ETSI TR 103 534-2 V1.1.1 (2019-10)

TECHNICAL REPORT

SmartM2M; Teaching material; Part 2: Privacy

Reference

DTR/SMARTM2M-103534-2

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

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 is to focus on producing teaching material on privacy and to direct the reader to other materials that are available in order to gain a basic understanding on what the privacy concept relates to that is particularly relevant, also, for the IoT environment. The present document is based on the Privacy Report ETSI TR 103 591 [i.1].

Taking into account the main gaps result of the STF 505 (https://portal.etsi.org/STF/STFs/STFHomePages/STF505) in relation to privacy and security as captured under ETSI TR 103 376 [i.13], the document starts by introducing the target audience to whom the present document is addressed to base on the assumption that the future reader has no knowledge on the issue of privacy. To this end and in view of achieving the maximum of the learning outcome, the document will address key aspects of privacy by raising a set of relevant questions. In line with the educational purpose envisioned, the document will be largely based on the use of examples.

In addition, the present document provides for other sources available for learners. In particular and in line with the approach taken under STF 515 (https://portal.etsi.org/STF/STFs/STFHomePages/STF515), a set of quizzes will allow the learner to verify the knowledge gained. Similarly, a set of slides will allow the learner to easily gain access to the contents of the present document. Both the quizzes and the slides are integrated in annex B of the present document.

1 Scope

1.1 Context for the present document

The design, development and deployment of - potentially large - IoT systems require to address a number of topics - such as privacy, interoperability or privacy - that are related and should be treated in a concerted manner. In this context, several Technical Reports have been developed that each address a specific facet of IoT systems.

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

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.14]

ETSI TR 103 534-1 [i.7]

ETSI TR 103 534-2 (the present document)

ETSI TR 103 535 [i.15]

ETSI TR 103 536 [i.16]

ETSI TR 103 537 [i.17]

ETSI TR 103 591 [i.1]

1.2 Scope of the present document

The focus of the present document is to present a summary of the teaching material to help in acquiring knowledge on IoT Privacy. The teaching slides are in annex B of the present document. The present document is to support the IoT Technical Report (TR) and it will re-enforce the knowledge in the TR such that reader can acquire basic knowledge to apply IoT privacy in their area of engagement or at least know where to obtain that information. The present document does not address IoT security, although closely linked but this is being addressed in a separate report which is ETSI TR 103 534-1 [i.7].

Learning Objective: Considering that the overarching objective of this teaching material is to provide learners with the necessary information, so as to gain basic knowledge on how the concept of privacy applies in the IoT environment. Allowing them to make decisions and act accordingly.

This teaching material is addressed to learners holding different functions in the supply chain. To this end, it provides for actors such as device manufacturers, software developers, and users benefiting from the delivery of service through the IoT supply chain.

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 103 591 (V1.1.1): "SmartM2M; Privacy study report; Standards Landscape and best practices".

[i.2] European Data Protection Supervisor: "Glossary".

NOTE: Available at https://edps.europa.eu/data-protection/data-protection/glossary_en.

[i.3] Cloud Service Level Agreement Standardisation Guidelines.

NOTE: Available at https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines.

[i.4] 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.5] 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.6] ETSI TS 103 485: "CYBER; Mechanisms for privacy assurance and verification".

[i.7] ETSI TR 103 534-1 (V1.1.1): "SmartM2M; Teaching Material; Part 1: Security".

[i.8] Protecting Privacy and Data in the Internet of Things: "Considerations and techniques for big data, machine learning and analytics February 2019 GSMA".

NOTE: Available at www.gsma.com.

[i.9] European Data Protection Supervisor: "Preliminary Opinion on privacy by design", 31 May 2018.

[i.10] Noto La Diega Guido and Walden Ian: "Contracting for the 'Internet of Things': Looking into the Nest" (February 1, 2016). Queen Mary School of Law Legal Studies Research Paper No. 219/2016.

[i.11] Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, adopted on 16 September 2014.

[i.12] ICO: "Privacy in Mobile Apps Guidance for app developers".

NOTE: Available at https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf.

[i.13] ETSI TR 103 376 (V1.1.1) (2016-10): "SmartM2M; IoT LSP use cases and standards gaps".

[i.14] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

[i.15] ETSI TR 103 535: "SmartM2M; Guidelines for using semantic interoperability in the industry".

[i.16] ETSI TR 103 536: "SmartM2M; Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms".

[i.17] ETSI TR 103 537: "SmartM2M; Plugtests™ preparation on Semantic Interoperability".

[i.18] Proposal for a Regulation of the European Parliament and of the Council on ENISA, theof the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation.

3 Definitions of terms, symbols and abbreviations

3.1 Terms

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

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.18]

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]:

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: bility 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 protection: The employment of technical, organisational and legal measures in order to achieve the goals of data security (confidentiality, integrity and availability), transparency, intervenability and portability, as well as compliance with the relevant legal framework.

NOTE: In the context of the present report, data protection refers to the protection of personal data. It is largely technically feasible that non-personal data become personal data.

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

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

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

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

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

The following terms are taken from [i.2]:

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. 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 have to purchase and install them in their computers) or be built into the architecture of information system.

3.2 Symbols

Void.

3.3 Abbreviations

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

AI	Artificial Intelligence
API	Application Programming Interface
CCTV	Closed Circuit TV
CIPM	Certified Information Privacy Manager
CIPP	Certified Information Privacy Professional
CIPP/E	Certified Information Privacy Professional/Europe
CIPT	Certified Information Privacy Technologist
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDPS	European Data Protection Supervisor
EEA	European Economic Area
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
HLA	High Level Architecture
IAPP	International Association of Privacy Professionals
IoT	Internet of Things
IT	Information Technology
MAC	Media Access Control
OTP	One Time Password
TR	Technical Report
TV	Television
WIFI	Wireless Networking

4 What is privacy?

4.1 Outline

This clause will introduce the learner to the concept of privacy, also, by using examples. It considers the related definitions from the EDPS glossary [i.2].

4.2 Privacy and data protection

Privacy is a concept used across different disciplines. From a legal standpoint its ability of an individual to be left alone, out of public view, and in control of information about oneself. As, also, illustrated under clause 3.1, 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 latter relates to what is known as personal data protection under EU law. In other terms, privacy is considered to be the underlying value of personal data protection. Note that for the purposes of the present document, privacy is conceived as personal data protection.

As further discussed under ETSI TR 103 591 [i.1] privacy is closely linked to security. Although, privacy and security are separate concepts in the sense, for example, that privacy can be perceived independently of security, yet, they are complementary, given that in reality security is an enabler of privacy. It can be stressed that security is a basic requirement for the effective protection of privacy.

4.3 The General Data Protection Regulation (GDPR)

4.3.1 Introduction

General Data Protection Regulation (GDPR) [i.4] provides exclusively for the protection of personal data in EU. The EU Institutions decided to repeal the Data Protection Directive [i.5] that provided for the protection of personal data at EU level as of 1995 by adopting a legislative instrument in the form of Regulation. The GDPR became applicable on the 25 May 2018 and it is directly applicable across all EU Member States.

The GDPR defines [i.4] the key concepts and the role of the main actors, as follows:

Personal Data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by 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.

Note that the GDPR provides separately for special categories of data, namely, genetic data, biometric data and data concerning health.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Subject: an 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.

Data Controller: Determines the purposes and means of the processing of personal data. The controller exercises control over the why and how of a data processing activity. Can be a person, Public authority, agency, organization, alone or jointly.

Data Protection Officer (DPO): A person who is formally tasked with ensuring that the organization is aware of and complies with its data protection responsibilities and obligations according to GDPR. The DPO, someone of expert knowledge on data protection law and practices. According to the GDPR, the DPO has an independent position and is not, therefore, assigned with tasks and duties that result in a conflict of interest.

Data Processor: a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller; Processor has to comply with instructions of the controller, Processors will now need to:

- Keep records of processing.
- Interact and assist supervisory authorities in the performance of their tasks.
- Implement appropriate technical and organizational measures ensure data security (now a legal obligation and will be exposed to fines for non-compliance).
- Notify any data breach to the controller without undue delay.
- Appoint a DPO where undertaking the following on a large scale: processing sensitive personal data or undertaking systematic monitoring of data subjects.

Third Party: natural or legal person, public authority, agency or body acting who are authorized to process personal data under the direct authority of the controller or processor.

Supervisory Authorities: they are independent public authorities their main responsibility is to monitor the application of GDPR with the aim to protect the fundamental rights and freedom of natural persons in relation to processing of data linking to them. Public authorities also promote public awareness and facilitate organizations' compliance by issuing guidance on actual implementation of the regulatory framework.

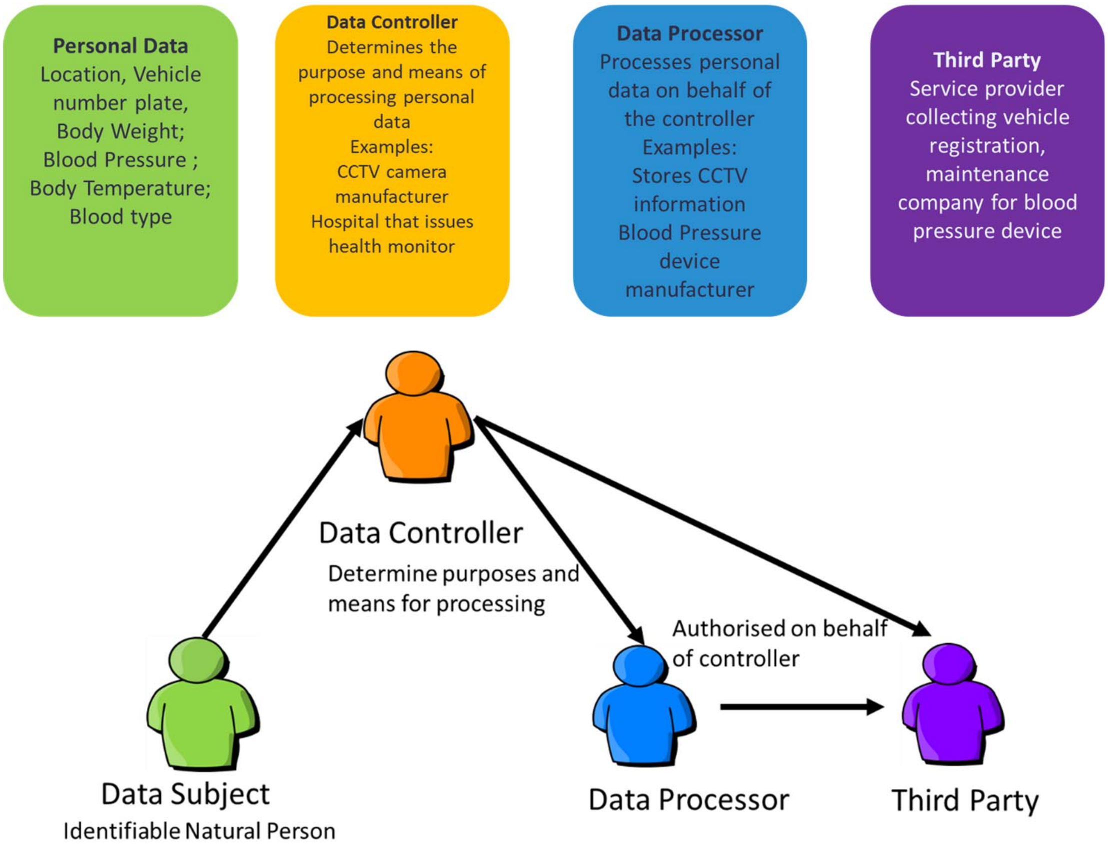
Personal Data
Location, Vehicle number plate, Body Weight; Blood Pressure ; Body Temperature; Blood type
Data Controller
Determines the purpose and means of processing personal data
Examples:
CCTV camera manufacturer
Hospital that issues health monitor
Data Processor
Processes personal data on behalf of the controller
Examples:
Stores CCTV information
Blood Pressure device manufacturer
Third Party
Service provider collecting vehicle registration, maintenance company for blood pressure device
Data Controller
Determine purposes and means for processing
Authorised on behalf of controller
Data Subject
Identifiable Natural Person
Data Processor
Third Party

Figure 4.3.1.1: Describes relations between roles

4.3.2 Data Protection Principles

There are six principles that define the condition under which data should be processed they define the ("HOW" and "WHY") underlying the processing of personal data under EU law.

Breaking any of these principles renders the processing unlawful.

These principles are as follows:

- **Lawfulness, Fairness and transparency:** Personal data should be processed lawfully, fairly ad in transparent manner in relation to the subject.
- **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.
- **Data minimization:** Personal data should be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.
- **Accuracy:** Personal data should be accurate, kept up to date if not they should be rectified.
- **Storage Limitation:** Personal data should be kept in a form that permits identification of data subjects for no longer than its necessary for the purpose for which the personal data is processed.
- **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.

4.3.3 Reasons to Process Data

There are also six reasons on the basis of which processing of personal data is allowed. These reasons mostly capture the "WHY" of processing. These six reasons are:

- **Consent:** The data subject has given clear consent for one or more specific purpose. Notably, under the GDPR, organizations acting as data controllers have to, also, provide for data subject's withdrawal of consent.
- **Contract:** Processing is necessary for the performance of contract to which the data subject is party to or to take steps prior to entering the contract.
- **Compliance:** Processing is necessary for compliance or legal obligation.
- **Vital interest:** Processing is necessary to protect vital interest of data subject or another natural person e.g. to save a life.
- **Public Interest:** Processing is necessary to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law, e.g. Private water companies are likely to be able to rely on the public task basis.
- **Legitimate Interest:** The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests as well as wider societal benefits. The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list.

4.3.4 Rights of Individual

The GDPR provides the following rights for individuals:

- **The right to be informed:** Be transparent about use of data collected, aim of collection and retention period. If collected from a 3rd party make this known within the month.
- **The right of access:** Individual have a right to have access to data either asking verbally or in writing and this should be provided free of charge within a month.
- **The right to rectification:** Individual can request data to be corrected or complete if incomplete either verbally or in writing and this has to be within a month.
- **The right to erasure:** Individual has the rights to have their data erased this is known as right to be forgotten.
- **The right to restrict processing:** Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.
- **The right to data portability:** Individuals has the right to ask their data to be copy or transfer easily from one IT environment to another in a safe and secure way, without affecting its usability.
- **The right to object:** Individuals has an absolute right to stop their data being used for direct marketing.
- **Rights in relation to automated decision making and profiling:** Dealt with in another article as not permitted however if this is used then the following should be provided; give individuals information about the processing; introduce simple ways for them to request human intervention or challenge a decision; carry out regular checks to make sure that your systems are working as intended.

4.4 The novelties of the GDPR

4.4.1 Overview

The GDPR introduces a series of novelties that create an impact on how organizations and, therefore, professionals acting on their behalf, are required to process personal data. Taking into account the target audience of the present document, the discussion below maps certain new requirements to actors holding diverse roles in the supply chain. The discussion that follows is particularly relevant, but not exclusively relevant for the actors mentioned below.

Data protection by design: Data protection by design is introduced under the GDPR. It implies that data protection is considered throughout the design process and it's not something that is considered only later, at the moment when service is launched. Data protection by design aims at building data protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with data protection. Data protection by design is particularly relevant for organizations and professionals involved in the design process of products and systems.

Data protection is best interwoven proactively and to achieve this, data protection principles should be introduced early on-during architecture planning, system design, and the development of operational procedures. Data protection by Design, where possible, should be rooted into actual code, with defaults aligning both data protection and business imperatives.

The GSMA document [i.8], describes a range of tools and techniques that practically support the concept of data protection by-design for big data, analytics and machine learning based services in the IoT. The document provides approaches to various topics which enhance data protection. Included in the document are case studies from a number of mobile operators, illustrating the adoption of such best-practice approaches.

Data protection by default: this is related to the importance of taking technical measures to meet the expectations of the individuals whose data are processed, not to have their data processed for other purposes than what the product and service is basically and strictly meant to do, leaving by default any further use turned off, for instance through configuration settings [i.9]. This is particularly relevant for organization -and professionals - involved, for example, in the development of interfaces.

Accountability: the GDPR requires organizations acting in their capacity as data controllers not only to be able to ensure they respected the six (6) data protection principles mentioned above, but also to be able to show that they did the right thing (accountability principle). This can be achieved through the implementation of both technical and organizational measures (e.g. maintenance of logs, practices of record keeping). Adherence to codes of conduct and certification are accountability tools encouraged by the GDPR, but they do not suffice to demonstrate compliance. Accountability is relevant for all actors in the IoT supply chain and, especially, for those organizations acting as data controllers, therefore, determining the purposes and the means of processing of personal data.

DPIA: The GDPR renders mandatory the performance of a DPIA under certain circumstances. The DPIA will, also, be discussed under clause 7.2 of the present document.

NOTE: ETSI TR 103 591 [i.1] expands on the necessity to perform a Data Protection Impact Assessment (DPIA).

4.4.2 Data Breach Notification

4.4.2.0 Introduction

The GDPR provides for the mandatory notification of a data breaches provided that certain requirements are met. The breaches need to be notified to the data protection authorities and, in certain cases, to the individuals/data subjects affected by the data breach.

According to the GDPR personal data breach is a breach of security leading to accidental or unlawful destruction. Loss, alteration, unauthorized disclosure, access to personal data transmitted stored or processed.

4.4.2.1 Who to Notify

Procedures to follow:

- Data protection authorities:
  - The GDPR introduces a duty on all organizations to report certain types of personal data breach to the relevant supervisory authority. This has to be done within 72 hours of becoming aware of the breach, where feasible.
- Data Protection Authorities and Affected Individuals:
  - If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the individuals involved should be informed without undue delay. Ensure there are robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not the relevant supervisory authority and the affected individuals are notified.
  - Note that it relevant, also, for end users of IoT devices given that in certain cases they are themselves the affected individuals so they will be directly notified.

Ensure there is a record of any personal data breaches, regardless of whether notification is required. More broadly, maintaining such a record would be in line with accountability principle mentioned above. In this context all breaches should be recorded regardless of whether or not they need to be reported to the Supervisory Authorities.

The notification of a data breach is relevant for all actors in the supply chain that they have to provide for it in accordance with their role.

4.4.2.2 What to Notify

According to article 33(5), when reporting a breach, the GDPR indicates that the following should be provided:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if the organization has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

5 Privacy in the Context of IoT

5.1 A holistic Approach of IoT Systems

5.1.1 Major characteristics of IoT systems

IoT systems are often seen as an extension to existing 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 is at the centre of attention of those who want to make them happen. This advocates for an "IoT-centric" 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, none of them can be ignored.

- **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 it is involving a variety of users in a variety of use cases.
- **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 without compromising the "IoT centric" approach.

5.1.2 The need for an "IoT-centric" view

5.1.2.1 Introduction

In support of an "IoT-centric" approach, some elements have been used in the present report 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.

5.1.2.2 Roles

A drawback of many current approaches to system development is a focus on the technical solutions, which may lead to suboptimal or even ineffective systems. In the case of IoT systems, a very large variety of potential stakeholders are involved, each coming with specific - and potentially conflicting - requirements and expectations. 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 discussed are:

- Device Manufacturers.
- Software Developers.
- End-users.

5.1.2.3 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.

5.1.2.4 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. The approach taken in the present report is to outline some solutions but also to provide guidelines on how they can be used depending on the target audience. Such guidelines are associated to the relevant roles and provide support for the decision-making.

5.2 Summary of Challenges of Privacy in IoT

IoT forms a clear example of hyper connectivity and distributed control, as such appropriate safeguards are needed to ensure that individuals' right to privacy is effectively protected. With respect to the IoT design, there are emerging challenges, for example, in identifying:

- the stakeholders for whom privacy is relevant;
- who is responsible for the personal data as how context is, especially, relevant of privacy (e.g. in smart living, smart home), for instance for software developers, when implementing data protection by default;
- how stakeholders need to think of privacy proactively as part of design not an afterthought.

5.3 Illustrating data processing within the IoT ecosystem

On the basis of the earlier provided explanation under clause 4, this clause will produce an overview of the relationships and the process of data processing within the IoT environment through the lenses of the GDPR.

Figure 5.3.1 taken from ETSI TS 103 485 [i.6] aims to give an overview of personal data processing, as described under clause 4. Nevertheless, the view given is somewhat over-simplistic when it comes to mapping the GDPR principles in an IoT environment, as it implies an atomic relationship of data subject and data controller, i.e. the consent to a single data controller is sufficient to address all possible uses of data within the accessed service. On the contrary, IoT deployment is about the service that is offered, it entails access to many sub-services that may not be directly associated to the purpose specified by the data controller and to which the data subject had originally consented to. Furthermore, it may not be clear to the data controller how the system has been developed that allows the data controller to give assurance to the data subject and provide evidence to the authorities that the consented purpose is followed.

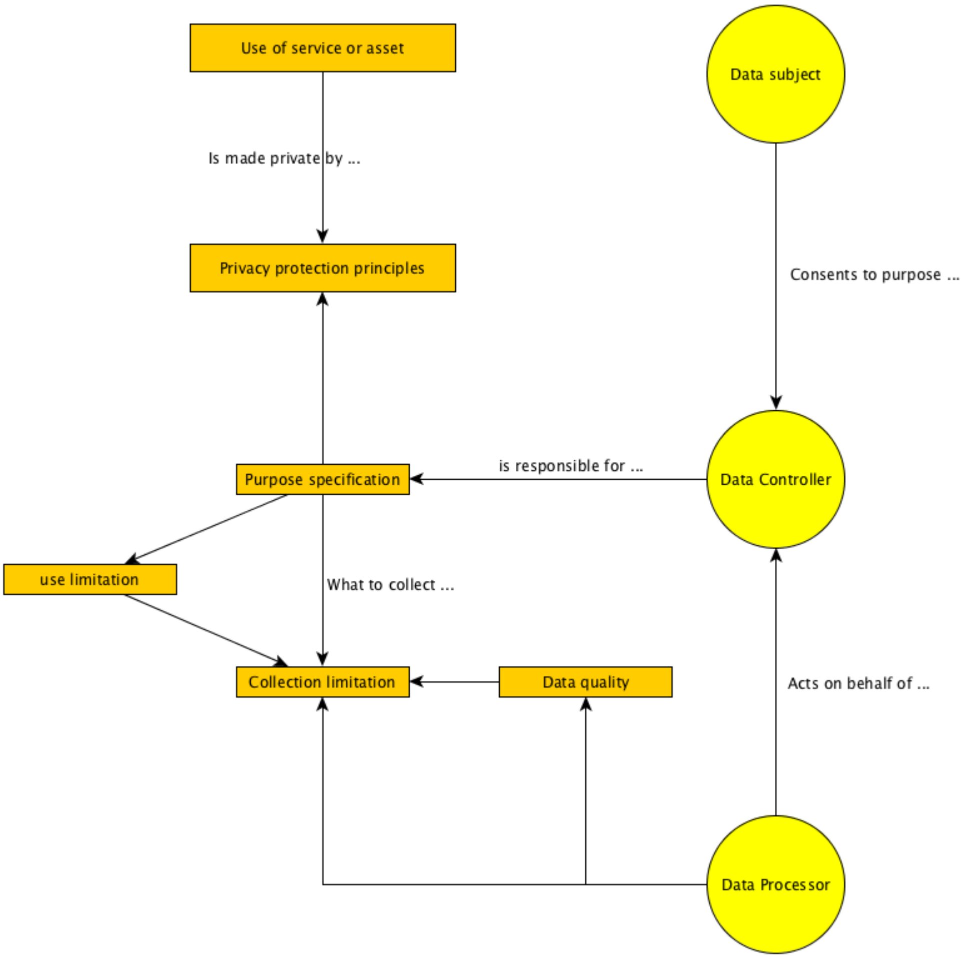

Figure 5.3.1: GDPR actors mapped to core privacy protection principles

6 Use case example of IoT Privacy

6.1 Introduction

This clause will exemplify privacy in IoT by emphasizing the role of context on the basis of examples. To this end, the clause will use as examples the use cases discussed under ETSI TR 103 591 [i.1]. Note that the use case description has been adjusted to further accommodate the objectives of the present document, therefore, discussing selected aspects in an understandable language for a non-expert audience. The teaching slides attached in appendix will explain in detail how the roles introduced in clause 4 can be assigned.

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

6.2.1 Overview

The 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 slightly modified in order to better cater to the objectives of the present document.

6.2.2 Background

One of the main 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 areas to cities and the reluctance of elderly people to move from their homes to geriatric centres 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.

6.2.3 Description

Angela is 83 and she lives alone in her apartment in La Coruña. She does not have serious medical condition, but is required to take some medication. In addition to having high blood pressure she has also 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, meet friends or neighbours, Alba can check her mother's blood pressure thereby feeling more confident about her health. Angela can also use the tracker to send a notification to the Spanish Red Cross in case she requires urgent medical assistance.

6.2.4 Data Protection Issues

The CCTV camera and the blood pressure tracker will be monitoring and maintaining a record Angela's location, blood pressure, body temperature and other forms of health data which will be accessible to the camera manufacturer, blood pressure device manufacturer, Spanish Red Cross and the like. That said, there can be concerns such as how these data, that fall special categories of personal as explained under clause 4.3. will be stored and used by the respective parties, for how long and whether sufficient safeguards have been implemented to protect the data from being accessed by an unauthorized party.

6.3 Use Case 2: Smart home solutions

6.3.1 Background

In today's crowded and busy world people are seeking comfort and security in their own home. 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.

6.3.2 Description

Movie night scenario: Erik is at home in the evening ready to see a movie in the living room. He sits 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 warmer 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 takes his mobile phone, starts the smart home app and looks at the video streams coming from the video cameras installed outside home. To be sure, he also checks the contact sensors installed on the windows to see if any of them is open. Being reassured that everything is OK, he goes 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. Every room has its own temperature sensor and there is a temperature sensor installed outside. The preferred room temperatures, the priority of the rooms and the consumption limits are set by Olaf through intelligent home mobile app. 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.

6.3.3 Data Protection Issues

While the concept of smart homes may seem intriguing, such homes require several sensors and actuators to be installed that allow it to be aware of the home parameters and events in every moment and take appropriate actions when needed. However, such new technologies entail high risks of profiling as they allow the capturing of individuals' behaviour on daily basis in their private space.

6.4 Use Case 3: Logistics and workplace

6.4.1 Background

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. The type and quantity 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.

6.4.2 Description

Peter an employee at Sky Shipping & Logistics Company Ltd where he coordinates the incoming and outgoing shipments, ensures that the traffic is managed in an effective 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 equipment allowed the respective managers to keep track of the time and duration for which the warehouse was accessed by their delivery representatives. Additionally, 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.

6.4.3 Data Protection Issues

Given that the smart watch can track and store different types of data with respect to Peter including his location, email address, heart rate and body temperature, it is essential that Sky shipping and Glitterati and Co ensure that effective measures are put in place to ensure that only the relevant personnel have access to such data and that such data is tracked during office hours when it is only necessary for the performance of an assignment and not for other purposes Note that Use Case 3, also, surfaced the role of the context regarding the applicable privacy laws.

7 How to assess risks in the IoT ecosystem?

7.1 Overview of risks linked to data protection

The processing and protecting of personal data in the context of IoT and IoT ecosystems entail risks and potential detrimental impact and other material negative consequences for the individual to whom the data relates to.

The GDPR is a dynamic, risk-based regulation requiring organizations to continuously take and monitor appropriate levels of technical measures and organizational measures on the basis of the risks identified taking into account various parameters such as for instance the specific type and classification of personal data to be processed and the scale, purpose and context, as well as the proportionality of processing itself.

As the GDPR is a framework regulation, within such boundaries the various relationships in IoT ecosystems can be finetuned and arranged on a contractual level, such as between chipset, component and device manufactures, respectively software developers, system integrators and service providers.

The risks pertaining to personal data protection relate to each individual separately, and are contextual. Since the harm proliferates within the hyper-connected IoT ecosystems, the risks incurred are not also relevant for users, but also quite relevant for society. For the purpose of the present document and for sake of convenience, privacy risks relating to the relevant stakeholders in IoT ecosystems are being approached with the help of the following subcategories, that are further illustrated in the figure 7.1.1:

a) Upstream: Parties that are directly involved in the creation of chipsets and other components to incorporate in IoT half products and devices, systems and services further downstream.

b) Midstream: Parties that combined or otherwise integrate those components into IoT devices and other technical layers necessary, or that build and offer IoT system and services downstream.

c) Downstream: The IoT customers and the end-users of the IoT devices, system and services.

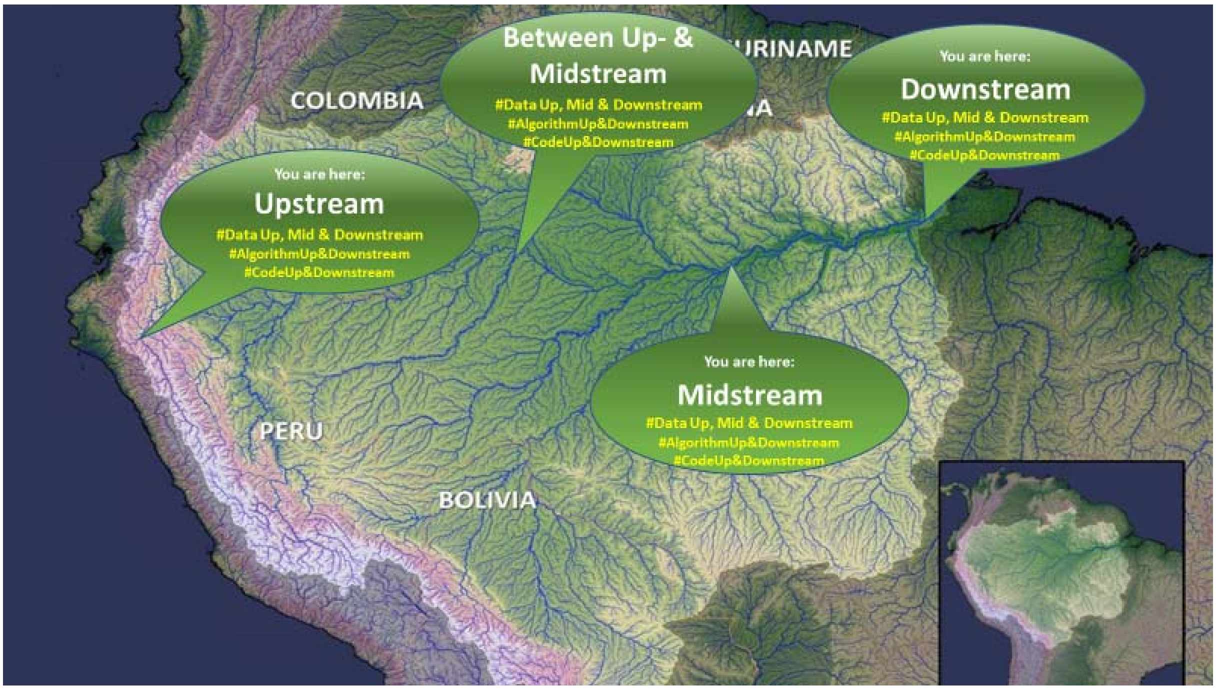

Figure 7.1.1

Parties at the upstream level i.e. the IoT component or device manufacturers play a fundamental role as far as personal data protection is concerned and their actions or inactions can expose IoT users to significant risks. To stay ahead of competitors, for instance for aiming at first mover advantage and while also providing an attractive price, there can be instances where component or device manufacturers may not make the necessary investments in implementing the appropriate level of security measures for an IoT device.

Failure to do so, however, can jeopardize the security and safety of personal data as they tend to opt for affordable prices while not realizing that the such products, systems and services can be easily hacked by third parties. Furthermore, various component or device manufacturers generally operate under the assumption that they would not be held accountable for breaches that may result due to the lack of care of third parties that may be helping it in creating the IoT device, system or service. Contrary to what they may believe, the GDPR can make such device manufacturers financially liable for failure to ensure the implementation of the required safeguards by such third parties. They would also run the risk of losing their goodwill in the market and the confidence of customers. The GDPR constitutes mandatory law, hence any contractual arrangement conflicting with the GDPR will be void.

The risks at the midstream level relating to the role of stakeholders such as OEMs, system integrators, infrastructure, platform and service providers are to an extent similar to those relating to the component or device manufacturers. With the IoT, the internet is everywhere, in every nook and cranny of private spaces which could potentially mean the generation of more data [i.10]. Such data may not only be processed by the component or device manufacturer but may be factually shared with its relevant third parties although there may be no valid legal ground for such data access or data sharing, and if they may be the use may be disproportionate for the purpose in the specific context.

It is for this reason that the GDPR also makes such parties, as either co-controller, processor or co-processor liable. These stakeholders in the midstream of an IoT ecosystem will be most probably be found in breach of contract that it would have with both their upstream respectively downstream partners.

From the perspective of IoT customers and the end-users of the IoT devices, system and services, data losses, unauthorized access to personal data, compromised or other false data, unlawful surveillance, profiling, and the like are some of the risks that they may be exposed to. More specifically, lack of control, transparency and information asymmetry are other major issues that IoT customer and users are faced with, in the sense that there is great imbalance of powers between large organizations accessing data (e.g. service providers) and end-users.

For example, the use of IoT home devices is associated to the use of several interconnected devices, possibly with some devices that are designed to operate in the background without individual end users being aware of their presence. In such a situation, individuals may be duly informed that the information relating to them is being collected, stored and used by such devices. An additional risk that relates to the use of IoT devices is that data that is being collected may continue to be used for other purposes, possibly, unrelated to the specific purpose an individual has consented when accepting the terms of a service.

Although certain risks may be more relevant for certain stakeholders, it is important to stress that risks and potential harm incurred cannot be strictly limited, they proliferate in the cloud environment and, therefore, they are simultaneously relevant for several actors.

7.2 Data Protection Impact Assessment

Data Protection Impact Assessment -is a tool to help identify, assess and mitigate the data protection risks of new projects. They are part of your accountability obligations under the GDPR, and an integral part of the 'data protection by default and by design' approach.

DPIA can address a single processing operation or a set of similar processing operations.

DPIA should be carried out prior to the processing, as early as practical in the design of the processing operation.

The five key stages of DPIA can be summarized as follows:

- Identify the need for DPIA (e.g. processing special categories of data).
- Describe the information Flow.
- Identify data protection related risks.
- Identify and evaluate privacy solutions.
- Sign-off and record the outcome.

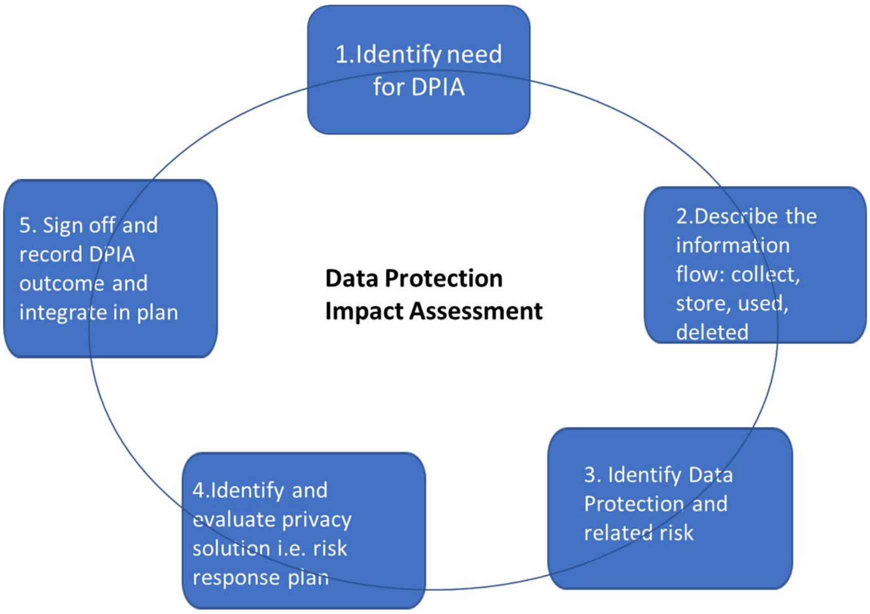
1.Identify need for DPIA
2.Describe the information flow: collect, store, used, deleted
3. Identify Data Protection and related risk
4.Identify and evaluate privacy solution i.e. risk response plan
5. Sign off and record DPIA outcome and integrate in plan
Data Protection Impact Assessment

Figure 7.2.1: Data Protection Impact Assessment Process

Note that a DPIA should reviewed at least when there is a change of the risk represented by processing operations.

8 How to mitigate risks in an IoT ecosystem?

8.1 Introduction

Taking into account the wide range of stakeholders with a role in the IoT ecosystem and how raising awareness can play a role in mitigating the risks pertaining to the protection of personal data, this clause will produce a set of recommendations addressed to actors representing roles held upstream, mid-stream or downstream of the supply chain of services pertaining to the IoT context. The recommendations below are primarily, but not exclusively relevant for the specific examples of stakeholders mentioned in the following clauses.

8.2 How to mitigate risks upstream?

Example: device manufacturers

Device manufacturers in the IoT do more than only sell physical items to their clients or white label products to other organizations. They may also have developed or modified the "thing's" operating system or installed software determining its overall functionality, including data and frequency of collection, when and to whom data be transmitted for which purposes (for instance, companies could price the insurance of their employees based on the data reported by the trackers they make them wear). Most of them actually collect and process personal data which is generated by the device, for purposes and means which they have wholly determined. They thus qualify as data controllers under EU law according to article 29 [i.11]. This effectively means if device manufacturers have built in sensors that collect data from devices for transmit for other purposes such as to track employee's usage in order to help determine what sites visited or to sell data to insurance companies, basically if the device collects and process personal data generated, this needs to be made clear to the users who are the data subjects.

In light of the GDPR, the following set of recommendations is relevant for actors holding a role upstream, such as device manufacturers [i.11] and [i.12]:

- **Data protection by design:** Privacy of users need be embedded into the design of business processes, technologies, end-to-end ecosystems, operations and information architectures. Each service or business process designed to use - or to may later on use - personal data need to take all the necessary security requirements into consideration at the initial stages of their developments.

- **Data Protection by default:** The strictest privacy settings and mechanisms automatically apply once a user acquires a new product or service; no manual change to the privacy settings should be required on the part of the user. The user 'own' or at least controls its own data, by law.

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

- **Non-discriminatory practices:** The vendor, supplier or other provider should ensure non-discriminatory practices against users and businesses on the basis of information derived from digital ecosystems and deployments.

- **Accountability:** Any vendor, supplier or other provider should have the appropriate levels of being accountable for regulatory, contractual and ethical compliance, both upstream, midstream and downstream in the ecosystem.

- Device manufacturers need to inform users about the type of data that are collected by sensors and further processed, the types of data that they receive and how it will be processed and combined.

- Device manufacturers should be able to communicate to all other stakeholders involved as soon as a data subject withdraws his consent or opposes the data processing.

- Device manufacturers need to provide granular choices when granting access to applications. The granularity should not only concern the category of collected data, but also the time and frequency at which data are captured. Similarly, to the "do not disturb" feature on smartphones, IOT devices should offer a "do not collect" option to schedule or quickly disable sensors.

- To prevent location tracking, device manufacturers should limit device fingerprinting by disabling wireless interfaces when they are not used or should use random identifiers (such as random MAC addresses to scan WIFI networks) to prevent a persistent identifier from being used for location tracking.

- To enforce transparency and user control, device manufacturers should provide tools to locally read, edit and modify the data before they are transferred to any data controller. Furthermore, personal data processed by a device should be stored in a format allowing data portability.

- Users are entitled to a right of access to their personal data. They should be provided with tools enabling them to easily export their data in a structured and commonly-used format. Therefore, device manufacturers should provide a user-friendly interface for users who want to obtain both aggregated data and/or raw data that they still store.

- Device manufacturers should provide simple tools to notify users and to update devices when security vulnerabilities are discovered. When a device becomes deprecated and is no longer updated, the device manufacturer should notify the user and make sure that he is aware that the device will no longer be updated. All the stakeholders that are likely to be impacted by the vulnerability should also be informed.

- Device manufacturers should follow a Security by Design process and dedicate some components to the key cryptography primitives.

- Device manufacturers should limit as much as possible the amount of data leaving devices by transforming raw data into aggregated data directly on the device. Aggregated data should be in a standardized format.

8.3 How to mitigate risks mid-stream?

Example: professionals designing IoT products as 3rd Party

In the world of IoT with connected devices where data from one device can be shared with other devices depending on the platforms, the owner of the platforms is responsible for maintaining the privacy of the data as this data is pushed by the user (data subject) onto them. The social platform owner now becomes the data controller and is subject to GDPR.

In light of the GDPR, the following set of recommendations is, especially, relevant for actors holding a role midstream, such as professionals designing IoT products as 3rd party and Platform [i.11] and [i.8]:

- Default settings of social applications based on IoT devices should ask users to review, edit and decide on information generated by their device before publication on social platforms.

- Default settings of IoT devices should allow end users to withdraw the originally given consent for the processing of their personal data.

- Information published by IoT devices on social platforms should, by default, not become public or be indexed by search engines.

In addition, for professionals using IoT products e.g. a 3rd party application developers an API is needed for the developer to access software needed or development. Some of this Applications may be installed on an "opt-in" or "opt-out" basis which is subject to user's prior consent. These authorization request made by third-party application developers needs to display sufficient information for users consent to be considered as specific and sufficiently informed, figure 8.3.1 shows an example of an App developer registering on an API to access a 3rd Party application, the API owner is acting as the Data controller here.

Recommendation:

- Notices or warnings should be designed to frequently remind users that sensors are collecting data. When the application developer does not have a direct access to the device, the app should periodically send a notification to the user to let him know that it is still recording data.

- Applications should facilitate the exercise of data subject rights of access, modification and deletion of personal information collected by IoT devices.

- Application developers should provide tools so that data-subjects can export both raw and/or aggregated data in a standard and usable format.

- Developers should pay special attention to the types of data being processed and to the possibility of inferring sensitive personal data from them.

- Application developers should apply a data minimization principle. When the purpose can be achieved using aggregated data, developers should not access the raw data. More generally, developers should follow a Privacy by Design approach and minimize the amount of collected data to that required to provide the service.

- **Continuous Updates:** From the inception of an IoT device, it should be continuously updated in order to reduce vulnerabilities. The life cycle of AI, and not just the creation AI, and the related device and systems needs to be dealt with, including for instance how it should maintain checks and balances to prevent known or currently unknown vulnerabilities from being exploited.

- Encryption can and should be used as an effective tool for ensuring the security of data. It has been used in the past for various technologies, it should remain a part of the design of IoT technologies, applications so that in the event of a hack, information is not easily available to unauthorized parties.

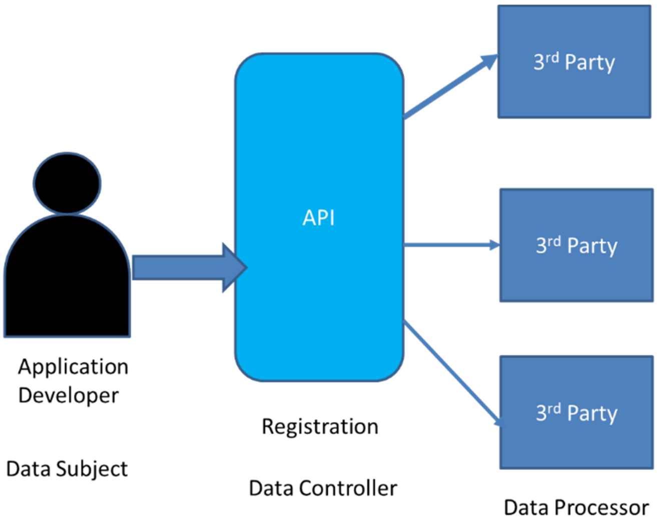

Figure 8.3.1: Example of an Application Developer role in GDPR

Example: IoT Platforms Manufacturers

IoT manufacturers are design standards platform interfaces with an aim to host the data collected through different devices in order to centralize and simplify their management. Examples are the HLA platform and oneM2M platform. Such platforms may qualify as data controllers in the fact that they collect user's personal data for their own purposes.

Recommendation:

- Consent to use connected device and the resulting data processing should be informed and freely given.
- Data subjects have to be provided with the option to withdraw their consent.
- Data subject whose data is being processed in the context of a contractual relationship with the user of a connected device should be in a position to administrate the device.

8.4 How to mitigate risks downstream?

Example: Individuals as Data Subjects: Subscribers, Users, Non-Users

GDPR applies to data relating to individuals. So, within IoT if data collected are machine data e.g. temperature in a factory or sensor data from a sensor in a vegetable farm and they are not linked directly or indirectly to individuals, then they are not subject to GDPR. Also, if personal data are collected or otherwise processed, but are used exclusively for personal or domestic purposes they will fall under the "house hold exemption". In IoT however this will be limited [i.11], as IoT by nature considers user's data that are systematically transferred to device manufacturer, application developers and other 3rd parties who qualify as data controllers.

Recommendation:

- Consent to the use of a connected device and to the resulting data processing should be informed and freely given. Users should not be economically penalized or have degraded access to the capabilities of their devices if they decide to use the device or a specific service.
- The data subject whose data is being processed in the context of a contractual relationship with the user of a connected device (i.e. hotel, health-insurance or a car renter) should be in a position to administrate the device. Irrespective of the existence of any contractual relationship, any non-user data subject should be in a capacity to exercise his/her rights, as well as to withdraw the consent that allowed for the processing of the personal data in the first place.
- Users of IoT devices should inform non-user data subjects whose data are collected of the presence of IoT devices and the type of collected data. They should also respect other data subject's preference not to have their data collected by the device.

9 Concluding Remarks

The present document and the teaching slides (in annex B) provide a quick guide to understanding GDPR in the context of IoT, the material offers a good background in privacy and how the concept of privacy applies in IoT environment. There is also opportunity to test one's knowledge of the material which is a means of embedding the information enclosed.

Finally, taking into account the challenges raised by hyper-connectivity and the main requirements framed under the GDPR regarding personal data processing, the present document contains a set of recommendations for the IoT stakeholders that have been identified. To this end and in line with the approach taken for the creation of concise privacy teaching materials appropriate to serve the learning goal set, meaning, offering learners with the basic knowledge on how the concept of privacy applies in the IoT ecosystems. The present document illustrates tangibly how fundamental concepts and responsibilities provided under EU Law apply in the IoT ecosystems [i.1].

Furthermore, acknowledging the support IoT stakeholder's need, in order to make well-educated decisions regarding personal data processing, the present teaching materials put particular emphasis on the role of data protection risks that occur upstream, midstream and downstream of the supply chain and how IoT stakeholders holding a role in the respective parts of the supply chain can mitigate them.

With respect to data protection risks and besides the specific recommendations captured in the present document, it is of key importance to highlight that:

- The understanding context matters for professionals to effectively protect personal information in practice.
- Risks in the IoT ecosystems concerning personal data protection could be merely mitigated, but not eliminated.
- Risks can be perceived on an individual basis but also at a societal level.
- Although data protection risks do not pertain solely to specific IoT stakeholders, the degree of relevance, though, may vary.
- Similarly, the recommendations produced are primarily relevant for certain professionals identified, but they remain relevant -to a lesser- extent for the other actors as well.

Note that the concluding remarks concerning privacy in IoT captured under [i.1] remain, of course, relevant, also, for the target audience of the present document.

Annex A: Guide to Certification in Privacy

A.0 Introduction

Aiming to increase organizations' accountability in relation to the processing of personal data of individuals, there may be need for training hence this clause describes potential certification area available today in the area of Privacy.

The International Association of Privacy Professionals (IAPP) is a non-profit, non-advocacy membership association founded in 2000. It provides a forum for privacy professionals to share best practices, track trends, advance privacy management issues, standardize the designations for privacy professionals and provide education and guidance on opportunities in the field of information privacy. The IAPP is responsible for developing and launching the only globally recognized credentialing programs in information privacy:

- The Certified Information Privacy Professional (CIPP).
- The Certified Information Privacy Manager (CIPM).
- The Certified Information Privacy Technologist (CIPT).

The CIPP, CIPM and CIPT are the leading privacy certifications for thousands of professionals around the world who serve the data protection, information auditing, information security, legal compliance and/or risk management needs of their organizations (https://iapp.org).

A.1 Certified Information Privacy Professional (CIPP)

The CIPP is for IT and other professionals whose responsibility involves data privacy and protection along with legal and compliance matters, plus information management, data governance, and human resources.

However, privacy is as much a matter of understanding governing laws and regulations as it is a matter of information technology-particularly data security and protection. As a result, the CIPP comes in a variety of "regional" versions: Asia, Canada, Europe, U.S. government, and U.S. private sector. Right now, the CIPP/E offers the most focused and intense coverage of GDPR. This credential targets those involved in governance and privacy program operation.

A.2 Certified Information Privacy Manager (CIPM)

The CIPM targets people responsible for managing information privacy programs. It stresses both knowledge of privacy law and regulations and how to translate that knowledge into workable practices, policies, and procedures for organizations to adopt and employ day to day. The curriculum covers topics that include creating a company (or organizational) vision for privacy and data protection, building and structuring a privacy team, developing and implementing a privacy program framework, communicating with stakeholders, measuring performance, and understanding the operational lifecycle for privacy programs.

A.3 Certified Information Privacy Technologist (CIPT)

The CIPT is for the people who implement the technical controls and components that go into a privacy program. This credential is the most likely starting point for IT professionals interested in working with data privacy and protection. It would be best coupled with the CIPP/E for those interested in coming fully up to speed on GDPR.

The CIPT seeks to ensure data privacy at stages of IT product and service lifecycles, including design, development, deployment, maintenance, and retirement/replacement. Candidates are expected to understand privacy concepts and practices as they affect IT operations, consumer expectations for privacy, and concomitant responsibilities. They should also know how to design privacy into early-stage IT product and service development; establish privacy practices for data collection and transfer; manage privacy for the Internet of Things (IoT); factor privacy into data classification and emerging technologies including cloud computing, biometrics, and surveillance; and finally, communicate privacy issues to an organization's management, development, marketing, legal, and operations functions.

Annex B:
IoT Privacy Teaching Slides

The full set of IoT Privacy Teaching Slides is publicly available in the form of a set of PowerPoint slides provided in archive tr_10353402v010101p0.zip as an electronic addition to the present document.

Annex C: Change History

Date	Version	Information about changes
16-06-2018	0.1.0	Initial input by Arthur's Legal
6-7 2018	0.2.0	Input by EX2 Management
11-07-2018	0.3.0	Revisions by Arthur's Legal
25-07-2018	0.4.0	Ex2 Management
20-07-2018	0.5.0	Revisions by Netellany
21-07-2018	0.6.0	Input based from the notes of the Face to Face Meeting
28-09-2018	0.6.1	Editorial change, addition of new clause 4 as general TR introduction and update on common text
31-05-2019	0.8.0	Conclusion and preparation for SmartM2M
04-07-2019	0.9a9.0	Revision following SmartM2M meeting
29-07-2019	0.9b9.0	Revision of final draft after SmartM2M plenary meeting and deep review conducted by ETSI Technical Officer
05-08-2019	0.9.0	Review of ETSI Technical Officer before submission for publication (before TB Approval)
08-10-2019	0.9.0	Last review by ETSI Techncial Officer before Publication (after TB Approval)

History

Document history		
V1.1.1	October 2019	Publication