that an controller holds during that data retention period. Controllers should document personally identifiable data retention and availability policies and disposal procedures, and specify requirements of data under policies and procedures.

9.1.19. *Cookies:* The system shall not store cookies on the data subjects' computers to prevent any unauthorized tracking of the data subjects' activities on the Internet.

9.1.20. *Data safety:* Details must be provided on data safety procedures (protective measures to avoid unforeseen usage or disclosure, including mosaic effect, i.e. obtaining identification by merging multiple sources).

9.1.21. *Encryption:* Encryption will be applied to personal data when in transit and when at rest. State-of-the-art encryption technology must be applied for all data exchange within the project: e.g. SSL, TLS.

9.1.22. *Hosting of Data:* All personal data must be stored on a verified secure server, preferably within the country from which it was collected.

9.1.23. *Disclosure, use and sale limitation:* A controller will not sell and/or disclose non-aggregated data subject's data to a third party without first securing a legally binding commitment to be bound by the same terms and conditions as the controller has with the data subject. Data subjects must be notified if such a sale is going to take place and have the option to opt out or have their data removed prior to that sale. A controller will not share or disclose original data subject's data with a third party in any manner that is inconsistent with the contract with the controller. If the agreement with the third party is not the same as the agreement with the controller, controllers must be presented with the third party's terms for agreement or rejection.

9.1.24. *Right of access:* Data subjects should have a right of access to personal data which have been collected concerning them, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.

9.1.25. *Contract termination:* Data subjects should be allowed to discontinue a service or halt the collection of data at any time subject to appropriate ongoing obligations. Procedures for termination of services should be clearly defined in the contract.

9.1.26. *Unlawful or anti-competitive activities:* Controllers should not use the data for unlawful or anti-competitive activities, such as a prohibition on the use of data subject's data by the controller to speculate in commodity markets.

9.1.27. *Liability and security safeguards:* The controller should clearly define terms of liability. Data subject's data should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure. Polices for notification and response in the event of a breach should be established.

9.1.28. *Secondary use:* If research involves further processing of previously collected personal data, the controller must provide details on the database used or of the source of the data, details of procedures for data processing, details of data safety procedures, confirmation that data is openly and publicly accessible or that consent for secondary use has been obtained, confirmation permissions by the owner of the data sets.

9.2. **Animals[43]:**

9.2.1. *Involvement of animals:* If the (research) activity involves animals, the controller must provide details of species and rationale for their use, numbers of animals to be used, nature of the experiments, procedures and techniques to be used. The controller should also provide justification of animal use (including the kind of animals to be used) and why alternatives cannot be used.

9.2.2. *Special groups:* Additional information must be provided in cases of the following special groups:

9.2.2.1. Non-human primates (NHP): Explanation of why are NHPs the only research subjects suitable for achieving the scientific objectives. Details of the purpose of the animal testing. Details of the animals' origin. Provide personal history file of NHP.

9.2.2.2. Genetically modified animals: Details of the phenotype and any inherent suffering expected. Details of the scientific justification present for producing such animals. Details on the measures to be taken to minimise suffering in breeding, maintaining the colony and using the GM animals. Provide copies of GMO authorisations.

9.2.2.3. Cloned farm animals: Details of the phenotype and any inherent suffering expected. Details on the scientific justification for producing such animals. Details on the measures taken to minimise suffering in breeding, maintaining the colony and using of the GM animals. Provide copies of authorisations for cloning (if required).

9.2.2.4. Endangered species: Give details on why there is no alternative to using this species. Give details on the purpose of the research. Provide copies of authorisations for supply of endangered animal species (including CITES).

9.2.3. *RRR:* Implement the principles of Replacement, Reduction and Refinement where possible. Replacement — replacing animal use by an alternative method or testing strategy (without use of live animals). Reduction — reducing the number of animals used. Refinement — improving the breeding, accommodation and care of animals and the methods used to minimise pain, suffering, distress or lasting harm to animals.

[43] Relevant for IoF2020.

9.2.4. *Authorisation:* Obtain authorisations for the supply of animals and the animal experiments (and other specific authorisations, if applicable).

9.3. **Environment, Health & Society[44]:**

9.3.1. *Possible harm to environment:* Further information about the possible harm to the environment caused by the (research) activity must be provided as well as the measures that will be taken to mitigate the risks, including risks due to underestimated methodological limitations or reliance on datasets of poor quality or reliability.

9.3.2. *Health and safety:* The applicant is required to apply the precautionary principle where there is plausible scientific evidence for serious risks and provide details on health and safety measures to be implemented.

9.3.3. *Use of harmful elements (humans):* Specify whether the (research) activities involve the use of elements that may cause harm to humans including research staff. Specify the nature of health and safety procedures applied.

9.3.4. *Use of harmful elements (environment):* Specify whether the (research) activities involve the use of elements capable of causing harm to the environment, animals or plants. Provide risk-benefit analysis. Show that the researcher applies the precautionary principle. Specify what safety measures will be taken.

9.3.5. *Endangered areas:* Specify whether the research will deal with endangered fauna and/or flora and/or protected areas.

APPENDIX II: DEFINITIONS[45]

1. **Personal data** means 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. (GDPR)
2. **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (GDPR)
3. **Profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. (GDPR)
4. **Pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. (GDPR)

[44] Relevant for SYNCHRONICITY, IoF2020 and AUTOPILOT.

[45] Further relevant definitions can be found in the text of the General Data Protection Regulation (GDPR)

5. **Filing system** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. (GDPR)
6. **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. (GDPR)
7. **Processor means** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. (GDPR)