INTERNATIONAL STANDARD

ISO/IEC 29100

First edition
2011-12-15

Information technology — Security techniques — Privacy framework

Technologies de l'information — Techniques de sécurité — Cadre privé

Reference number
ISO/IEC 29100:2011(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Figures

Tables

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29100 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

This International Standard provides a high-level framework for the protection of personally identifiable information (PII) within information and communication technology (ICT) systems. It is general in nature and places organizational, technical, and procedural aspects in an overall privacy framework.

The privacy framework is intended to help organizations define their privacy safeguarding requirements related to PII within an ICT environment by:

- specifying a common privacy terminology;
- defining the actors and their roles in processing PII;
- describing privacy safeguarding requirements; and
- referencing known privacy principles.

In some jurisdictions, this International Standard's references to privacy safeguarding requirements might be understood as being complementary to legal requirements for the protection of PII. Due to the increasing number of information and communication technologies that process PII, it is important to have international information security standards that provide a common understanding for the protection of PII. This International Standard is intended to enhance existing security standards by adding a focus relevant to the processing of PII.

The increasing commercial use and value of PII, the sharing of PII across legal jurisdictions, and the growing complexity of ICT systems, can make it difficult for an organization to ensure privacy and to achieve compliance with the various applicable laws. Privacy stakeholders can prevent uncertainty and distrust from arising by handling privacy matters properly and avoiding cases of PII misuse.

Use of this International Standard will:

- aid in the design, implementation, operation, and maintenance of ICT systems that handle and protect PII;
- spur innovative solutions to enable the protection of PII within ICT systems; and
- improve organizations' privacy programs through the use of best practices.

The privacy framework provided within this International Standard can serve as a basis for additional privacy standardization initiatives, such as for:

- a technical reference architecture;
- the implementation and use of specific privacy technologies and overall privacy management;
- privacy controls for outsourced data processes;
- privacy risk assessments; or
- specific engineering specifications.

Some jurisdictions might require compliance with one or more of the documents referenced in ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) — *Official Privacy Documents References* [3] or with other applicable laws and regulations, but this International Standard is not intended to be a global model policy, nor a legislative framework.

Information technology — Security techniques — Privacy framework

1 Scope

This International Standard 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.

This International Standard 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.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE In order to make it easier to use the ISO/IEC 27000 family of International Standards in the specific context of privacy and to integrate privacy concepts in the ISO/IEC 27000 context, the table in Annex A provides the ISO/IEC 27000 concepts that correspond with the ISO/IEC 29100 concepts used in this International Standard.

2.1
anonymity
characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly

2.2
anonymization
process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

2.3
anonymized data
data that has been produced as the output of a personally identifiable information anonymization process

2.4
consent
personally identifiable information (PII) principal's freely given, specific and informed agreement to the processing of their PII

2.5
identifiability
condition which results in a personally identifiable information (PII) principal being identified, directly or indirectly, on the basis of a given set of PII

2.6
identify
establish the link between a personally identifiable information (PII) principal and PII or a set of PII

2.7
identity
set of attributes which make it possible to identify the personally identifiable information principal

2.8
opt-in
process or type of policy whereby the personally identifiable information (PII) principal is required to take an action to express explicit, prior consent for their PII to be processed for a particular purpose

NOTE A different term that is often used with the privacy principle 'consent and choice' is "opt-out". It describes a process or type of policy whereby the PII principal is required to take a separate action in order to withhold or withdraw consent, or oppose a specific type of processing. The use of an opt-out policy presumes that the PII controller has the right to process the PII in the intended way. This right can be implied by some action of the PII principal different from consent (e.g., placing an order in an online shop).

2.9
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

NOTE To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

2.10
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes

NOTE A PII controller sometimes instructs others (e.g., PII processors) to process PII on its behalf while the responsibility for the processing remains with the PII controller.

2.11
PII principal
natural person to whom the personally identifiable information (PII) relates

NOTE Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

2.12
PII processor
privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

2.13
privacy breach
situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements

2.14
privacy controls
measures that treat privacy risks by reducing their likelihood or their consequences

NOTE 1 Privacy controls include organizational, physical and technical measures, e.g., policies, procedures, guidelines, legal contracts, management practices or organizational structures.

NOTE 2 Control is also used as a synonym for safeguard or countermeasure.

2.15
privacy enhancing technology
PET
privacy control, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system

NOTE 1 Examples of PETs include, but are not limited to, anonymization and pseudonymization tools that eliminate, reduce, mask, or de-identify PII or that prevent unnecessary, unauthorized and/or undesirable processing of PII.

NOTE 2 Masking is the process of obscuring elements of PII.

2.16
privacy policy
overall intention and direction, rules and commitment, as formally expressed by the personally identifiable information (PII) controller related to the processing of PII in a particular setting

2.17
privacy preferences
specific choices made by a personally identifiable information (PII) principal about how their PII should be processed for a particular purpose

2.18
privacy principles
set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems

2.19
privacy risk
effect of uncertainty on privacy

NOTE 1 Risk is defined as the “effect of uncertainty on objectives” in ISO Guide 73 and ISO 31000.

NOTE 2 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

2.20
privacy risk assessment
overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personally identifiable information (PII)

NOTE This process is also known as a privacy impact assessment.

2.21
privacy safeguarding requirements
set of requirements an organization has to take into account when processing personally identifiable information (PII) with respect to the privacy protection of PII

2.22
privacy stakeholder
natural or legal person, public authority, agency or any other body that can affect, be affected by, or perceive themselves to be affected by a decision or activity related to personally identifiable information (PII) processing

2.23
processing of PII
operation or set of operations performed upon personally identifiable information (PII)

NOTE Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.

2.24
pseudonymization
process applied to personally identifiable information (PII) which replaces identifying information with an alias

NOTE 1 Pseudonymization can be performed either by PII principals themselves or by PII controllers. Pseudonymization can be used by PII principals to consistently use a resource or service without disclosing their identity to this resource or service (or between services), while still being held accountable for that use.

NOTE 2 Pseudonymization does not rule out the possibility that there might be (a restricted set of) privacy stakeholders other than the PII controller of the pseudonymized data which are able to determine the PII principal's identity based on the alias and data linked to it.

2.25
secondary use
processing of personally identifiable information (PII) in conditions which differ from the initial ones

NOTE Conditions that differ from the initial ones could involve, for example, a new purpose for processing PII, a new recipient of the PII, etc.

2.26
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

NOTE 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.

2.27
third party
privacy stakeholder other than the personally identifiable information (PII) principal, the PII controller and the PII processor, and the natural persons who are authorized to process the data under the direct authority of the PII controller or the PII processor

3 Symbols and abbreviated terms

The following abbreviations are common to ISO/IEC 29100.

ICT Information and Communication Technology

PET Privacy Enhancing Technology

PII Personally Identifiable Information

4 Basic elements of the privacy framework

4.1 Overview of the privacy framework

The following components relate to privacy and the processing of PII in ICT systems and make up the privacy framework described in this International Standard:

- actors and roles;
- interactions;
- recognizing PII;
- privacy safeguarding requirements;
- privacy policies; and
- privacy controls.

For the development of this privacy framework, concepts, definitions and recommendations from other official sources have been taken into consideration. These sources can be found in ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) — *Official Privacy Documents References* [3].

4.2 Actors and roles

For the purposes of this standard, it is important to identify the actors involved in the processing of PII. There are four types of actors who can be involved in the processing of PII: PII principals, PII controllers, PII processors and third parties.

4.2.1 PII principals

PII principals provide their PII for processing to PII controllers and PII processors and, when it is not otherwise provided by applicable law, they give consent and determine their privacy preferences for how their PII should be processed. PII principals can include, for example, an employee listed in the human resources system of a company, the consumer mentioned in a credit report, and a patient listed in an electronic health record. It is not always necessary that the respective natural person is identified directly by name in order to be considered a PII principal. If the natural person to whom the PII relates can be identified indirectly (e.g., through an account identifier, social security number, or even through the combination of available attributes), he or she is considered to be the PII principal for that PII set.

4.2.2 PII controllers

A PII controller determines why (purpose) and how (means) the processing of PII takes place. The PII controller should ensure adherence to the privacy principles in this framework during the processing of PII under its control (e.g., by implementing the necessary privacy controls). There might be more than one PII controller for the same PII set or set of operations performed upon PII (for the same or different legitimate purposes). In this case the different PII controllers shall work together and make the necessary arrangements to ensure the privacy principles are adhered to during the processing of PII. A PII controller can also decide to have all or part of the processing operations carried out by a different privacy stakeholder on its behalf. PII controllers should carefully assess whether or not they are processing sensitive PII and implement reasonable and appropriate privacy and security controls based on the requirements set forth in the relevant jurisdiction as well as any potential adverse effects for PII principals as identified during a privacy risk assessment.

4.2.3 PII processors

A PII processor carries out the processing of PII on behalf of a PII controller, acts on behalf of, or in accordance with the instructions of the PII controller, observes the stipulated privacy requirements

and implements the corresponding privacy controls. In some jurisdictions, the PII processor is bound by a legal contract.

4.2.4 Third parties

A third party can receive PII from a PII controller or a PII processor. A third party does not process PII on behalf of the PII controller. Generally, the third party will become a PII controller in its own right once it has received the PII in question.

4.3 Interactions

The actors identified in the previous clause can interact with each other in a variety of ways. As far as the possible flows of PII among the PII principal, the PII controller and the PII processor are concerned, the following scenarios can be identified:

a) the PII principal provides PII to a PII controller (e.g., when registering for a service provided by the PII controller);

b) the PII controller provides PII to a PII processor which processes that PII on behalf of the PII controller (e.g., as part of an outsourcing agreement);

c) the PII principal provides PII to a PII processor which processes that PII on behalf of the PII controller;

d) the PII controller provides the PII principal with PII which is related to the PII principal (e.g., pursuant to a request made by the PII principal);

e) the PII processor provides PII to the PII principal (e.g., as directed by the PII controller); and

f) the PII processor provides PII to the PII controller (e.g., after having performed the service for which it was appointed).

The roles of the PII principal, PII controller, PII processor and a third party in these scenarios are illustrated in Table 1.

There is a need to distinguish between PII processors and third parties because the legal control of the PII remains with the original PII controller when it is sent over to the PII processor, whereas a third party can become a PII controller in its own right once it has received the PII in question. For instance, where a third party makes the decision to transfer PII it has received from a PII controller to yet another party, it will be acting as a PII controller in its own right and will therefore no longer be considered a third party.

As far as the possible flows of PII among the PII controllers and PII processors on the one hand, and third parties on the other hand are concerned, the following scenarios can be identified:

g) the PII controller provides PII to a third party (e.g., in the context of a business agreement); and

h) the PII processor provides PII to a third party (e.g., as directed by the PII controller).

The roles of the PII controller and a third party in these scenarios are also illustrated in Table 1.

Table 1 – Possible flows of PII among the PII principal, PII controller, PII processor and a third party and their roles

	PII principal	PII controller	PII processor	Third party
Scenario a)	PII provider	PII recipient	—	—
Scenario b)	—	PII provider	PII recipient	—
Scenario c)	PII provider	—	PII recipient	—
Scenario d)	PII recipient	PII provider	—	—
Scenario e)	PII recipient	—	PII provider	—
Scenario f)	—	PII recipient	PII provider	—
Scenario g)	—	PII provider	—	PII recipient
Scenario h)	—	—	PII provider	PII recipient

4.4 Recognizing PII

To determine whether or not a natural person should be considered identifiable, several factors need to be taken into account. In particular, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person. ICT systems should support mechanisms that will make the PII principal aware of such PII and provide the natural person with appropriate controls over the sharing of that information. The following sub-clauses provide additional clarification on how to determine whether or not a PII principal should be considered identifiable.

4.4.1 Identifiers

In certain instances, identifiability of the PII principal might be very clear (e.g., when the information contains or is associated with an identifier which is used to refer to or communicate with the PII principal). Information can be considered to be PII in at least the following instances:

- if it contains or is associated with an identifier which refers to a natural person (e.g., a social security number);
- if it contains or is associated with an identifier which can be related to a natural person (e.g., a passport number, an account number);
- if it contains or is associated with an identifier which can be used to establish a communication with an identified natural person (e.g., a precise geographical location, a telephone number); or
- if it contains a reference which links the data to any of the identifiers above.

4.4.2 Other distinguishing characteristics

Information does not necessarily need to be associated with an identifier in order to be considered PII. Information will also be considered PII if it contains or is associated with a characteristic which distinguishes a natural person from other natural persons (e.g., biometric data).

Any attribute which takes on a value which uniquely identifies a PII principal is to be considered as a distinguishing characteristic. Note that whether or not a given characteristic distinguishes a natural person from other natural persons might change depending on the context of use. For instance, while the last name of a natural person might be insufficient to identify that natural person on a global scale, it will often be sufficient to distinguish a natural person on a company scale.

In addition, there can also be situations in which a natural person is identifiable even if there is no single attribute that uniquely identifies him or her. This is the case where a combination of several attributes taken together distinguishes this natural person from other natural persons. Whether or not a natural person is identifiable on the basis of a combination of attributes might also be dependent on the specific domain. For instance, the combination of the attributes “female”, “45” and “lawyer” can be sufficient to identify a natural person within a particular company, but will often be insufficient to identify that natural person outside of that company.

Table 2 provides some examples of attributes that could be PII, depending on the domain. These examples are informative.

Table 2 – Example of attributes that can be used to identify natural persons

Examples
Age or special needs of vulnerable natural persons
Allegations of criminal conduct
Any information collected during health services
Bank account or credit card number
Biometric identifier
Credit card statements
Criminal convictions or committed offences
Criminal investigation reports
Customer number
Date of birth
Diagnostic health information
Disabilities
Doctor bills
Employees’ salaries and human resources files
Financial profile
Gender
GPS position
GPS trajectories
Home address
IP address
Location derived from telecommunications systems
Medical history
Name
National identifiers (e.g., passport number)
Personal e-mail address
Personal identification numbers (PIN) or passwords
Personal interests derived from tracking use of internet web sites
Personal or behavioural profile
Personal telephone number
Photograph or video identifiable to a natural person
Product and service preferences
Racial or ethnic origin
Religious or philosophical beliefs
Sexual orientation
Trade-union membership
Utility bills

4.4.3 Information which is or might be linked to a PII principal

If the information in question does not identify a PII principal, it should be determined whether the information is or can be linked to an identity of a natural person.

Once the relationship with an identifiable natural person is established, it needs to be decided whether the information says something about this natural person, for instance if it refers to her or his characteristics or behaviour. Examples include medical records, financial profiles, or the personal interests derived from tracking use of internet websites. Also, simple attribute statements about a natural person such as age or gender of a natural person can qualify the linked information as PII. Regardless, if the relationship with an identifiable natural person can be established, such information must also be treated as PII.

4.4.4 Pseudonymous data

In order to restrict the ability of PII controllers and processors to identify the PII principal, identity information can be replaced by aliases. This replacement is usually performed by a PII provider before transmitting the PII to a PII recipient, in particular in scenarios a, b, c, g and h of Table 1.

Certain business processes rely on designated processors who perform the substitution and control the assignment table or function. This is often the case wherever sensitive data needs to be processed by privacy stakeholders that did not collect them.

The substitution is considered pseudonymization provided:

(a) the remaining attributes linked to the alias do not suffice to identify the PII principal to whom they relate; and

(b) the alias assignment is such that it cannot be reversed by reasonable efforts of the privacy stakeholders other than those that performed them.

Pseudonymization retains linkability. Different data associated with the same pseudonym can be linked. The larger the set of data associated with a given pseudonym, the larger is the risk that property (a) is violated. Moreover, the smaller the group of natural persons to which a set of pseudonymous data relates, the greater the likelihood of a PII principal being identifiable. Attributes contained directly in the information in question and attributes that can be easily linked to this information (e.g., by using a search engine or cross-referencing with other databases) should be taken into account when determining whether or not the information relates to an identifiable natural person.

Pseudonymization contrasts with anonymization. Anonymization processes also fulfil properties (a) and (b) above, but destroy linkability. During anonymization, identity information is either erased or substituted by aliases for which the assignment function or table is destroyed. Thus, anonymized data is no longer PII.

4.4.5 Metadata

PII can be stored in an ICT system in such a way that it is not readily visible to the system user (i.e. to the PII principal). Examples include the PII principal's name stored as metadata in the properties of a document, and comments or tracked changes stored as metadata in a word processing document. If the PII principal became aware of the existence of the PII or the processing of the PII for such a purpose, he or she might prefer that the PII not be processed in such a way or be shared publicly.

4.4.6 Unsolicited PII

PII that was unsolicited by a PII controller or PII processor (i.e. unintentionally obtained) might also be stored in an ICT system. For example, a PII principal could potentially provide PII to a PII controller that was not requested or sought by the PII controller (e.g., additional PII provided in the context of an anonymous feedback form on a website). The risk of collecting unsolicited PII can be reduced by considering privacy safeguarding measures at the time of the design of the system (also referred to as the concept of "privacy by design").

4.4.7 Sensitive PII

Sensitivity extends to all PII from which sensitive PII can be derived. For instance, medical prescriptions can reveal detailed information about the PII principal's health. Even if PII does not contain direct information about the PII principal's sexual orientation or health, if it could be used to infer such information, the PII could be sensitive. For purposes of this standard, PII must be treated as sensitive PII where such inference and knowledge of the identity of the PII principal is reasonably possible.

In some jurisdictions, what constitutes sensitive PII is also defined explicitly in legislation. Examples include information revealing race, ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, sexual lifestyle or orientation, and the physical or mental health of the PII principal. In other jurisdictions, sensitive PII might include information that could facilitate identity theft or otherwise result in significant financial harm to the natural person (e.g., credit card numbers, bank account information, or government-issued identifiers such as passport numbers, social security numbers or drivers' license numbers), and information that could be used to determine the PII principal's real time location.

The processing of sensitive PII requires special precautions. In some jurisdictions, the processing of sensitive PII might be prohibited by applicable law even with the PII principal's opt-in consent. Some jurisdictions might require implementation of specific controls where certain types of sensitive PII are processed (e.g., a requirement to encrypt medical PII when transmitting it over a public network).

4.5 Privacy safeguarding requirements

Organizations are motivated to protect PII for a variety of reasons: to protect the PII principal's privacy, to meet legal and regulatory requirements, to practice corporate responsibility, to enhance consumer trust, etc. The purpose of this clause is to provide an overview of the different factors that can influence the privacy safeguarding requirements that are relevant to a particular organization or privacy stakeholder processing PII.

Privacy safeguarding requirements can relate to many different aspects of PII processing, e.g., the collection and retention of PII, the transfer of PII to third parties, the contractual relationship among PII controllers and PII processors, the international transfer of PII, etc. Privacy safeguarding requirements can also vary in specificity. They might be very general in nature, e.g., consisting of an enumeration of high-level privacy principles which an organization is expected to take into account when processing PII. However, privacy safeguarding requirements can also involve very specific restrictions on the processing of certain types of PII, or mandate the implementation of specific privacy controls.

The design of any ICT system that involves the processing of PII should be preceded by an identification of relevant privacy safeguarding requirements. The privacy implications of new or substantially modified ICT systems involving the processing of PII should be resolved before those ICT systems are implemented. Organizations routinely perform broad risk management activities and develop risk profiles related to their ICT systems.

Risk management is defined as "coordinated activities to direct and control an organization with regard to risk" (ISO Guide 73:2009). The privacy risk management process comprises the following processes:

- establishing the context, by understanding the organization (e.g., PII processing, responsibilities), the technical environment and the factors influencing privacy risk management (i.e. legal and regulatory factors, contractual factors, business factors and other factors);
- risk assessment, by identifying, analysing and evaluating risks to PII principals (risks that they can be adversely affected);
- risk treatment, by defining privacy safeguarding requirements, identifying and implementing privacy controls to avoid or reduce the risks to PII principals;
- communication and consultation, by getting information from interested parties, obtaining consensus on each risk management process, and informing PII principals and communicating about risks and controls; and
- monitoring and review, by following up risks and controls, and improving the process.

One deliverable can be a privacy impact assessment, which is the component of risk management that focuses on ensuring compliance with privacy and data protection legislation requirements and assessing the privacy implications of new or substantially modified programs or activities. Privacy impact assessments should be framed within an organization's broader risk management framework.

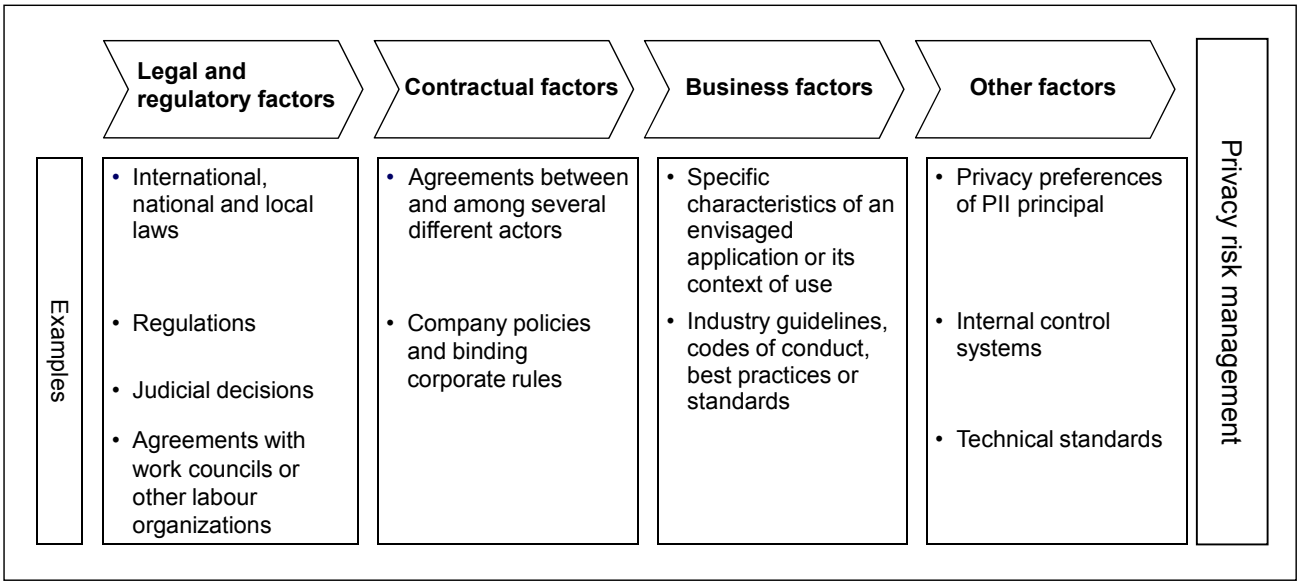

Figure 1 – Factors influencing privacy risk management

Privacy safeguarding requirements are identified as part of the overall privacy risk management process which is influenced by the following factors (as depicted in Figure 1 above and described below):

- legal and regulatory factors for the safeguarding of the natural person's privacy and the protection of their PII;
- contractual factors such as industry guidelines, professional standards, company policies;
- business factors predetermined by a specific business application or in a specific use case context; and
- other factors that can affect the design of ICT systems and the associated privacy safeguarding requirements.

4.5.1 Legal and regulatory factors

Privacy safeguarding requirements are often reflected in (1) international, national and local laws, (2) regulations, (3) judicial decisions or (4) negotiated agreements with work councils or other labour organizations. Some examples of local and national legislation include data protection laws, consumer protection laws, breach notification laws, data retention laws, and employment laws. Relevant international law might contain rules affecting cross-border transfer of PII. PII controllers should be aware of all relevant privacy safeguarding requirements arising from legal or regulatory factors. To achieve this goal they can coordinate closely with legal experts. While in many jurisdictions it will be the PII controller who is ultimately responsible for ensuring compliance, all actors involved in the processing of PII should take a proactive approach in identifying relevant privacy safeguarding requirements arising from legal or other factors.

4.5.2 Contractual factors

Contractual obligations can also influence privacy safeguarding requirements. These obligations can stem from agreements between and among several different actors, such as PII processors, PII controllers, and third parties. For example, a privacy stakeholder might require third parties to use specific privacy controls and agree to specific PII disposal requirements before PII is transferred to them. Privacy safeguarding requirements could also be the result of company policies and binding corporate rules that the privacy stakeholder has set out for itself, for example, to protect its brand from negative publicity in the event of a privacy breach.

In principle, any party that has access to PII should be made aware of its obligations by the respective PII controller(s) in a formalized manner, for example, by entering into third party agreements. Such agreements are likely to contain a number of privacy safeguarding requirements the third party (PII recipient) will have to take into account. In certain jurisdictions, national and regional authorities might have established legal and contractual instruments that enable the transfer of PII to third parties.

4.5.3 Business factors

Privacy safeguarding requirements can also be influenced by business factors which include the specific characteristics of an envisaged application or its context of use. Business factors can vary widely depending on the type of privacy stakeholder and type of business. For example, they can relate to the sector in which an organization is active (e.g., industry guidelines, codes of conduct, best practices, standards) or the nature of its business model (e.g., 24/7 online services, information sharing service, banking application).

Many business factors do not have a direct impact on privacy safeguarding requirements as such. The envisaged use of PII is likely to affect an organization's implementation of privacy policies, as well as the choice of privacy controls, but this should not affect the privacy principles to which the organization subscribes. For example, offering a certain service might require a service provider to collect additional PII or to allow more of its employees to access certain types of PII. However, this does not mean that a PII controller that has subscribed to the principles contained in this framework should no longer carefully assess which types of PII are strictly needed to provide the service (principle of collection limitation) and to limit access by its employees to the PII in question to those that need to have access in order to fulfil their duties (principle of information security).

4.5.4 Other factors

The most important factor for organizations to consider when identifying privacy safeguarding requirements relates to the privacy preferences of PII principals. The personal disposition of a natural person towards privacy and what risks a natural person considers can depend on a number of factors including the natural person's understanding of the technology used, their background, the information being provided, the purpose of the transaction, the natural person's past experience, and socio-psychological factors.

ICT system designers should attempt to understand the likely privacy concerns of a PII principal and understand the types of PII that will be processed through their system. Just as a system developer or an application or service provider studies customer target groups for usage expectations and their wants and needs, it is important to try and understand the expectations and preferences of relevant natural persons with respect to privacy. Although it is not always possible for ICT systems designers to provide PII principals with choices that match their privacy preferences, it is an important design consideration.

Examples of privacy preferences could include a preference for anonymity or pseudonymity, the ability to restrict who can access specific PII, or the ability to restrict the purpose for which the PII will be processed. To the extent feasible, the PII principal should be given a choice of preferences for the processing of his data, for example whether the PII is used for secondary purposes such as marketing. The ability to express privacy-friendly preferences can be implemented using the graphical user interface of the ICT system. It can assist the PII principal in making a choice by presenting a set of pre-defined options for common privacy preferences using easily understandable language. The implementation of the user interface can be based on elements such as checkboxes or dropdown menus.

In addition to the factors listed in the previous clauses, there are still other factors that can influence the design of ICT systems and the associated privacy safeguarding requirements. For example, privacy safeguarding requirements could be influenced by internal control systems or technical standards an organization has adopted (e.g., a voluntary standard, such as an ISO standard).

4.6 Privacy policies

The top management of the organization involved in the processing of PII should establish a privacy policy. The privacy policy should:

- be appropriate to the purpose of the organization;
- provide the framework for setting objectives;
- include a commitment to satisfy applicable privacy safeguarding requirements;
- include a commitment to continual improvement;
- be communicated within the organization; and
- be available to interested parties, as appropriate.

The organization should document its privacy policy in writing. Where an organization processing PII is a PII processor, these policies can be determined to a large extent by the PII controller. The privacy policy should be supplemented by more detailed rules and obligations of the different privacy stakeholders involved in the processing of PII (e.g., procedures for specific departments or employees). In addition, the controls that are used to enforce the privacy policy in a particular setting (e.g., access control, notice provisions, audits, etc.) should be clearly documented.

The term “privacy policy” is often used to refer to both internal and external privacy policies. An internal privacy policy documents the objectives, rules, obligations, restrictions and/or controls an organization has adopted to satisfy the privacy safeguarding requirements that are relevant to its processing of PII. An external privacy policy provides outsiders to the organization with a notice of the organization’s privacy practices, as well as other relevant information such as the identity and official address of the PII controller, contact points from which PII principals might obtain additional information, etc. In the context of this framework, the term “privacy policy” is used to refer to the internal privacy policy of an organization. External privacy policies are referred to as notices.

4.7 Privacy controls

Organizations should identify and implement privacy controls to meet the privacy safeguarding requirements identified by the privacy risk assessment and treatment process. In addition, the identified and implemented privacy controls should be documented as part of the organization’s privacy risk assessment. Certain types of PII processing can warrant specific controls for which the need only becomes apparent once an envisaged operation has been carefully analyzed. A privacy risk assessment can assist organizations in identifying the specific risks of privacy breaches involved in an envisaged operation.

Effort should be taken by organizations to develop their privacy controls as part of a general “privacy by design” approach, i.e. privacy compliance should be taken into account at the design phase of systems processing PII, rather than being bolted on at a subsequent stage.

As far as information security controls are concerned, it is important to note that not all PII processing requires the same level or type of protection. Organizations should distinguish among PII processing operations according to the specific risks they present to help determine which information security controls are appropriate in which instance. Risk management is a central method in this process, and the identification of privacy controls should also be an integral part of an organization’s information security management framework.

5 The privacy principles of ISO/IEC 29100

5.1 Overview of privacy principles

The privacy principles described in this standard were derived from existing principles developed by a number of states, countries and international organizations. This framework focuses on the implementation of the privacy principles in ICT systems and the development of privacy management systems to be implemented within the organization's ICT systems. These privacy principles should be used to guide the design, development, and implementation of privacy policies and privacy controls. Additionally, they can be used as a baseline in the monitoring and measurement of performance, benchmarking and auditing aspects of privacy management programs in an organization.

Despite the differences in social, cultural, legal, and economic factors that can limit the application of these principles in some contexts, the application of all the principles defined in this International Standard is recommended. Exceptions to these principles should be limited.

The following privacy principles form the basis for this International Standard.

Table 3 – The privacy principles of ISO/IEC 29100

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

5.2 Consent and choice

Adhering to the consent principle means:

- 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;
- obtaining the opt-in consent of the PII principal for collecting or otherwise processing sensitive PII except where applicable law allows the processing of sensitive PII without the natural person's consent;
- informing PII principals, before obtaining consent, about their rights under the individual participation and access principle;
- providing PII principals, before obtaining consent, with the information indicated by the openness, transparency and notice principle; and
- explaining to PII principals the implications of granting or withholding consent.

Provisions should be made to provide PII principals with the opportunity to choose how their PII is handled and to allow a PII principal to withdraw consent easily and free of charge. This request should be dealt with in

accordance with the privacy policy. Even if consent is withdrawn, the PII controller might need to retain certain PII for a period of time in order to comply with legal or contractual obligations (e.g., data retention, accountability). Where the PII processing is not based on consent but instead on another legal basis, the PII principal should be notified wherever possible. Where the PII principal has the ability to withdraw consent and has chosen to do so, this PII should be exempted from processing for any purpose not legally mandated.

For a PII controller, adhering to the choice principle means:

- providing PII principals with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice and to give consent in relation to the processing of their PII at the time of collection, first use or as soon as practicable thereafter; and
- implementing the PII principal's preferences as expressed in their consent.

Moreover, additional provisions can be defined for processing PII other than consent (e.g., the performance of a contract, the vital interest of the PII principal, or compliance with the law). Applicable law in some instances provides that the consent of the PII principal does not constitute a sufficient legal basis to process PII (e.g., the consent of a minor given without a parent or guardian's approval). Moreover, additional requirements on transferring PII internationally are to be considered. It is the responsibility of the PII controller to comply with these additional provisions before processing or transferring data.

5.3 Purpose legitimacy and specification

Adhering to the purpose legitimacy and specification principle means:

- 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;
- using language for this specification which is both clear and appropriately adapted to the circumstances; and
- if applicable, giving sufficient explanations for the need to process sensitive PII.

With regard to sensitive PII, stricter rules can apply to the purpose of processing. A purpose can require a legal basis or a specific authorization by a data protection authority or a government authority. If the purpose(s) for processing PII does not conform to applicable law, processing should not take place.

5.4 Collection limitation

Adhering to the collection limitation principle means:

- limiting the collection of PII to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s).

Organizations should not collect PII indiscriminately. Both the amount and the type of PII collected should be limited to that which is necessary to fulfil the (legitimate) purpose(s) specified by the PII controller. Organizations should carefully consider what PII will be needed to realize a particular purpose before proceeding with the collection of PII. Organizations should document the type of PII collected, as well as their justification for doing so as part of their information-handling policies and practices.

A PII controller might wish to collect additional PII for purposes other than the provision of a particular service requested by the PII principal (e.g., for direct marketing purposes). Depending on the jurisdiction, such additional information might only be collected with the consent of the PII principal. It is also possible that the collection of certain information is mandated by applicable law. Whenever possible, the PII principal should be given the ability to choose whether or not to provide such information. The PII principal should also be clearly informed of the fact that their response to such requests for additional information can be optional.

5.5 Data minimization

Data minimization is closely linked to the principle of “collection limitation” but goes further than that. Whereas “collection limitation” refers to limited data being collected in relation to the specified purpose, “data minimization” strictly minimizes the processing of PII.

Adhering to the data minimization principle means designing and implementing data processing procedures and ICT systems in such a way as to:

- minimize the PII which is processed and the number of privacy stakeholders and people to whom PII is disclosed or who have access to it;
- ensure adoption of a “need-to-know” principle, i.e. one should be given access only to the PII which is necessary for the conduct of his/her official duties in the framework of the legitimate purpose of the PII processing;
- use or offer as default options, wherever possible, interactions and transactions which do not involve the identification of PII principals, reduce the observability of their behaviour and limit the linkability of the PII collected; and
- delete and dispose of PII whenever the purpose for PII processing has expired, there are no legal requirements to keep the PII or whenever it is practical to do so.

5.6 Use, retention and disclosure limitation

Adhering to the use, retention and disclosure limitation principle means:

- limiting the use, retention and disclosure (including transfer) of PII to that which is necessary in order to fulfil specific, explicit and legitimate purposes;
- limiting the use of PII to the purposes specified by the PII controller prior to collection, unless a different purpose is explicitly required by applicable law;
- retaining PII only as long as necessary to fulfil the stated purposes, and thereafter securely destroying or anonymizing it; and
- locking (i.e. archiving, securing and exempting the PII from further processing) any PII when and for as long as the stated purposes have expired, but where retention is required by applicable laws.

When PII is transferred internationally, the PII controller should be cognizant of any additional national or local requirements specific to cross-border transfers.

5.7 Accuracy and quality

Adhering to the accuracy and quality principle means:

- 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;
- verifying, through appropriate means, the validity and correctness of the claims made by the PII principal prior to making any changes to the PII (in order to ensure that the changes are properly authorized), where it is appropriate to do so;
- establishing PII collection procedures to help ensure accuracy and quality; and
- establishing control mechanisms to periodically check the accuracy and quality of collected and stored PII.

This principle is particularly important in cases where the data could be used to grant or deny a significant benefit to the natural person or in which inaccurate data could otherwise result in significant harm to the natural person.

5.8 Openness, transparency and notice

Adhering to the openness, transparency and notice principle means:

- 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;
- disclosing the choices and means offered by the PII controller to PII principals for the purposes of limiting the processing of, and for accessing, correcting and removing their information; and
- giving notice to the PII principals when major changes in the PII handling procedures occur.

Transparency, including general information on the logic underlying the PII processing, can be required, particularly, if the processing involves a decision impacting the PII principal. Privacy stakeholders that process PII should make specific information about their policies and practices relating to the management of PII readily available to the public. All contractual obligations that impact PII processing should be documented and communicated internally as appropriate. They should also be communicated externally to the extent those obligations are not confidential.

In addition, the purpose of the processing of PII should be sufficiently detailed in order to allow the PII principal to understand:

- the specified PII required for the specified purpose;
- the specified purpose for PII collection;
- the specified processing (including collection, communication and storage mechanisms);
- the types of authorized natural persons who will access the PII and to whom the PII can be transferred; and
- the specified PII data retention and disposal requirements.

5.9 Individual participation and access

Adhering to the individual participation and access principle means:

- 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.

The PII controller should apply appropriate controls to ensure that PII principals access strictly their own PII and not that of other PII principals, unless the natural person accessing is acting under authority on behalf of a PII principal who is unable to exercise their right of access. Applicable law can provide the natural person with the right to access, review and object to the processing of PII under certain circumstances. When a challenge is not resolved to the satisfaction of the natural person, the substance of the unresolved challenge should be recorded by the organization. When appropriate, the existence of the unresolved challenge should be transmitted to PII processors and other third parties having access to the information in question.

5.10 Accountability

The processing of PII entails a duty of care and the adoption of concrete and practical measures for its protection. Adhering to the accountability principle means:

- documenting and communicating as appropriate all privacy-related policies, procedures and practices;
- assigning to a specified individual within the organization (who might in turn delegate to others in the organization as appropriate) the task of implementing the privacy-related policies, procedures and practices;
- when transferring PII to third parties, ensuring that the third party recipient will be bound to provide an equivalent level of privacy protection through contractual or other means such as mandatory internal policies (applicable law can contain additional requirements regarding international data transfers);
- providing suitable training for the personnel of the PII controller who will have access to PII;
- setting up efficient internal complaint handling and redress procedures for use by PII principals;
- informing PII principals about privacy breaches that can lead to substantial damage to them (unless prohibited, e.g., while working with law enforcement) as well as the measures taken for resolution;
- notifying all relevant privacy stakeholders about privacy breaches as required in some jurisdictions (e.g., the data protection authorities) and depending on the level of risk;
- allowing an aggrieved PII principal access to appropriate and effective sanctions and/or remedies, such as rectification, expungement or restitution if a privacy breach has occurred; and
- considering procedures for compensation for situations in which it will be difficult or impossible to bring the natural person's privacy status back to a position as if nothing had occurred.

Measures to remediate a privacy breach should be proportionate to the risks associated with the breach but they should be implemented as quickly as possible (unless otherwise prohibited, e.g., interference with a lawful investigation).

Establishing redress procedures is an important part of establishing accountability. Redress provides a means for the PII principal to hold the PII controller accountable for PII misuse. Restitution is one form of redress which involves providing compensation to the aggrieved PII principal. This is important not only in the situation of identity theft, reputational damage or misuse of PII but also where mistakes have been made in modifying or changing the respective PII.

Where redress processes are in place, PII principals might feel more confident entering into a transaction because the perceived risk for the natural person with regard to the outcome is effectively reduced. For some services redress is easier to achieve (e.g., financial loss) than for others (e.g., a stolen identity, damage to the image or reputation of the natural person), where the ability to quantify and compensate for the loss could be somewhat harder. Redress works best when based on transparency and honesty. Required types of redress measures can be governed by law.

5.11 Information security

Adhering to the information security principle means:

- 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;
- choosing PII processors that provide sufficient guarantees with regard to organizational, physical and technical controls for the processing of PII and ensuring compliance with these controls;
- basing these controls on applicable legal requirements, security standards, the results of systematic security risk assessments as described in ISO 31000, and the results of a cost/benefit analysis;
- implementing controls in proportion to the likelihood and severity of the potential consequences, the sensitivity of the PII, the number of PII principals that might be affected, and the context in which it is held;

- limiting access to PII to those individuals who require such access to perform their duties, and limit the access those individuals have to only that PII which they require access to in order to perform their duties;
- resolving risks and vulnerabilities that are discovered through privacy risk assessments and audit processes; and
- subjecting the controls to periodic review and reassessment in an ongoing security risk management process.

5.12 Privacy compliance

Adhering to the privacy compliance principle means:

- 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;
- having appropriate internal controls and independent supervision mechanisms in place that assure compliance with relevant privacy law and with their security, data protection and privacy policies and procedures; and
- developing and maintaining privacy risk assessments in order to evaluate whether program and service delivery initiatives involving PII processing comply with data protection and privacy requirements.

Applicable law can provide that one or more supervisory authorities are responsible for monitoring compliance with applicable data protection law. In those cases, adhering to the privacy compliance principle also means cooperating with these supervisory authorities and observing their guidelines and requests.

Annex A
(informative)

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

In order to make it easier to use the ISO/IEC 27000 family of International Standards in the specific context of privacy and integrate privacy concepts in the ISO/IEC 27000 context, the following table presents the relations between their main concepts:

Table A.1 — Matching ISO/IEC 29100 concepts to ISO/IEC 27000 concepts

ISO/IEC 29100 concepts	Correspondence with ISO/IEC 27000 concepts
Privacy stakeholder	Stakeholder
PII	Information asset
Privacy breach	Information security incident
Privacy control	Control
Privacy risk	Risk
Privacy risk management	Risk management
Privacy safeguarding requirements	Control objectives

Bibliography

[1] ISO Guide 73, *Risk management — Vocabulary*

[2] ISO 31000, *Risk management — Principles and guidelines*

[3] ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) — *Official Privacy Documents References*, available at http://www.jtc1sc27.din.de

ICS 35.040

Price based on 21 pages