ETSI TR 103 370 V1.1.1 (2019-01)

Practical introductory guide
to Technical Standards for Privacy

Reference
DTR/CYBER-0010

Keywords
confidentiality, privacy

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights 4
Foreword 4
Modal verbs terminology 4
Executive summary 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definition of terms, symbols and abbreviations 7
3.1 Terms 7
3.2 Symbols 7
3.3 Abbreviations 7
4 Glossary of terms 7
4.1 Collation of terms 7
4.2 Taxonomy of terms 14
5 Standards and guidelines to management of privacy 16
5.1 Privacy Impact Assessment 16
5.2 Guidelines and best practices 17
5.3 Impact assessment and analysis 17
5.4 Codes of practice 17
5.5 Cryptographic mechanisms 17
5.6 Management system including privacy protection 18
6 General principles 18
6.1 Caveats and warnings 18
6.2 EU regulatory and legal context 19
6.3 Privacy management principles 19
7 Application of principles to example use cases 22
7.1 Least to know/collect 22
7.2 Data/privacy protection and data brokering 22
7.3 The Right to be forgotten 24
8 Gaps in standardization 24
Annex A: Bibliography 26
History 27

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 Cyber Security (CYBER).

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.

Executive summary

The present document has been prepared in response to Mandate M/530 [i.9] and presents a guide to the application of standards in the implementation of privacy management. The present document has been structured in four parts to achieve the goals of the Mandate:

Part 1: Privacy terms and definitions based on existing documents.

Part 2: Status of standardization work considering existing or future work in ISO, CEN/CENELEC, ETSI and other bodies - identification of the basic building blocks.

Part 3: General principles how to introduce privacy management in equipment, services and solutions.

Part 4: Application of the principles for privacy by design to some examples:

- Least to know/collect.
- Data/privacy protection and data brokering (especially considering aggregated data, here in many legal systems it is the case that applying advanced algorithms on open data may result in private data).
- The right to be forgotten.

In addition, the present document identifies gaps in standardization and makes a number of recommendations for addressing those gaps.

1 Scope

The present document gives a guide to the use of standards to assist in the management of privacy. The present document contains the following key elements:

- Table 1 contains a collation of terms related to data protection and privacy from selected SDOs and comparison to the GDPR [i.1].
- Privacy terms and definitions based on existing documents (ISO, ENISA, and others).
- Status of standardization work including consideration of existing or future work in ISO, CEN/CENELEC, ETSI and other bodies.
- Identification of the basic building blocks and main principles for privacy protection and their mapping to available standards.
- Fundamental privacy by design principles that are commonly recognized.
- Examples of application of the privacy by design principles.

In addition, the present document identifies gaps in standardization and makes several recommendations for addressing those gaps.

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] 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).

[i.2] European Convention of Human Rights.

NOTE: Available at www.echr.coe.int.

[i.3] Universal Declaration of Human Rights.

NOTE: Available at http://www.un.org/en/universal-declaration-human-rights/.

[i.4] ETSI TS 103 486: "CYBER; Identity management and naming schema protection mechanisms".

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

[i.6] ETSI TR 187 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity imanagement and their resolution in the NGN".

[i.7] ISO/IEC 29100:2011 amended by ISO/IEC 29100:2011/Amd 1:2018: "Information technology -- Security techniques -- Privacy framework".

[i.8] ISO/IEC 29191:2012: "Information technology -- Security techniques -- Requirements for partially anonymous, partially unlinkable authentication".

[i.9] M/530 Commission Implementing Decision C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy.

[i.10] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

[i.11] ETSI TS 103 532: "CYBER; Attribute Based Encryption for Attribute Based Access Control".

[i.12] Charter of Fundamental Rights of the European Union.

[i.13] ISO/IEC 29134:2017: "Information technology -- Security techniques -- Guidelines for privacy impact assessment".

[i.14] ISO/IEC 27001:2013: "Information technology -- Security techniques --Information security management systems - Requirements".

[i.15] ISO/IEC 27552: 2019: "Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines (PIMS)".

NOTE: At the time of publication of the present document ISO/IEC 27552 is not yet published.

[i.16] ETSI TR 103 305-5: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement".

[i.17] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.18] ETSI TR 103 305-1: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.19] ETSI GS NFV-SEC 006: "Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns".

[i.20] ISO/IEC 15408 series: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.21] ISO/IEC 20889:2018: "Privacy enhancing data de-identification terminology and classification of techniques".

[i.22] ISO/IEC 29151:2017: "Information technology -- Security techniques -- Code of practice for personally identifiable information protection".

[i.23] ISO/IEC 27018:2014: "Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors".

[i.24] ISO/IEC CD 29184: "Information technology -- Online privacy notices and consent" (under develpment).

[i.25] ISO/IEC PDTR 27550: "Information technology -- Security techniques -- Privacy engineering" (under develpment).

[i.26] ISO/IEC 29146:2016: "Information technology -- Security techniques -- A framework for access management".

[i.27] ISO/IEC 29190:2015: "Information technology -- Security techniques -- Privacy capability assessment model".

[i.28] ISO/IEC 27002:2013: "Information technology -- Security techniques -- Code of practice for information security controls".

[i.29] 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).

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in clause 4 apply.

3.2 Symbols

Void.

3.3 Abbreviations

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

ABE	Attribute Based Encryption
DPIA	Data Protection Impact Assesment
EC	European Commission
ECHR	European Court of Human Rights
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IOT	Internet Of Things
ISMS	Information Security Management System
ISO	International Standard Organization
IV	Initial Value
NGP	Next Generation Protocol
PET	Privacy Enhancing Technology
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIMS	Privacy Impact Management System
TE	Terminal Equipment
TEDDI	Terms and Definitions Database Interactive
TS	Technical Specification
UDHR	Universal Declaration of Human Rights

4 Glossary of terms

4.1 Collation of terms

Table 1 presents a general collation of the terms from a small set of primary sources of the terms used in addressing privacy in standards. The primary sources that have been used to build this collation are:

- Regulation (EU) 2016/679 (GDPR) [i.1];
- ISO/IEC 29000 series [i.8], [i.7] and [i.13];

- ISO/IEC 15408 series [i.20];
- ISO/IEC 20889 [i.21]; and
- ETSI TEDDI repository https://webapp.etsi.org/Teddi/.

Table 1: Collation of terms related to data protection and privacy from selected SDOs and comparison to the GDPR

Term	Definition	Source of definition	Remarks
anonymity	characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly	ISO/IEC 29100	To determine whether an individual is identifiable, account should be taken of all the means likely reasonably to be used by the entity holding the data or by any other party, to identify that individual
	principle whereby ones identity is withheld from other parties (see note 1)	ETSI TEDDI, group NA	Identical text
	'Anonymity' is the principle whereby ones identity is withheld from other parties (see note 1)	ETSI TEDDI, group SMG	
	ability of a user to use a resource or service without disclosing the user's identity (see note 2)	ETSI TEDDI, group ITS	Derived from ISO/IEC 15408-2
	act of ensuring that a user may use a resource or service without disclosing the user's identity (see note 2)	ETSI TEDDI, group SMG	
anonymization	process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party	ISO/IEC 29100	
	process that replaces an actual identifier with an attribute obtained by randomization or generalization in such a way that there is a reasonable level of confidence that no individual can be identified	ETSI TEDDI, group CYBER	
de-anonymization	Any process in which anonymous data is cross-referenced with other sources of data to re-identify the anonymous data source	ETSI TEDDI, group CYBER ISO/IEC 20889	
anonymized data	data that has been produced as the output of a personally identifiable information anonymization process		
de-identification	process of removing the association between a set of identifying data and the data principal	ISO/IEC 20889	

Term	Definition	Source of definition	Remarks
enterprise	natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity	GDPR	See also 'undertakings' in GDPR
	unit of economic organization or activity, especially a business organization	ETSI TEDDI groups 3GPP&TISPAN	
identifiability	condition which results in a personally identifiable information (PII) principal being identified, directly or indirectly, on the basis of a given set of PII		
identifier	set of attribute values that unambiguously distinguish one entity from another one in a given context		
	total list of attribute values of an entity that allows this entity to be unambiguously distinguished from all other entities within a context and to be recognized as a single identity in that specific context		Appears to overlap with definition of identity below
	means of indicating a point of contact, intended for public use such as on a business card. Telephone numbers, email addresses, and typical home page URLs are all examples of identifier in other systems	ETSI TEDDI, group 3GPP	
	series of digits, characters and symbols used to identify uniquely subscriber(s), user(s), network element(s), function(s) or network entity(ies) providing services/applications	ETSI TEDDI, group TISPAN	
	user's name and optionally a password		
	attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context	ETSI TEDDI, group ITS	
	series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g. physical or logical objects)	ETSI TEDDI, group NGP	
	user identification (name and, where appropriate, password) which can be supplied during the call in order to indicate entitlements with regard to operations on files	ETSI TEDDI, group TE	

Term	Definition	Source of definition	Remarks
identity	set of attributes which make it possible to identify the personally identifiable information principal		
	technical label which may represent the origin or destination of any telecommunications traffic, as a rule clearly identified by a physical telecommunications identity number (such as a telephone number) or the logical or virtual telecommunications identity number (such as a personal number) which the subscriber can assign to a physical access on a case-by-case basis	ETSI TETRA	
	attributes by which an entity or person is described, recognized or known	ETSI TEDDI, group OCG	
	data or information (identifier) that are used to distinguish one object or person from others. These data can take many forms, and also a single object or person may have different identities associated. Authentication can be used to verify purported identities. An identity, which has been so verified, is called an authenticated identity	ETSI TEDDI, group HF	
	essence of an entity and often described by its characteristics	ETSI TEDDI, group BROADCAST	
	identifier allocated to a particular entity, e.g. a particular end-user, provides an Identity for that entity	ETSI TEDDI, group TISPAN	
	a system unique tag applied to an entity	ETSI TEDDI, group SMG	
	information about an entity that is sufficient to identify that entity in a particular context	ETSI TEDDI, group NGP	
opt-in	process or type of policy whereby the personally identifiable information (PII) principal is required to take an action to express explicit, prior consent for their PII to be processed for a particular purpose (see note 7)	ISO/IEC 29100	

Term	Definition	Source of definition	Remarks
personally, identifiable information (PII)	any information that: a) can be used to establish a link between the information and the natural person to whom such information relates, or b) is or might be directly or indirectly linked to a natural person (see note 10)	ISO/IEC 29100	Regulation (EU) 2016/679 defines 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"
PII controller	privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes (see note 8)	ISO/IEC 29100	Regulation (EU) 2016/679 defines controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law"
PII principal	natural person to whom the personally identifiable information (PII) relates (see note 9)	ISO/IEC 29100	Data subject indirectly defined in Regulation (EU)2016/679 as part of the definition of personal data: "identified or identifiable natural person ('data subject')"

Term	Definition	Source of definition	Remarks
processing of PII	operation or set of operations performed upon personally identifiable information (PII)	ISO/IEC 29100	Regulation (EU) 2016/679 defines processing as "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"
PII processor	privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller	ISO/IEC 29100	Regulation (EU) 2016/679 defines data processor: "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"
privacy breach	situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements	ISO/IEC 29100	Regulation (EU) 2016/679 defines personal data breach: "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed"
privacy controls	measures that treat privacy risks by reducing their likelihood or their consequences (see notes 3 and 4)	ISO/IEC 29100	
privacy-enhancing technology PET	privacy control, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system	ISO/IEC 29100	
privacy impact	anything that has an effect on the privacy of a PII principal and/or group of PII principals	ISO/IEC 29134	The privacy impact might result from the processing of PII in conformance or in violation of privacy safeguarding requirements

Term	Definition	Source of definition	Remarks
Privacy Impact Assessment (PIA)	overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information, framed within an organization's broader risk management framework	ISO/IEC 29134	
privacy risk assessment (also known as privacy impact assessment PIA)	overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personally identifiable information (PII) specific choices made by a personally identifiable information (PII) principal about how their PII should be processed for a particular purpose	ISO/IEC 29100	Data Protection Impact Assessment in Regulation (EU) 2016/679
privacy policy	overall intention and direction, rules and commitment, as formally expressed by the personally identifiable information (PII) controller related to the processing of PII in a particular setting	ISO/IEC 29100	
privacy preferences	specific choices made by a personally identifiable information (PII) principal about how their PII should be processed for a particular purpose	ISO/IEC 29100	
Privacy principles	set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems	ISO/IEC 29100	
pseudonymization	process applied to personally identifiable information (PII) which replaces identifying information with an alias (see notes 5 and 6)	ISO/IEC 29100	Regulation (EU) 2016/679 defines pseudonymisation as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"

Term	Definition	Source of definition	Remarks
Third-party	privacy stakeholder other than the personally identifiable information (PII) principal, the PII controller and the PII processor, and the natural persons who are authorized to process the data under the direct authority of the PII controller or the PII processor	ISO/IEC 29100	Regulation (EU) 2016/679 defines third party as "natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data"

NOTE 1: Other party refers to parties not directly involved in the transaction (see 3rd party).
NOTE 2: Party in this context means the party offering the service.
NOTE 3: Privacy controls include organizational, physical and technical measures, e.g. policies, procedures, guidelines, legal contracts, management practices or organizational structures (from ISO/IEC 29100). Privacy controls include policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature.
NOTE 4: Control is also used as a synonym for safeguard or countermeasure (from ISO/IEC 29100).
NOTE 5: Pseudonymization can be performed either by PII principals themselves or by PII controllers. Pseudonymization can be used by PII principals to consistently use a resource or service without disclosing their identity to this resource or service (or between services), while still being held accountable for that use (from ISO/IEC 29100).
NOTE 6: Pseudonymization does not rule out the possibility that there might be (a restricted set of) privacy stakeholders other than the PII controller of the pseudonymized data which are able to determine the PII principal's identity based on the alias and data linked to it.
NOTE 7: A different term that is often used with the privacy principle 'consent and choice' is "opt-out". It describes a process or type of policy whereby the PII principal is required to take a separate action in order to withhold or withdraw consent, or oppose a specific type of processing. The use of an opt-out policy presumes that the PII controller has the right to process the PII in the intended way. This right can be implied by some action of the PII principal different from consent (e.g. placing an order in an online shop) (from ISO/IEC 29100).
NOTE 8: A PII controller sometimes instructs others (e.g. PII processors) to process PII on its behalf while the responsibility for the processing remains with the PII controller (from ISO/IEC 29100).
NOTE 9: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal" (from ISO/IEC 29100).
NOTE 10: The "natural person" in the definition is the PII principal. To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person (from ISO/IEC 29100).

4.2 Taxonomy of terms

Taxonomy is defined as the practice and science of classification of things or concepts, including the principles that underlie such classification. The precursor to developing a simple taxonomy is to identify many of the key concepts such as those identified from the viewpoint of Privacy Protecting Technologies or Privacy Enhancing Technologies in Figure 1. This may be extended by taking an alternative view based on the principles that are introduced in clause 6 of the present document and by identifying the key actors in data protection: the data subject (i.e. the entity to whom the PII or data refers); the PII controller (i.e. the entity responsible for defining the data use and collection policies and to whom liability falls also called data controller in the present document); and the PII processor (i.e. the entity that acts on behalf of the PII controller to process data from the data subject in accordance with the purpose agreed between the PII controller and data subject, also called data processor in the present document). For the purposes of the present document the term data subject is synonymous with the term PII principal (also called data principal in the present document).

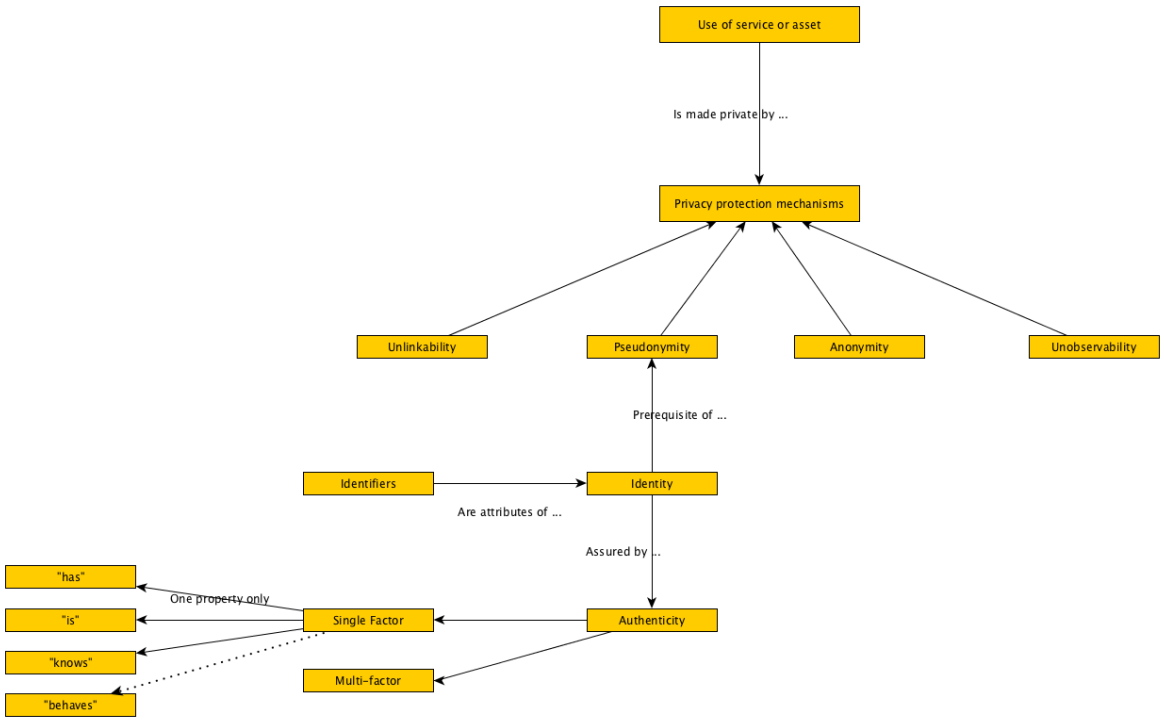

Figure 1: Role of protection mechanisms in privacy protection

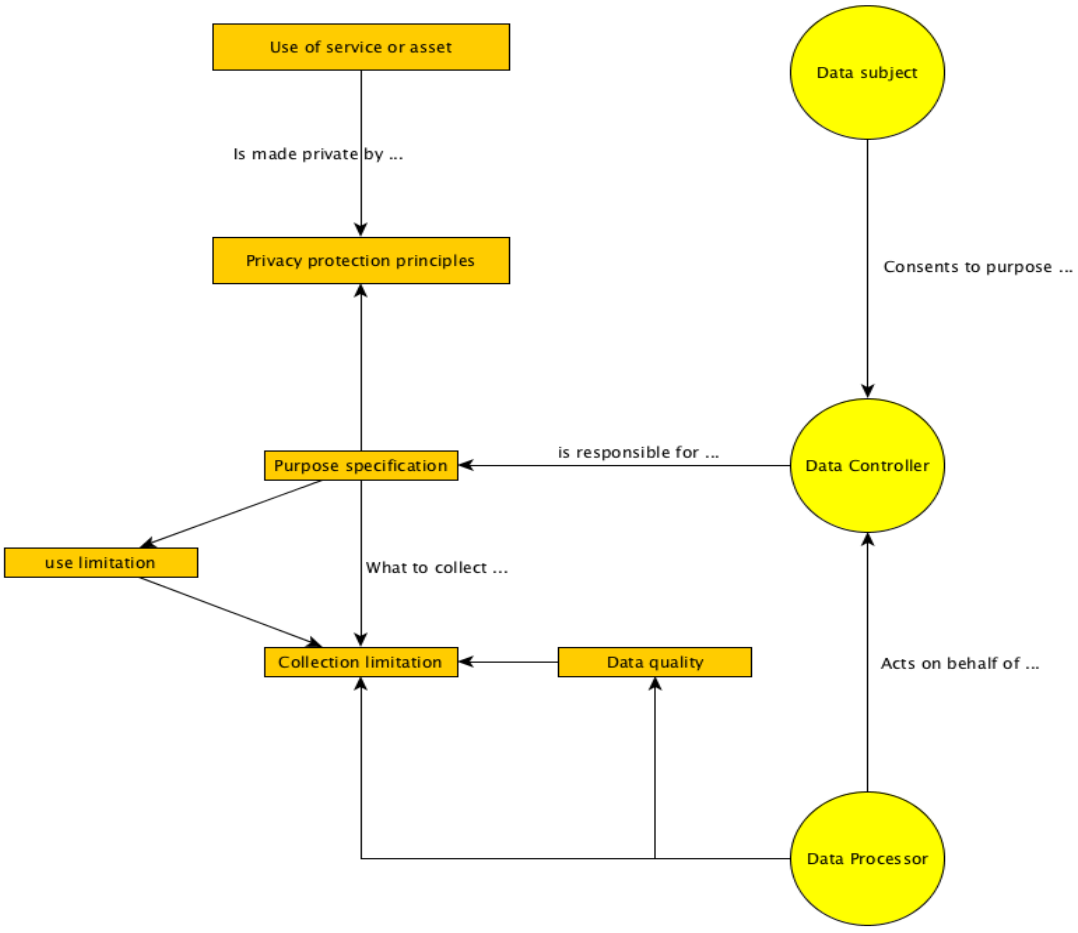

Figure 2: Extending privacy protection to address principles of privacy protection

5 Standards and guidelines to management of privacy

5.1 Privacy Impact Assessment

The GDPR [i.1] addresses Data Protection Impact Assessment (DPIA) in chapter IV, section 3, Articles 35 and 36 and is also addressed in the Article 29 Data Protection Working Party Guidelines [i.10], annex 2. With regard to privacy the division between a privacy impact assessment, and a data protection impact assessment, is considered as identical in the present document. In addition, ISO/IEC 29134:2017 [i.13] gives guidelines for each of:

- a process on privacy impact assessments; and
- the structure and content of a PIA report.

ETSI TR 103 305-5 [i.16] provides a guide to undertaking a Privacy Impact Assessment using the Critical Security Controls defined in ETSI TR 103 305-1 [i.18] as well as guidance on how the Critical Security Controls can be used when aiming to comply with GDPR [i.1], in identifying how data is collected and processed as part of the collation of the inventory of assets. This is shown in figure 3.

Within the context of Network Functions Virtualisation, ETSI GS NFV-SEC 006 [i.19] also addresses the requirement to perform a PIA and specifically extends the overall risk analysis approach given in ETSI TS 102 165-1 [i.17] by recommending consideration of the principles given in clause 6 against the assets of the system.

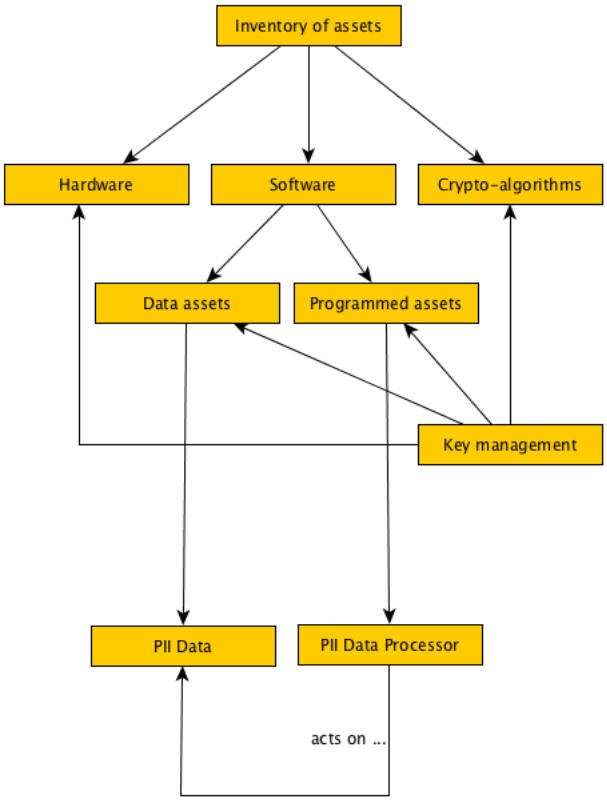

Figure 3: Identification of PII data in inventory of assets

5.2 Guidelines and best practices

For general identification of the principles to be followed the GDPR [i.1] and the data management principles identified in clause 6 of the present document together act to identify the objectives and core requirements. The means to instantiate these objectives and requirements into systems is less well documented although a very large number of guides to implementation and preparation for the impact of GDPR have been published. Most of these are widely available. It should be noted however that in all cases the GDPR makes strong recommendations for national and regional advisors on the implementation of GDPR with specific actions being placed on the data protection officer and on the supervisory authority to give guidance to those who ask.

ISO has published both general codes of practice and codes of practice aimed at the cloud computing market:

- ISO/IEC 29151 [i.22]: Code of practice for PII protection.
- ISO/IEC 27018 [i.23]: Code of practice for protection of personally identifiable information (PII) in public clouds.

In GDPR Article 6 a key component of the implementation is the concept of informed and explicit consent. This is addressed in the following:

- ISO/IEC 29184 [i.24]: Guidelines for online privacy notices and consent.

In article 6 of GDPR [i.1], "Lawfulness of processing", there are a number of alternatives that allow processing of personal data if a discrete data subject cannot be identified in advance and consent sought for the processing. Thus one of the rules identified in Article 6.1d (processing is necessary in order to protect the vital interests of the data subject or of another natural person), 6.1e (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller), or 6.1f (processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child) may apply.

5.3 Impact assessment and analysis

ISO/IEC 29134 [i.13] (privacy impact assessment Methodology) defines a framework in order to perform privacy impact assessment. Relevant published standards in this domain include the following:

- ISO/IEC 27550 [i.25]: Privacy engineering.
- ISO/IEC 29146 [i.26]: A framework for access management.
- ISO/IEC 29190 [i.27]: (Privacy capability maturity model) proposes a maturity capability model to be used by organizations.

5.4 Codes of practice

As a support to privacy management it is important to have code of practice in order to identify good practices for personal data protection:

- ISO/IEC 29151 [i.22]: Code of practice for PII protection proposes controls (see sections 4.3 and 4.4).

A specific document on cloud computing has been developed and published by ISO:

- ISO/IEC 27018 [i.23]: Code of practice for protection of personally identifiable information (PII) in public clouds. This document in particular takes into account terms and definitions of cloud computing.

5.5 Cryptographic mechanisms

ETSI TS 103 485 [i.5] provides an analysis of the privacy preserving characteristics of a number of cryptographic key management schemes. Of themselves cryptographic algorithms do not directly impact privacy although their application may be an element of asserting elements of privacy, for example authentication may be used to in the act of verifying the authority to view data, encryption may be used to enforce data confidentiality.

Furthermore, the key is a PII element as it contains one of two attributes for asymmetric keyed cryptography: The private part is treated as private and not disclosed to any party; the public part is treated as open or public information and deliberately shared with multiple parties. For symmetric keyed cryptography the key is known only to the 2 trusted parties.

NOTE: For Identity Based Cryptography, and Attribute Based Cryptography in general, the private part of the key pair is generated by a trusted system element and given back to the data subject so varies a little from the assertion made above.

For the purposes of the present document it is asserted that the key management system is subject to the personal data requirements for data processing that fall in the remit of GDPR and that as such the key management procedures should be included in the scope of a PIA/DPIA. This scope should be extended to ciphertexts in ABE systems (e.g. as defined in ETSI TS 103 532 [i.11]) as attributes and policies have the potential to hold personal data. Nevertheless, cryptographic mechanisms may be used in support of the privacy protection implementation, e.g. to encrypt data and enforce access control. However, in order to enable many of the processes that may be used to provide privacy protection, common mappings between intent and cryptographic support mechanism such as {confidentiality, encryption}, {authenticity, crypto-authentication} may be enforced within the data collection and processing policies established by the data controller. There is a very large body of work on the application of cryptographic techniques to various forms of data protection and which identify specific algorithms.

5.6 Management system including privacy protection

For the management of a risk approach basis, an Information security management system should be implemented. Furthermore, security represents one of the key principles defined in GDPR article 5 [i.1] and is associated with risk management as described in GDPR article 32 (specified in section 5.3).

ISO/IEC 27001 [i.14] which defines the requirements for a risk-based information security management systems (ISMS) is highly relevant for organizations needing to comply with provision of the regulation.

ISO/IEC 27552 [i.15] extension to ISO/IEC 27001 [i.14] and ISO/IEC 27002 [i.28] for privacy information management-requirements and guidelines intends to extend ISO/IEC 27001 [i.14] to cover privacy management through a specific set of requirements. ISO/IEC 27552 [i.15] specifies a Privacy Information Management Systems (PIMS). An informative annex of the standard matches the specifications of ISO/IEC 27552 with the obligations of the GDPR in order to demonstrate how complying with the standard can be used in meeting the obligations indicated in the regulation.

6 General principles

6.1 Caveats and warnings

Privacy is a complex concept and cannot be easily bounded. There are complexities of interpretation as whilst private and public may appear to be opposites to each other it is possible to apply both private and public interpretations to the same data of the same entity. Much of the concern in the protection of privacy is to establish a clear boundary around what can be done with data that is both made public and which can be at the same time interpreted as private. For example, when buying a travel ticket information has to be given regarding the traveller, the start and end points and the time of travel, for some travel additional data may be required regarding the age, sex and physical status of the traveller to enable things such as discount policies (e.g. children's tickets may be lower cost), assistance requirements (e.g. more time required to transfer between modes of transport or need to allow wheelchair access), offers to have single sex accommodation and so forth. The normal expectation of human communication is that the sharing of this level of information between the individual and the agent for buying the travel ticket is only used in the context of buying the travel ticket and once the transaction is complete the agent is mostly expected to forget it. However, in practice the agent needs to share some of the information with other entities to complete the transaction, for example to inform the train or plane operating company, or the airport staff, to arrange for a wheelchair and assistance, and so forth. Furthermore, if part of the service is unfulfilled data should be retained to allow for post-event analysis, e.g. if a claimed request for assistance is not fulfilled it would be useful to be able to identify if such data was collected and passed through the system.

The various legislative documents identify some of this data as PII - Personally Identifiable Information - but of itself not all data items will be PII but some combinations will be PII. This is complex so identifying a passenger as female is not of itself PII but if combined with other data it may be able to be used to uniquely identify an individual. A concern is that with access to enough nominally benign data a search can be performed to uniquely identify someone at which point that data set may be considered as PII.

It should be noted that there are many laws to protect victims of public statements including those of libel and slander, of copyright, and so forth, in addition to the laws surrounding data protection captured in the GDPR [i.1]. Thus, if Alice makes a public statement regarding Bob that Bob believes reveals data that is private or wrong whilst Bob is not directly in the GDPR chain his rights are still protected.

The revealing of private data in content is difficult to protect against when the intent of the author is to publish (make public). It is essential therefore to be clear about what can be protected in the privacy domain using the toolkit of security, and what has to be protected by other measures, e.g. judicial measures, against attacks in the content of messages.

6.2 EU regulatory and legal context

The primary EU regulation that appears to apply is the General Data Protection Regulation [i.1]. However, the GDPR seeks to protect data and the fundamental rights and freedom of natural persons as indicated in its Article 1, to which privacy is a component. The relationship of the GDPR to privacy should be understood as that of an enabler in relation to Directive 2002/58/EC [i.29] (under re-examination to be replaced) 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 which is cited in recital 173 of the GDPR, as well as to the Charter of Fundamental Rights of the European Union [i.12] cited in its recital 1. The right to privacy of an individual is enshrined in EU law by means of the European Convention on Human Rights (ECHR) [i.2], which is closely linked to the Universal Declaration of Human Rights (UDHR) [i.3].

Article 8 of the ECHR [i.2] states:

QUOTE 1: *"Everyone has the right to respect for his private and family life, his home and his correspondence".*

QUOTE 2: *"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".*

Article 12 of the UDHR [i.3] states:

QUOTE 3: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

The ECHR recital does not imply that "authority" is a synonym of "nation state" or "government" but that modern business and governmental practice should not be able to interfere in the right to, and expectation of, privacy.

NOTE: Many modern businesses use personal data and the data subjects' willingness to offer such data in lieu of a direct payment for service. The business then monetises that data by selling it onto advertisers and other channels to provide a service to the data subject. The profit driver in such businesses is that the consented use of knowledge (raw data or inferred information) given by the data subject, across a wide enough set of data subjects, offsets the cost of delivery of the actual service offered to the data subject.

6.3 Privacy management principles

Several recognized sets of privacy principles have been developed. A synthesis of these sets was adopted in ISO/IEC 29100:2011 [i.7] which post-dates similar activity undertaken in ETSI TR 187 010 [i.6] and restated in general terms in table 2 of the present document:

1) Consent and Choice (addressed by the use limitation principle in ETSI TR 187 010 [i.6]).

2) Purpose Legitimacy Specification (purpose specification principle from ETSI TR 187 010 [i.6]).

3) General avoidance of collecting and processing private data as much as possible (collection limitation principle from ETSI TR 187 010 [i.6]).

4) Data Minimization (collection limitation principle from ETSI TR 187 010 [i.6]).

5) Use, Retention and Disclosure Limitation (use limitation and purpose specification principles from ETSI TR 187 010 [i.6]).

6) Accuracy and Quality (data quality principle from ETSI TR 187 010 [i.6]).

7) Openness, Transparency and Notice.

8) Individual Participation and Access (addressed by individual participation principle from ETSI TR 187 010 [i.6]).

9) Accountability.

10) Information Security (security safeguards principle from ETSI TR 187 010 [i.6]).

11) Privacy Compliance.

These principles which have been stated in ISO (ISO/IEC 29100 [i.7], clause 6) and identified in the list above are strongly recommended in ISO to be used as the basis of privacy management. In the ETSI context recommendations have been made in ETSI TR 187 010 [i.6] to identify specific actions on fixed networks telecom operators and act as 11 principles that map to the list of 11 from ISO. The principles from ETSI TR 187 010 [i.6] are tabulated and generalized for any operator type in table 2. The model adopted and extrapolated from best practice in which it is a data controller that defines the purpose of data, and the processer that enacts the purpose, has been assumed in table 2 and is consistent with the obligations defined in the GDPR [i.1]. The principles act as indicators of best practice and should be examined in detail against national and other legislation prior to implementation.

Table 2: Privacy and data protection principles derived from ETSI TR 187 010 [i.6]

Principle	Sub-principle	Comments and remarks
Collection limitation	Limits to data collection	Before collecting personal data - for example, when contracting with the data subject - a data controller should obtain the prior and unambiguous consent of the data subject or inform the data subject of the collection of personal data and the indicated purposes of use according to domestic regulations
		From the viewpoint of the data controller, consent is mostly required when personal data is used in commercial services. However, in cases of safety and public services, prior explicit consent may not be required although implicit consent is likely to have been given as part of the user's contractual agreement with the service provider
	Data collection methods	A data controller should not acquire personal data by fraudulent or other dishonest means
	Data collection without consent	The limits to data collection do not apply to cases in which the handling of personal data is restricted by national regulation. Data controllers should collect data without consent for example when authorized by a domestic court order or equivalent legal instrument

Principle	Sub-principle	Comments and remarks
	Exclusion of data capable of identifying an individual from collected data	A data controller should take reasonable measures to avoid collecting data from which an individual could be identified by referring to a database in cases where such a possibility exists
	Confirmation of a data subject's consent about data collection	A data controller should take suitable measures to confirm the consent of a data subject about data collection
Data quality principle		A data controller should endeavour to keep personal data accurate and up to date within the scope necessary for the achievement of the purposes of use
Purpose specification principle	Specification of the purposes of use	When handling personal data, a data controller should specify the purposes of use of personal data
	Limits on changing the purposes of use	A data controller should not change the purposes of use beyond the scope in which new purposes can reasonably be considered to be compatible with the original purposes
	Change of the purposes of use required prior consent	Before a data controller changes the purposes of use beyond the scope in which new purposes can reasonably be considered to be compatible with the original purposes, it should inform a data subject of the change or obtain prior and unambiguous consent
Use limitation principle	Use limitation	A data controller should not handle personal data, without obtaining the prior consent of the data subject, beyond the scope necessary for the achievement of the specified purposes of use
	Restriction of disclosure to third parties	A data controller should not provide personal data to a third party without obtaining the prior consent of the data subject except for very limited and well-defined cases (for example legal request)
	Use without consent	The provisions of the preceding two paragraphs do not apply to cases in which the handling of personal data is based on domestic laws. Data controllers should grant access only to law enforcement authorities as authorized by a domestic court order or equivalent legal instrument
Security safeguards principle		Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data
Openness principle		There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data collector

Principle	Sub-principle	Comments and remarks
Individual participation principle		An individual may have the right, among others, to: (a) obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) have communicated to him, data relating to him: (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
Accountability principle		A data controller should be accountable for complying with measures which give effect to the principles stated above, and for ensuring that data processor(s) similarly comply
Equality of regime principle		A data controller should not transfer personal data across borders unless the destination has an equivalent privacy regime as the origin
NOTE 1: A right to anonymity is often cited as a principle but has not been included above as it is possible to offer anonymity as a means of complying to the principles, thus the right to anonymity is not declared as a principle. NOTE 2: Applicable regulation may provide for different requirements that those given in the "comments and remarks" column.		

7 Application of principles to example use cases

7.1 Least to know/collect

The broad requirement to only capture essential data is addressed by the collection limitation principle and the use limitation principle. It is these principles that contribute to the content of the contract of consent between the data subject and the data controller.

NOTE: There is an implied contract of consent between the data subject and the data controller that is addressed for both explicit consent and implicit consent in the identity management work in ETSI TS 103 486 [i.4].

7.2 Data/privacy protection and data brokering

Recognizing that there are limitations on the scope of some schemes such as anonymity processing when multiple data sets are combined, the data subject is protected to some extent from the aggregation of data from multiple sources by applying the following principles:

- individual participation principle; openness principle;
- use limitation principle; and

- by the collection limitation principle.

If a data controller allows for the aggregation of data in such a way that PII is not revealed there may be a reasonable claim, depending on the law, that there is no direct link to the impacted individual and thus that there is no obligation to inform the data subject and request consent for that particular data controller. However, as part of the collection limitation principle, use limitation principle, and the openness principle there should be a cascade of consent such that if the initial scope of consent is between the data subject and data-controller-#1 then if data-controller-#1 decides to submit data to a second or third data controller to be aggregated then the openness principle of informing the data subject of a change in use should be clearly made. This obligation should be extended even if in the view of data-controller-#1 the data being exported has been anonymized.

NOTE 1: The recommendations given above are in the spirit of best practice and are not obligations under the GDPR [i.1].

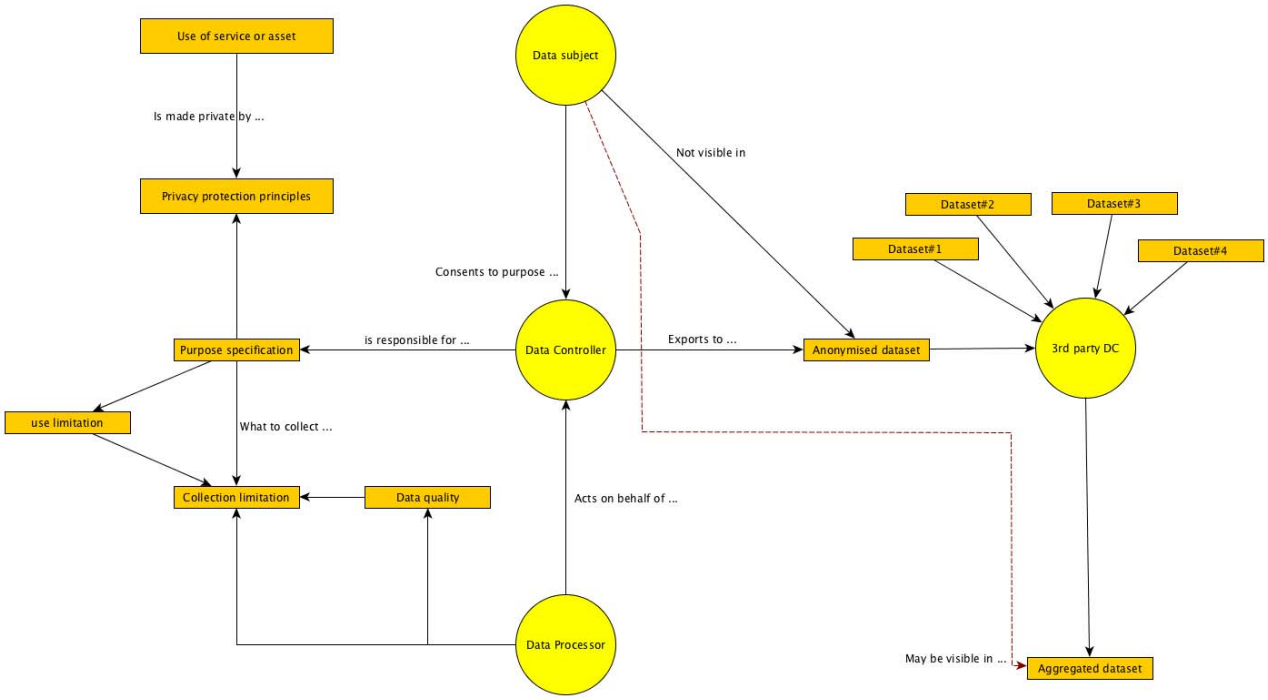

Figure 4: The problem of data aggregation de-anonymizing an anonymized dataset

As shown in figure 4, whilst the export of an anonymized dataset may be within the scope of legitimate practice, it is possible, with appropriate technology, to re-identify the data subject when aggregated with other data sets even if all of the data sets are anonymized. As best practice, any export made by the originating data controller should advise the data subject of the risk that anonymized data may be de-anonymized if aggregated with sufficient resources. If a dataset is de-anonymized the responsible data controller should inform the data subject.

In addressing anonymization techniques, the functional structure of the Anonymity group in the Privacy class of ISO/IEC 15408-2 [i.20] and the following apply:

- ISO/IEC 20889 [i.21]: Privacy enhancing data de-identification techniques.

NOTE 2: An analysis of the privacy preserving aspects of various forms of cryptography are given in ETSI TS 103 485 [i.5] and should be carefully considered when applying any analysis of the privacy concerns in any system.

7.3 The Right to be forgotten

The right to be forgotten (right to erasure as defined in GDPR Article 17 [i.1]) is addressed in the individual participation principle combined with the openness principle. In conforming to these principles both data subject and data controller should be aware of where data is held and when the data controller receives a request for erasure this knowledge can be enacted upon to erase data pertaining to a specific data subject. This should also address where data has been archived. As misuse of the right to be forgotten can undermine the objectives of data protection the data controller should take measures to ensure that the request is legitimate.

NOTE 1: If a dataset is archived and its integrity verified then when it is modified to delete the data subject enforcing the right to be forgotten that dataset is no longer verifiable as untainted. As such measures should be put into place to give assurance of the integrity of the dataset both before and after acting on a right to be forgotten order without adding data referring to the data subject to the audit logs.

NOTE 2: It is not clear if a person who is identified in the content of a publication can have the entry in the publication removed under the right to be forgotten principle, as it is not clear if that content was collected by the PII controller or is known to the PII controller.

NOTE 3: If an individual can be identified by third party linking to content, or citation of content, it is not clear that the data controller will be aware of such links and be in a position to enact the right to be forgotten. What may happen is that citations and links to forgotten data will no longer work.

Where there is a direct link between the data subject exercising the right to be forgotten the obligations enacted under the GDPR in the "individual participation principle" and the "openness principle" should be sufficient to ensure that the data controller has mechanisms in place to ensure data pertaining to the data subject can be removed. However, if an individual is cited in a publication made by another person under the auspices of a second, unrelated, data controller these same principles may not be sufficient.

EXAMPLE: If personal information about Alice is made by Bob in a public posting (say a social media post) and Alice is neither the poster nor associated to the data controller of the site Alice should be able to find public details of how to ask the data controller to delete the data, provided it meets the criteria for the "right to be forgotten". In such cases Bob may seek to deny the request within the criteria of the "right to be forgotten".

The Right to be Forgotten is detailed in Article 17 of the GDPR [i.1] as the Right to Erasure. Article 18 of the GDPR, the right to restriction of processing, may be invoked alongside Article 17 either independently or as a precursor to validation of the request under Article 17. The right to restriction of processing halts all form of processing except storage, as such the "security safeguards principle" continues to apply to the data.

NOTE 4: An analysis of the privacy preserving aspects of various forms of cryptography are given in ETSI TS 103 485 [i.5] and should be carefully considered when applying any analysis of the privacy concerns in any system.

8 Gaps in standardization

Many standards exist to give assurance of data integrity, of the identification and authentication of actors in systems, and to give assurance of confidentiality of data. In addition to the technical domain there are many standards, guides and best practice methods that encourage the application of the technical tools that may give privacy protection. The purpose of the present document has been to give an overall view of the role of standards in addressing privacy requirements.

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. Thus, the gap identified is to ensure appropriate application of the principles identified in clause 6 and to ensure that future technical systems have privacy by default and by design as an immutable and enforceable attribute.

The domains of interest for the future focus of privacy by default and by design include but are not limited to:

- Communications security (infrastructure and wireless).
- Impact of NGP (next generation protocol).

- IOT implementation.
- Connected and autonomous cars.
- Intelligent transport systems.
- Smart Energy networks.

All of the SDOs need to work together to ensure that privacy by default and by design are thus integrated.

Annex A: Bibliography

- Directive 95/46/EC (superseded by the GDPR).
- WG5 road map ISO/IEC JTC1/SC27/WG5 standing document 1.
- Privacy reference lists ISO/IEC JTC1/SC27/WG5 standing document 2.
- NIST Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT).
- Standards Privacy Assessment (SPA) ISO/IEC JTC1/SC27/WG5 standing document 4.
- ISO/IEC 29101:2013: "Information technology -- Security techniques -- Privacy architecture framework".
- CEN EN 16571:2014: "Information technology - RFID privacy impact assessment process".
- Standards Privacy Assessment (SPA) ISO/IEC JTC1/SC27/WG5 standing document 4.

History

Document history		
V1.1.1	January 2019	Publication