SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**

M6 - Certification and Frameworks for Organizations and management systems

Contents

3. Personal data processing and Information Security. Law and certifications

- Definitions, roles and principles through the relevant law
- ISO/IEC 27701: PIMS
- ISO/IEC 29100: privacy framework
- Other standards and certifications

Personal data and definitions

ROLES AND DEFINITIONS

How can we define ‘**privacy**’?

“the state of being alone, or the right to keep one’s personal matters and relationships secret:

‘A **fence** would give us more privacy in the backyard.’ ”

[*Source: Cambridge Academic Content Dictionary © Cambridge University Press*]

Personal data and definitions

ROLES AND DEFINITIONS

How can we define ‘**privacy**’?

*“Privacy is the **right** of an entity (normally a person or an organization), acting on its own behalf, to **determine** the degree to which the confidentiality of their private information is maintained.”*

[SOURCE: IEC Vocabulary, www.electropedia.org, from ISO/IEC 24775-2:2014, 3.1.45, modified – In the definition, "an individual" has been replaced by "a person" for consistency within this document.]

Privacy law

GDPR

Why is **privacy so important**?

Many jurisdiction consider protection of natural persons a primary objective:

*'The protection of **natural persons** in relation to the processing of personal data is a **fundamental right**. Article 8 of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16 of the Treaty on the Functioning of the European Union (TFEU) provide that **everyone** has the **right** to the **protection** of **personal data concerning him or her**.'*

[Source: GDPR, Recital 1]

Personal data and definitions

ROLES AND DEFINITIONS

How ISO/IEC 29100:2011 can help by giving some basic definitions

privacy principles

set of **shared values** governing the **privacy protection** of personally identifiable information (PII) when processed in information and communication technology systems.

[source: ISO/IEC 29100:2011, 2.18, preview: iso.org]

privacy risk:

effect of uncertainty on privacy

(…) **Risk** is defined as the “effect of uncertainty on objectives” in ISO Guide 73 and ISO 31000.

(…) **Uncertainty** is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

[source: ISO/IEC 29100:2011, 2.19, preview: iso.org]

Personal data and definitions

ROLES AND DEFINITIONS

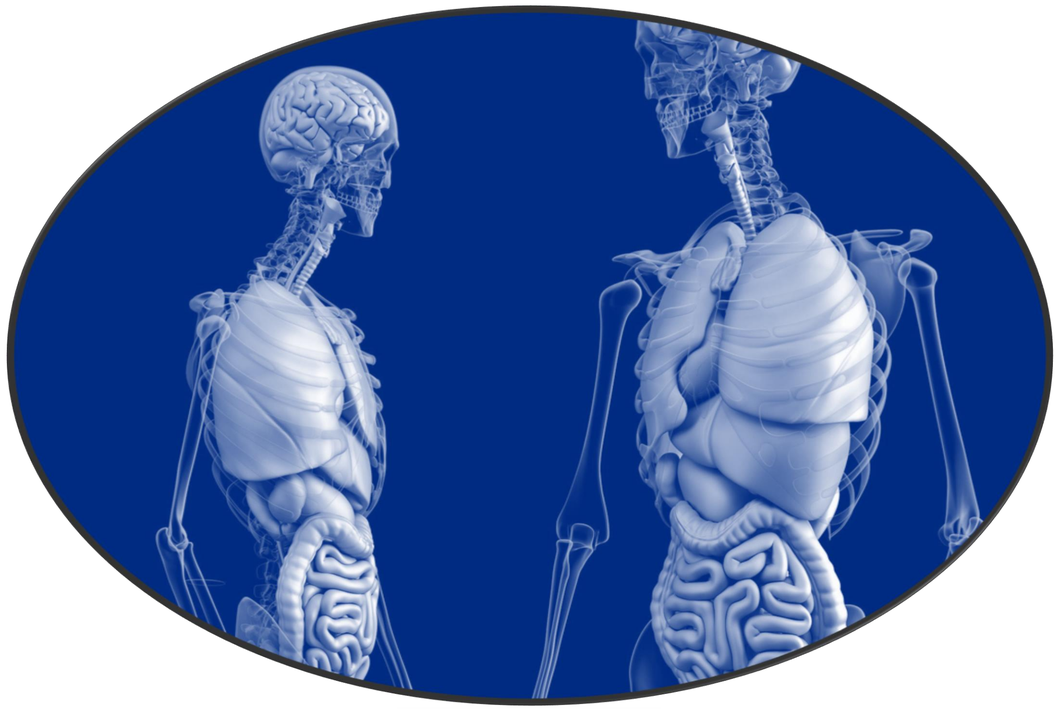
sensitive PII

category of personally identifiable information (PII), either whose nature is sensitive, such as those that relate to the PII principal's ***most intimate sphere****, or that might have* ***a significant impact*** *on the PII principal*

(…) In some jurisdictions or in specific contexts, sensitive PII is defined in reference to the nature of the PII and can consist of PII revealing the ***racial origin****,* ***political opinions*** *or* ***religious*** *or other* ***beliefs****, personal data on* ***health****,* ***sex life*** *or* ***criminal*** *convictions, as well as* ***other*** *PII that might be defined as sensitive.*

[source: ISO/IEC 29100:2011, 2.26, preview: iso.org]

Please keep also note of the definition of '*special categories of personal data*' given by the GDPR, that you'll find in the following slides.



Personal data and definitions

ROLES AND DEFINITIONS

Why is it important, for organizations, to protect PII?

- Almost everyone these days deals with compliance functions within the organization bundaries, wheter it is finance law, tender law, etc.
- Privacy law is becoming of vital importance nowadays for various businesses.
- It imposes some rules that are relevant for reducing not only the risk of compliance itself (penalties and/or brand image damage), but also a **substantial risk of compromising people's life**, at many different levels.

Please note: '*PII*' ('*personally identifiable information*'), '*personal data*', '*personal information*', are usually used as synonymous.

Privacy law in Europe

GDPR

Reg. (UE) 2016/679

European General Data Protection Regulation (which basically applies to european citizens personal data) is one of the most famous examples of rules set to achieve an ambitious, but **necessary** objective in the current digital era: protecting natural persons when their personal data is processed.

Privacy law in the World

CCPA

The California Consumer Privacy Act of 2018 (CCPA) gives consumers (…) *control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law.*

Some

*The right to **know** about the personal information a business collects about them and how it is used and shared;*

*The right to **delete** personal information collected from them (with some exceptions);*

*The right to **opt-out of** the sale of their personal information; and*

*The right to **non-discrimination** for exercising their CCPA rights.*

[Source: oag.ca.gov/privacy/ccpa]

Privacy law in the World

OTHER RELEVANT LAWS

LGPD: Brazilian General Data Protection Law

POPI: Protection of Personal Information Act (often called the POPI Act or POPIA) for South Africa

The Data Protection Act 2018: is the UK's implementation of the General Data Protection Regulation (GDPR).

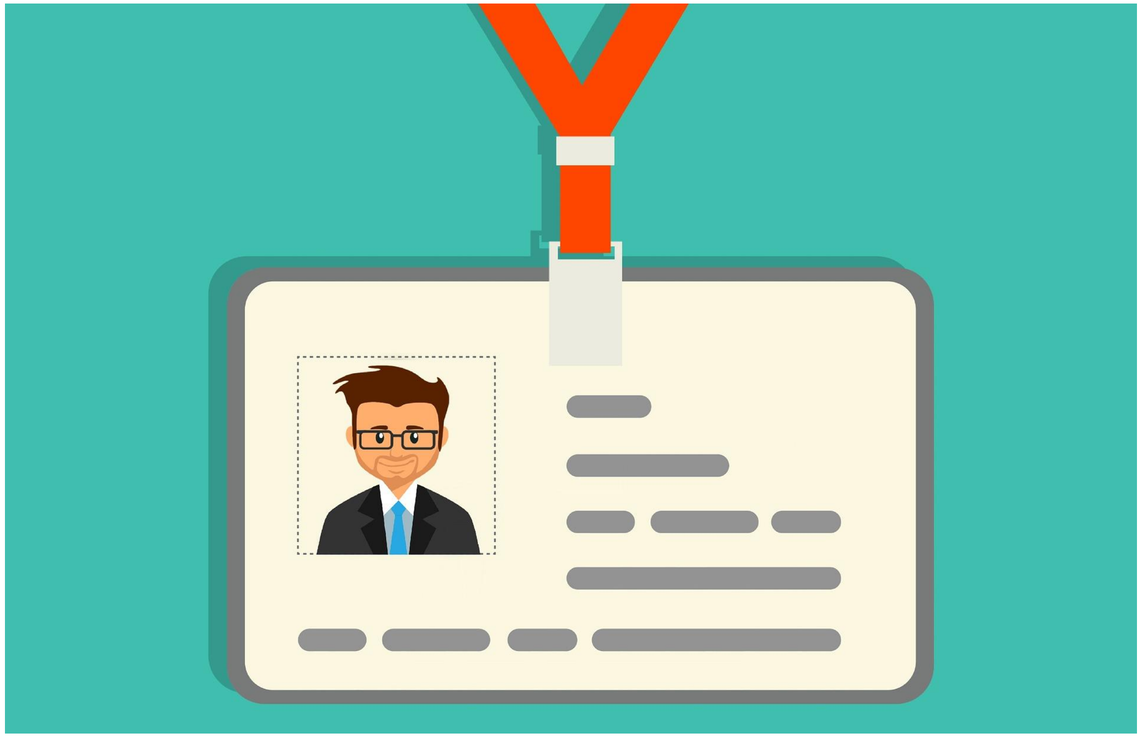
The Privacy Act 1988 (Privacy Act): is the principal piece of Australian legislation protecting the handling of personal information about individuals.

Privacy law

GDPR AND DEFNITIONS

*'**Personal data**' means any information relating to an identified or identifiable natural person ('**data subject**' → 'PII principle' in the ISO/IEC 29100'); 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*

[Source: GDPR, Art. 4]



Privacy law

GDPR AND DEFNITIONS

Processing of special categories of personal data
'Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
(...)'
[Source: GDPR, art. 9]

There are some **exceptions** to the processing of such information, including, for example, the danger of life or the explicit consent given by the *data subject*.

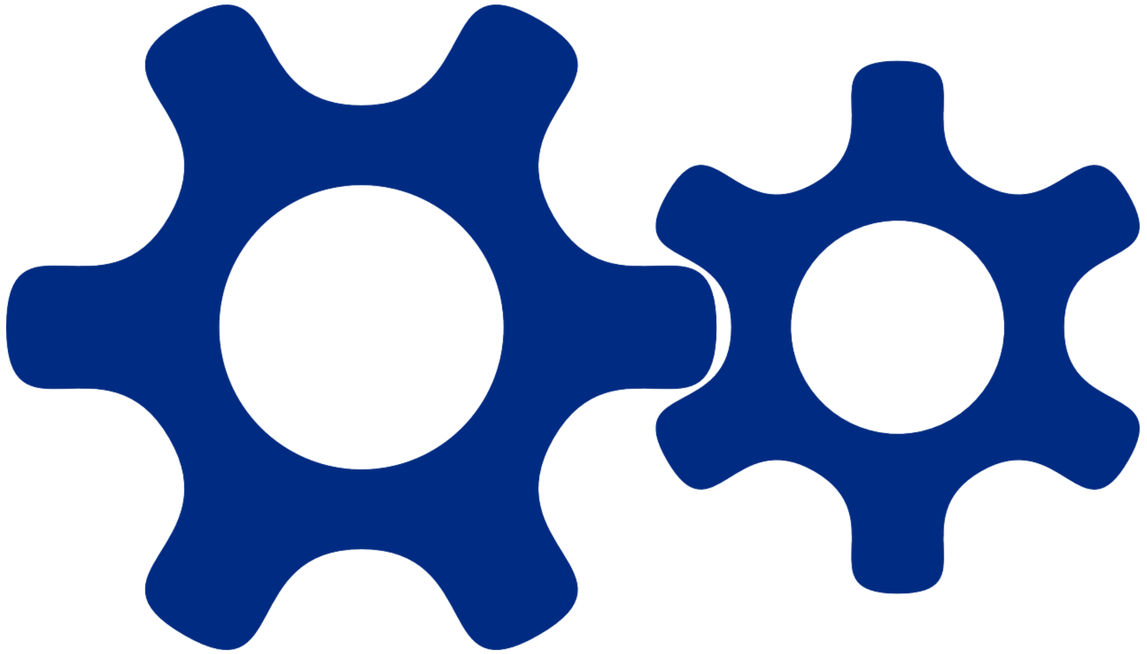
*Personal data which are, by their nature, **particularly sensitive** in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.*
[Source: GDPR, Recital 51]

Privacy law

GDPR AND DEFNITIONS

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

[Source: GDPR, Art. 4]



Privacy law

GDPR AND DEFNITIONS

*‘**Controller**’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*

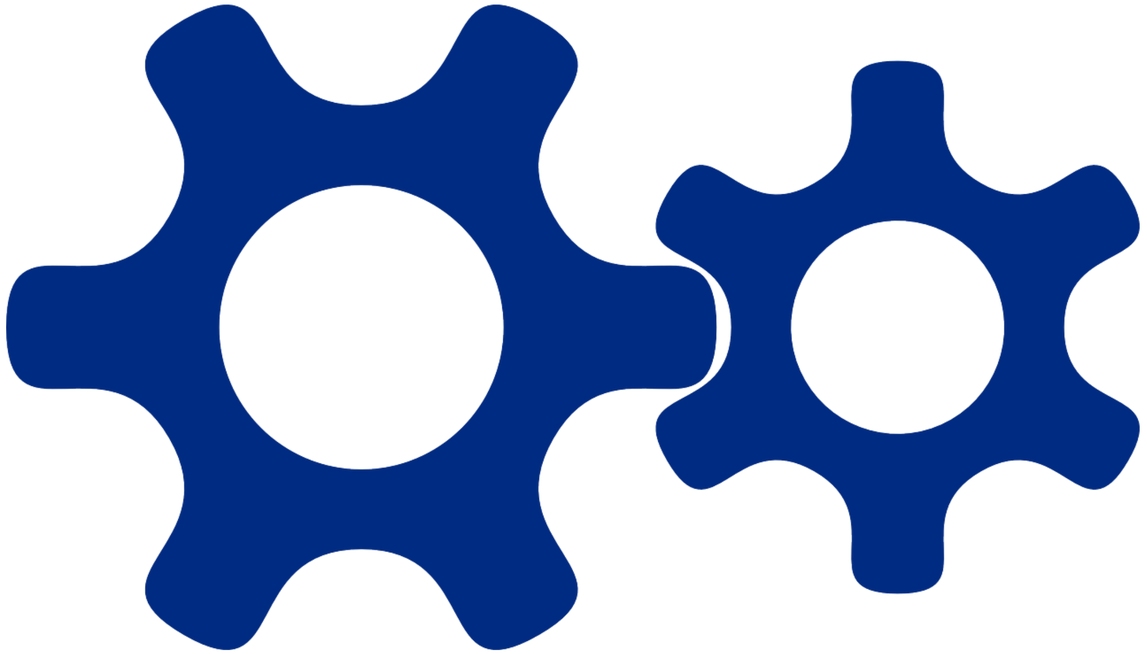
[Source: GDPR, Art. 4]

Privacy law

GDPR AND DEFNITIONS

‘***Processor***’ *means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*

[Source: GDPR, Art. 4]



Privacy law

GDPR AND DEFNITIONS

Information to be provided where personal data are collected from the data subject *(GDPR, art. 13) and* ***when personal data haven't been obtained from the data subject*** *(GDPR, art. 14).*

This information must be provided to the interested party, so that he or she can be aware, among other things, especially of:

- Why data is collected,
- what is the legal basis of the processing (consent? Contract? Public interest, or a legal obligation?),
- what are the categories of recipients of the data (to whom it will be transmitted and why);
- Data retention period;
- transfer personal data to a third country or international organization;
- The existence of the rights of data subject (articles 15 to 22)

Please note: **Privacy policy / notice** is the way the document that contains these information is commonly known as.

Privacy law

GDPR AND DEFNITIONS

Security of processing *(GDPR, art. 32)*

1. Taking into account the state of the art, the ***costs*** *of implementation and the* ***nature***, ***scope***, ***context*** *and* ***purposes*** *of processing as well as the risk of varying* ***likelihood*** *and* ***severity*** *for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security* ***appropriate*** *to the risk, including* inter alia *as appropriate:*

(a) the ***pseudonymisation*** *and* ***encryption*** *of personal data;*

(b) the ability to ***ensure*** *the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*

(c) the ability to ***restore*** *the* ***availability*** *and* ***access*** *to personal data in a timely manner in the event of a physical or technical incident;*

(d) a process for regularly ***testing***, ***assessing*** *and* ***evaluating*** *the effectiveness of technical and organisational measures for ensuring the security of the processing.*

Privacy law

GDPR AND DEFNITIONS

2. In assessing the appropriate level of security account shall be taken in particular of ***the risks that are presented by processing****, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*

3. Adherence to an ***approved code of conduct*** *as referred to in Article 40 or an approved* ***certification mechanism*** *as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.*

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on ***instructions*** *from the controller, unless he or she is required to do so by Union or Member State law.*

[Source: GDPR, art. 32]

Privacy law and certification

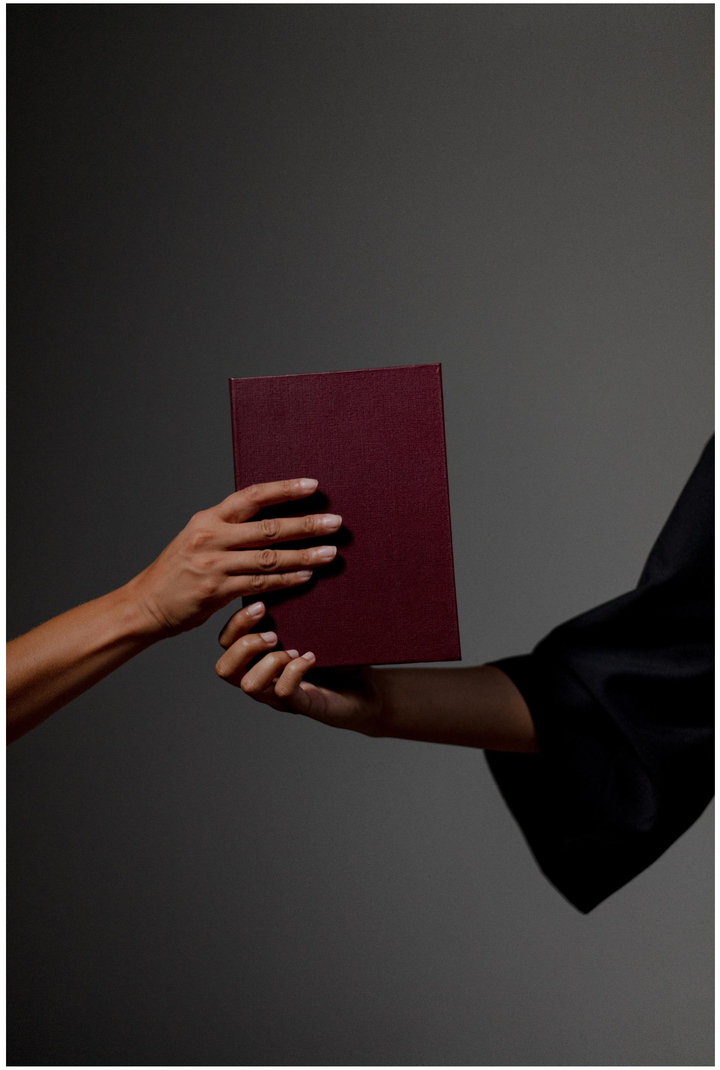
GDPR AND DEFNITIONS

Certification

'1. The Member States, the supervisory authorities, the Board and the Commission shall ***encourage****, in particular at Union level, the establishment of data protection* ***certification mechanisms*** *and of data protection seals and marks, for the purpose of* ***demonstrating compliance*** *with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.*

(…)'

[Source: GDPR, Art. 42]



Privacy law and certification

GDPR AND DEFNITIONS

Certification bodies [=accredited companies that issue the certificates]

'1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, ***issue*** *and* ***renew*** *certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:*

a) the ***supervisory authority*** *which is competent pursuant to Article 55 or 56;* [e.g. Garante per la Protezione dei dati personali, in Italy]

(b) the ***national accreditation body*** [e.g. Accredia in Italy] *named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council (20) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.*

(…)'

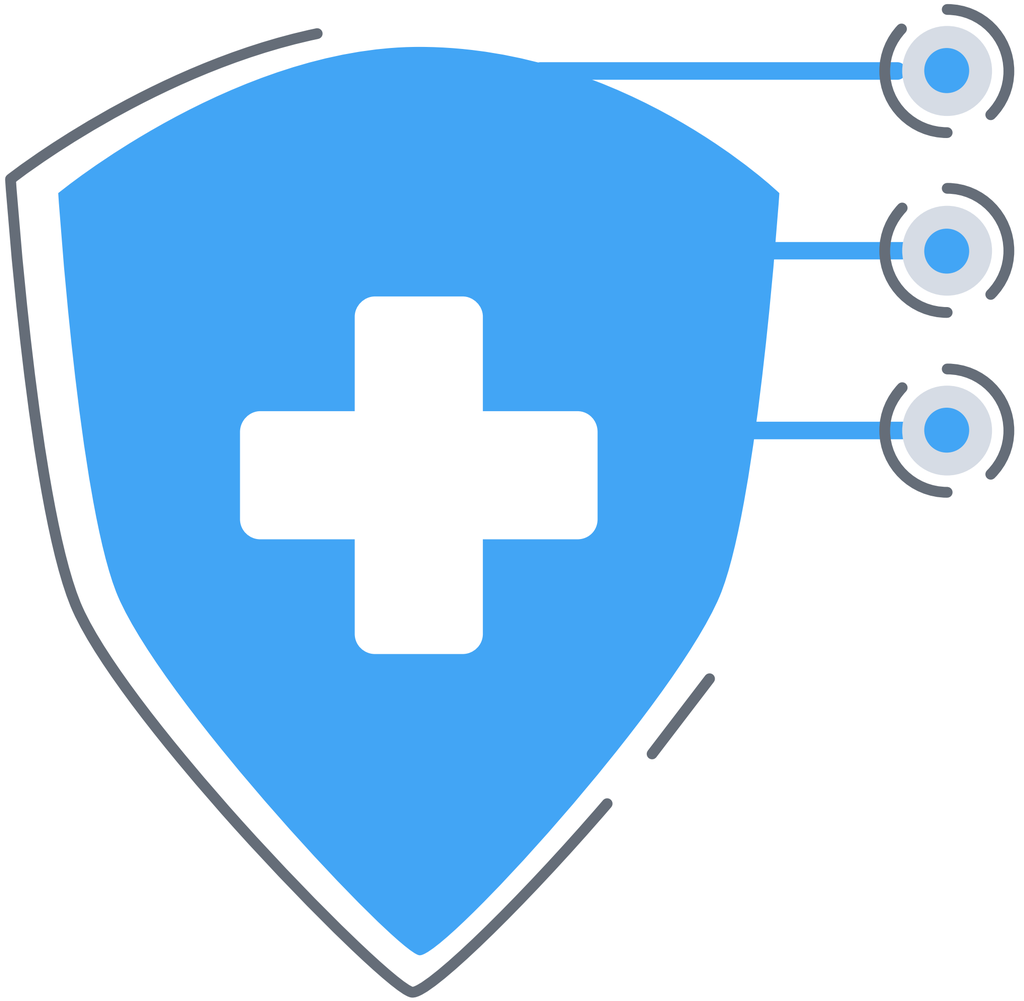
[Source: GDPR, Art. 43]

Privacy standards and certifications

STANDARDS ABOUT CERTIFICATION

Currently, through accredited certification, companies and professionals **cannot demonstrate compliance** with EU Regulation 679/2016, but can exhibit the independent certification of a third-party body and obtain advantages in terms of safety, effectiveness and competitiveness.

[SOURCE: https://www.accredia.it/]

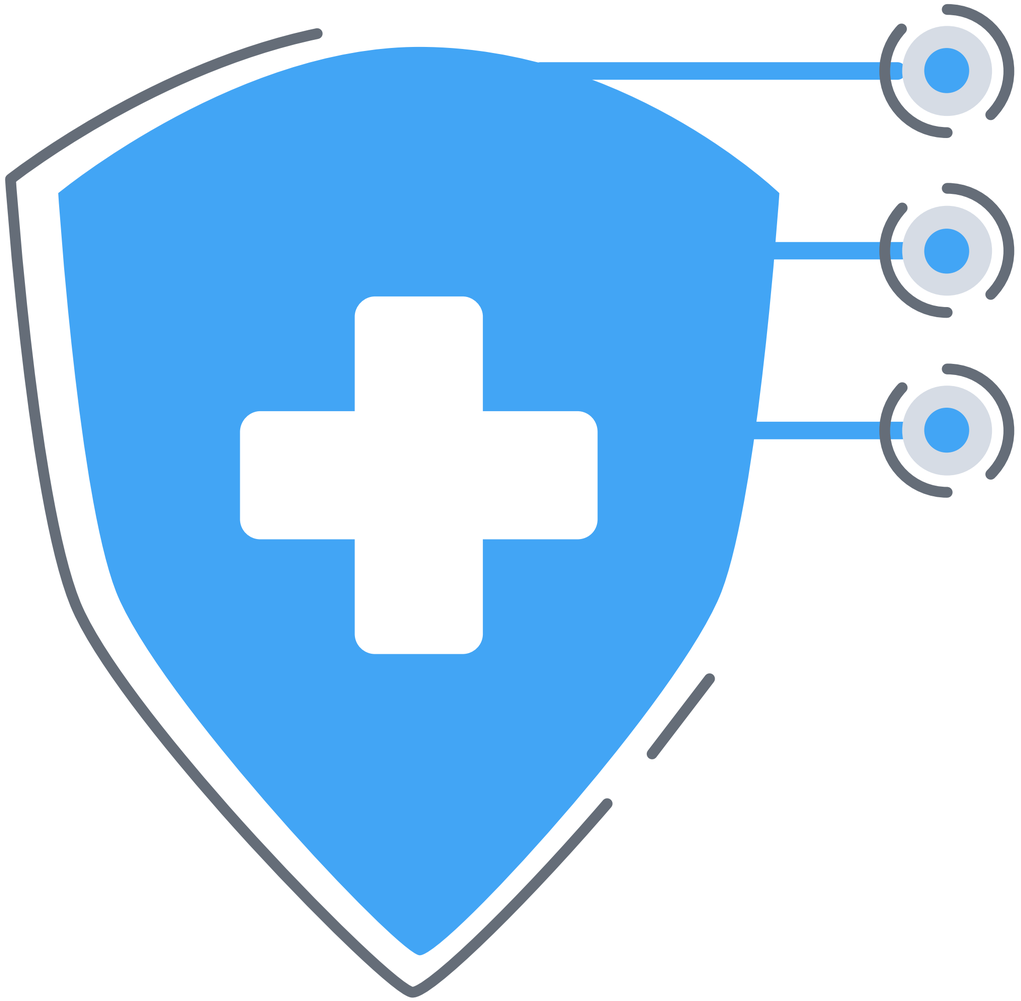


Privacy standards and certifications

STANDARDS ABOUT CERTIFICATION

…But the compliance assessment sector has activated a series of **privacy certifications** that have been recognized as a *guarantee*, and an *act of diligence* towards the interested parties, of the voluntary adoption of a system of analysis and control of the principles and of the rules of the GDPR.

[SOURCE: https://www.accredia.it/]



Privacy standards and certifications

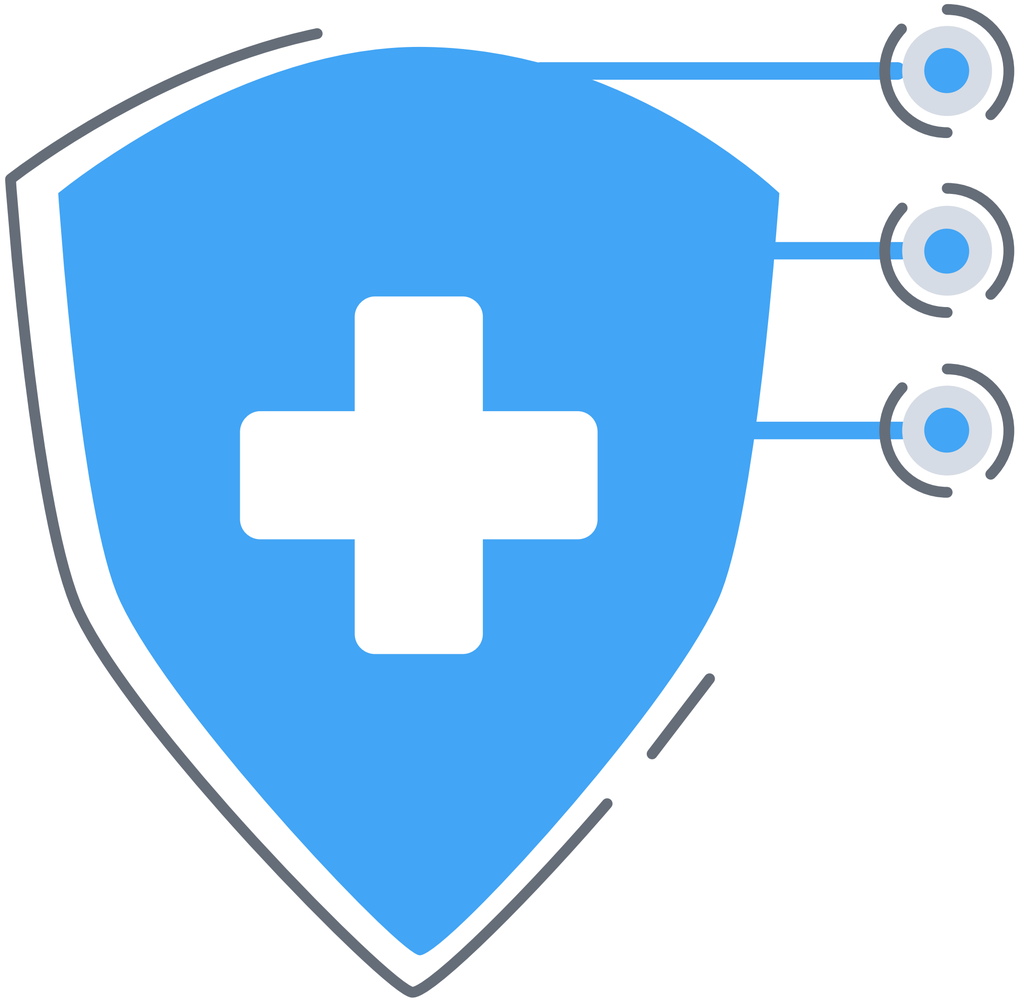
STANDARDS ABOUT CERTIFICATION

How do they work?

Public and **private** companies and **professionals** can request them from accredited certification bodies based on international standards:

- ISO / IEC 17065 for the certification of **products** and **services**
- ISO / IEC 17021-1 for the certification of **management systems**
- ISO / IEC 17024 for the certification of **people**

[SOURCE: https://www.accredia.it/]



ISO/IEC 27701:2019

PII MANAGEMENT SYSTEM («PIMS»)

ISO / IEC 27701, extending ISO / IEC 27001, can be accredited according to ISO / IEC 17021, which contains the requirements for bodies providing audits and certification of management systems.

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an **extension to ISO/IEC 27001 and ISO/IEC 27002** for privacy management within the context of the organization.

It specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

It is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS.
[source:iso.org]

ISO/IEC 27701:2019

PII MANAGEMENT SYSTEM («PIMS»)

Structure of the standard (1/2):

6.2 Information security policies

6.3 Organization of information security

6.4 Human resource security

6.5 Asset management

6.6 Access control

6.7 Cryptography

6.8 Physical and environmental security

6.9 Operations security

6.10 Communications security

6.11 Systems acquisition, development and maintenance

6.12 Supplier relationships

6.13 Information security incident management

6.14 Information security aspects of business continuity management

6.15 Compliance

ISO/IEC 27701:2019

PII MANAGEMENT SYSTEM («PIMS»)

Structure of the standard (2/2):

7 Additional ISO/IEC 27002 guidance for PII controllers

7.1 General

7.2 Conditions for collection and processing

7.3 Obligations to PII principals

7.4 Privacy by design and privacy by default

7.5 PII sharing, transfer, and disclosure

8 Additional ISO/IEC 27002 guidance for PII processors

8.1 General8.2 Conditions for collection and processing

8.3 Obligations to PII principals

8.4 Privacy by design and privacy by default

8.5 PII sharing, transfer, and disclosure

Annex A PIMS-specific reference control objectives and controls (PII Controllers)

Annex B PIMS-specific reference control objectives and controls (PII Processors)

Annex C Mapping to ISO/IEC 29100

Annex D Mapping to the General Data Protection Regulation

Annex E Mapping to ISO/IEC 27018 and ISO/IEC 29151

Annex F How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

F.1 How to apply this document

F.2 Example of refinement of security standards

ISO/IEC 27701:2019

ISO/IEC 27001 ADDITIONAL GUIDANCE

4	**Context of the organization**	**Additional requirements**
5	Leadership	No PIMS-specific requirements
6	**Planning**	**Additional requirements**
7	Support	No PIMS-specific requirements
8	Operation	No PIMS-specific requirements
9	Performance evaluation	No PIMS-specific requirements
10	Improvement	No PIMS-specific requirements

ISO/IEC 27701:2019

ISO/IEC 27001 ADDITIONAL GUIDANCE

It is **essential** to consider the external context. In particular, for personal data, the Organization must take into account the legislation that can have impacts on the achievement of its purposes.

In planning the **risk analysis**, the organization must take into account the risk of loss of integrity, confidentiality and availability of **personal information**.

ISO/IEC 27701:2019

ISO/IEC 27002 ADDITIONAL GUIDANCE

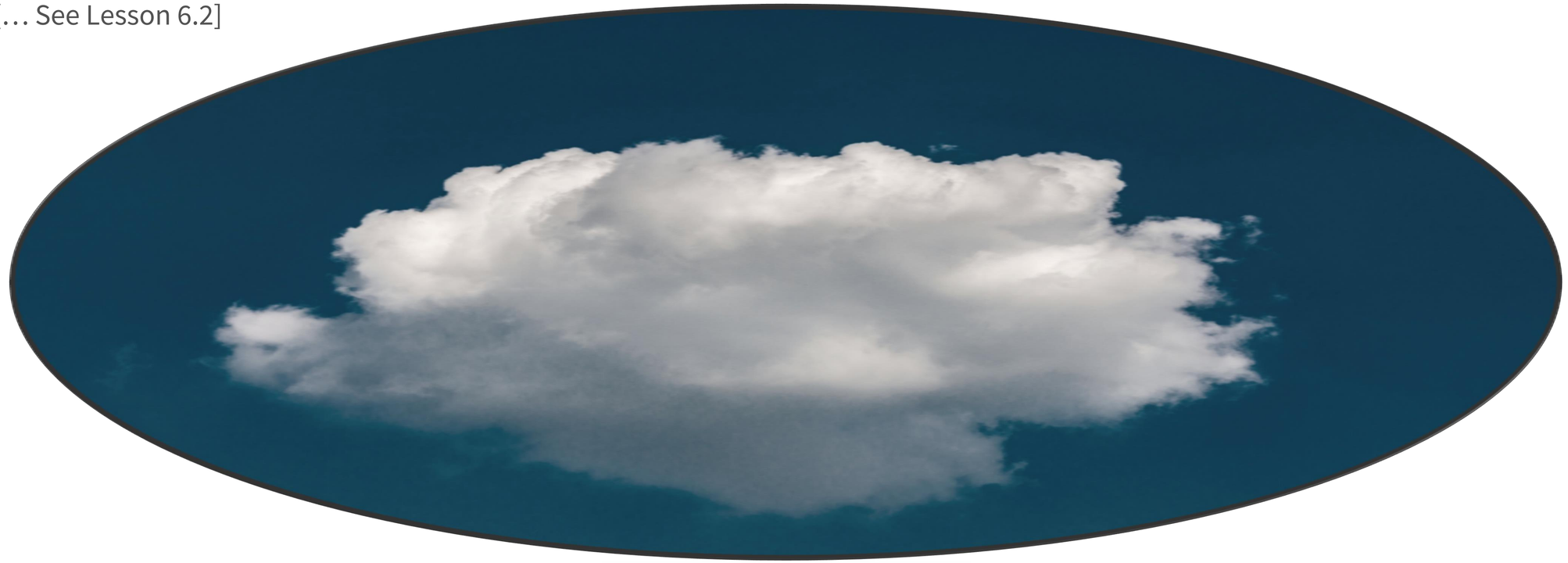
5	Information security policies	Additional guidance
6	Organization of information security	Additional guidance
7	Human resource security	Additional guidance
8	Asset management	Additional guidance
9	Access control	Additional guidance
10	Cryptography	Additional guidance
11	Physical and environmental security	Additional guidance
12	Operations security	Additional guidance
13	Communications security	Additional guidance
14	System acquisition,development andmaintenance	Additional guidance
15	Supplier relationships	Additional guidance
16	Information security incident management	Additional guidance
17	Information security aspects of business continuity management.	**No PIMS-specific guidance**
18	Compliance	Additional guidance

ISO / IEC 27018:2019

CERTIFICATION OF MANAGEMENT SYSTEMS

ISO/IEC 27018 «Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors»

[… See Lesson 6.2]



ISO/IEC 29100

PRIVACY FRAMEWORK

ISO/IEC 29100:2011 provides a privacy **framework** which

- specifies a common privacy **terminology**;
- defines the **actors** and their **roles** in processing personally identifiable information (PII);
- describes privacy **safeguarding** considerations; and provides references to known privacy principles for information technology.

[Source: iso.org]

ISO/IEC 29100

PRIVACY FRAMEWORK

- ISO/IEC 29100:2011 is applicable to **natural persons** and **organizations** involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.

[Source: iso.org]

ISO/IEC 29100

PRIVACY FRAMEWORK

Standard overview:

4.1 Overview of the privacy framework

4.2 Actors and roles

4.3 Interactions

4.4 Recognizing PII

4.5 Privacy safeguarding requirements

4.6 Privacy policies

4.7 Privacy controls

5 The privacy principles of ISO/IEC 29100

5.1 Overview of privacy principles

5.2 Consent and choice

5.3 Purpose legitimacy and specification

5.4 Collection limitation

5.5 Data minimization

5.6 Use, retention and disclosure limitation

5.7 Accuracy and quality

5.8 Openness, transparency and notice

5.9 Individual participation and access

5.10 Accountability

5.11 Information security

5.12 Privacy compliance

Annex A Correspondence between ISO/IEC 29100 concepts and ISO/IEC 27000 concepts

Other privacy certifications

CERTIFICATION OF PRODUCTS AND SERVICES

ISDP 10003 - PROTECTION OF PERSONAL DATA

The accredited certification is issued on the basis of the ISDP © 10003 private scheme, which follows EU Reg. 679/2016.

The scheme specifies the requirements for the correctness, security and compliance management of the personal data of individuals, with particular regard to personal data, and provides the principles and control elements for a complete assessment of the compliance of internal processes with regard to protection of personal data, with specific reference to the **correct management of risks**.

The certification covers all types of organizations that want to demonstrate their accountability through the voluntary adoption of a system of analysis and control of the principles and standards of reference on the subject of data protection.

Other privacy certifications

CERTIFICATION OF PRODUCTS AND SERVICES

SGCMF 10002 - COMPLIANCE OF THE FILES OF HEALTHCARE OPERATORS

The accredited certification is issued on the basis of the private SGCMF © 10002 scheme which concerns the processing of personal data of **healthcare** professionals of **pharmaceutical** companies, in accordance with the combined provisions of the regulations in force regarding the protection of personal data and the rules governing the advertising of medicines.

Through the instrument of certification, the pharmaceutical company can keep internal strategic variables under control, rationalize processes and operate in accordance with the law.

Other privacy certifications

CERTIFICATION OF PRODUCTS AND SERVICES

UNI / PDR 43 - MANAGEMENT OF PERSONAL DATA IN THE ICT FIELD

The accredited certification is issued in accordance with the UNI 43: 2018 Reference Practice "Guidelines for the management of personal data in **the ICT field** according to EU Regulation 679/2016 (GDPR)", designed for all organizations that process data with electronic tools , in particular to small and medium-sized enterprises.

The PdR consists of two sections: the first provides the guidelines for the definition and implementation of the processes relating to the processing of personal data, using electronic tools (ICT); the second provides a set of requirements that allows organizations, in particular SMEs, to effectively comply with the provisions of the European and national regulatory framework, and can be used for certification activities.

Through the certification, the organization aims to demonstrate the management of personal data in the ICT field in line with the provisions of the **GDPR**, in terms of security and correctness of the management of the personal data processing process by the owners and responsible.

Other privacy certifications

CERTIFICATION OF PEOPLE (AS COMPETENCE IS RELEVANT TO THE ISMS AND PIMS)

UNI 11697 - DATA PROTECTION OFFICER (DPO)

The accredited certification is issued in accordance with UNI 11697 "Non-regulated professional activities - Professional profiles relating to the processing and protection of personal data - Requirements for knowledge, skills and competence" to the professional Data Protection Officer (DPO), the person responsible for data protection introduced by the GDPR.

The standard defines the professional profiles relating to the processing and protection of personal data in accordance with the definitions provided by the EQF (European Qualifications Framework) and provides for a series of specialized figures for the business management of all aspects relating to privacy.

Some online resources

GDPR (full text):

- https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex%3A32016R0679

Register of certification mechanisms, seals and marks (from European Data Protection Board):

- https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en

Italian Supervisory authority website:

- https://www.garanteprivacy.it/web/garante-privacy-en/home_en

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**
Simone **Soderi**
antonio.belli@unipd.it
simone.soderi@unipd.it

Thanks for your attention!

M1 - Certification and Frameworks for Organizations and management systems