Guidance and gap analysis for European standardisation

Quemard, Jean-Pierre; Schallabok, Jan; Kamara, Irene; Pocs, Matthias

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

Guidance and gaps analysis for European standardisation

Privacy standards in the information security context

DECEMBER 2018

www.enisa.europa.eu European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contributors

Jean-Pierre Quemard (KAT), Jan Schallabök (iRights.Law), Irene Kamara (Tilburg University/Vrije Universiteit Brussel) and (Stelar Security Technology Research)

Editors

Prokopios Drogkaris (ENISA), Athena Bourka (ENISA)

Contact

For queries in relation to this paper, please use isdp@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

We would like to thank Alex Li (Microsoft) for his valuable comments during the preparation of this document.

ISBN 978-92-9204-283-7, DOI 10.2824/698562

Table of Contents

Executive Summary

Standards are essential components of almost all aspects of the organisation and functioning of modern societies including information security. Through the development and adoption of standards, best practices are shared among organisations, integration and interoperability of systems is promoted, complex environments are simplified, and information systems are shielded against cyber threats. Privacy standards can be seen as an application area of the broader area of information security standards.

Over the last decade, there has been a significant development of privacy standards, which aim at contributing to the integration of privacy requirements into information processes, systems and services. Such integration is fundamental for the protection of individuals' personal identifiable information (PII), particularly in digital environments, while it may also support the implementation of relevant privacy and data protection legislation.

Against this background, ENISA elaborated further on the area of privacy standards considering the developments at legislative, policy, and standardisation level. The current study explores how the standards-developing world is responding to the fast-changing, demanding realm of privacy by mapping existing available standards and initiatives in the area and provides insights on the "state-of-the-art" of privacy standards in the information security context through a relevant gap analysis. To this end, the main findings of the study are presented below.

International vs. European standards

Since the references to standards in the Union legislation are becoming more regular, and there are considerable differences of Union privacy and security regulations with other jurisdictions, the need for analysis of mapping of international standards and European regulatory requirements is intensified.

Standardisation and conformity assessment mechanisms in information security

Proving compliance with privacy standards in information security is not as straightforward as one would expect. While there are some approaches for conformity assessment available in specific sectors, others are still lacking appropriate mechanisms.

Selection, agreement, and prioritisation of standardization activities

A consistent analysis of sector-specific needs for privacy standardisation is essential, especially in the context of information security, before moving ahead with the adoption or development of new standards. Through such an analysis, common issues that may be addressed with baseline cross-sector standards, and additional issues to be dealt with in sector-specific standards can be identified and thus avoid duplication of efforts.

The role of technology and privacy by design

Standardisation activity is mainly focused on covering technological approaches/solutions. Among those solutions, many address the introduction of privacy-preserving technologies throughout the whole lifecycle of a product or a system. Despite a general common agreement on the value of privacy by design, the concept and its implementation are still not clearly elucidated in standardization activities.

1. Introduction

1.1 Importance of privacy standards in the information security context

Standards are essential components of almost all aspects of the organisation and functioning of modern societies. Critical infrastructures, quality management, and a broad range of other topics are covered by the standardisation activity of Standards Development Organisations (SDOs). Standards are also of great importance for information security. Through the development and adoption of standards, best practices are shared among organisations, integration and interoperability of systems is promoted, complex environments are simplified, and information systems are shielded against cyber threats.[1]

However, there are also challenges in the deployment and use of standards. Based on previous work of ENISA in this area[2,3&4], it is apparent that information security standards do not evolve in a pace commensurate with the perceived threat level, and that there is lack of awareness and information among stakeholders (e.g. public authorities or Small Medium Enterprises (SMEs)) that could adopt and benefit from them. Additionally, there is limited coordination among SDOs, which results in the proliferation of multiple standards on one topic and scarcity of standards on another.

Privacy standards can be seen as an application area of the broader area of information security standards. Over the last decade, there has been a significant development of privacy standards, as illustrated by the activities of ISO/EC, CEN and CENELEC discussed in Sections 3 and 4 respectively, which aim at contributing to the integration of privacy requirements into information processes, systems and services. Such integration is fundamental for the protection of individuals' personal identifiable information (PII), particularly in digital environments, while it may also support the implementation of relevant privacy and data protection legislation (e.g. the General Data Protection Regulation – GDPR in EU[5]). This having said, the inherent limitations of standardisation activities are also present in this area, especially with regard to co-ordination and coverage of the whole spectrum of requirements that is relevant to privacy.

In 2017, the first edition of the CEN-CENELEC - ENISA workshop[6] on standards took place in Brussels under the theme "Cybersecurity and Data Protection Standards". In the course of this workshop, the need to identify and possibly adopt standards by relevant stakeholders already available or under development in the area of Network and Information Security (NIS) was highlighted, towards supporting the EU Digital Single Market and the underlying EU policy and regulatory framework. In that workshop, privacy standards were particularly outlined as an important area (under the broader area of NIS) where further work is needed, in terms of both gap analysis, as well as technical implementation.

Against this background, ENISA, in its 2018 programming document[7] elaborated further on the area of privacy standards. As the Agency has by virtue of its Regulation a role on standards, it is logical that addressing standards associated with privacy is a reasonable extension of its work. The expected outcome of this undertaking is that greater understanding by means of analysis can be reached and that gaps can be

[1] Steve Purser, Standards for Cyber Security, in Hathaway, Melissa (ed.) *Best Practices in Computer Network Defense: Incident Detection and Response*. Vol. 35. IOS Press, 2014.
[2] https://www.enisa.europa.eu/publications/gaps-eu-standardisation
[3] https://www.enisa.europa.eu/publications/definition-of-cybersecurity
[4] https://www.enisa.europa.eu/publications/standardisation-for-smes
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
[6] https://www.enisa.europa.eu/events/enisa-cscg-2017
[7] https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2018-2020

identified in a way that, if conveyed to SDOs, suitable remedies can be put in place. As a result, stakeholders interested in network and information security measures concerning PII, can get better control and enhance their ability to successfully mitigate risks identified.

1.2 Aim and structure of the report

Building on the previous studies of ENISA and considering the developments at legislative, policy, and standardisation level, this study aims to:

- explore how the standards-developing world is responding to the fast-changing, demanding realm of privacy by mapping existing available standards and initiatives in the area and
- provide insights on the "state-of-the-art" of privacy standards in the information security context through a relevant gap analysis.

It is important to stress that, although information security standards have a broader scope than privacy standards, the latter is an essential part of the former. In the context of this report, the focus is mainly on the information security dimension of these standards, while also providing a general description of their overall application area.

To this end, the study provides an overview of existing standardisation initiatives at European Union and international level. At the European level, the study examines the European Standards Organisations (ESOs): CEN, CENELEC, and ETSI [8]. At international level, the focus is on the following organisations: the International Organisation for Standardisation (ISO) and the International Electrotechnical Committee (IEC).

Next, standards are presented per organisation and categories of standard, namely fundamental standards, specifications, guidelines and codes of practice.[9] Moreover, the study presents the results of a gap analysis, which may indicate possible next areas to be considered towards the development or repositioning of standards/ongoing initiatives. The report concludes with a number of additional considerations drawn by the research conducted for the study and the contributors' and reviewers' expertise and engagement in the area of standardisation.

The intended audience of the study is NIS practitioners and relevant MS authorities, while on the other hand it is also meant to serve as a non-binding guidance document for ESO's.

1.3 Methodological approach

Following the discussion on the existing SDO's and working groups, the gap analysis is based on the Privacy Principles provided in the broadly referenced fundamental standard ISO/IEC 29100[10]. This international standard entails a privacy framework comprising of common privacy terminology, actors and roles, privacy safeguarding considerations and privacy principles for information technology. The Privacy Principles have been developed taking into account the privacy principles adopted in different countries and regions, such

[8] See Art.2 (8) and (9) Regulation (EU) 1025/2012 .
[9] https://www.bsigroup.com/en-GB/standards/Information-about-standards/different-types-of-standards/
[10] ISO/IEC 29100:2011 Information technology - Security techniques - Privacy framework

as the Fair Information Principles in the US[11] and the Data Quality principles of the EU data protection legislation,[12] as well as the OECD guidelines on privacy.[13]

Key concepts discussed within the study

Information Security: Preservation of confidentiality, integrity, and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. [14]

Standard: Technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory. [15]

Personally Identifiable Information (PII): Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

Privacy Standard: Standard that includes privacy controls, requirements and/or guidance related to the processing of personally identifiable information. The focus of the study is mainly on the information security dimension of privacy standards.

Privacy Controls: Measures that treat privacy risks by reducing their likelihood or their consequences. According to ISO/IEC 29100: 2011 Privacy controls include organizational, physical and technical measures, e.g., policies, procedures, guidelines, legal contracts, management practices or organizational structures.

[11] The Fair Information Principles were introduced in the US Privacy Act of 1974 (updated in 2015).
[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
OJ L 281, 23.11.1995, p. 31–50
[13] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, updated in 2013), http://oe.cd/privacy [accessed 10 September 2018]
[14] ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary
[15] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC, OJ L 316, 14.11.2012

2. EU context overview

2.1 EU standardisation legal framework

Since 2012, the EU Regulation 1025/2012 provides the legal framework on standardisation in the EU and replaced former Directives addressing aspects of standardisation in the Union[16]. The Regulation, among other issues, established obligations for transparency and stakeholder participation and reformed the framework on standards in support of Union legislation and policies.

With regard to this study, a relevant provision of the Regulation is the one on standardisation requests to the European Standardisation Organisations (ESOs). According to Article 10, the Commission may request (formerly called 'mandate') the ESOs to draft a standardisation deliverable (standard or other deliverable), stating the policy objectives aimed to be achieved with the requested standard. After the ESO accept the request and develop the standard, the Commission together with the ESO, assesses the compliance with the initial request.

The Commission has issued two standardisation requests in relation to privacy: i) The mandate M/289 in support of the European Directive on the protection of individuals with regard to the processing of personal data, published in 1999[17] and ii) The mandate M/530 on privacy management standards for security technologies[18].

2.2 EU legal framework & privacy standards in information security

Standards are often developed in support of Union policy and legislation. In the field of privacy and information security, reference to standards or acknowledgement of their significance has also been introduced in the EU legislative instruments[19]. The overview of the Union legislation (and proposals for legislation), in Table 1 below, outlines the main areas where standards may play a role. However, unless the primary or secondary legislation specifically refers to standards or technical regulations, the application of those is on a voluntary basis[20].

EU LEGISLATIVE INSTRUMENTS/PROPOSALS	ARTICLE NR.	TOPIC
Network and Information Security Directive[21]	Recital 66 Article 14 Article 16	- Harmonised standards for high level of security of network and information systems at Union level. - Standards for security requirements and incident notification

[16] Regulation (EU) No 1025/2012 of the European Parliament and of the Council, OJ L 316/12

[17] http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=167 [accessed 2 September 2018]

[18] http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548 accessed 2 September 2018]

[19] The legislation in this section is provided by means of example and does not aim to be exhaustive or offer in-depth analysis.

[20] See the example of harmonised standards: https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_en [accessed 10 September 2018]

[21] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

EU LEGISLATIVE INSTRUMENTS/PROPOSALS	ARTICLE NR.	TOPIC
	Article 19 Annex I	- Standardised practices for CSIRTs for incident and risk-handling procedures, incident, risk and information classification schemes.
General Data Protection Regulation[22]	Article 12 Article 21 Article 32 Article 33 Article 34 Article 35 Article 40 Article 43	- Standardised Icons - Technical specifications to exercise the right to object - Data security, data breach notification - Data Protection Impact Assessment (DPIA) - Codes of Conduct - Technical standards for data protection certification
Proposal for a Regulation on Privacy and Electronic Communications[23]	Article 8	- Standardised icons for informing users about the collection of information.
Proposal for a Cybersecurity Act[24]	Recital 34 Recital 47 Recital 49 Article 8 Article 46 Article 47	- Standards for risk management and for measurable security of electronic products, systems, networks and services. - Technical standards on cyber security requirements - interoperability standards - Standards for risk management and the security of ICT products and services - Standards for security requirements for operators of essential services and digital service providers

Table 1: EU Legislative Instruments and references to standards and technical specifications overview

[22] 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. See also: https://www.enisa.europa.eu/events/enisa-cscg-2017/presentations/kamara [accessed 2 September 2018]

[23] Since the legislative reform is ongoing, we refer to the Commission's proposal. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC

[24] Since the legislative reform is ongoing, we refer to the Commission's proposal. Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM (2017) 477 final

3. International privacy standards for information security: ISO/IEC

3.1 Introduction

General privacy standardisation in the field of Information Technology is within the Scope of ISO/IEC JTC 1/SC 27 IT Security Techniques (SC 27). SC 27 is a subcommittee of the Joint Technical Committee 1 (JTC 1) of ISO and IEC, scoped to address Information Technology. Within the SC 27, a number of standards of relevance to the field of privacy have been developed within ISO/IEC JTC 1SC 27/WG 5 - the Working Group on Identity Management, Privacy and Biometrics. While this Working Group (WG) takes on a specific privacy perspective, its neighbouring Working Groups (WGs 1-4, see Figure 1 below), may also include privacy topics, although typically with a more security oriented viewpoint.

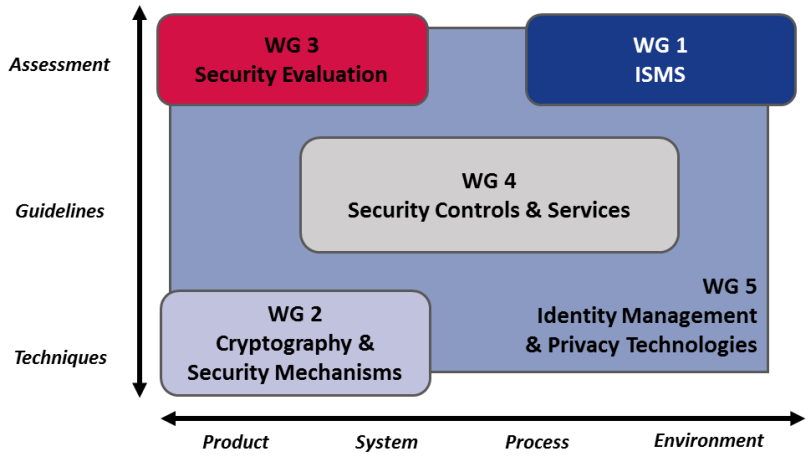

Figure 1: ISO/IEC JTC 1/SC 27 IT Security Techniques working groups overview

It should be noted, that the general understanding is that these fields are interconnected by way of overlapping areas; i.e. there are areas of security standards with relevance to privacy and vice versa. The following overview of activities is mainly derived from the aforementioned Working Groups, which mostly take a generic approach towards the topic of privacy. It should be noted however, that there are numerous sectorial efforts, which have been looking at several related topics and need to be taken into account, when working in the respective areas. For reasons of brevity, only a limited number of those standards are mentioned in this study.

It is helpful to understand the process, i.e. the different steps often followed in developing an international standard. New projects are often prepared with a six to twenty-four months Study Period (SP) which may deliver a formal New Work Item Proposal (NWIP). This form also entails a table of contents, some example clauses, and often a preliminary working draft for the project. After approval of such a proposal, the project evolves via several Working Drafts (WDs), where expert opinions on the text are exchanged and incorporated. If the project is considered sufficiently stable, it will then be progressed to become a Committee Draft (CD). At this stage further technical comments submitted as agreed upon by the corresponding mirror committees of National Bodies will be taken into consideration. If the Committee Draft meets sufficient consensus a Final Draft International Standard (FDIS) is produced to resolve any remaining editorial issues, before an International Standard is published.

The ISO may opt to produce Technical Specifications in cases where a field has not sufficiently matured for a standard, as well as Technical Reports providing any other information of relevance, that are not standards and specifications. While the aforementioned process is used, applicable directives allow for deviations, such as omitting certain stages, including – in some cases - to directly table a FDIS under the "fast track" procedure.

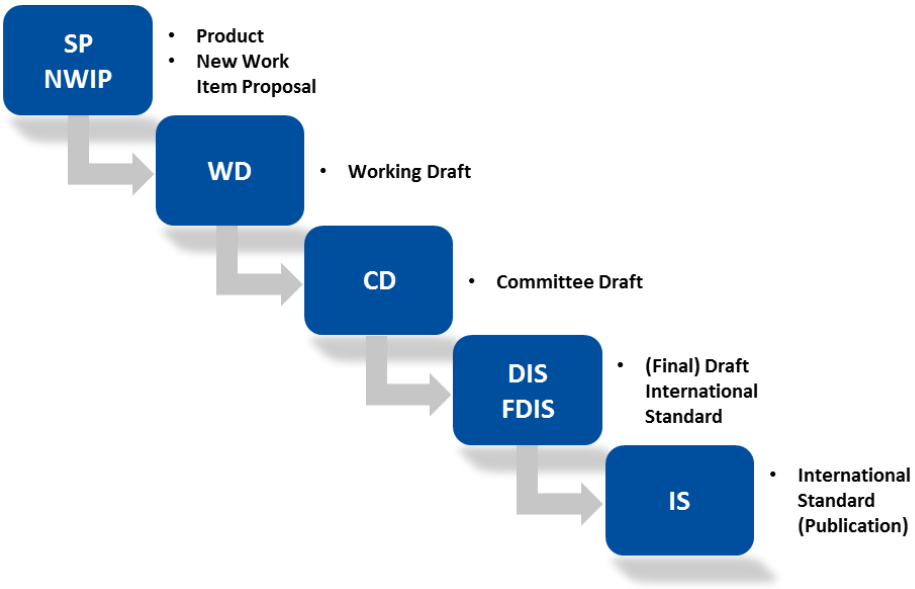

Figure 2: Standards development process in ISO and ISO/IEC JTC 1

3.2 Privacy-focused standards

The privacy-focused standards of WG 5 are generally making use of the privacy principles presented earlier in section 1.3. As such, many of the projects can be allocated to different categories of documents, such as: i) general frameworks, ii) management standards and iii) standards more focussed on the implementation aspects, or supporting documents as illustrated in Figure 3 below.

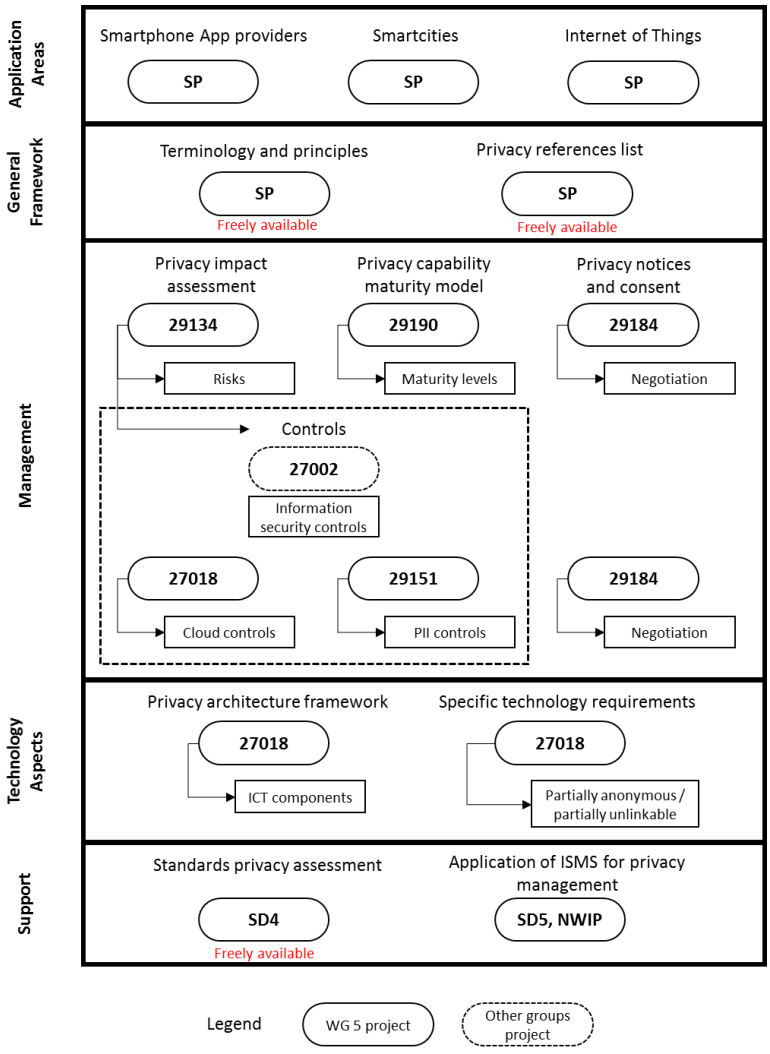

Figure 3: Overview of some Standards with Privacy Relevance in ISO/IEC JTC 1/SC27/WG 5 and their relationships

3.2.1 Framework documents

The most relevant framework document in WG 5 in the context of this report is ISO/IEC 29100 – Privacy Principles, as described and outlined above (1.3).[25] The document is freely available[26] under the ISO

[25] It may be important to note, that the main achievement of 29100 lies not so much within the development of privacy principles, which are also enshrined in many other documents, such as the OECD-Guidelines on Privacy, but in laying a sound policy foundation for the later work in international standardisation.

[26] http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html (2018-10-20)

Customer License Agreement[27]. Equally, WG 5 maintains – upon updates by its members – a list of privacy references as their Standing Document 2[28].

3.2.2 Privacy management

A number of standards address privacy management from different perspectives. For example, the ISO/IEC 29190:2015 provides a "Privacy capability assessment model", which was the first ISO standard to transfer the underlying concept of continuous quality control in the context into privacy management.

Later standards, such as the ISO/IEC 29151:2017 – "Code of practice for personally identifiable information protection", establish a closer link with Information Security Management Systems, by describing "control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of Personally Identifiable Information (PII)."[29] The latter standard is based on ISO/IEC 27002, "taking into consideration the requirements for processing PII which may be applicable within the context of an organization's information security risk environment(s)."[30]

Recently ISO/IEC 27552 – "Privacy-specific application of ISO/IEC 27001 Requirements (PIMS)", which is still under development, "provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS)"[31], which is also supposed to extend ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization. It is targeted towards PII controllers and PII processors, and intends to provide mechanisms for conformity assessment.

ISO/IEC 29134:2017 – Privacy Impact Assessment – Methodology allows for an assessment taking into account either of the above standards and it "gives guidelines for a process on privacy impact assessments (PIA), and a structure and content of a PIA report".[32]

Finally, some Identity Management related standards may also provide guidance in this context, such as:

- ISO/IEC 24760 A framework for identity management
- ISO/IEC 29115 Entity Authentication Assurance Framework
- ISO/IEC 29146 A framework for access management

3.2.3 Technical implementation of privacy

One of the first published standard highlighting some technical aspects is the ISO/IEC 29101:2013 – Privacy architecture framework, which "specifies concerns for ICT systems that process PII; lists components for the implementation of such systems; and provides architectural views contextualizing these components"[33]. Currently, it is being supplemented by the Technical Recommendation ISO/IEC 27550 – Privacy engineering for system life cycle processes, which is supposed to be published within 2019. ISO/IEC 27550 will describe "*the relationship between privacy engineering and other engineering viewpoints (system engineering, security engineering, risk management); and privacy engineering activities in key engineering processes such as knowledge management, risk management, requirement analysis, and*

[27] https://www.iso.org/terms-conditions-licence-agreement.html#Customer-Licence (2018-10-20)
[28] WG 5 Standing Document 2 (SD2) -- Privacy references list online https://www.din.de/en/meta/jtc1sc27/downloads (2018-10-20)
[29] ISO/IEC 29151: 2017, Scope section.
[30] As above.
[31] ISO/IEC 27552, Scope section of the 2nd CD.
[32] ISO/IEC 29134:2017, Scope section.
[33] ISO/IEC 29101 Privacy architecture framework, Scope section.

architecture design"[34]. The fact that it was developed as a technical recommendation also supports the assumption that privacy engineering is still a field in its early days, where only few common best practises have evolved. However, compliance requirements are now an accelerating development of the field.

However, there are some specific technology oriented standards available, e.g. ISO/IEC 29191 Requirements for partially anonymous , partially unlikable authentication, and ISO/IEC 27551 requirements for attribute based unlikable entity authentication – currently at WD stage, and finally ISO/IEC 20889 Privacy enhancing data de-identification techniques which "*specifies terminology, a classification of de-identification techniques according to their characteristics, and their applicability for reducing the risk of re-identification*"[35].

Lastly, there is also work under preparation, transferring a national standard on conceptualizing deletion of PII, including but not limited to an approach for "*defining deletion/de-identification rules in an efficient way, a description of required documentation, and a definition of roles, responsibilities and processes*"[36].

3.2.4 Examples of sector-specific privacy standards

There are also a number of projects within WG5 and beyond that address sector specific requirements for privacy, such as:

- 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
- ISO/IEC 27570 Privacy guidelines for smart cities.
- ISO/IEC 17030 Guidelines for security and privacy in Internet of Things (IoT)
- ISO/IEC 29184 Guidelines for online privacy notices and consent

The last three are still under development, but nearing publication.

3.3 Information security management systems standards with privacy relevance

Beyond the privacy-focused standards outlined in the previous section, ISO and IEC have been developing information security standards that, while not focused on privacy as such, are relevant for privacy in a broader context.

3.3.1 Generic information security management standards

A list of information security management standards with a broad application area is presented below.

- ISO/IEC 27000 Information security management systems - Overview and Vocabulary
- ISO/IEC 27001 Information security management systems – Requirements
- ISO/IEC 27005 Information security risk management
- ISO/IEC 27006 Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007 Information security management systems - auditor guidelines

[34] ISO/IEC 27550 – Privacy engineering for system life cycle processes, Scope section.
[35] ISO/IEC 20889 Privacy enhancing data de-identification techniques, Scope section.

[36] NWIP on Developing a PII deletion concept in organizations, Scope.

- ISO/IEC 27008 Guidelines for the assessment of information security controls
- ISO/IEC 27009 Sector-specific application of ISO/IEC 27001 – Requirements
- ISO/IEC 27013 Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014 Governance of information security

3.3.2 Examples of sector-specific information security management standards

A list of information security management standards with a more sector specific application area is presented below.

- ISO/IEC 27002 Code of practice for information security controls
- ISO/IEC 17030 Guidelines for security and privacy in Internet of Things (IoT)
- ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services

3.4 Security evaluation standards with privacy relevance

Similarly to the information security management system standards, we can find security evaluation standards with privacy references or relevance at large, especially in relation to data security measures. A list of security evaluation standards with privacy relevance is presented below:

- ISO/IEC 15408 Evaluation criteria for IT security
- ISO/IEC 18045 Methodology for IT security evaluation
- ISO/IEC 19608 Guidance for developing security and privacy functional requirements based on ISO/IEC 15408

3.5 Standards on the implementation of security techniques with privacy relevance

To comply with the eleven privacy principles technical mechanisms and functions are necessary. For example, anonymization is mandatory and attribute based credentials are key technologies to support privacy management. The promise of homomorphic encryption may allow for suitable privacy geared calculations without compromising confidentiality. Crypto mechanisms are supporting privacy implementation, while key management procedures may be included in the scope of a Privacy Impact Assessment (PIA)/ Data Protection Impact Assessment (DPIA).

Many of these techniques are based on cryptographic techniques and a few examples are listed hereinafter[37]:

- ISO/IEC 18033 Encryption algorithms
- ISO/IEC 18370 Blind digital signatures
- ISO/IEC 20008 Anonymous digital signatures
- ISO/IEC 20009 Anonymous entity authentication
- ISO/IEC 29191 Partially anonymous partially unlinkable authentication
- ISO/IEC 20889 Privacy enhancing data de-identification techniques
- ISO/IEC 27551 Attribute based unlinkable entity authentication (This document provides a framework and establishes requirements for attribute-based unlinkable entity authentication.)

[37] For more information see ISO/IEC JTC1/WG2 work plan and standards

3.6 Privacy by default and consumers interests

The Copolco committee[38] (ISO's Committee on consumer policy) has initiated a new project committee (PC 317) on "Consumer protection: privacy by design for consumer goods and services". However, at the time of preparing this study, this Committee has only been approved by the Technical Management Board of ISO, and is only on its way to establishing its scope and timeline, which limits actual results. However, in view of its apparent close relationship to the topics of this study, the work of this Committee should be taken into account in the future. In order to avoid duplication of efforts a liaison has been requested between JWG8 and with ISO/IEC JTC1/SC27.

[38] https://www.iso.org/copolco.html

4. European privacy standards

4.1 Introduction

In the EU there are three standardisation bodies, which work independently of each other; CEN and CENELEC on the one hand and ETSI on the other hand.

In 2011, CEN, CENELEC and ETSI set up the Cyber security coordination group (CSCG) to identify overlaps, gaps and limitations in coordination in European Cybersecurity standardisation. ETSI left the group in 2015 and in 2016, this group was renamed to the CEN CENELEC Focus group. This focus group, which was established for a limited period, was disbanded in 2018 and further integrated in WG1 of the newly created CEN CENELEC JTC13.

4.2 Standardisation request M/530

In 2014, the European Commission issued mandate M/530 on standardisation, a request addressed to the European standardisation organisations in support of the implementation of privacy and personal data protection management in the design and development and in the production and service provision processes of security technologies.

This mandate was prepared by DG HOME, after consultation with relevant stakeholders, including the European Data Protection Supervisor, and information security industry representatives.

4.2.1 CEN and CENELEC

To respond to the mandate, CEN and CENELEC created in 2015 a Joint working group between CEN and CENELEC named JWG8[39]. JWG8 proposed to the Technical Board to prepare three deliverables:

- WI 001- Data protection by design and by default (type of deliverable: EN)
- WI 002- Video surveillance (CEN/ TR)[40]
- WI 003- Biometric for access control including face recognition (CEN/TR)

Within its scope, JWG8 has proposed to recognize ISO/IEC 29134 (privacy impact assessment Methodology) as a European standard (EN).

4.2.2 ETSI

ETSI on its side also prepared the following deliverables as a contribution to the mandate:

- DTR/CYBER-0010, TR 103 370, Practical introductory guide to privacy
- DTS/CYBER-0013, TS 103 485, Mechanisms for privacy assurance and verification
- DTS/CYBER-0014, TS 103 486, Identity management and naming schema protection mechanisms
- DTS/CYBER-0020, TS 103 458, Application of Attribute Based Encryption (ABE) for data protection on smart devices, cloud and mobile services

[39] Initially, ETSI also participated in the JWG8

[40] CEN TR stands for CEN Technical Report, which are informative documents providing information on the technical content of standards. https://www.cen.eu/work/products/TR/Pages/default.aspx [accessed 10 September 2018]

4.3 ETSI TC Cyber

The ETSI Technical Committee Cyber (TC Cyber), created in 2014, was designated by ETSI Board as the coordinator of the work to be handled to fulfil the EC mandate. TC Cyber has identified several privacy topics as a priority domain to be tackled by ETSI.

4.4 CEN CENELEC new TCs on privacy and cybersecurity

In addition to the above activity, CEN and CENELEC decided in 2017 to set up a new Technical Committee to handle in a more generic basis data protection and privacy by design and by default (CEN/CENELEC JTC13). This newly created Committee has several objectives:

- Import relevant ISO/IEC JTC1 SC27 standards and create European standards following the Vienna agreement. The following standards were identified as potential candidates : ISO/IEC 27006, ISO/IEC 27007, ISO/IEC 27008, ISO/IEC 27010,ISO/IEC 27011, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27019, ISO/IEC 15408, ISO/IEC 18045, ISO/IEC 19790, ISO/IEC 30111,ISO/IEC 29147, ISO/IEC 19608
- Act as a European mirroring committee to SC27 with according structure:
    - WG1 Advisory group
    - WG2 Management systems
    - WG2 evaluation and certification systems
    - WG4 Applications
    - WG5 Privacy
    - WG6 Products security
- Integrate JTC8 To JTC13 WG5
- Develop necessary Complementary standards to fulfil European regulations and mandates.

5. Privacy information security standards: Gap analysis

This section provides a gap analysis and mapping of standards mentioned earlier to the ISO/IEC 29100 Privacy Principles. Following this analysis, the main points raised are discussed in Section 6.

5.1 Principle #1: Consent and choice

With regard to online services, the consent and choice principle is covered by ISO/IEC 29184 (draft) outlining possibilities to present PII principal's choice, obtain their consent, providing them prior information, etc. Both, consent and choice are decisions taken by the data subject consciously also assessing the security profile of the data processor, therefore the due application of the standard is important.

5.2 Principle #2: Purpose legitimacy & specification

Concerning online services, the purpose legitimacy and specification principle is addressed by ISO/IEC 29184 (draft), outlining possibilities to communicate the purposes to the PII principal before PII collection and the linguistic style used. Clearly the security of PII needs to be properly spelled out.

5.3 Principle #3: Collection limitation

At European level, EN 'Data protection and privacy by design and by default' (M/530), being developed by CEN-CENELEC/JTC 8 (and to be maintained by JTC 13/WG 5), covers the collection limitation principle, as it has a direct impact on design and development of data processing activities. Moreover, draft ISO/IEC 27550 includes engineering practices that reduce the collection of PII. Both of these standards are supported by a terminology on de-identification techniques defined in ISO/IEC 20889, thereby indirectly covering the collection limitation principle.

ISO/IEC 29191, 27551 (draft), ETSI/TS 103 458 (draft) cover partial anonymisation and unlinkability, attribute based unlinkability and encryption, respectively, generating information sources that can render PII collection unnecessary. Indirectly, collection limitation is covered by ISO/IEC 24760, 29115, ETSI/TS 103 486 (draft) providing the framework for the management and assurance of identity and authentication standards such as those dealing with anonymisation, unlinkability and attribute based encryption. With regard to IoT and smart cities, respectively, the collection limitation principle is included in draft ISO/IEC 27030 and 27570.

5.4 Principle #4: Data minimisation

The European Standard "Data protection and privacy by design and by default" (M/530) covers the data minimisation principle, as it has a direct impact on design and development of data processing activities (e.g. the limitation of linkability of PII collected). Moreover, draft ISO/IEC 27550 includes engineering practices that minimise the processing of PII. Both of these standards are supported by a terminology on de-identification techniques defined in ISO/IEC 20889, thereby indirectly covering the data minimisation principle.

ISO/IEC 29191, 27551 (draft), ETSI/TS 103 458 (draft) cover partial anonymisation and unlinkability, attribute based unlinkability and encryption, respectively, generating options for interactions and transactions not requiring identification of PII principals, reduce the observability of their behaviour, etc. Indirectly, data minimisation is covered by ISO/IEC 24760, 29115, ETSI/TS 103 486 (draft) providing the framework for the management and assurance of identity and authentication standards such as those

dealing with anonymisation, unlinkability and attribute based encryption. With regard to IoT and smart cities, respectively, the data minimisation principle is included in draft ISO/IEC 27030 and 27570.

5.5 Principle #5: Use, retention, and disclosure limitation

EN 'Data protection and privacy by design and by default' (M/530) covers the use, retention and disclosure limitation principle, as it has a direct impact on design and development of data processing activities. Moreover, draft ISO/IEC 27550 includes engineering practices that reduce the use, retention period and disclosure of PII. Both of these standards are supported by a terminology on de-identification techniques defined in ISO/IEC 20889, thereby indirectly covering the use, retention and disclosure limitation principle.

ISO/IEC 29191, 27551 (draft), ETSI/TS 103 458 (draft) cover partial anonymization and unlinkability, attribute based unlinkability and encryption, respectively, preventing the use of PII from being linked across different purposes and providing options for anonymising PII after the stated purposes for their retention have been fulfilled. Indirectly, the use, retention and disclosure limitations are covered by ISO/IEC 24760, 29115, ETSI/TS 103 486 (draft) providing the framework for the management and assurance of identity and authentication standards such as those dealing with anonymisation, unlinkability and attribute based encryption. With regard to IoT and smart cities, respectively, the use, retention and disclosure principle is included in draft ISO/IEC 27030 and 27570.

5.6 Principle #6: Accuracy & quality

ISO/IEC 27000 and 27001 and 27005, 27006, 27007, partly cover vocabulary, requirements and risks and auditing/certification requirements, auditing guidelines, respectively, for the management of accuracy and quality of information including PII. Moreover, ISO/IEC 27002, 27008, 27014, 27017, 15408, 18045 in part include controls and assessment of controls and governance and cloud-specific controls and evaluation criteria and evaluation methodology, respectively, for accuracy and quality.

Indirectly, accuracy and quality is covered by ISO/IEC 27009, 27013, specifying sectorial use of International Standard 27001 (which according to ISO/IEC language includes the privacy sector). With regard to IoT and smart cities, respectively, the accuracy and quality principle is included in draft ISO/IEC 27030 and 27570.

5.7 Principle #7: Openness, transparency & notice

With regard to online services, the openness, transparency, and notice principles are covered by ISO/IEC 29184 (draft), outlining possibilities to provide PII principals information about the controller's policies, procedures and practices, the purposes, types of recipient privacy stakeholders, the controller's identity, the PII principal's means of participation and access and other notices.

5.8 Principle #8: Individual participation & access

In relation to online services, the individual’s participation and access principle is covered by ISO/IEC 29184 (draft), outlining options to enable PII principals to access, correct and remove PII, to communicate such actions to third parties, and to securely establish procedures for exercising the rights of PII principals.

5.9 Principle #9: Accountability

Concerning privacy management systems, ISO/IEC 27552 provides a framework extending the existing ISMS standards. Furthermore, ISO/IEC 19608 (draft), 27018, 29134, ETSI/TS 103 485 (draft) cover the management of privacy-related practices within an organisation and PII in cloud computing and privacy impact assessments and assurance mechanisms, respectively. Indirectly, accountability, which is a trust invoking measure, is covered by ISO/IEC 29101, 29151, 29190 specifying the privacy principles defined in

International Standard 29100, whereas ETSI/TR 103 370 (draft) lists and classifies the most relevant ISO/IEC privacy standards.

5.10 Principle #10: Information security

ISO/IEC 27000 and 27001 and 27002 and 27005, 27006, 27007, cover information security management vocabulary and requirements and controls and risks and auditing/certification requirements, auditing guidelines, respectively. Moreover, ISO/IEC 27002, 27008, 27014, 27017, 15408, 18045 include controls and assessment of controls and governance and cloud-specific controls and evaluation criteria and evaluation methodology, respectively, for information security.

At European level, EN 'Data protection and privacy by design and by default' (M/530) covers the information security principle, as it has a direct impact on design and development of data processing activities (e.g. implementing controls in proportion to likelihood and severity of potential consequences, sensitivity of PII, and number of possible PII principals). Moreover, draft ISO/IEC 27550 includes engineering practices that support information security from the point of view of the PII principal. Both of these standards are supported by a terminology on de-identification techniques defined in ISO/IEC 20889, thereby indirectly covering the information security principle.

Indirectly, information security is covered by ISO/IEC 27009, 27013 specifying sectorial use (which according to ISO/IEC language includes the privacy sector) and implementation of, respectively, International Standard 27001. With regard to IoT and smart cities, respectively, the information security principle is included in draft ISO/IEC 27030 and 27570.

5.11 Principle #11: Privacy compliance

The dedicated privacy management system currently being developed in ISO/IEC 27552 includes aspects of privacy compliance verification. Besides, ISO/IEC 19608 (draft), 27018, 29134, ETSI/TS 103 485 (draft) cover the verification of privacy-related practices within an organisation and PII in cloud computing and privacy impact assessments and verification mechanisms, respectively. Indirectly, privacy compliance is covered by ISO/IEC 29101, 29151, 29190 operationalising and in an information security context, specifying the privacy principles that have been defined in International Standard 29100; ETSI/TR 103 370 (draft) categorises the most relevant ISO/IEC privacy standards.

At European level, EN 'Data protection and privacy by design and by default' (M/530) covers the privacy compliance principle, as it needs to be verified, supervised and demonstrated that the design and development of data processing activities meets the legal data protection and privacy requirements based on the associated risks for PII protection (particularly Article 25 GDPR “Data protection by design and by default”).

6. Further considerations and recommendations

Following the overview of existing standardization initiatives at EU and International level, the gap analysis and mapping of them against the privacy principles, this section presents some findings of this exercise, derives some key conclusions and makes relevant proposals and recommendations. The non-exhaustive list of considerations and recommendations aims to prioritise potential areas of action for the near future.

6.1 International vs. European standards

The activity of the international standard-setting organisations is rapidly growing in a way that seeks to keep up with their prominence and importance in a changing privacy and cybersecurity policy landscape. European Standards Organisations often adopt international standards as European ones, based on the premise that ESOs do not need to re-invent the wheel. The adoption of international standards however often takes place in the absence of thorough examination on whether the needs of the Europe-based industry, market, and the EU legislation require standards tailored to the European reality. Since the references to standards in the Union legislation are becoming more regular, and there are considerable differences of Union privacy and security regulations with other jurisdictions, the need for analysis of mapping of international standards and European regulatory requirements is intensified.

As a significant set of requirements in the area intersecting privacy and cybersecurity currently originates from the EU it is logical that the standardisation efforts in this area need to be led and guidance needs to be made available by ESOs active in the field. In this case, it is reasonable to expect that ESOs will drive standards development for the internal EU market.

EU policy makers and European Standards Organisations should promote the development of European input to privacy and cybersecurity standards. While leadership is needed, to drive standardization efforts in this area, the stakeholders' need to be provided with guidance might be met with private initiatives from beyond the EU. In addition, the aforementioned stakeholders should also establish a mechanism to assess the viability of adopting international standards with European (legal) requirements and filter international efforts to match EU levels.

ESOs should develop dependable privacy and security-centric mechanisms and associated pools of experts to support them, for the purpose of assessing the adoption of international standards and their alignment with European legal requirements and market needs. The existence of stable mechanisms and experts pools would guarantee consistency in the long-term and ensure avoidance of overlap of standards. Furthermore, such practice would identify potential overlap even among European standards developed by CEN and CENELEC on the one hand, and ETSI on the other.

In the absence of EU initiatives and leadership in this area there is a growing risk of de facto standardisation of practices via market consolidation as innovative EU-based service providers may gradually be consolidated in non-EU-led groups of companies.

6.2 Standardisation and conformity assessment mechanisms in information security

Proving compliance with privacy standards in information security is not as straightforward as one would expect . While there are some approaches for conformity assessment available in specific sectors, others are still lacking appropriate mechanisms. An example is the way in which the proposed EU cybersecurity certification framework proposal under the Cybersecurity Act is likely to work out in practice; how different approaches are likely to be combined and put to use. In addition, as shown in the gap analysis, privacy and information security standards adopt different approaches with regard to the privacy principles of the ISO/IEC 29100 and their implementation. High-level principles often leave room for interpretation in individual cases. There is therefore a need for coordinated guidance in that respect.

EU policy makers and European Cybersecurity Certification Group members should promote the endorsement and adoption of privacy and information security standards, including conformity assessment standards specific to privacy matters.

One recommendation to the above issue would be to incorporate privacy and information security standards into the upcoming Cybersecurity Certification Framework. This approach can offer better positioning that improves on the current sectorial-based approach.

EU policy makers and European Standards Organisations should further promote coordination and collaboration with a range of stakeholders throughout the process of standards developments and standardisation activity.

Coordination and collaboration with a range of stakeholders throughout the standardisation activity as well as the development of conformity assessment schemes are necessary to meet various types of expectations. In addition, easier direct participation of stakeholders to complement participation via national only committees could also be considered.

6.3 Selection, agreement, and prioritisation of standardization activities

The example of the Joint Working Group 8, and the subsequent split of the mandated work in to two different groups at CEN/CENELEC on the one hand and ETSI on the other hand, clearly shows that issues pertaining to selection, agreement, and prioritisation of standardisation activities may arise. A consistent analysis of sector-specific needs for privacy standardisation is essential, especially in the context of information security, before moving ahead with the adoption or development of new standards. Such an analysis might lead to the identification of common issues that may be addressed with baseline cross-sector standards, and additional issues to be dealt in sector-specific standards.

EU bodies and competent authorities in the Member States should promote the adoption of a structured approach on the analysis of sector-specific needs with regard to privacy standardisation, especially in information security context and then proceed with the adoption or development of new standards.

Relevant regulatory authorities, e.g. in the areas of privacy, cybersecurity, telecommunications etc, need to be involved further in standardisation activities, e.g. in defining, endorsing, or affirming potential standardisation goals in the areas of privacy and information security. This could be done in several manners by means of standardisation requests pursuant Art. 10 Regulation 1025/2012, EU policy documents with clear objectives explicitly referring to standardisation, but also via research, namely by aligning relevant aspects of the new Framework Programme. A joint agenda meeting the needs of regulatory authorities across the board in the policy areas of privacy, cybersecurity and telecommunications needs to be set up and coordination across all of them needs to take place at MS and EU levels.

EU policy makers and relevant EU bodies need to be further involved in the standardisation process, so as to define, endorse or affirm potential standardisation goals in the areas of privacy and information security.

6.4 The role of technology and privacy by design

As discussed in chapters 3 and 4, much of the standardisation activity is focused on standardisation of technological solutions. Among those solutions, many address the introduction of privacy-preserving technologies throughout the whole lifecycle of a product or a system. Many stakeholders, ranging from regulators, consumers, to the industry have acknowledged the value of privacy by design. In a recent opinion, the European Data Protection Supervisor made a pledge for Privacy by design to be treated as a landmark for values driven technology development[41]. Despite a general common agreement on the value of privacy by design, the concept and its implementation are still not clearly elucidated in standardization activities.

Competent bodies at EU and Member State level should further promote their research and standardisation activities to support the realization of Privacy by Design principle.

Continuous research on Privacy by Design is valuable, as well as platforms where experts can exchange knowledge on the latest technological developments such as the EDPS Internet Privacy Engineering Network (IPEN).[42] Standardisation of aspects of Privacy by Design would also prove to be helpful, in terms of making technology accessible to a broader audience. A good example of such initiative is the recently developed ISO Committee on Consumer protection and privacy by design for consumer goods and services.[43]

[41] EDPS Opinion on Privacy by Design 2018, p.19.
[42] Read more: https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en [accessed 10 September 2018].
[43] ISO/PC 317 https://www.iso.org/committee/6935430.html [accessed 10 September 2018]

7. Bibliography

- Bock, Kirsten 'Data protection certification: Decorative or effective instrument? Audit and seals as a way to enforce privacy' In *Enforcing Privacy,* pp. 335-356. Springer, Cham, 2016.
- CEN/ISSS Initiative on Privacy Standardization in Europe, Final Report, 2002.
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50
- European Commission, M/436 Standardisation mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of information and communication technologies applied to radio frequency identification (RFID) and systems.
- European Commission, M/530 Commission Implementing Decision 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 (2015), 102 final of 20.1.2015
- European Data Protection Supervisor, 'Preliminary Opinion on Privacy by Design 5/2018', (2018), https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf [accessed 10 September 2018]
- ISO/IEC JTC 1/WG 5 Standing Document 1, https://isotc.iso.org/livelink/livelink?func=ll&objId=9384365&objAction=browse&sort=name [accessed 10 September 2018]
- Kamara, Irene, 'Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'', in European Journal of Law and Technology, Vol 8, No 1, 2017
- Mitrakas, Andreas. 'The emerging EU framework on cybersecurity certification' Datenschutz und Datensicherheit-DuD 42, no. 7 (2018): 411-414.
- OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, updated in 2013)
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC
- Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act''), COM (2017) 477 final
- Purser Steve, 'Standards for Cyber Security', in Hathaway, Melissa (ed.) *Best Practices in Computer Network Defense: Incident Detection and Response*. Vol. 35. IOS Press, 2014.
- 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.
- Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and

2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC, OJ L 316, 14.11.2012

- US Privacy Act of 1974, 5 U.S.C. § 552a (updated in 2015).
- Winn, Jane K. "Technical standards as data protection regulation." in Gutwirth et al. (eds.) *Reinventing Data Protection?* pp. 191-206. Springer, Dordrecht, 2009.
- WTO Agreement on Technical Barriers to Trade, Annex 1A WTO Agreement, 1868 U.N.T.S. 120 (1994)

Annex A: ISO/IEC 29100 privacy principles overview

#	PRIVACY PRINCIPLE	BRIEF EXPLANATION[44]
1	Consent and Choice	• Presenting to the PII principal the choice whether or not to allow the processing of their PII except where the PII principal cannot freely withhold consent or where applicable law specifically allows the processing of PII without the natural person's consent. The PII principal's choice must be given freely, specific and on a knowledgeable basis.
2	Purpose Legitimacy & Specification	• Ensuring that the purpose(s) complies with applicable law and relies on a permissible legal basis; • Communicating the purpose(s) to the PII principal before the time the information is collected or used for the first time for a new purpose;
3	Collection Limitation	• Limiting the collection of PII to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s).
4	Data Minimisation	• Minimizing the PII which is processed and the number of privacy stakeholders and people to whom PII is disclosed or who have access to it
5	Use, Retention, and Disclosure Limitation	• Limiting the use, retention and disclosure (including transfer) of PII to that which is necessary in order to fulfil specific, explicit and legitimate purposes; retaining PII only as long as necessary to fulfil the stated purposes, and thereafter securely destroying or anonymizing it.
6	Accuracy & Quality	• Ensuring that the PII processed is accurate, complete, up-to-date (unless there is a legitimate basis for keeping outdated data), adequate and relevant for the purpose of use; • Ensuring the reliability of PII collected from a source other than from the PII principal before it is processed;
7	Openness, Transparency, & Notice	• Providing PII principals with clear and easily accessible information about the PII controller's policies, procedures and practices with respect to the processing of PII; • Including in notices the fact that PII is being processed, the purpose for which this is done, the types of privacy stakeholders to whom the PII might be disclosed, and the identity of the PII controller including information on how to contact the PII controller;
8	Individual Participation & Access	• Giving PII principals the ability to access and review their PII, provided their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law; • Allowing PII principals to challenge the accuracy and completeness of the PII and have it amended, corrected or removed as appropriate and possible in the specific context; • Providing any amendment, correction or removal to PII processors and third parties to whom personal data had been disclosed, where they are known; and • Establishing procedures to enable PII principals to exercise these rights in a simple, fast and efficient way, which does not entail undue delay or cost.

[44] For extensive explanation, see ISO/IEC 29100 (publicly available: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html [accessed 10 September 2018]).

#	PRIVACY PRINCIPLE	BRIEF EXPLANATION[44]
9	Accountability	• Among others: documenting and communicating as appropriate all privacy-related policies, procedures and practices & assigning to a specified individual within the organization, the task of implementing the privacy-related policies, procedures and practices.
10	Information Security	• Protecting PII under its authority with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the PII, and protect it against risks such as unauthorized access, destruction, use, modification, disclosure or loss throughout the whole of its life cycle.
11	Privacy Compliance	• Verifying and demonstrating that the processing meets data protection and privacy safeguarding requirements by periodically conducting audits using internal auditors or trusted third-party auditors

Table 2: ISO/IEC 29100 privacy principles overview

Annex B: Brief overview of standards developing organisations

This annex provides an overview of Standard Developing Organizations (SDOs) working on the development of privacy and data protection standards.

International Organisation for Standardisation (ISO)

The ISO is a non-governmental organisation, operating under the Swiss law. ISO develops international standards through its Technical Committees. Today, approximately 160 national standardisation bodies are members of ISO and collaborate in over 750 Technical Committees. The ISO standards are voluntary, even though it is also possible they sometimes carry more weight than a mere voluntary agreement; international standards may be required to be followed as in the case of the World Trade Organisation (WTO)[45] Barriers to Trade Agreement or referenced in regional or national legislation.[46] ISO, together with IEC, has a longstanding tradition in developing information security standards, the framework of the Joint Technical Committee 1 (JTC 1) on information technology standards.

International Electrotechnical Committee (IEC)

While the ISO work spans over a range of fields, the IEC is focused on international standards for electrical, electronic, and related fields. IEC is a non-for-profit, quasi-governmental organisation, with National Committees (one per country) as members.[47] Unlike ISO, the IEC also offers conformity assessment via the Conformity Assessment Board.[48]

International Telecommunication Union (ITU)

The International Telecommunication Union is a United Nations' specialized agency, working on the development of voluntary recommendations (standards) for the telecommunication sector. ITU has numerous publications on cybersecurity and Internet of Things that often address privacy aspects.

European Committee for Standardisation (CEN)

CEN is one of the three European Standardisation Organisations (ESO). CEN is set up as an association under the Belgian law. Participation in CEN is based on national representation, via the national standardization bodies of the European Union Member States, and other countries participating in the European Single Market, such as Switzerland and Turkey. CEN develops consensus-based voluntary European standards (EN), but also other deliverables of softer nature in the form of CEN Workshop Agreements.[49] Approximately 1/3 of the CEN's European Standards are developed in response to standardization requests coming from the European Commission.[50] CEN has been working on privacy standards since 1997, when the CEN Information Society Standardization System (CEN/ISSS) was established. The CEN/ISSS was focused on Information and

[45] WTO Agreement on Technical Barriers to Trade: https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm [accessed 2 September 2018]
[46] See for example Art. 43 Regulation (EU) 679/2016
[47] See http://www.iec.ch/about/?ref=menu [accessed 2 September 2018]
[48] See https://www.iso.org/conformity-assessment.html [accessed 2 September 2018] Read more about the conformity assessment activities of IEC: http://www.iec.ch/about/activities/conformity.htm [accessed 2 September 2018]
[49] Read more about CEN Workshop Agreements: https://www.cen.eu/work/products/CWA/Pages/default.aspx [accessed 2 September 2018]
[50] https://www.cen.eu/you/EuropeanStandardization/Pages/default.aspx [accessed 2 September 2018]

Communication Technologies (ICT), with a working group on privacy and data protection.[51] Recently, CEN created a new Technical Committee on Data Protection, as elaborated later in this Report.

European Committee for Electrotechnical Standardisation (CENELEC)

CENELEC is a non-for profit organisation operating under the Belgian law. It develops voluntary standards in the field of electrotechnical engineering and collaborates closely with the IEC. Like CEN, the participation in CENELEC is through national representation. The IEC is mainly involved in privacy and data protection related standards in the information security context through its collaboration with CEN. An example is the Standardisation request by the European Commission M/530 to develop privacy management standards for security technologies.[52]

European Telecommunications Standards Institute (ETSI)

ETSI is a non-for-profit organisation established in France. Stakeholders-members of ETSI may join ETSI's standardisation work via direct participation. In addition, the standards developed by ETSI are made publicly available free of charge. ETSI develops standards on different technology clusters: security, interoperability, connecting things, wireless systems and networks, and others.[53] ETSI's Technical Committee on Cyber security (TC Cyber) is mostly active in privacy standardisation for information security.

Cooperation Agreements

The recognised standard-setting organisations have concluded collaboration agreements, that address issues of participation to each other's work, but also – very importantly- the avoidance of duplication of work. The Vienna Agreement concluded between ISO and CEN for example, underlines that international standardisation takes precedence over national standardisation, but also recognises that the Single European Market has particular needs for European standards.[54] A similar agreement is signed between IEC and CENELEC (Dresden and Frankfurt agreements).[55]

Other Fora

Beyond the aforementioned renowned Standardisation Organisations there are numerous other fora and consortia developing specifications and standards. Most notably the ISOC/IETF and the W3C, whose relevance to the Internet and the World Wide Web can hardly be underestimated. Equally, there are numerous sector-specific, but also cross-cutting organisations, that may provide relevant advice in the field. Finally, with regards to privacy, there is also a number of regulators providing relevant information, with the European Data Protection Board (and before that the Article 29 Working Party) issuing relevant guidance.

---

[51] CEN/ISSS Initiative on Privacy Standardization in Europe, Final Report, 2002. Read further: Winn, Jane K. "Technical standards as data protection regulation." In Gutwirth et al. (eds.) *Reinventing Data Protection?* pp. 191-206. Springer, Dordrecht, 2009.

[52] M/530 Commission Implementing Decision C (2015) 102 final of 20.1.2015, http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548 [accessed 2 September 2018]

[53] See https://www.etsi.org/technologies-clusters/clusters [accessed 2 September 2018]

[54] See the Agreement here: https://isotc.iso.org/livelink/livelink/fetch/2000/2122/3146825/4229629/4230450/4230458/01__Agreement_on_Technical_Cooperation_between_ISO_and_CEN_(Vienna_Agreement).pdf?nodeid=4230688&vernum=-2 and the 2006 Guidelines for its implementation here: https://boss.cen.eu/ref/VA_Guidelines_implementation.pdf [accessed 2 September 2018]

[55] See the Agreement here: https://www.cenelec.eu/aboutcenelec/whoweare/globalpartners/iec.html [accessed 2 September 2018]

ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Catalogue Number TP-03-18-571-EN-N

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-283-7
DOI: 10.2824/698562