ETSI TR 103 591 V1.1.1 (2019-10)

TECHNICAL REPORT

SmartM2M; Privacy study report; Standards Landscape and best practices

Reference

DTR/SmartM2M-103591

Keywords

cybersecurity, IoT, oneM2M, privacy, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

List of Figures

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Smart Machine-to-Machine communications (SmartM2M).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document focuses on privacy, which is particularly relevant within the IoT environment due to a series of emerging challenges resulting from hyper-connectivity. The approach adopted builds on the fundamental assumption that even though it is generally considered that privacy and security are separate concepts, they are actually interconnected, and they should therefore be treated in practice in a coordinated manner. Security constitutes a prerequisite for the effective protection of privacy, as it has also been confirmed by the General Data Protection Regulation (GDPR).

NOTE: See also the Preamble of the Regulation (EU) 2016/679 [i.16] on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [i.23].

1 Scope

1.1 Context of the present document

In order to provide a global and coherent view of all the topics addressed, a common approach has been outlined across the Technical Reports concerned (see below) with the objective to ensure that the particularities of the IoT systems are properly addressed and that the overall results are coherent and complementary.

In this context, the present document has been built with this common approach also applied in all of the other documents listed below:

- ETSI TR 103 533 [i.2]
- ETSI TR 103 534 (part 1 and 2) [i.28]
- ETSI TR 103 535 [i.33]
- ETSI TR 103 536 [i.34]
- ETSI TR 103 537 [i.35]
- ETSI TR 103 591 (the present document)

1.2 Scope of the present document

The present document elaborates on how to ensure effective protection of individuals' privacy in the IoT environment. It acknowledges the challenges for privacy and data protection and stresses the necessity for a human centred approach.

To this end, the present document will:

- highlight the role of social values in the design of IoT systems;
- discuss the role of standards under the GDPR and the proposed ePrivacy Regulation;
- outline the role of the individual, also, through a set of use cases drawn from an ongoing EU project and further adapted for the needs of the present document;
- produce an overview of the main privacy and data protection challenges emerging in the IoT environment;
- review the privacy standardization gaps identified in ETSI TR 103 376 [i.1] and how some of these gaps have been resolved since the completion of the work if at all;
- illustrate current best practices across industrial and other organizations in the processing of personal information to meet, and in some cases exceed, the minimum requirements for compliance in view of maximizing the protection of personal information;
- point at the fundamental shifts taking place in relation to privacy under EU Law, including the shift from rule-based frameworks to principle-based frameworks, the necessity to go beyond mere compliance to meaningful accountability and the implementation of impact-based measures.

For reasons explained below under clause 7.3, the development of new standards falls outside the scope and the objectives of the present document.

Notably, the present document is addressed to the entire set of stakeholders with a role in the IoT environment and it complements ETSI TR 103 533 [i.2].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document, but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 103 376: "SmartM2M; IoT LSP use cases and standards gaps".

[i.2] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

[i.3] European Commission: "Cloud Service Level Agreement Standardisation Guidelines".

[i.4] European Data Protection Supervisor: "Glossary".

NOTE: Available at https://edps.europa.eu/node/3110#privacy.

[i.5] GHOST Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control: "D3.9: Trials use case specification and report (1^{rst} release).

NOTE: Available at https://www.ghost-iot.eu/results-documents.

[i.6] ISO/IEC 20547-3: "Information technology - Big data reference architecture - Part 3: Reference architecture".

[i.7] ISO/IEC 20547-4: "Information technology - Big data reference architecture. Part 4: Security and privacy fabric".

[i.8] ISO/IEC TR 27550: "Information technology - Security techniques - Privacy engineering [Draft]".

[i.9] ISO/IEC 27552: "Information technology - Security techniques - Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy management - Requirements and guidelines [Draft]".

[i.10] ISO/IEC CD 3014: "Internet of Things Reference Architecture (IoT RA)".

[i.11] ISO/IEC 29100:2011: "Information technology - Security techniques - Privacy framework".

[i.12] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, Interinstitutional File: 2017/0003(COD), Brussels.

[i.13] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union OJ L 303/59.

[i.14] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).

[i.15] European Union, Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 December 2007, 2007/C 306/01.

[i.16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[i.17] 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.

[i.18] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), 13.9.2017.

[i.19] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free flow of non-personal data in the European Union.

[i.20] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[i.21] Council of the European Union (2018) Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, Interinstitutional File: 2017/0003(COD), Brussels.

[i.22] 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.

[i.23] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data).

[i.24] European Data Protection Supervisor: Preliminary Opinion on privacy by design, 31 May 2018.

[i.25] "IoT LSP Standards Framework Concepts", Release 2.8, White Paper, AIOTI, 2017.

[i.26] ETSI TR 103 370: "Practical introductory guide to Technical Standards for Privacy".

[i.27] ETSI TS 118 103: "oneM2M; Security solutions".

[i.28] ETSI TR 103 534 (part 1 and 2): SmartM2M; Teaching Material; Part 1:Security and Part 2: Privacy.

[i.29] ISO/IEC 27030: "Information technology - Security techniques - Guidelines for security and privacy in Internet of Things".

[i.30] Directive 2010/40/EU: of the European Parliament and of the council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

[i.31] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 19 October 2018.

[i.32] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 15 February 2019.

[i.33] ETSI TR 103 535: "SmartM2M; Guidelines for using semantic interoperability in the industry".

[i.34] ETSI TR 103 536: "SmartM2M; Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms".

[i.35] ETSI TR 103 537: "SmartM2M; Plugtests$^{\text{TM}}$ preparation on Semantic Interoperability".

[i.36] ISO/IEC 29151:2017: "Information technology - Security techniques - Code of practice for personally identifiable information protection".

[i.37] ISO/IEC 29134: "Information technology - Security techniques - Guidelines for privacy impact assessment".

[i.38] ISO 27018: "Information technology - Security techniques - Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors".

[i.39] ISO/IEC 27000: "Information Technology - Security Techniques - Information Security Management Systems - Overview And Vocabulary".

[i.40] ISO/IEC 27001: "Information Security Management".

[i.41] ISO/IEC 27002: "Information Technology - Security Techniques - Code Of Practice For Information Security Controls".

[i.42] BS 10012:2017: "Data protection. Specification for a personal information management system. Specification for a personal information management system".

[i.43] Recommendation ITU-T X.1231:"Supplement on guidance to assist in countering spam for mobile phone developers".

[i.44] Recommendation ITU-T X.1155: "Guidelines on local linkable anonymous authentication for electronic services.

[i.45] Recommendation ITU-T TD 733-PLEN: "Technical framework of PII (Personally Identifiable Information) handling system in IoT environment".

[i.46] Recommendation ITU-T TD 731-PLEN: "Security guidelines for smart metering service in smart grids".

[i.47] Recommendation ITU-T TD 962-PLEN: "Security Requirements and Framework for Big Data Analytics in mobile Internet services".

[i.48] British Information Commissioner's Office (ICO) Guidance to Privacy in mobile apps.

[i.49] British Code of Practice for consumer IoT security UK Gov: Dept of Digital, Culture, Media & Sport.

[i.50] GSMA Report on Protecting Privacy and Data in the Internet of Things.

[i.51] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC OJ L 337/35.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

biometric data: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data [i.16]

cyber security (or cybersecurity): comprises all activities necessary to protect network and information systems, their users, and affected persons from cyber threats [i.18]

NOTE: There are multiple definitions on cybersecurity each of which pertains to a specific domain. The definition above has been considered appropriate for the purpose of the present document.

data concerning health: personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status [i.16]

data protection: protection of data relating to an identified or identifiable natural person. In the context of the present report, data protection refers to personal data protection. Notably, it is largely technically feasible that non-personal data become personal data

genetic data: personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

The following terms are taken from [i.3] and [i.4]:

authentication: verification of the claimed identity of an entity

availability: property of being accessible and usable upon demand by an authorized entity

data: data of any form, nature or structure, that can be created, uploaded, inserted in, collected or derived from or with cloud services and/or cloud computing, including without limitation proprietary and non-proprietary data, confidential and non-confidential data, non-personal and personal data, as well as other human readable or machine-readable data

data controller: natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data

data integrity: property of protecting the accuracy and completeness of assets

data portability: ability to easily transfer data from one system to another without being required to re-enter data

data processor: natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller

data retention period: length of time which the cloud service provider will retain backup copies of the cloud service customer data during the termination process (in case of problems with the retrieval process or for legal purposes); this period may be subject to legal or regulatory requirements, which can place lower or upper bounds on the length of time that the provider can retain copies of cloud service customer data

data subject: identified or identifiable natural person, being an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

information security: preservation of confidentiality, integrity and availability of information

personal data: 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

privacy: ability of an individual to be left alone, out of public view, and in control of information about oneself

NOTE: One can distinguish the ability to prevent intrusion in one's physical space ("physical privacy", for example with regard to the protection of the private home) and the ability to control the collection and sharing of information about oneself ("informational privacy"). The concept of privacy therefore overlaps, but does not coincide, with the concept of data protection. The right to privacy is enshrined in the Universal Declaration of Human rights (Article 12) as well as in the European Convention of Human Rights (Article 8). (Also, see the definition in [i.4]). The concept of privacy within the context of data protection entails that personal data is entrusted to the data controller and/or data processor. The data controller and/or data processor are responsible to keep the data as "private" as possible, in the sense that data needs to be protected, as if it was not disclosed.

privacy by design: approach that aims to build privacy and data protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles

NOTE: It is considered that a wider spectrum of approaches may be taken into account for the objective of privacy by design which includes a visionary and ethical dimension, consistent with the principles and values enshrined in the EU Charter of Fundamental Rights of the EU [i.24]. In practice, organizations often confuse privacy by design with data protection; privacy by design forms the broader concept, part of which is data protection.

privacy enhancing technologies (PETs): coherent system of information and communication technology (ICT) measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system

NOTE: The use of PETs can help to design information and communication systems and services in a way that minimizes the collection and use of personal data and facilitates compliance with data protection rules. It should result in making breaches of certain data protection rules more difficult and/or helping to detect them. PETs can be stand-alone tools requiring positive action by consumers (who does purchase and install them in their computers) or be built into the very architecture of information system.

processing purposes: list of processing purposes (if any) which are beyond those requested by the customer acting as a controller

recital: part of a legal document that sets out the reasons for the contents of the enacting terms (i.e. the articles) of an article

vulnerability: weakness of an asset or group of assets, e.g. software or hardware related, that can be exploited by one or more threats

3.2 Symbols

Void

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AIOTI	Alliance for the Internet of Things Innovation
BS	British Standard
CCTV	Closed Circuit Television
DCMS	Digital, Culture, Media and Sport
DPIA	Data Protection Impact Assessment
EC	European Commission
EDPS	European Data Protection Supervisor
EEA	European Economic Area
ERP	Enterprise-Resource-Planning
ETSI	European Telecommunication Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
GSMA	Global System for Mobile Communications Association
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITS	Intelligent Transport System
ITU	International Telecommunications Union
ITU-T	ITU Telecom sector
LIBE	committee on civil Liberties, Justice and Home Affairs

NCSC	National Cyber Security Centre
NIS	Network Information Security
OTP	One Time Password
PET	Privacy Enhancing Technology
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIMS	Personal Information Management System
PLEN	Plenary
PPM	Privacy Policy Manager
PSD	Payment Service Directive
PSD2	Revised Payment Service Directive
STF	Specialist Task Forces
TB	Technical Body
TC	Technical Committee
TD	Temporary Document
TR	Technical Report
TV	Television
UK	United Kingdom
UML	Unified Modelling Language

4 Privacy in the context of IoT

4.1 A holistic approach of IoT systems

4.1.1 Major characteristics of IoT systems

IoT systems are often seen as an extension to existing ICT systems needed because of the (potentially massive) addition of networked devices. However, this approach does not take stock of a set of essential characteristics of IoT systems that push for an alternative approach where the IoT system in its entirety is at the centre of attention of those who want to make them happen. This advocates for a "holistic IoT approach" view.

Most of the above-mentioned essential characteristics may be found in other ICT-based systems. However, the main difference with IoT systems is that they all have to be dealt with simultaneously. The most essential ones are:

- Stakeholders: there is a large variety of potential stakeholders with a wide range of roles that shape the way each of them can be considered in the IoT system. Moreover, all these stakeholders need to be taken into account equally.

- Privacy: in the case of IoT systems that deal with critical data in critical applications (e.g. e-Health, Intelligent Transport, Food, Industrial systems), privacy becomes a make or break property.

- Interoperability: there are very strong interoperability requirements because of the need to provide seamless interoperability across many different systems, sub-systems, devices, etc.

- Security: as an essential enabling property for Trust, security is a key feature of all IoT systems and needs to be dealt with in a global manner. One key challenge is that IoT involves a variety of users in a variety of use cases, thus rendering trust highly dynamic.

- Technologies: by nature, all IoT systems have to integrate potentially very diverse technologies, very often for the same purpose (with a risk of overlap). The balance between proprietary and standardized solutions has to be carefully managed, with a lot of potential implications on the choice of the supporting platforms.

- Deployment: a key aspect of IoT systems is that they emerge at the very same time where Cloud Computing and Edge Computing have become mainstream technologies. All IoT systems have to deal with the need to support both Cloud-based and Edge-based deployments with the associated challenges of management of data, etc.

- Legacy: many IoT systems have to deal with legacy (e.g. existing connectivity, back-end ERP systems). The challenge is to deal with these requirements in a pragmatic manner, while safeguarding the "holistic IoT approach".

4.1.2 The need for a new approach

4.1.2.1 Introduction

In support of an "IoT-centric" approach, some elements have been used in the present document in order to:

- Support the analysis of the requirements, use cases and technology choices (in particular related to interoperability).
- Ensure that the target audience can benefit from recommendations adapted to their needs.

4.1.2.2 Roles

A drawback of many current approaches to system development is an exclusive focus on the technical solutions without considering the individual in these multiple capacities (e.g. user of an IoT device, professional) which may lead to suboptimal or even ineffective systems that hinder maximizing the benefits of IoT. In the case of IoT systems, a very large variety of potential stakeholders are involved, each coming with specific - and potentially conflicting - requirements, expectations and, possibly, vested interests. Their elicitation requires that the precise definition of roles that can be related to in the analysis of the requirements, of the use cases, etc.

Examples of such roles to be characterized and analysed are System Designer, System Developer, System Deployer, End-user, Device Manufacturer. Certain roles are to an extent addressed in the present document.

4.1.2.3 Reference Architecture(s)

In order to better achieve interoperability, many elements (e.g. vocabularies, definitions, models) have to be defined, agreed and shared by the IoT stakeholders. This can ensure a common understanding across them of the concepts used for the IoT system definition. They also are a preamble to standardization. Moreover, the need to be able to deal with a great variety of IoT systems architectures, it is also necessary to adopt Reference Architectures, in particular Functional Architectures. The AIOTI High-Level Architecture (see [i.25]) will be referred to in the present document.

4.1.2.4 Guidelines

The very large span of requirements, Use Cases and roles within an IoT system make it difficult to provide prototypical solutions applicable to all of the various issues addressed. In the context of the approach adopted under the present report, the stakes for individuals from the point of view of privacy are surfaced and appropriate guidelines are provided adapted to the respective target audience. Such guidelines are associated to the relevant roles and provide support for the decision-making involved.

4.2 Main objectives of the present document

A holistic approach of IoT systems implies the holistic consideration of human values by all IoT stakeholders. The consideration of those values underlie, of course, the fundamental texts of International and European Law, such as the Universal Declaration of Human Rights [i.14] and the Lisbon Treaty [i.15]. In the era of hyper-connectivity that entails extensive technical complexities and growing dependencies between networks and connected devices, the fundamental human values remain relevant and need to be safeguarded, also, within the new context created. Despite the challenges posed within non-linear environments such as IoT, respective decisions need to be made in accordance with those values and, certainly, with privacy. In a timely manner and in any event before the operationalization stage organizations and professionals assigned with a role as IoT stakeholders, need to raise and get confronted with a set of key relevant questions such as:

- How to design an IoT device?
- How to manufacture an IoT device?
- How to implement privacy in an already in use IoT device?

- How to deploy privacy-friendly software?
- How to upgrade software in a safeguarding individuals' privacy?
- How to engineer a privacy proof IoT system?
- How to monitor privacy within an IoT ecosystem?
- How to react if something goes wrong?

Notably those questions should not be addressed in an isolated manner. On the contrary, the hyper-connectivity pertaining to the IoT requires that certain critical decisions are taken jointly by IoT stakeholders, taking also into account the broader societal and economic interests involved. In this respect, although the General Data Protection Regulation (GDPR) [i.16] forms a technologically neutral legal instrument and, therefore, does not make any explicit reference to IoT, Recital 78 of the GDPR [i.16] emphasizes the responsibility of the series of actors involved in a supply chain without exclusively focusing on a single actor. More specifically, the specific Recital states that *"When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations"*. Under a wider perspective, an overarching question for IoT community would then be how to facilitate society and economy by systemizing and enabling privacy through IoT systems, while safeguarding fundamental human values such as human dignity, health and safety. The earlier stated human centred approach is captured by figure 1.

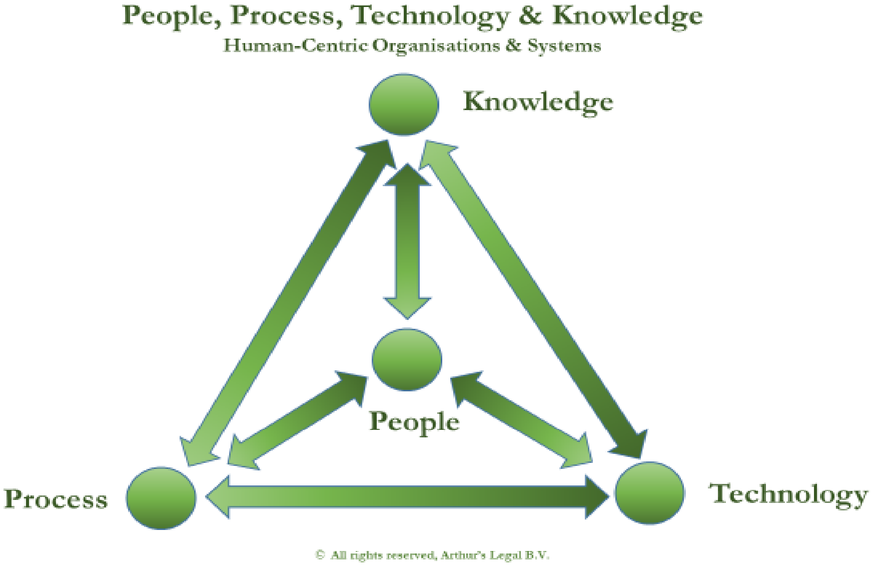

People, Process, Technology & Knowledge
Human-Centric Organisations & Systems
Knowledge
People
Process
Technology
© All rights reserved, Arthur's Legal B.V.

Figure 1: The Process, People, Technology & Knowledge Approach ("all rights are reserved by Arthur's Legal B.V")

Nevertheless, an effective and pragmatic approach mandates there are mechanisms in place enabling the assurance of values in practice and, in that sense, security can be considered as an enabler of privacy or, in other words, as a basic requirement for the effective protection of privacy. As an example, designing for privacy by default may use Privacy-Enhancing Technologies (PET) which is a security tool to reinforce the privacy design [i.4]. The present document aims at showing the role of technical and organizational measures in view of ensuring effective protection of privacy as well as the associated role of standards under the GDPR [i.16] and the proposed ePrivacy Regulation, stressing the exact time that it is anticipated that an IoT stakeholder will enter into action.

4.3 Purpose and target group

The purpose of the present document is to demonstrate that in view of the increasingly growing number of connected objects anticipated in the near future, effective protection of privacy and data protection would require that the relevant decisions are made upfront, at the design stage of the IoT systems. In addition, the present document will produce guidelines from which the target audience, i.e. the entire chain of IoT stakeholders, will be able - to the extent relevant - to benefit.

4.4 Content of the present document

Clause 5 reviews the role of standards primarily under the GDPR [i.16], that potentially create an impact on IoT ecosystems, and discusses briefly the role of standards under the proposed ePrivacy Regulation.

Clause 6 draws upon a set of use cases surfacing privacy challenges in the IoT environment. The use cases are related to smart home environment and the employment context (logistics).

Clause 7 produces an overview of the existing standards in the domain of privacy, reviews any potential gaps and suggests possible ways forward.

Clause 8 produces some available guidance for the safeguard of privacy in the IoT environment.

Clause 9 summarizes the main findings and lessons learned from the present document.

5 The role of standards under the GDPR

5.1 Setting the scene

In the context of the changing regulatory landscape, the present clause investigates the role envisioned for standards under the GDPR [i.16] and the proposed ePrivacy Regulation. It focuses on the new elements introduced creating possibly additional incentives and resulting benefits from the use of standards in the IoT. Notably, the most recent regulatory developments pertaining to the IoT environment include the application of the Network Information Security Directive (NIS Directive) [i.17], the recent agreement on the proposed Cybersecurity Act [i.18], as well as the Free Flow of Non-Personal Data Regulation [i.19] and the Payment Services Directive (PSD) [i.20] that mandates the European Banking Authority to draft regulatory technical standards. The GDPR [i.16] introduces one explicit reference to standards under Article 43 on Certification bodies authorizing the European Commission to adopt implementing acts that lay down technical standards for certification mechanisms and data protection seals and marks, as well as mechanisms that promote and recognize those certification mechanisms, seals and marks. Nevertheless, the limited references to technical standards in the regulation does not in any way negate the relevance of standards with respect to new obligations introduced.

Furthermore, on the basis of the latest amendments made on the proposed ePrivacy Regulation, standardized icons are envisioned for a specific purpose, which forms a rather new element with respect to the processing of personal data and the protection of privacy in the electronic communications sector [i.21]. The currently applicable ePrivacy Directive [i.22], being a legislative act that would be implemented at national level, focuses primarily at ensuring that Member States would inform the European Commission accordingly, while making explicit that any additional measures on technical equipment should be in accordance with the data protection law.

5.2 Standards under the GDPR

As opposed to its predecessor the Data Protection Directive [i.23], the GDPR [i.16] creates room for standards. The Preamble of the GDPR does shed some light on the regulatory intentions, while the new provisions on the principles of privacy by design and privacy by default, as well as the provision on the Data Protection Impact Assessment (DPIA) further frames the role of standards.

In particular, Recital 78 of the GDPR [i.16] states that: *"The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features"*. Notably, the GDPR [i.16] stresses the necessity of both technical and organizational measures (e.g. appointment of data protection officer), while focusing clearly on transparency and on the significance to create and improve security features, thus, surfacing the role of security in safeguarding protection of personal data.

As far as the obligation for data protection by design is concerned, Article 25 of the GDPR [i.16] mandates that it be taken into account both at the stage of the determination of the means of processing as well as at the time of the actual processing. In relation to this new obligation, the European Data Protection Supervisor (EDPS) [i.24] identifies four dimensions of data protection by design. Firstly, data protection requirements should be taken into account in view of the whole project lifecycle. Secondly, the technical and organizational measures should be selected on the basis of a risk-based approach, while taking into account specific criteria, i.e. the nature, scope, context, purposes of processing, the "state of the art" of available measures and the cost of implementation. In this respect, Article 32 of the GDPR [i.16] on the Security of Processing forms another clear illustration of the risk-based approach. The third dimension identified by the EDPS is the need for organizations to select appropriate measures with respect to the goals to be achieved. Finally, the fourth dimension identified is the necessity to actually integrate those measures into the processing. Notably, GDPR [i.16] does not provide for an exhaustive listing of the organizational and technical measures, leaving organizations with the freedom to choose.

The establishment of an explicit obligation to conduct a DPIA, provided that certain requirements are met, forms another example of a GDPR provision that illustrates the enhanced role of standards under the current European Data Protection Law. In particular, Article 35 of the GDPR [i.16] allows for the undertaking of Data Protection Impact Assessment, provided that certain requirements are met. In this respect, Article 35 paragraph 7 of the GDPR provides for the minimum information to be included in DPIA dictating in this respect the following: *"(…) The assessment shall contain at least:(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1[of Article 35]; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned"*. Notably, the DPIA does not limit the envisaged measures to the implementation of only technical measures, thus, bringing forward the role of organizational measures as well. Moreover, listing of the minimum content of a DPIA allows organizations to provide for additional contents, possibly, dictated under relevant standards. In any event, Article 35, also requires that "*Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations*". In this respect, the DPIA should be considered as an accountability tool that does not entail a single assessment but rather forms an assessment that is subject to continuous review. Therefore, it is likely that the DPIA results in an update of the measures in place to ensure that the necessary level of protection is continuously met.

Nevertheless, although the role of standards is strengthened under the GDPR [i.16], especially in light of the new principles and obligations mentioned above, the mere adherence to standards does not constitute a presumption of conformity with the provisions of the GDPR.

5.3 The proposed ePrivacy Regulation and standardization

Lawmakers in the EU have recently initiated steps with the view of updating rules relating to privacy and electronic communications and reinforcing trust and security in the Digital Single Market. Having identified areas to be addressed (including stronger protection online, simpler rules on cookies, and transparency on direct marketing, to name a few), the Commission released a Proposal for the Regulation in January 2017 [i.12]. In June 2017, this was followed by the Parliament's Committee for Civil Liberties, Justice and Home Affairs (LIBE) publishing a report with amendments to the Commission's proposal) [i.21]. It should be noted that, although the ePrivacy Directive is still applicable, the discussion below focuses exclusively on the proposed ePrivacy Regulation that in terms of scope constitutes a specific law in relation to the GDPR [i.16] that is a general law.

The text of the proposed ePrivacy Regulation strengthens privacy protection for individuals. It provides clarity regarding what legitimate grounds for processing prevail if both the GDPR [i.16] and the ePrivacy Regulation apply to a processing operation and prohibits all further use of electronic communications data collected under ePrivacy rules. In addition, significantly stronger obligations for privacy by default are proposed, including end-to-end encryption (with no backdoors) proposed as a security default measure for ensuring confidentiality of communications. Most importantly, the amendments provide for an extension of the principle of confidentiality of communications to machine-to-machine communications as well as enhanced definitions of 'electronic communications metadata' and 'direct marketing'.

More specifically, the latest version of the amended proposal published in October 2018 [i.31] briefly considers standardization in the communications systems domain. Recognizing the need for an easily visible and intelligible overview of the collection of information emitted by terminal equipment, the proposal also calls for the adoption of standardized icons to provide such overview. However, the proposal does not prescribe any details of such symbols and calls for delegated acts to be adopted for this.

According to paragraph 41 of the preamble of the ePrivacy Regulation delegated acts should be adopted in respect of the information to be presented, including by means of standardized icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimize the collection.

In addition, Article 8 on Protection of end-user's terminal equipment dictates the following:

"(2) The collection of information emitted by terminal equipment of the end-user to enable it to connect to another device and, or to network equipment shall be prohibited, except ~~if~~ on the following grounds:(b) the end-user has given his or her consent; or

(c) it is necessary for the purpose of statistical counting that is limited in time and space to the extent necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose.

2a. For the purpose of paragraph 2 points (b) and (c), a clear and prominent notice ~~is~~ shall be displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.

2b. For the purpose of paragraph 2 points (b) and (c), the collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.

(3) The information to be provided pursuant to paragraph 2a may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner".

Note that an updated draft on the proposal for the ePrivacy Regulation was published by the Council of the European Union on 15 February 2019 [i.32]; it is pertinent to note that the said draft does not modify the provisions of the proposal that have been inserted and discussed in this clause.

Overall, standards under the proposed ePrivacy Regulation standards are envisioned as a means to strengthen transparency, educate and empower end users in relation to the processing of their personal information.

6 Use Cases for IoT Privacy

6.1 Selection of Use Cases

This clause outlines how much IoT Security can improve IoT Privacy, aiming to discuss and reflect upon use case scenarios pertaining to the IoT domain. In view of drawing links and strengthening synergies with other EU ongoing work, certain of the use cases discussed are drawn from the ongoing EU Project, GHOST [i.5].

Taking into account the approach endorsed by the present document in favour of a human-centric approach, the use case scenarios to be presented bring forward the interaction between individuals and IoT devices, thus, being of direct relevance from privacy perspective. The specific use case scenarios have been considered appropriate in view of capturing concrete behaviours of ordinary users of IoT devices, thus, further allowing for specific guidance, setting clearly the individual as a priority. Furthermore, the overall approach and the objectives of this EU project, GHOST, have been deemed representative to bring forward the necessity for a human centric approach in the IoT environment, as suggested by the present document.

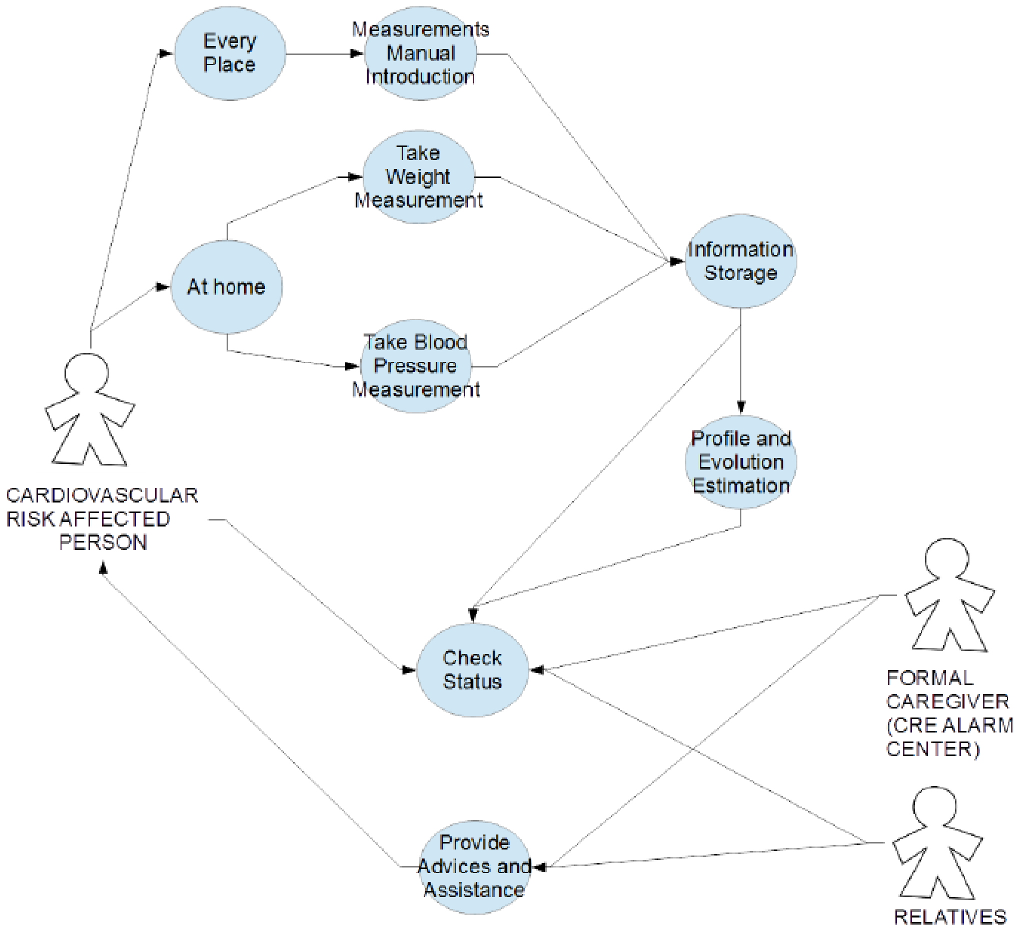
The discussion of the use cases is based on publicly available material [i.5], it provides the description of use case scenarios presented below under clauses 6.2 and 6.3. Use Case 4 has been developed for the purposes of the present report. The discussion below maps roughly the actors holding a role in the use case scenarios with the roles envisioned under the GDPR (e.g. organizations acting as data controllers or data processors).

6.2 Use Case 1: Ambient assisted living in smart homes, older people

This clause will expand on a use case scenario currently developed under the ongoing EU Project GHOST [i.5], that aims to deploy a highly usable and effective security framework for smart home residents applying a human-centric approach in its design. The initial use case scenario has been to an extent modified in order to better cater to the objectives of the present document. To this end, the narration of the use case scenario was summarized and the description linked to the specific technologies developed under GHOST project was removed. In addition, the discussion below produces a rough mapping of the actors in accordance with the roles provided under the GDPR [i.16] (e.g. data subject, data controller, data processor). Moreover, the discussion adds a rough categorization of the personal data presumably collected and further processed by the IoT devices employed.

Table 1

Context of use	One of the main lines and goals of the Spanish Red Cross is to provide care to more needed sectors of the society. Due to the demographic evolution of the population in Europe (and particularly in Spain), the number of people aged 65 years, or more is continuously increasing and the ratio of young persons to elderly persons is changing (fewer working people by each person older than 65). This situation is putting pressure over the public social and health care systems that will have problems in the near future to give high-quality assistance under these circumstances. Besides, the shift of the population from rural to cities and the reluctance of elderly people to move from their homes to geriatrics is increasing the number of elderly people that live alone in their own home, without direct assistance of any person. In this scenario, telecare and telehealth systems will be a highly demanded solution, both by those elderly people who live alone and by their formal and informal caregivers.
Story line	Ángela is 83 and she lives alone in her apartment in La Coruña. She does not have serious medical condition, but takes some chronic medication, she has to control her blood pressure, and her mobility is not very good. She fell on the street a few weeks ago. Also, she has been losing hearing in long distances. By installing CCTV cameras inside Angela's house, Alba - her daughter - can check at any time, through a website after signing in through a secure account, where her mother is present inside the flat. When Alba consults the information and sees that Ángela is near the phone in the living-room, she can make a call. Additionally, a wearable blood pressure tracker will help Alba to keep a check on her mother's blood pressure. Thus, even when Ángela leaves her home to go around the neighbourhood, do some shopping and sometimes meet friends or neighbours for a cup of coffee, Alba can check her mother's blood pressure thereby feeling more confident about her health. If, for example, Ángela falls and needs to ask for help or medical assistance, she can do so through a provision on the blood pressure tracker which will send a notification to the Spanish Red Cross, whose staff would then initiate the usual protocols to deal with such cases.

UML-oriented model	 Every Place Measurements Manual Introduction Take Weight Measurement At home Take Blood Pressure Measurement Information Storage Profile and Evolution Estimation CARDIOVASCULAR RISK AFFECTED PERSON Check Status FORMAL CAREGIVER (CRE ALARM CENTER) Provide Advices and Assistance RELATIVES **Figure 2: UML-oriented model (Use Case 1)** NOTE: Some secondary functionalities as mobility estimation or reminder scheduling are not indicated in figure 2.
Main stakeholders	As it is possible to see in the diagram, the main stakeholders are: • Elderly people with raised cardiovascular risk: inhabitant of the home that it is the beneficiary of telecare service. • Family caregiver: the relatives or family caregiver are the people the person with interest and with permission to check the status of the beneficiary. Normally, this role is played by the son/daughter of the beneficiary. • Formal caregiver: in this case, the Spanish Red Cross that provides the 24/7 telecare and assistance service. Note that it is presumed that the relative acting in her capacity as a caregiver is not member of the Spanish Red Cross.
Data Subject	Angela
Data Controller	Determines the purpose and means of processing personal data: • CCTV camera manufacturer • Blood pressure device manufacturer
Data Processor	Processor personal data on behalf of the controller: • Location service provider (provides Angela's location service to Alba) • Caregiver -Spanish Red cross company (provides staff that reviews Angela medical record) • Relative • Blood Pressure device manufacturer
Example of Personal Data	Angela's location
Example of Health Data	• Body Weight • Blood Pressure • Body Temperature • Blood type

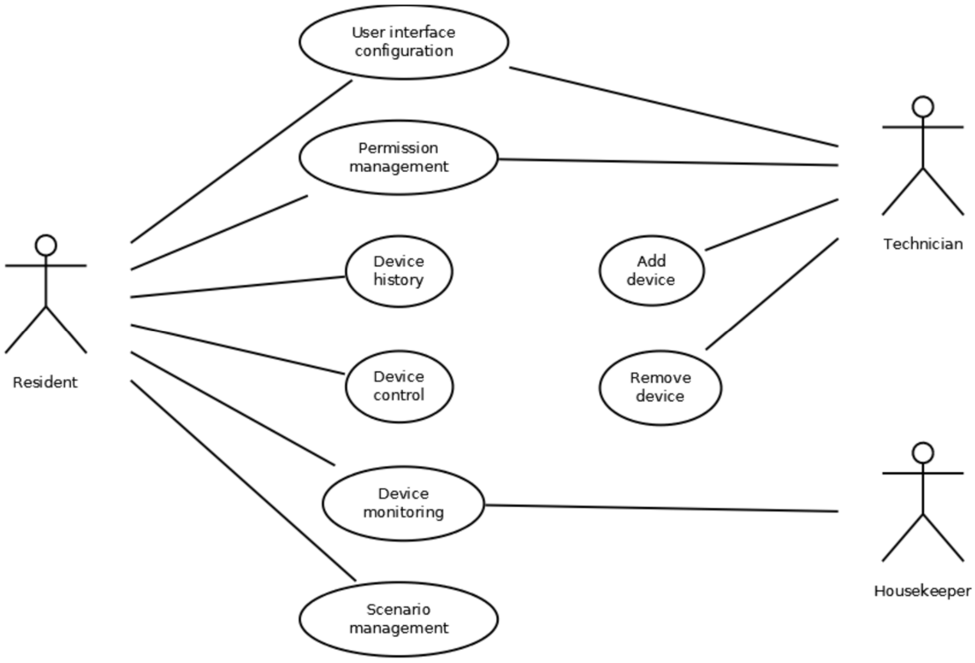
6.3 Use Case 2: Smart home solutions

In line with the paradigm of clause 6.2, this clause, also, presents a scenario from the ongoing EU Project, GHOST [i.5]. Same us it was the case for clause 6.1, original use case scenario has been to an extent modified in order to better cater to the objectives of the present document. To this end, the description linked to the specific technologies developed under GHOST project and how these technologies meet the project's objectives was removed.

In addition, the discussion below produces a rough mapping of the actors in the "Movie night scenario" in accordance with the roles provided under the GDPR (e.g. data subject, data controller, data processor). Moreover, the discussion adds a rough categorization of the personal data presumably collected and further processed by the IoT devices used under the same scenario.

Table 2

Context of use	In today's crowded and busy world people are seeking comfort and security in their own home. There is no better recovery from a hard-working day than a quiet relaxation at home or a weekend at one's cottage. But, as the world advances in density of the population, diversity and technology, there are many challenges to be solved: complexity of the technology and appliances installed in homes, increased power consumption, security of the people when at home or of the home when traveling. In this context, people are looking at the technology to solve their home issues by automating some of the repetitive actions, monitoring the power consumption and taking actions to reduce it or providing remote access to the devices installed in home in periods of absence. Having the home performing these chores automatically allows people to do more of what they like: work, family, friends, traveling or anything else. The smart home is solving some of these issues by being equipped with many sensors and actuators that allow it to be aware of the home parameters and events in every moment and take appropriate actions when needed. But, as with any new technology, the smart home brings specific threats related to the network security, people's privacy and complexity of the installation and maintenance of the devices. That is why solutions for identifying and analysing these threats and designing tools to prevent them are needed.
Story lines	**Movie night scenario** Erik is at home in the evening ready to see a movie in the living room. He wants a cosy atmosphere in the flat and does not want to be disturbed during the movie, so he can fully enjoy his experience. He sits on the sofa, in front of the TV screen, ready to start the movie, picks up his mobile phone and starts the smart home app. He is searching through already defined scenarios and finds what he needs: the movie night scenario. With a press of a button his flat door is locked, lights are off all over the house but in the living room where a dimmed discrete illumination is still present and the temperature in the living room is set a bit wormer than usual. Now Erik can enjoy the movie. **Security at night** Daniel is in his bedroom sleeping. It is late in the night when he wakes up because of a loud noise. He is still sleepy and does not want to go out of bed as it will be very difficult for him to go back to sleep after that. He takes his mobile phone, starts the smart home app and looks at the video streams coming from the video cameras installed outside home. Seeing nothing unusual, he checks the motion detectors around the home, but he sees no motion since last evening. To be sure, he also checks the contact sensors installed on the windows to see if any of them is forgotten open. Being reassured that everything is all right, he goes easily back to sleep. **Power saving** Olaf lives in a remote cottage in the mountains. He is using electrical power to heat up is home but the electricity in his region is very expensive and limited in periods of severe cold. All his heating radiators have a relay associated with them that can turn them on and off and the relay can also measure instant power consumption and the accumulated power consumption. Every room has its own temperature sensor and there is a temperature sensor installed outside. There is a script running in the home gateway installed in Olaf's home that is reading periodically the consumption in all the radiators and switching them on and off depending on the preferred temperature in each room, the temperature measured outside, priority of the rooms and a total consumption limitation for the instant and accumulated power. The preferred room temperatures, the priority of the rooms and the consumption limits are set by Olaf in the intelligent home mobile application In this way Olaf can control his electricity bill and make sure he keeps his instant power consumption within the required limits all the time.

UML-oriented model	 User interface configuration Permission management Device history Device control Device monitoring Scenario management Add device Remove device Resident Technician Housekeeper **Figure 3: UML-oriented model (Use Case 2)**
Main stakeholders	The main stakeholders are: • home residents • housekeeper (with a passive role in the solution) • technician
Data Subject	Depending on the story line: Erik, Daniel or Olaf
Data Controller	Smart home application developer
Data Processor	Video camera manufacturer Technician
Example of Personal Data	Home address Email address Telephone number
Example of Health Data	Not applicable

6.4 Use Case 3: Logistics and workplace

The use case scenario below has been developed for the purpose of the present document.

Table 3

Context of use	The port of Rotterdam is a multipurpose port with numerous terminals. Different types of cargo are transferred, and hundreds of employees are involved in the related procedures. Goods arriving on a daily basis from countries of the European Economic Area (EEA) and outside have to be stored under the appropriate conditions for different periods, before being possibly reshipped. Similarly, goods intended to be shipped to countries within EEA and beyond may be stored for different periods before beings shipped. The type and volume of data to be processed through a sophisticated equipment and IT systems, which are coordinated by employees from IT Department and protected under the supervision of the Department for port's security. The overall system is constantly checked through a sophisticated internal system, which allows the interchange of data with external entities and logistic actors, including processing of personal data of employees. The involved organisations are shipping companies, shipping agents, forwarders and train operators. During the logistic process, the main data exchanged relate among other to the type of cargo, the number of containers, type of equipment, registration of goods stored in the port, estimated time of arrival, estimated time of departure, usernames, passwords, e-mail addresses, phone numbers, contacts, personnel numbers and other personal data linked to employees. Cameras, also, installed in the port. Depending on the legal ground in place (e.g. contract in place providing for data flows), data may be transferred outside EEA.

Story line	Peter has been employee at Sky Shipping & Logistics Company Ltd for the last 2 years. As a part of his everyday work routine, Peter coordinates the incoming and outgoing shipments, ensures that the traffic is managed in an effective manner and most importantly, that the cargo is unloaded from the ships in a timely manner. During a quarterly meeting, it was decided that all the delivery representatives of the company would be equipped with a smart watch which they would be required to wear during office hours. The reason for the equipment was two-fold. Firstly, it allowed the respective managers to keep track of the time and duration for which the warehouse was accessed by their delivery representatives. Secondly, a secure system would be created that would only allow the deliver representatives to pick up the cargo after clearance was given by their managers along with a 4-digit OTP (One Time Password) which would be sent to their smart watches. Recently, Peter was assigned to the high-profile diamond merchants Glitterati and Co. Given the high value of the shipments, access to the data on the watch was given to a specific team in Glitterati and Co after obtaining Peter's consent. Moreover, it was clarified that access to the information on the watch would be only be provided when the diamond cargo would be arriving or was at the premises of the port. This will allow Glitterati and Co to reassure itself that their cargo is unloaded and delivered in a safe and secure manner.
Main stakeholders	The main stakeholders are: • Peter • Sky Shipping & Logistics Company Ltd • Glitterati and Co • Watch Company • Location service provider
Data Subject	Peter
Data Controller	Sky Shipping & Logistics Company Ltd
Data Processor	Sky Shipping & Logistics Company Ltd Glitterati and Co
Example of Personal Data	Peter's Location Email address Telephone number
Example of Health Data	Heart Rate Body Temperature

The earlier use case scenarios illustrate the overarching set of common data protection challenges that are associated to the IoT environment. Those can be summarized as follows:

- the high risk of profiling, for example, of a user of an IoT device or for a resident of a smart home;
- the lack of transparency resulting from hyper-connectivity hindering the exercise of data protection rights (e.g. right to object to further processing of personal information);
- increased dependencies raise concerns on the acquisition of a *freely* given and well-informed consent (e.g. elderly people residing in a smart home, employee in the port).

Overall, it seems less likely for the individual to be able to exercise control over the information concerning him and to be able to retain his anonymity within an IoT environment, while the large amounts of data collected create stakes not only at an individual but also at a societal level. Moreover, it can be argued that the growing lack of control further increases the imbalance of powers in relationships such as employer-employee.

7 IoT Privacy Standards landscape

7.1 Overview of Privacy Standards

Outside the context of the IoT environment, current standards on privacy are usually separated from security standards. However, recent standards in progress such as ISO/IEC 20547-4 [i.7] or ISO/IEC 27030 [i.29] on big data and IoT combine both security and privacy. Therefore, it can be stated that standardization bodies are gradually recognizing the hyper-connectivity and interconnectivity related developments, including IoT.

Moreover, although existing standards focus on risk management, recent standards in progress such as ISO/IEC 27550 [i.8] on privacy engineering take a global system lifecycle process viewpoint.

For example, it is worth noting that standards in progress such as ISO/IEC 20547-3 [i.6] or ISO/IEC 3014 [i.10] on big data and IoT architecture consist of sections elaborating on roles in the ecosystem, and further ISO/IEC 27552 [i.9] provides a list of privacy controls for data controllers and a separate list for data processors.

The table below list existing standards in the area of Privacy.

Table 4

Title	Summary	Reference
ISO/IEC 29100:2011: Information technology -- Security techniques -- Privacy framework [i.11]	ISO/IEC 29100:2011 [i.11] provides a privacy framework for when dealing with personal data. The standard: • specifies a common privacy terminology; • defines the actors and their roles in processing PERSONAL DATA; • describes privacy safeguarding considerations; and • provides references to known privacy principles for information technology. The framework provided in ISO/IEC 29100 [i.11]:2011 is as much applicable to persons as it is to organizations if they are using information and communication technology systems or services where privacy controls are required for processing personal data. Key Features and Benefits: • Provides a privacy framework that can be employed to safeguard personal data. Using the controls within this framework can mitigate significant risks posed to the personal data. • The information within the standard is as much usable by persons as it is to organizations if they are using information and communication technology systems or services where privacy controls are required for processing personal data. Making this standard applicable to both sole traders as much as it is to multinationals.	https://www.itgovernance.co.uk/
ISO/IEC 29151:2017 Information technology -- Security techniques -- Code of practice for personally identifiable information protection [i.36]	ISO/IEC 29151:2017 [i.36] establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of personal information. In particular, this Recommendation | International Standard specifies guidelines based on ISO/IEC 27002 [i.41], taking into consideration the requirements for processing of personal data that may be applicable within the context of an organization's information security risk environment(s). ISO/IEC 29151 [i.36]:2017 is applicable to all types and sizes of organizations acting as data controllers (as defined in ISO/IEC 29100 [i.11]), including public and private companies, government entities and not-for-profit organizations that process personal data.	https://www.iso.org/standard/62726.html
ISO/IEC 29134 Information technology -- Security techniques -- Guidelines for privacy impact assessment [i.37]	ISO/IEC 29134: Information technology [i.37] contains security techniques, provides a guideline for Privacy Impact Assessment (PIA) as an instrument for assessing the potential impacts on privacy of a process, information system, programme, software module, device or other initiative which processes personal data and, in consultation with stakeholders, for taking actions as necessary in order to treat privacy risk. A PIA report may include documentation about measures taken for risk treatment, for example, measures arising from the use of the Information Security Management System (ISMS) in ISO/IEC 27001 [i.40]. A PIA is more than a tool: it is a process that begins at the earliest possible stages of an initiative when there are still opportunities to influence its outcome and thereby ensure privacy by design. It is a process that continues until, and even after, the project has been deployed.	https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:ed-1:v1:en

Title	Summary	Reference
ISO 27018 Information technology -- Security techniques -- Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors [i.38]	ISO 27018 [i.38] is fully called ISO/IEC 27018 Code of practice for protection of personally identifiable information in public clouds acting as data processors [i.38], and it focuses on protecting the personal data in the cloud. ISO 27018 [i.38] works in two ways: (1) it augments existing ISO 27002 [i.41] controls (ISO 27002 provides a detailed explanation of ISO 27001 [i.40] security controls) with specific items for cloud privacy, and (2) it provides completely new security controls for personal data. Annex A of ISO 27018 [i.38] lists the following additional controls (that do not exist in ISO 27001 [i.40] and ISO 27002 [i.41]) that should be implemented in order to increase the level of protection of personal data in the cloud: • Rights of the customer to access and delete the data • Processing the data only for the purpose for which the customer has provided this data • Not using the data for marketing and advertising • Deletion of temporary files • Notification to the customer in case of a request for data disclosure • Recording all the disclosures of personal data • Disclosing the information about all the sub-contractors used for processing the personal data • Notification to the customer in case of a data breach • Document management for cloud policies and procedures • Policy for return, transfer and disposal of personal data • Confidentiality agreements for individuals who can access personal data • Restriction of printing the personal data • Procedure for data restoration • Authorization for taking the physical media off-site • Restriction of usage of media that does not have encryption capability • Encrypting data that is transmitted over public networks • Destruction of printed media with personal data • Usage of unique IDs for cloud customers • Records of user access to the cloud • Disabling the usage of expired user IDs • Specifying the minimal security controls in contracts with customers and subcontractors • Deletion of data in storage assigned to other customers • Disclosing to the cloud customer in which countries will the data be stored • Ensuring the data reaches the destination In order to be certified under ISO 27018 [i.38], a cloud service provider need to undergo an audit by an accredited certification body. Would-be cloud customers can verify a provider's compliance with the standard via the provider's certificate of conformity. To maintain its certification, a cloud services provider has to subject itself to periodic third-party reviews. By assuring that organizations can address security issues related to personally identifiable information stored on the public cloud, ISO 27018 [i.38] can help demonstrate commitment to protecting personal records.	https://www.iso.org/standard/61498.html

Title	Summary	Reference
ISO/IEC 27000 Information Technology -- Security Techniques Information Security Management Systems -- Overview And Vocabulary [i.39]	ISO 27001 [i.40] could be of help on serving the purpose of demonstrating that the organization is actively managing its data security in line with international best practice and the GDPR. Yet, as per the data centric and human centric approach endorsed by the GDPR, linear standards such as ISO 27001 [i.40] could only partially facilitate compliance with the GDPR. ISO 27001 [i.40] is the international best practice standard for information security and is a certifiable standard that is broad-based and encompasses the three essential aspects of a comprehensive information security regime: people, processes and technology. By implementing measures to protect information using this three-pronged approach, the company is able to defend itself from not only technology-based risks, but other, more common threats, such as poorly informed staff or ineffective procedures. ISO/IEC 27001 [i.40] meets these needs, addressing the encryption of data, confidentiality, integrity, availability, risk assessment, and business continuity. Ultimately, the guidelines and controls set forth by ISO/IEC 27001 [i.40] as an organization's best practice framework position it to identify its requirements for the GDPR. Furthermore, these guidelines not only assist in responding to contractual and regulatory requirements, but also implement appropriate controls to manage risks to the business's information, such as personal records. By implementing ISO 27001 [i.40], an organization will be deploying an Information Security Management System (ISMS): a system that is supported by top leadership, incorporated into the organization's culture and strategy, and which is constantly monitored, updated and reviewed.	https://www.itgovernance.co.uk/blog/how-iso-27001-can-help-to-achieve-gdpr-compliance/
BS 10012:2017 Data Protection. Specification For A Personal Information Management System. Specification For A Personal Information Management System [i.42]	The objective of the BS 10012:2017 [i.42] British Standard is to enable organizations to put in place, as part of the overall information governance infrastructure, a Personal Information Management System (PIMS) which provides a framework for maintaining and improving compliance with data protection requirements and good practice. This new edition of BS 10012 [i.42] has been written in recognition of the publication of the European Union General Data Protection Regulation (GDPR), which was approved by the European Parliament on 14th April 2016. This replaces the European Directive 95/46/EC [i.23] which was implemented in the UK by the Data Protection Act 1998, on 25th May 2018. The GDPR will be directly applicable to the UK and member states who retain the ability to introduce national level derogations where these are required for specific purposes; however, the results of the referendum on the UK's membership of the European Union make it unclear how the GDPR will be implemented - such issues will be monitored and updates to this British Standard will be issued where necessary. Amongst the changes from the 2009 edition of BS 10012 [i.42], are: • New definition of personal and sensitive data. • Restrictions on profiling using personal data. • New administrative requirements for data privacy officers. • Pseudonymous data specifically covered. • Abolishing of notification/registration requirement. • New stricter require for consent for processing. • Changes to subject access and other rights for data subjects. • Enhanced right to erasure and new right to profitability. • Security breach notification requirement. • Privacy by design and privacy impact assessment requirements. • Extension of the law to cover data processors. • Removal of the Safe Harbour ground for data transfers to the U.S.A. BS 10012:2017 [i.42] enables organizations to put in place a Personal Information Management System (PIMS). This provides the framework for maintaining and improving compliance with data protection guidelines and good practice, and, when used alongside a robust Information Security Management System (ISMS), can place an organization in a good position to demonstrate GDPR compliance.	https://shop.bsigroup.com/ProductDetail/?pid=000000000030339453

Title	Summary	Reference
Recommendation ITU-T X.1231 - Supplement on guidance to assist in countering spam for mobile phone developers [i.43]	As mobile phones are widely used, malicious attackers tend to send spam intentionally to mobile application users, which causes financial problems and creates privacy issues. This Supplement 25 to Recommendation ITU-T X.1231 [i.43] provides guidance to assist in countering spam for mobile phone developers. In addition, this Supplement describes the following elements: - Security threats of mobile phones with application level aspects; - Guidance to assist in countering spam for mobile phone developers.	https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=10479
ITU-T X.1155 Guidelines on Local Linkable Anonymous Authentication for Electronic-Services [i.44]	In electronic services or e-services, there are various occasions where privacy violations are of concern. Service providers may gather users' personal information in the process of subscription, purchase or delivery. They may be able to access and exploit users' personal data that is collected during the service processes. The consequences these threats pose to user privacy, such as personal data leakage and tracking, are very serious emerging social issues. Therefore, technological solutions for preserving privacy in e-services are necessary. Anonymous authentication that allows users to be able to authenticate themselves without revealing their identity is the most fundamental means of addressing the privacy threats associated with e-services. Recommendation ITU-T X.1155 [i.44] provides guidelines on local linkable anonymous authentication for e-services. This includes the privacy threats of e-services, the requirements of local linkable anonymous authentication, the functions that satisfy these requirements, and a general model of local linkable anonymous authentication for e-services.	https://www.itu.int/rec/T-REC-X.1155-201510-I
ITU-T TD 733-PLEN Technical framework of PII (Personally Identifiable Information) handling system in IoT environment [i.45]	IoT devices can collect many kinds of data, including personal data. Because personal data is useful for several kinds of services, they can be shared with multiple service providers. It is better for users to handle own data, including personal data, in IoT environment based on their intention. Because the situation of data usage in IoT environment with multiple service providers will be complicated, the user's intention on data usage should be reflected flexibly. For example, if the IoT platform has the following functions, the user can recognize that the collected data including personal data can be controlled properly. The users can set up personal data control preference. This preference includes the list of permitted data for shared by each service provider. The collected data is controlled access based on the personal data control preference. Unauthorized data cannot be shared with other service providers. The users can check the history log of data sharing among the service providers. The users can understand the timing of data usage. This Recommendation will provide the technical framework of personal data handling system for IoT environment to fulfil these functions.	https://www.itu.int/md/T17-SG17-170829-TD-PLEN-0733/en
ITU-T TD 731-PLEN Security guidelines for smart metering service in smart grids [i.46]	Smart metering services are widely deployed in many countries (including developed and developing countries) in order to make electricity grid efficient and reliable by gathering and providing electricity usage information from and to customers. Based on this information, providers can estimate customers' electricity demands, and can shift the demand or make customers use their own electricity by providing information on electricity usage to customers. However, there are various kinds of threats that may cause the malfunction of the smart metering service. Invalid metering information can lead to erroneous decision on demand management and abuse of load control function can result in customers' economic and physical damage. In addition, when the 3rd party service providers can use the metering information, personally identifiable information (Personal Data) protection issue should be considered. When smart metering services do not have enough security measures, customers may protest against smart meter installation, which has happened in many countries.	https://www.itu.int/md/T17-SG17-170829-TD-PLEN-0731/en

Title	Summary	Reference
ITU-T TD 962-PLEN Security Requirements and Framework for Big Data Analytics in mobile Internet services [i.47]	Currently, according to the computation and storage ability improvements in the mobile devices and also with the enhanced transmission rate in telecommunication networks, the mobile Internet services are more and more popular and widely used. Due to the frequent interaction among the users, multiple types of devices, networks, and services providers, in a broad range of mobile Internet service areas, data is growing at unprecedented scale. In mobile Internet service, the increase of cost efficiency is important, but the next generation of mobile Internet services need a new business insight. Since the data source is not fixed and will be diverse, the analysis system could be used by malicious users or attackers to achieve illegal or unethical purposes. Mobile Internet services obtain big data from multiple sources and multiple data dimensions with characteristics including scale (volume), diversity (variety), high speed (velocity) and possibly others like credibility (veracity) or business value. Such big data analysis now drives nearly every aspect of mobile Internet service to improve service quality and user experience. Based on big data aggregation and analytics, the service provider can analyse user's interests more effectively and evaluate user's expectation more accurately thus significantly improving and adding value to their services, for example: - Mobile search application: to precision target users' search intention timely; - Mobile financial application: to customize users' financial solution timely; - Mobile application recommendation: to improve successful rate of recommendation timely. As the new technology develops, big data analytics will bring new security issues comparing to previous data analytics in mobile Internet services domain, such as, how to secure storage big volume data with ensuring consistency, availability, tolerance and synchronism; how to preserve availability, integrity, and confidentiality when collecting, storing, and analysing big data. Without comprehensive security mechanism, the unsecure/spiteful big data analysis will do harm to mobile Internet service provider's business security, user's data security, and even user's privacy. To ensure secure big data analysis in mobile Internet services, consequently, the security requirements need to be analysed exhaustively and the overall security framework need to be established.	https://www.itu.int/md/T17-SG17-180320-TD-PLEN-0962
ETSI TS 118 103 [i.27]	This Recommendation provides normative and informative specifications for oneM2M Security and Privacy protection.	http://www.onem2m.org/technical/published-drafts

7.2 Example of Privacy Solution - oneM2M Architecture

Obtaining and maintaining the relevant appropriate level of protection envisaged by the GDPR can be, though, to a certain extent facilitated by the use, for example, of a Privacy Policy Manager (PPM) architecture described in oneM2M Technical specification [i.27]. The specification covers process for registration of end user privacy preference and customization of user information. The specification [i.27] also addresses implementation models for PPM. A simplified version of PPM architecture is shown in the diagram below. The AIOTI reference architecture [i.25] provides a common architecture for IoT and like the oneM2M PPM can support the elements of GDPR.

As a relevant example of practical implementation of Privacy policy for IoT the oneM2M Privacy Policy Manager (PPM) architecture [i.27], is a distributed authorization privacy protection architecture that takes into consideration the user's privacy preference. The PPM handles the user's consent, stores the access log, and keeps track of data that was collected. The PPM can store access control policies and with a PPM portal it can give the data subjects the ability to configure their preference. Table 5 describes possible ways in which the PPM can meet the GDPR principle.

Table 5: Comparison of GDPR Principle to PPM Design

GDPR Principle	PPM design support
Lawfulness, Fairness and transparency: Personal data should be processed lawfully, fairly and in transparent manner in relation to the subject	Sophisticated consent mechanism for privacy policy: When an end user subscribes to a service which uses an application server in oneM2M architecture, the end user becomes a data subject, and the data subject creates a privacy preference and registers it on the PPM.
Purpose Limitation: Personal data should be collected for specified, explicit and legitimate purposes and not for further processing in a manner that is incompatible with those purposes.	When a data subject joins an application entity, the data subject configures a privacy preference using the PPM. A privacy preference explains what kind of data are allowed to be accessed. Note: It does not state if too much data has been collected. This could be done from the point of development and not when data subject is stating the privacy preference.
Data minimization: Personal data should be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.	When a data subject joins an application entity, the data subject configures a privacy preference using the PPM. A privacy preference explains what kind of data are allowed to be accessed.
Accuracy: Personal data should be accurate, kept up to date if not they should be rectified.	When a data subject joins an application entity, the data subject configures a privacy preference using the PPM. A privacy preference explains what kind of data are allowed to be accessed.
Storage Limitation: Personal data should be kept in a form that permits identification of data subjects for no longer than it is necessary for the purpose for which the personal data is processed.	The PPM should create or update access control policies using the privacy policy that the data subject accepts.
Integrity and Confidentiality: Personal data should be processed in a manner that ensures appropriate security including protection against unauthorized or unlawful processing against accidental loss, destruction or damage.	The data subject can subscribe to various kinds of services. Service lists are registered on an M2M portal and the data subject can select services to subscribe to. When the data subject subscribes to a service, the data subject needs to accept a privacy policy. In order for the data subject to easily understand this policy, the PPM should create the customized privacy policy based on the privacy policy provided by the application entity and the data subject's privacy preference. Therefore, the data subject can control personal data and agreement implies understanding of the privacy policy. The policy will state the integrity and confidentiality policy of the data controller. Traceability of personal data usage: PPM should store the access log that records which application entity accessed which kind of collected data.

Overall, standards may serve as a useful tool towards compliance, but they do not suffice to ensure compliance with the GDPR, in the sense that they are not meant to ensure conformity with the GDPR.

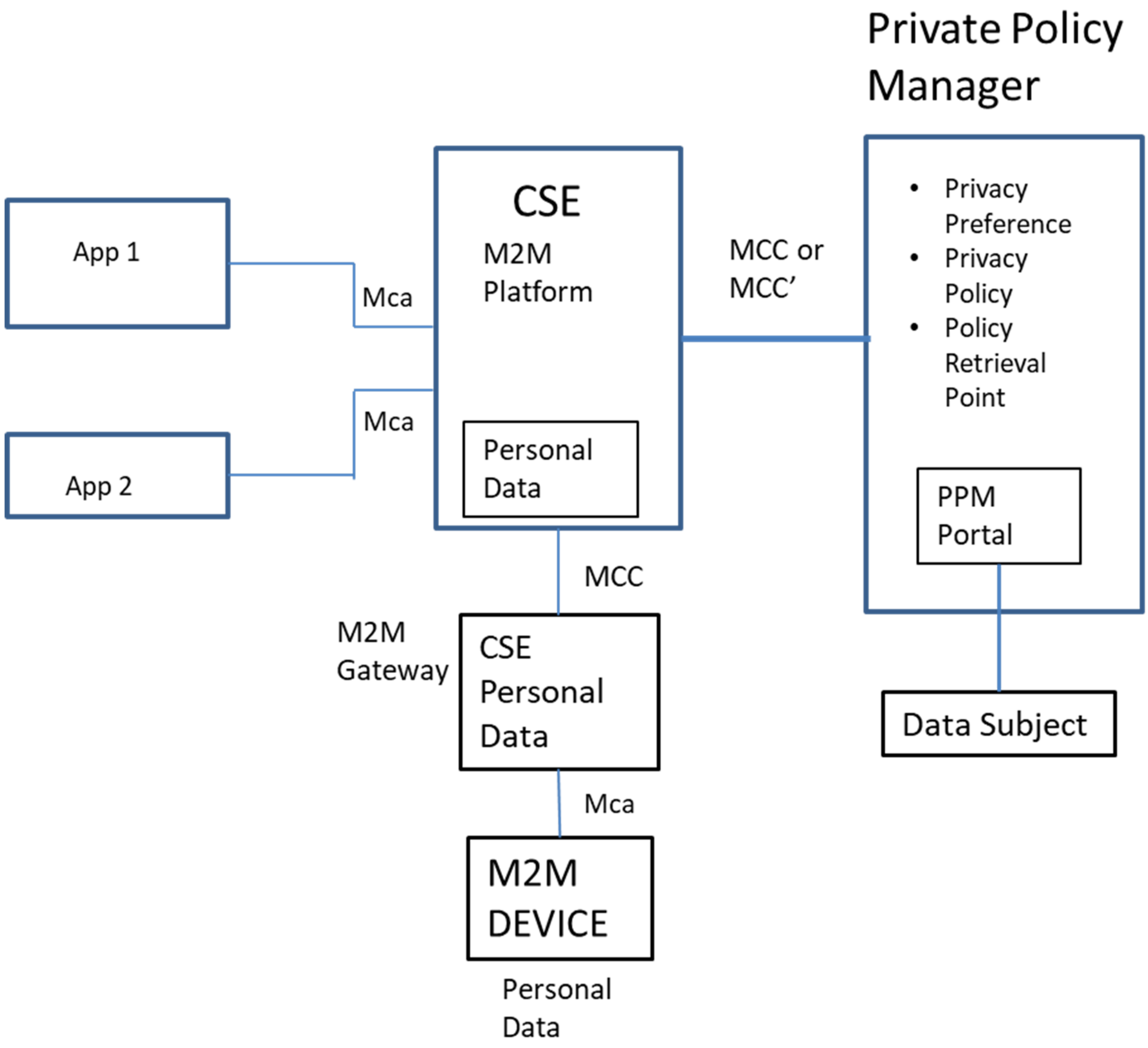


Figure 4: Simplified version of the Policy Manager Architecture

7.3 Addressing the Privacy Gap

As part of its conclusion, ETSI TR 103 376 [i.1] mentioned that Data ownership is a key user requirement, and that Privacy is priority to ownership. The survey carried out in ETSI TR 103 376 [i.1] for seven verticals domains pointed out the gaps identified in the table below. The conclusion of ETSI TR 103 376 [i.1], indicated that these areas are major concerns to stakeholders and need to be addressed. Table 6 reviews the gaps and suggests how these gaps have been addressed thus far.

Table 6: Relevant instruments to address privacy in IoT areas

IoT Area	Consolidated Gap on Security/Privacy	Relevant instruments to address area
Smart Environment	Security and privacy: Smart environment data, especially those from utilities (energy/water) can be very sensitive. Security and data privacy standards are necessary. The lack of these standards prevents large scale deployments. Societal- Data privacy (storage, transport, processing).	a) General and specific b) International and national c) Regulation and standards The Directive on security of network and information systems (NIS Directive) [i.17] forms an example of a specific regulation to applicable across EU Member States. NIS Directive is highly relevant, also, for the smart environment, given that drinking water supply and distribution forms an example of critical infrastructure, defined under the Directive.
Smart Mobility	a) Security and privacy: data security, data privacy and ownership. b) rules to ensure trust in a common good objective and avoid vehicle spoofing.	a) General and specific b) International and national c) Regulation and standards Directive 2010/40/EU [i.30] on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, also, known as ITS Directive forms an example of a specific regulation applicable across EU Member States.
Smart Wearables	Security and privacy: Since Smart Wearables devices are dealing with very sensitive and personal data. Security and data privacy standards are necessary. The lack of these standards prevents user acceptability from both enthusiasts and rejecters.	a) General and specific b) International and national c) Regulation and standards The GDPR constitutes an example of a general regulation, applicable across Member States, providing, also, for the protection of health data often collected by wearable devices (e.g. blood pressure).
Smart Farming	a) Security and privacy: data security, data privacy and ownership. b) rules to ensure trust in a common good objective.	a) General and specific b) International and national c) Regulation and standards The Trade Secrets Directive forms an example of a sector specific regulation applicable across Member States.
Smart Living	a) Security and privacy: data security, data privacy and ownership. b) rules to ensure trust in a common good objective.	a) General and specific b) International and national c) Regulation and standards The GDPR constitutes an example of a general regulation, applicable across Member States, providing for the protection of personal data (e.g. name, address). The GDPR explicitly refers to the role of standards in the field of personal data protection.

IoT Area	Consolidated Gap on Security/Privacy	Relevant instruments to address area
Smart Cities	Security and Privacy: IoT platforms have to ensure data privacy, integrity and transmission accordingly to the information sensibility.	a) General and specific b) International and national c) Regulation and standards The GDPR constitutes an example of a general regulation, applicable across Member States. It provides, also, for the protection of personal data, when it is necessary that they are processed for the performance of a task carried out in the public interest, as it is largely the case in the context of Smart Cities.
Smart Manufacturing	Cyber Security. There is still a difficulty to provide end-to-end security for complex manufacturing systems, in particular considering the large span of virtual actors (from devices and sensors up to enterprise level systems) and the overall need for human presence and decisions. Approaches such as security by design will change the current approaches (e.g. to certification). The related standards are still to come.	a) General and specific b) International and national c) Regulation and standards The Free Flow of Non-Personal Data Regulation forms an example of a general regulation, applicable across EU that would allow the flow of data, other than personal, across Member States, unless, of course, dictated otherwise (e.g. for reasons of public security).

The review of the above shows that there does not appear to be any new standards or regulations needed with respect to privacy within the seven verticals domains according to the concerns raised in ETSI TR 103 376 [i.1]. The effective use of existing standards and regulation in a circular manner would seem to be sufficient to maximize the possible resulting benefits. Although it falls outside the scope the present document, it is worthwhile noting that there is room for new codes of conduct and certification, as they are clearly embraced as accountability tools under the GDPR and they are, of course, highly relevant, also, for the IoT environment. It should be stressed, though, that for a holistic IoT approach, taking into account only the GDPR and standards does not suffice for the effective protection of privacy and security in the IoT environment. As shown in table 6, there is a series of relevant instruments pertaining to IoT, including, laws of general application and laws governing a specific subject matter.

7.4 The way forward

There are no obvious missing gaps in standardization but there is a significant gap in application of privacy protection capability in general, and of standards based of privacy protection capability specifically. This was the same conclusion that was deduced in ETSI TR 103 370 [i.26]. The report indicates that gaps are in the appropriate application of the privacy principle which can be resolved by proper code of conduct and certification as mention in the above clause. One of the guidance to code of conduct is for technical system to consider privacy by default and by design as explained below.

8 IoT Privacy guidance and best practices

8.1 IoT Privacy Guidance pursuant to current best practices

In line with the spirit of the best available techniques in the domain of data protection for which it is considered that "best" is meaning the most effective in achieving a high general level of protection [i.15], best practices should similarly be defined for the purpose of the present discussion as the optimum practices endorsed by public and private organizations as the most effective in achieving a high level of protection within the IoT ecosystem. Taking into account the general data protection principles provided under the GDPR, the clause below discusses how these principles can be narrowed for the IoT ecosystem. Furthermore, it makes certain suggestions how these principles can be implemented in practice through concrete actions.

8.2 IoT framework principles pursuant to the GDPR

Based on the discussion of the data protection-related requirements set forth by the GDPR, and in light of the human centric approach put forward by the present document, this clause examines and suggests some of the best practices to be adopted by organisations. This guidance can be of great relevance, especially, for organizations that are aiming to go beyond the threshold of compliance, beyond the minimum requirements for compliance.

For example, data protection by design, established under Article 25 of the GDPR, could be broken down into the following set of principles:

1) No personal data by default principle: avoid personal data collection or creation by default, except where, when and to the extent required.

2) 'As-If' principle: design and engineer IoT ecosystems as-if these will process personal data, now or in a later phase.

3) De-Identification by default principle: de-identify, sanitise or delete personal data as soon as there is no longer any valid legal basis.

4) Data minimization by default: only process data where, when and to the extent required, and delete or de-identity other data.

5) Encryption by default principle: encrypt personal data by default and include digital rights and digital rights management thereto.

Analysing high level concepts such as the "no personal data by default" principle, concrete guidelines could increase the likelihood of their endorsement in practice by organizations and professionals.

8.3 Proposed guidelines on meeting GDPR principles

The following elaborates on the above principles and suggest guidelines needed to meet these principles in practice:

1) No personal data by default principle: avoid personal data collection or creation by default, except where, when and to the extent required.

2) Provide a Short Contextual Privacy Notice at the point of collection.

3) If relying on consent, provide granular choices - do not bundle consent - and ensure individuals are aware of the persistency of consent and how to revoke it.

4) Capture and retain evidence of consent revocation.

5) Identify the legal basis for processing special categories of personal data such as biometrics.

6) Use language that can easily be understood by target audience.

7) Place a hyperlink in the short Privacy Notice to the more detailed company Privacy Statement.

'As-If' principle: design and engineer IoT ecosystems as-if these will process personal data, now or in a later phase:

1) Help cloud customers comply when individuals assert their access rights.

2) Disclose the names of any sub-processors and the possible locations where personal information may be processed prior to entering into a services contract.

De-Identification by default principle: de-identify, sanitise or delete personal data as soon as there is no longer any valid legal basis:

1) Set a data retention policy specifying the period for which personal information should be retained, including log files.

2) Ensure data are securely deleted when no longer required, including log files.

3) Implement a policy for the return, transfer or disposal of personal data, for instance when the service comes to an end.

4) Help customers comply when individuals assert their access rights.

5) Establish a process (free of charge) by which users can update their information and correct any inaccuracies.

6) Disclose information to law enforcement authorities only when legally bound to do so.

Data minimization by default: only process data where, when and to the extent required, and delete or de-identity other data:

1) Only collect personal information that is necessary for example if data is for marketing or advertising purposes with the customer's express consent, let the data collected be for such purpose as its needed.

2) Specify data to be collected and identify the reasons for collecting personal data (e.g. necessary for billing purposes).

Encryption by default principle: encrypt personal data by default and include digital rights and digital rights management thereto:

1) Document the security measures to be adopted through the data lifecycle.

2) Assign responsibility to an appropriate person for monitoring and ensuring compliance.

3) Ensure data is transferred securely between all parties involved in the verification or sharing of personal data and attributes. The security should be commensurate to the risks associated with the data types and sensitivity, potential for harm and impact on the user if the data are compromised, and any local regulatory or legal requirement.

4) Use appropriate access controls to limit access to attribute databases and attribute sources to authorized persons.

5) Enter into confidentiality agreements with staff who have access to personal data and provide appropriate staff training.

6) Establish system and procedural controls to verify and maintain the accuracy and reliability of personal data and attributes.

7) Establish system and procedural controls to capture and address data corruptions and mismatches.

8) Subject their services to independent information security reviews at scheduled intervals (or when significant processing changes occur).

8.4 Existing guidelines: the paradigm of privacy by design

This clause presents some of the best practices that could be very useful when it comes to privacy design [i.4]. Privacy by design refers to considering privacy aspect from the onset of any design. It is about being proactive rather than being reactive. Privacy is considered as the default and embedded in any architecture design. Some organisations have provided guidelines in this area and the table below indicates some of the guidelines that have been published. Some do not directly mention IoT but they give good relevant guidance to components that are used in IoT environment.

Table 7

Title	Summary	Reference
British Information Commissioner's Office (ICO) Guidance to Privacy in mobile apps [i.48]	The guidance [i.48] has been produced to help application developers comply with the Data Protection Act 1998 and 2018 and ensure users' privacy. Additionally, an organization based outside of the UK that develops apps for the UK market, should consider that its users in the UK will clearly expect any application they use to respect their privacy according to the above-mentioned legislative acts. While a typical mobile device would be a smartphone or tablet, this guidance can also be applied to other devices using similar app technology, for instance living-room devices such as smart TVs or games consoles. Throughout, the guidance concentrates on the issues most specific to the mobile environment and includes references to more detailed guidance where relevant. Document addresses the following: • Will the application deal with personal data? • Who will control the personal data? • What data will be collected? • How will the application inform users and gain their consent? • How will it give users feedback and control? • How will it keep the data secure? • How will it be tested and maintained?	https://ico.org.uk/media/1596/privacy-in-mobile-apps-dp-guidance.pdf
British Code of Practice for consumer IoT security UK Gov: Dept of Digital, Culture, Media & Sport [i.49]	The Government's Code of Practice for Consumer Internet of Things (IoT) Security for manufacturers, with guidance for consumers on smart devices at home [i.49]. The aim of this Code of Practice is to support all parties involved in the development, manufacturing and retail of consumer IoT with a set of guidelines to ensure that products are secure by design and to make it easier for people to stay secure in a digital world. The Code of Practice brings together, in thirteen outcome-focused guidelines, what is widely considered good practice in IoT security. It has been developed by the Department for Digital, Culture, Media and Sport (DCMS), in conjunction with the National Cyber Security Centre (NCSC), and follows engagement with industry, consumer associations and academia. The Code was first published in draft in March 2018 as part of the Secure by Design report. Implementing the Code of Practice may help organizations achieve compliance with applicable data protection laws. For example, the EU General Data Protection Regulation (GDPR) requires personal data to be processed securely. In March 2018 the Government published the Secure by Design report which advocated a fundamental shift in approach to securing IoT devices, by moving the burden away from consumers and ensuring that security is built into products by design. Central to the report was a draft Code of Practice primarily for manufacturers of consumer IoT devices and associated services.	https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security
GSMA report [i.50].	GSMA report on: Protecting Privacy and Data in the Internet of Things Report [i.50]. The GSMA, together with the mobile industry, has devised a range of valuable resources tools and techniques which can be applied to IoT applications and services, particularly where big data storage, analytics and machine learning are employed, providing guidance and expertise to help companies with the challenge of securing the connected future.	https://www.gsma.com/iot/resources/protecting-privacy-and-data-in-the-internet-of-things-report/

9 Concluding Remarks

The key takeaways resulting from the present document can be summarized as follows:

- The requirements set under the GDPR are mandatory.

- The effective protection of privacy and (personal) data protection, also, within the IoT environment requires appropriate technical and organizational measures. The implementation, monitoring and optimization of those measures are to be planned and taken both in advance as well as during the related data collecting, data processing and data management pertaining to the life cycle of the respective IoT ecosystem.The GDPR further requires organizations not only to be able to ensure, but also to deliver documented and continuous proof of appropriate levels of compliance - defined in the GDPR as: accountability, on a continuous basis.

- In essence, the GDPR provides for a general and principle-based framework.

- Therefore, there is a clear role for standards and related certification schemes to play. This could be achieved, for example, by loading and otherwise contextualising and deploying the various principles and adapting those with risk-based and impact-based frameworks, measures, metrics, measurements and methodologies.

- The GDPR is the 2.0 version of the Data Protection Directive. GDPR constitutes an upgraded version of the Data Protection Directive by introducing new obligations and principles such as, for instance, the performance of a Data Protection Impact Assessment (DPIA) and the principles of data protection by design and by default. These novelties of the GDPR create concrete new opportunities for standards.

- There is a plethora of standards relevant for the IoT environment. There is no need, thus, to create additional standards reflecting the rational of the existing ones. However, it is needed that when new standards emerge focussing on the differentiated perspective that is reflected in the GDPR; such that are produced under a differentiated perspective. Such a perspective would imply the adoption of a human-centred approach as highlighted by the present document.

- Taking into account the low penetration rate of the existing standards, a holistic approach of IoT would presume the engagement of all IoT stakeholders and would, therefore, possibly, increase the likelihood of their wide adoption and actual implementation. In the context of the currently changing regulatory landscape at EU level, there is a series of developments that has recently taken place, including the Cybersecurity Act [i.18] and the NIS Directive [i.17] discussed in detail under ETSI TR 103 533 ([i.2]) on "Security; Standards Landscape and Best Practices", as well as the Free Flow of Non-Personal Data Regulation [i.13] and the PSD2 Directive [i.51].

- A pragmatic approach aiming at increasing effectiveness of standards would imply that any new standards to be adopted in light of the GDPR that they are created take into account how these standards would interoperate with the rest of the legislative acts pertaining to the IoT ecosystem as well as any other standards developed in line with those acts.

- Finally, bearing, also, in mind that standards do not meant to guarantee conformity with the GDPR, the development of new standards suggesting the approach above could steer organizations going beyond mere compliance with the applicable legal framework towards meaningful and now mandatory accountability.

Annex A:
Change History

Date	Version	Information about changes
May 2018	0.1.0	Initial draft version submitted to SmartM2M for review and possible acceptance during SmartM2M #46 on June 21st, 2018.
December 2018	0.2.0	Preparation for advanced stable draft to be submitted for review to SmartM2M.
December 2018	0.3.0	Stable draft delivered for consensus review to SmartM2M TC.
March 2019	0.4.1	Final draft delivered for consensus review to SmartM2M TC.

History

Document history		
V1.1.1	October 2019	Publication