INTERNATIONAL STANDARD

ISO/IEC 29101

First edition
2013-10-15

Information technology — Security techniques — Privacy architecture framework

Technologies de l'information — Techniques de sécurité — Architecture de référence de la protection de la vie privée

Reference number
ISO/IEC 29101:2013(E)

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 29101 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

Introduction

This International Standard describes a high-level architecture framework and associated controls for the safeguarding of privacy in information and communication technology (ICT) systems that store and process personally identifiable information (PII).

The privacy architecture framework described in this International Standard

— provides a consistent, high-level approach to the implementation of privacy controls for the processing of PII in ICT systems;

— provides guidance for planning, designing and building ICT system architectures that safeguard the privacy of PII principals by controlling the processing, access and transfer of personally identifiable information; and

— shows how privacy enhancing technologies (PETs) can be used as privacy controls.

This International Standard builds on the privacy framework provided by ISO/IEC 29100 to help an organization define its privacy safeguarding requirements as they relate to PII processed by any ICT system. In some countries, privacy safeguarding requirements are understood to be synonymous with data protection/privacy requirements and are the subject of data protection/privacy legislation.

This International Standard focuses on ICT systems that are designed to interact with PII principals.

Information technology — Security techniques — Privacy architecture framework

1 Scope

This International Standard defines a privacy architecture framework that:

— specifies concerns for ICT systems that process PII;

— lists components for the implementation of such systems; and

— provides architectural views contextualizing these components.

This International Standard is applicable to entities involved in specifying, procuring, architecting, designing, testing, maintaining, administering and operating ICT systems that process PII.

It focuses primarily on ICT systems that are designed to interact with PII principals.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

ISO/IEC/IEEE 42010:2011, *Systems and software engineering — Architecture description*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29100 and ISO/IEC/IEEE 42010 apply.

4 Symbols and abbreviated terms

The following abbreviations apply to ISO/IEC 29101:

ICT Information and Communication Technology

PET Privacy Enhancing Technology

PII Personally Identifiable Information

5 Overview of the privacy architecture framework

5.1 Elements of the framework

The privacy architecture framework presented in ISO/IEC 29101 is intended as a technical reference for developers of ICT systems that process PII. This standard does not set requirements for privacy policies; it assumes that a privacy policy is in place and that privacy safeguarding requirements have been defined and that appropriate safeguards will be implemented within the ICT system.

This architecture framework focuses on the protection of PII. Since this is partly a security goal, ICT systems processing PII should also follow information security engineering guidelines. This architecture framework lists some information security components that are critical for safeguarding PII processed within ICT systems. The architecture framework presented is based on the model used in ISO/IEC/IEEE 42010.

The stakeholders related to these concerns are the privacy stakeholders defined in ISO/IEC 29100. They are discussed in more detail in Clause 6.

The concerns for the architecture framework are described in Clause 7 and include the privacy principles of ISO/IEC 29100 and privacy safeguarding requirements specific to an ICT system.

The architecture framework is presented as follows:

a. the layers of the technical architecture framework in 8.2 show the architecture from a component viewpoint. Each layer groups components with a common goal or a similar function;

b. the deployment model in 8.3 shows the architecture framework from a standalone ICT system viewpoint. Each view shows a grouping of the components based on their deployment in the stakeholders' ICT systems; and

c. the views in 8.4 show the architecture framework from an interaction viewpoint. The views illustrate how the components interact between ICT systems of different stakeholders.

The architecture framework also presents correspondence rules between the concerns and viewpoints through the use of mapping tables.

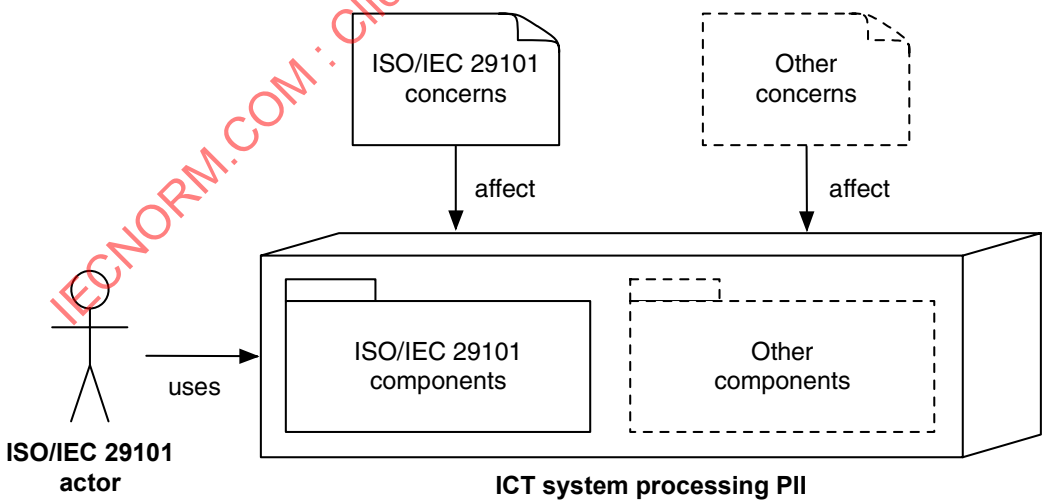

Figure 1 — Elements of the privacy architecture framework in context

Figure 1 illustrates the relationship between the elements of the privacy architecture framework. The central element of the architecture framework is the ICT system being built. An ISO/IEC 29101 actor uses the ICT system. The design of the ICT systems is affected by both ISO/IEC 29101 concerns and also other concerns.

Examples of other concerns include non-functional requirements that affect the performance, accessibility and design of the ICT system and do not affect the functional processing of PII. These other concerns are out of the scope of ISO/IEC 29101.

The ICT system may contain components from the ISO/IEC 29101 privacy architecture framework as well as other components. These components do not process PII, but instead handle other functionality in the ICT system like providing accessibility or rendering special user interfaces. Such components are out of the scope of this standard.

5.2 Relationship with management systems

The use of a management system enables PII controllers and processors to more effectively meet their privacy safeguarding requirements using a structured approach. This structured approach also provides PII controllers and processors the ability to measure outcomes and continuously improve the management system's effectiveness.

An effective management system is as transparent as possible but still impacts people, processes and technology. It should be part of the internal control program and risk mitigation strategy of an organization and its implementation helps to satisfy compliance with data protection and privacy regulations.

6 Actors and PII

6.1 Overview

The actors of the ISO/IEC architecture framework are the privacy stakeholders involved in PII processing described in ISO/IEC 29100. These actors are

a. the PII principal;

b. the PII controller; and

c. the PII processor.

NOTE The "third party" defined as one of the four categories of the actors in ISO/IEC 29100 is out of the scope of the architecture framework specified in this standard.

From the deployment viewpoint, the architecture framework is divided into three parts. Each part applies to the ICT system deployed from the viewpoint of each of these actors.

Figure 2 shows the ICT systems of the actors and the flows of PII between these ICT systems. It illustrates the logical division of functionality for the architecture framework described in this standard. It is not intended as a representation of the physical structure, organisation or ownership of ICT system hardware.

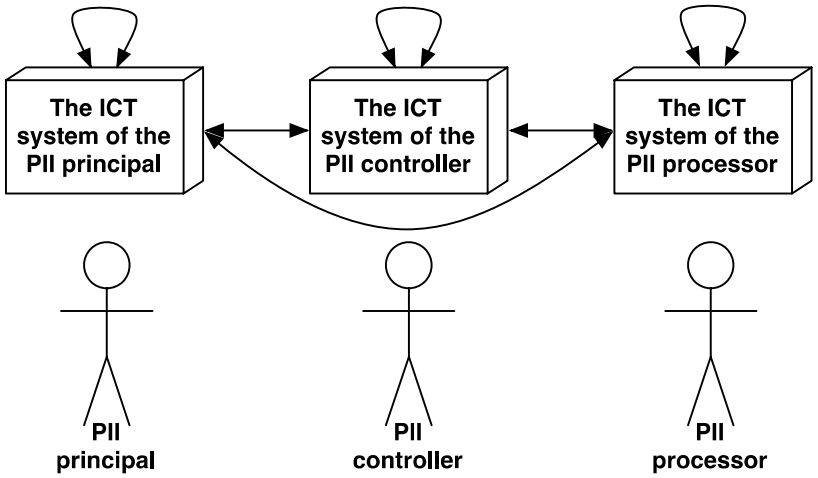

Figure 2 — The actors and their ICT systems according to ISO/IEC 29101

An actor may or may not be responsible for building the ICT systems that it uses. For example, the PII principal may use a system built by and the responsibility of the PII controller or the ICT system of the PII principal may be a part of the ICT system of the PII controller. Furthermore, the functionality of the ICT system of the PII principal might be split across different ICT hardware systems owned by the PII principal and the PII controller. Similarly, the PII controller may provide the ICT system of the PII processor. Business processes in which ICT systems are employed use a wide range of communication and trust models. The architecture framework in this international standard builds on an abstraction of these models.

If the PII principal is using a privately owned ICT system, the other privacy stakeholders may impose requirements on this ICT system. For example, the ICT system of the PII principal may have to meet a minimum baseline of security requirements to be allowed to connect to the other ICT systems. Other examples include the use of special security components like hardware authentication tokens, certain operating system versions or special web browser versions.

For example, in ICT systems employing peer-to-peer communications (communication method, communication model or communication technology featuring communication in between/among the entities that are peer to each other without central servers), every application may take the roles of all three listed actors. Information is both sent and received by each peer, so each peer could be a PII controller or processor for PII transferred by another party in the role of a PII principal.

In social networking applications, PII may be processed by anyone with access to other people's profiles. Web-based social networking applications allow all the authorized and possible anonymous users of the service to process PII provided by the PII principals connected to the social network.

6.2 Phases of the PII processing life cycle

6.2.1 Collection

Many organizations collect information from PII principals. This information can contain PII.

When collecting PII, organizations should always consider the privacy preferences and legal rights of the PII principal and privacy safeguarding requirements as stated by applicable law. Factors such as the type of PII, consent given, or any privacy preferences stated need to be considered throughout all stages of processing. PII should only be collected if it is needed for the declared purposes.

Documentation should be associated with the PII. Examples include, but are not limited to:

a. software tags that state the purpose(s) the PII can be used for;

b. records describing the purpose(s) that PII can be used for; and

c. records of the consent given and any specific sensitivities that should be observed (e.g., certain PII categories should be encrypted or deleted after a certain period of time).

Privacy controls should be implemented wherever data is tagged as PII or wherever PII is marked with additional information concerning the PII principal. It is also important to preserve tags that are relevant to processing PII during the usage, transfer, storage and disposal phases. If stored PII may have been modified, it should be validated for accuracy and currency before use.

In addition, PII collection processes should be designed to collect only the PII that is necessary for the respective transaction. Organizations should take steps to minimize the inadvertent/unintended collection of PII through data entry systems (e.g., web application forms that allow the entry of any information). The entry of arbitrary PII should be minimized through the use of context specific display of input fields reducing or eliminating areas in the web form where this information could be entered (e.g., removing unnecessary check boxes and free text fields). In addition, the use of fields with predefined entries (e.g., list boxes and drop-down lists), containing non-PII options, should be considered. When free form text fields are necessary, the User Interface (UI) should provide:

a. warnings to alert the PII principal not to enter PII other than that which is explicitly asked for and consented to or required by applicable law;

b. clear indication of those fields where PII is to be entered and what PII should be entered (e.g. name, address, health information); and

c. clear indication of those fields where PII should not be entered.

6.2.2 Transfer

Transferring, disseminating, or releasing PII to others means that the PII is no longer under the sole control of the PII principal. Transfer is usually the term given for dissemination of PII from the PII controller or PII processor to other PII controllers and processors. If PII is transferred from the PII controller to another actor, transfer is sometimes also referred to as disclosure.

Accountability and responsibility for the transferred PII should be agreed upon and maintained by each party involved in the PII processing. This agreement should be in writing where required by applicable law. Furthermore, such agreements will need to be compliant with data protection legislation in the source and destination domains of the transfers. When relevant and appropriate, or when legally required to do so, the PII principal should be notified that transfer is taking place and should be informed of the content and purpose of the transfer. If a dispute occurs between the PII principal and the PII controller or PII processor, records of relevant PII transfer transactions should be available to assist in resolving any such dispute.

The transfer of sensitive PII should be avoided unless it is necessary to provide a service that the PII principals has requested, it fulfils a business requirement for offering the requested service, or unless it is required by law. Some jurisdictions have instituted laws that specifically require formal contractual agreements that include all privacy safeguarding requirements between the involved parties when PII is transferred outside a jurisdiction that has a prescribed level of privacy protection. Where cross-border transfers are used, particular attention should be given to protection measures for the PII being transferred.

Appropriate protection mechanisms should be in place during the transfer of PII. In the case of a digital transfer, PII should be transmitted over a secure channel or in encrypted form if the transmission is over an insecure channel. If PII is transferred on physical media, it should be encrypted. If encryption is used, the encryption key should not be stored or transmitted together with the encrypted PII.

6.2.3 Use

Using PII means any form of PII processing that does not include “collect”, “transfer”, “store”, “archive” or “dispose”. The privacy principles described in ISO/IEC 29100 (Privacy Framework), as well as some data

protection and privacy laws, may limit the processing of PII if that processing is incompatible with the originally specified purposes. Therefore, PII should only be processed for the declared purposes for which it was collected.

If the PII is to be processed for any other purpose that is not covered by applicable law, consent should be obtained from the PII principal or his agent. The PII principal should be provided a means for contacting the PII controller or processor in the event there are any questions about any activities about which the PII principals is unclear.

Where such processing is considered necessary the consent of the PII principal should be obtained unless otherwise permitted by law. PII principals should be provided clear notice about the specific use of the PII.

Additionally, protection mechanisms appropriate to the usage of PII should be applied as deemed necessary by a thorough risk analysis. This includes the use of anonymization or pseudonymization techniques prior to processing and the use of secure computation techniques during processing.

6.2.4 Storage

When it is necessary to store PII, the consent of the PII principal should be obtained, taking into account any specific measures that may be required by law. In such cases, the PII should be stored only for the amount of time necessary to achieve the specific business purpose.

PII should be stored with appropriate controls and mechanisms to prevent unauthorized access, modification, destruction, removal, or other unauthorized use. Such controls include, but are not limited to, encryption, secret sharing, pseudonymization and anonymization.

Archived PII needs careful attention. The privacy principles state that PII should be retained only as long as necessary to fulfil the stated purposes and then be securely destroyed or anonymized. However, if the PII controller or PII processor is required by applicable law to retain PII after the other purposes have expired, the PII should be locked (i.e., archived and protected with an access control mechanism to prevent further usage). The primary considerations in archiving PII should be to ensure that the appropriate data protection mechanisms are in place, including access management solutions that provide access to archived PII only to authorized users.

The PII controller should implement controls in storage systems to dispose of PII when it expires or when the purpose for the storing or processing of the PII is no longer valid.

6.2.5 Disposal

In the final stage of the PII processing life cycle, PII gets deleted, anonymized, destroyed, returned or disposed of in some other way. Specific PII within PII records might get locked from unauthorized use by marking it for disposal. It should be noted that deleting PII does not necessarily mean that the PII is ultimately disposed of because PII deleted in ICT systems can often be recovered. Although it might seem to be an obvious task in PII handling, procedures concerning disposal of PII sometimes do not comply with privacy safeguarding requirements. Specifications given by the PII principal (e.g., usage purpose) or requirements specified by legislation (e.g., expiration date for specific PII) should be considered before PII is disposed of.

7 Concerns

7.1 Overview

A concern as defined in ISO/IEC/IEEE 42010 is an interest in a system relevant to one or more of its stakeholders. The privacy architecture framework in ISO/IEC 29101 focuses on concerns of the privacy stakeholders related to the processing of PII. The ISO/IEC 29101 concerns include the privacy principles of ISO/IEC 29100 and any privacy safeguarding requirements derived from and complying with these principles.

The privacy safeguarding requirements should be determined by following a privacy risk management process complying with the process described in 4.5 of ISO/IEC 29100. Any individual or organization that is designing an ICT system that processes PII should follow this process. All the identified privacy safeguarding requirements should conform to applicable privacy legislation.

7.2 The privacy principles of ISO/IEC 29100

The PII controller is responsible for the protection of PII and the fair and lawful handling of it at all times, throughout the organization, as well as for PII processing outsourced to PII processors.

The PII controller is ultimately responsible for implementing privacy controls in an ICT system. Privacy controls are intended to ensure that the privacy safeguarding requirements set for a specific PII principal, transaction, or scenario are addressed and consistently fulfilled. Evidence of implementation should be provided by properly documenting the privacy controls that are in place and providing audit documents that verify that the controls exist, that they have been implemented correctly and that they are functioning properly. Ultimately, the PII controller should accept and adhere to the privacy principles that are described in ISO/IEC 29100.

a. consent and choice;

b. purpose legitimacy and specification;

c. collection limitation;

d. data minimization;

e. use, retention and disclosure limitation;

f. accuracy and quality;

g. openness, transparency and notice;

h. individual participation and access;

i. accountability;

j. information security; and

k. privacy compliance.

7.3 Privacy safeguarding requirements

ICT systems should implement privacy controls as a primary element in every phase of the PII processing life cycle. The privacy safeguarding requirements enable the designer of the ICT system to operationalize the link between privacy principles and the architectural components laid down in Clause 8.

In order to implement effective privacy controls in an ICT system, PII processing flows describing the PII processing should be created. PII processing flow diagrams are a graphical representation of the “flow” of PII through the ICT system and between the different actors. For example, if an actor transfers PII to other actors (e.g., PII processors) the PII processing flow diagram should include those PII transfers.

A PII processing flow diagram may also be represented as a PII flow table. This diagram or table follows the collection, transfer, use, storage or disposal of PII and includes information such as the type of PII, who collected the PII, the purpose for processing, to whom the PII is going to be transferred, the receipt of consent by the PII principal, the retention period and at which location it will be stored and the resulting privacy risk level. The PII processing flow information will be an input to the privacy risk management process that outputs the privacy safeguarding requirements.

After the requirements analysis of an ICT system has been completed, the developers should cross-reference the privacy safeguarding requirements of the ICT system with the list of concerns in this standard. The privacy safeguarding requirements should then be used for choosing the architectural components that satisfy said requirements.

Annex A of this international standard contains an example list of concerns and illustrates how to link concerns to the privacy principles of ISO/IEC 29100 and the architectural components of ISO/IEC 29101.

8 Architectural views

8.1 Introduction

The architectural views in this clause are structured into three views. First, the component view describes the ICT system components in detail and separates them into layers based on their functionality. Each layer groups components that help to contribute to the proper processing of PII. Limited implementation guidance is given for each component. Actor-specific guidance is given where applicable. This view is helpful for understanding the building blocks in the privacy architecture framework.

Tables showing examples of typical relationships between the privacy principles of ISO/IEC 29100 and the components of the architecture are provided in the component view. Such mapping tables are helpful for understanding how an ICT system adheres to the privacy principles of ISO/IEC 29100. Similar tables could be used as examples and updated during system design to describe how a particular ICT system adheres to the privacy principles in ISO/IEC 29100.

The actor view looks at the components described in the component view from the perspective of the ICT system of an individual actor. This view is helpful in the design of the architecture of a particular ICT system. The interaction view looks at the components from a deployment perspective. This view is helpful for understanding how components in the ICT systems of different actors interact with each other.

8.2 Component view

The component view is meant to describe ICT system components that are involved in the processing of PII.

The choice of components should be guided by the appropriate privacy safeguarding requirements. The developer of the ICT system for a specific actor(s) (see Figure 2) should use the component view to determine the components that need to be included in the architecture of the system that they are developing. This architecture should be based on the privacy safeguarding requirements established using the guidance given in Clause 7. Note that not all components described in this international standard will necessarily be appropriate in a particular ICT system.

The component view is presented in three layers. Each layer is a logical group of components that contribute to a specific goal in the processing of PII. Components in the privacy settings layer handle the management of metadata about PII processing including, among others, the exchange of information on the purpose of processing, consent and preferences of the PII principal. Components in the identity and access management layer are responsible for ensuring that proper identity information is used in PII processing and access to the PII is controlled according to the privacy safeguarding requirements. Finally, components in the PII layer perform various tasks to process the PII.

The architecture framework is designed with the assumption that all components interact with several other components. However, in order to maintain generality and readability, the possible interactions between components have been omitted from the representation.

Some of the components in the architecture framework are Privacy Enhancing Technologies (PETs). This selection of PETs is not comprehensive. There exist other PETs that are not described within this standard and the developer of the ICT system is responsible for choosing appropriate PETs and adapting them to this architecture framework.

Annex B of this international standard gives an example of an ICT system architecture that applies PETs for securely processing PII. Annex C of this international standard gives an example of how to use attribute-based credentials to build an ICT system that provides pseudonymous identity and access control management.

The following sections describe the layers, the components within them and the actors that interact with the components. A general description of each component is given and it is followed by actor-specific guidelines. For some components, no guidance specific to the ICT systems of a particular actor is given, as the behaviour of the component is similar in the ICT systems of all actors.

8.2.1 Privacy settings layer

The privacy settings layer comprises components that communicate the system privacy policy to the relevant actors and implement the system privacy safeguarding requirements. These components let the ICT system communicate the system privacy policy and implement the corresponding privacy safeguarding measures.

In addition, the components in this layer should convey to the PII controller and PII processor any privacy preferences and consent information that have been collected from the PII principal.

8.2.1.1 Policy and purpose communication

General. This component is responsible for relaying information, including updates, about the privacy policy of the PII controller and the purpose of PII collection to the ICT systems of privacy stakeholders.

The communicated information should contain at least the following:

a. the identities of the PII controllers and any associated PII processors;

b. policies regarding the transfer of PII to PII processors;

c. the use of privacy enhancing technologies (such as anonymization) with their respective goals;

d. the purposes for which the PII is collected;

e. identification of the PII to be collected; and

f. the legal rights of the PII principal to access their PII to determine the extent of the PII stored and to check for and correct any inaccuracies, and the procedures for doing so.

PII principal. The policy and purpose communication component of the ICT system of the PII principal should:

a. receive policy and purpose information from the corresponding component in the ICT system of the PII controller;

b. interpret the received information and display or otherwise convey to the PII principal in a clearly comprehensible manner its meaning;

c. offer the PII principal the opportunity to locally store the received information; and

d. confirm to the PII controller that the policy and purpose information has been received by the PII principal.

PII controller. The policy and purpose communication component of an ICT system under the control of the PII controller should:

a. store policy and purpose information that has been conveyed to PII principals;

b. log the acts of conveying policy and purpose information to PII principals in such a way that it can be established which information was current and was conveyed to PII principals at which time, along with confirmation of receipt of this information;

c. convey the current policy and purpose information to the corresponding component of the ICT system of the PII principal in such a manner that it can be used by this system directly to inform the PII principal in a complete and comprehensible manner, or that it can be mapped by said component to such a form by some pre-defined mapping;

d. convey a reference to the displayed policy and purpose information to those components which handle the storage of consent information and storage of PII itself; and

e. transmit updates about changes to policy and purpose information to the corresponding components of the ICT systems belonging to those PII principals who have consented to receive such information.

PII processor. The ICT system of the PII processor typically should receive digital copies of the privacy policy and the processing purpose from the ICT system of the PII controller. The ICT system of the PII processor should present the privacy policy and processing purpose documentation received from the PII controller in a clearly comprehensible form to everyone with access to PII governed by that policy.

The PII controller may arrange the processing of PII by various PII processors. The purpose communication component in the ICT system of the PII controller should transmit the purpose associated with the PII provided to all relevant PII processors. Each PII processor should be informed of the purpose(s) for processing the PII.

8.2.1.2 PII categorization

General. An ICT system processing PII has to be aware of the categories of PII that it processes so that it can distinguish between different types of data (e.g., sensitive PII, PII and non-PII). This is necessary for services processing PII differently depending on category. Additionally, the ICT system should be aware of PII values that contain direct identifiers such as names and social security numbers. This component should implement the functions that provide such a categorization in the ICT system.

When dealing with non-PII, the risk of combining non-PII to infer or derive an identity or profile of a unique user or at least small enough subset of users should be understood and evaluated.

All PII should be categorized correctly in order that it is processed and stored by the ICT system in accordance with its marked sensitivity. If PII has been unknowingly collected, e.g. as a result of unsolicited input, it may not be possible to do this and measures should therefore be taken to minimise the possibility of unsolicited PII collection.

While the ICT system should be aware of PII values that contain direct identifiers such as names and social security numbers, it may not be possible to do this if unsolicited PII has been collected.

PII principal. The ICT system of the PII principal should be capable of identifying the categorization marking associated with the PII and should process the PII in accordance with its category. The categorisation can also be used to identify the PII that should be protected using PETs (e.g. sensitive PII). The PII categorization component also provides further categorization of the PII into sub-categories where sub-categories are a requirement of a specific application domain.

PII controller. The ICT system of the PII controller should contain a comprehensive categorization of PII used in the ICT systems processing the categorized PII. This information should be transmitted to PII processors. Also, this categorization can be used by the audit logging, PII pseudonymization, PII disclosure and PII archiving and retention components so they can determine which parts of the data contain PII.

PII processor. The ICT system of the PII processor should be capable of processing the PII categorization associated with the received PII. The information should be used in PII auditing and secure PII processing.

8.2.1.3 Consent management

General. Consent of the PII principal is an important prerequisite of PII processing, unless such processing is otherwise permitted by law.

This component handles consent management tasks including, but not limited to:

a. obtaining the informed consent of the PII principal;

b. storing consent information in the ICT systems of a privacy stakeholder;

c. relating the stored consent information to the version of policy and purpose information for which the consent was given;

d. checking consent prior to PII processing; and

e. maintaining the status of consent information.

Applicable law may result in the overriding of absence or limitation of consent expressed by the PII principal.

PII principal. The PII controller should obtain the informed consent of the PII principal with the help of the consent management component in the ICT system of the PII principal. Under certain circumstances, the PII principal may modify or withdraw consent and this information should be relayed to the ICT system of the PII controller.

PII controller. In the ICT system of the PII controller, this component should maintain up to date information about the status of consent. The ICT system of the PII controller should be capable of retrieving, storing, managing and maintaining the consent information.

The ICT system of the PII controller should transmit consent information to other parties in the system that require it. Additionally, this component should accept updates to the PII principal's consent status (e.g., modification or withdrawal of consent). The ICT system of the PII controller should present and propagate this information as necessary.

PII processor. The ICT system of the PII processor should verify the existence of consent from all PII principals associated with the PII provided to it. This information should comes from the ICT system of the PII controller. Before any processing, the ICT system of the PII processor should make sure that it has current consent information about the respective PII principals. The ICT system of the PII processor should be ready to accept changes to the consent status when such changes are notified by the PII controller.

8.2.1.4 Privacy preference management

General. In some situations, the PII principal may be able to express his/her preferences as to how his/her PII may be processed by a PII controller or processor. In these instances, the respective ICT systems of the actors should be capable of recording those preferences and making them known to the PII controller and processor as appropriate. The PII controller and processor should be capable of understanding those preferences and should, to the maximum extent possible, respect those preferences when processing PII.

PII principal. If the PII processing is based upon privacy preference settings, then the PII principal should be provided with an interface for choosing the settings most suitable for his/her purpose. For example, these may include settings determining how the ICT system uses, transfers or discloses PII.

PII controller. If the PII principal has specified any privacy preferences, the ICT system of the PII controller should present these choices to the PII controller.

The ICT system of the PII controller should collect the relevant privacy preferences the PII principal may have indicated from the choices available, if any. The controller should also propagate this information to any parties that process the PII associated with these preferences.

PII processor. If relevant to the PII processor's assigned tasks, the ICT system of the PII processor should be aware of and act upon any restrictions set on PII processing by the selected privacy preferences of the PII principal. This information and its possible updates should be acquired from the PII controller or directly from the PII principal via their respective ICT systems.

8.2.1.5 Relationship between privacy principles and components in the privacy settings layer

Table 1 shows an example mapping from the privacy principles of ISO/IEC 29100 to the components of the privacy settings layer. An 'X' in the table indicates a relationship between a component of the layer and a principle. This relationship, however, is only shown as an example.

Table 1 — Example of the relationship between privacy principles and the components in the privacy settings layer

Components \ Principles	Consent and choice	Purpose legitimacy and specification	Collection limitation	Data minimization	Use, retention and disclosure limitation	Accuracy and quality	Openness, transparency and notice	Individual participation and access	Accountability	Information security controls	Compliance
Policy and purpose communication	X	X	X	X			X		X		X
PII categorization			X	X	X						
Consent management	X	X	X					X			
Privacy preference management	X	X	X		X		X				

8.2.2 Identity management and access management layer

Components in the identity and access management layer help to identify the actors of ISO/IEC 29101 and their ICT systems and manage the related identity information. Additionally, components in this layer control how the actors of ISO/IEC 29101 access PII. The components implement the following functionality:

a. managing the identities of the privacy stakeholders;

b. managing the identities of the actors who are using the ICT systems;

c. providing this information to other components in the ICT systems; and

d. managing the mappings between PII principal identities and pseudonyms for the pseudonymization of PII.

The identity and access management layer provides identity information to components in other layers that require it. Note that this standard does not specify the identity management techniques that should be used.

8.2.2.1 Identity management system

General. This component can have several purposes, each one can be implemented by a distinct identity management system.

First, the component could manage the identities of the PII principals whose PII is processed in the ICT system. Second, the component could manage the identities of the users of the ICT systems that process PII. Third, the component could manage the identities of the ICT systems of the privacy stakeholders. This would allow the ICT systems of different privacy stakeholders to mutually authenticate each other during PII transfer. This list of examples is not exhaustive.

Mechanisms for addressing the nature and accuracy of the underlying identity information are not defined by this standard. The functionality of the identity management component is similar for all actors.

8.2.2.2 Pseudonymization scheme

General. If pseudonymization is used in PII processing, the ICT systems involved should have functions for managing the individual pseudonymization function instances that are in use.

The pseudonymization scheme component in the identity and access management layer contains information about the implemented pseudonymization scheme and its parameters. For example, if an encryption scheme is used, this component stores the keys used.

The related PII pseudonymization component in the PII layer is used to perform the actual transformations on PII.

PII principal. If pseudonymization is used in the ICT system of the PII principal, the system should have a description of the implemented pseudonymization scheme. The pseudonymization component in the PII layer of the ICT system of the PII principal should then apply this pseudonymization scheme to PII.

PII controller. Pseudonymization schemes may be managed by the ICT system of the PII controller. In this case, the ICT system of the PII controller transmits information about the pseudonymization schemes used to the ICT systems of the PII principals and PII processors. This may be needed in order to ensure that the pseudonymized PII from the PII principal's ICT system can be processed in the ICT systems of the PII controller and the PII processor. Also note that multiple instances of a pseudonymization scheme may be necessary, for example, to pseudonymize PII differently for different processors.

PII processor. If the PII processor needs to perform pseudonymization according to the instructions of the PII controller, it also needs to implement this component to manage the schemes.

8.2.2.3 Access control

General. Access control mechanisms should ensure that access to the features in the PII-handling ICT system is only granted within the restrictions set by the privacy safeguarding requirements. For example, if PII collection from the PII principal is performed using a web form and it takes place over a certain period of time, access to the web form should be provided only during that time. In this example, the ICT system of the PII controller should restrict the access of PII principals to the PII collection form.

The functionality of the access control component is similar for all actors. The rules and methods for access control in each ICT system will be derived from the privacy safeguarding requirements.

8.2.2.4 Authentication

General. Authentication is an important security component of an ICT system that processes PII. It can ensure the confidentiality and integrity of PII collected, stored and processed by the system.

The authentication component can have several purposes. First, it can handle the authentication of the users operating the ICT system. Second, it can handle the mutual authentication of ICT systems or their components as part of secure PII access and transfer. This list of examples is not exhaustive.

The rules and methods used in each deployment of the ICT system should be considered separately, taking into account the security goals of the actor who uses the ICT system.

As an example, the ICT system of the PII principal should authenticate the PII principals using the system. Similarly, the ICT system of the PII principal should authenticate the PII controller before transferring PII to the ICT system of that PII controller.

The functionality of the authentication component is similar in the ICT systems of all actors.

8.2.2.5 Authorization

General. In ICT systems where the access of any actor is restricted, an authorization system should be in place. Only authorized users of the ICT system should be given access to PII. For example, the PII principals targeted in PII processing can access the PII they are associated to.

The functionality of the authorization component is similar for all actors. The rules and methods for authentication in each ICT system will be derived from the privacy safeguarding requirements.

8.2.2.6 Relationship between privacy principles and components in the identity and access management layer

Table 2 shows an example mapping from the privacy principles of ISO/IEC 29100 to the components of the identity and access management layer. An 'X' in the table indicates a relationship between a component of the layer and a principle. This relationship, however, is only shown as an example.

8.2.3 PII layer

The components in the PII layer should implement the following functionalities:

a. PII collection and transfer;

b. PII processing, including secure processing, and presentation;

c. storing and archiving of PII; and

d. auditing PII and logging transactions occurring on it.

Table 2 — Example of the relationship between privacy principles and the components in the identity and access management layer

Components \ Principles	Consent and choice	Purpose legitimacy and specification	Collection limitation	Data minimization	Use, retention and disclosure limitation	Accuracy and quality	Openness, transparency and notice	Individual participation and access	Accountability	Information security controls	Compliance
Identity management system					X		X			X	
Pseudonymization scheme				X	X				X	X	
Access control					X	X		X	X	X	
Authentication					X	X		X	X	X	
Authorization					X	X		X	X	X	

This standard only proposes generic PII management requirements, leaving the specifics up to the application designer. Relevant privacy safeguards (or controls) should be used to reduce the risk of privacy breaches during the processing of PII.

The PII layer uses information from the privacy settings layer to enforce the measures in the privacy safeguarding requirements that relate to the processing of PII.

8.2.3.1 PII management

General. Any ICT system processing PII should have certain basic features for managing PII in the ICT system. These include PII entry, access, update and removal. When needed, the ICT system should be able to support a continuous process that provides for the collection and processing of PII over the lifetime of the system.

PII principal. The PII management component of the ICT system of the PII principal focuses on the collection and local processing of PII collected from the PII principal.

PII controller. The PII management component of the ICT system of the PII controller should be capable of exchanging PII with the ICT systems of the PII principals (PII collection) and PII processors (to delegate processing). Note that the privacy policy, the use of various PETs and other factors may restrict the PII management tools available in the ICT system of the PII controller. For example, the ICT system of the PII controller may be forbidden from adding or linking PII with other information.

PII processor. The PII management component of the ICT system of the PII processor handles the PII received from the PII controller.

8.2.3.2 PII transfer

General. The PII transfer component is responsible for PII exchanges between the ICT systems of the various privacy stakeholders. PII transfer should include mutual authentication and encryption between the source

and destination points in order to protect the PII transfer and ensure its confidentiality. In that case, the PII transfer component should use the Authentication and PII encryption components.

8.2.3.3 PII validation

General. The PII that is being processed should be validated for accuracy of data and correctness of format. The component should have sufficient information about the data model and the range of permissible values in order to warn the privacy stakeholder using the ICT system about possible errors in PII input.

PII principal. The ICT system of the PII principal performs validation on the data collected from the PII principal or PII principals using the ICT system.

PII controller. Even when the ICT system of the PII principal is designed to perform PII validation, the ICT system of the PII controller should perform the same and possibly additional checks to ensure the accuracy of data and correctness of format of the PII. The ICT system of the PII controller may also perform global checks for outliers and statistical deviations.

PII processor. The ICT system of the PII processor should perform duties similar to the ones of the ICT system of the PII controller.

8.2.3.4 PII pseudonymization

General. The pseudonymization component in the PII layer uses a pseudonymization scheme as described in the identity and access management layer to replace the identifiers that reveal the true identity of PII principals with pseudonyms that hide the true identities.

The other way for achieving the goals of pseudonymization can often be achieved by rendering the information partially anonymous.

Examples of when pseudonymization can be used include cases when:

a. the identity of the PII principal is not required for achieving the goals of PII processing; and

b. the pseudonymous identifier is required for processing PII (e.g., to link several databases or re-identify an individual).

PII principal. The ICT system of the PII principal performs pseudonymization on the PII that has been collected before it is sent to the ICT system of the PII controller.

PII controller. The pseudonymization component in the ICT system of the PII controller can be used for processing the pseudonymized identities in PII received from the ICT system of the PII principal. If the pseudonymization scheme is based on a two-way function that is shared by the PII principal and the PII controller, then the latter can also re-identify the PII when needed. The ICT system of the PII controller can also use pseudonymization on PII that is transmitted to the ICT system of the PII processor. Different or differently parameterized pseudonymization functions should be used when disclosing PII to different actors.

For example, if the PII is transferred to the ICT systems of several PII processors, different pseudonymization functions should be used on the PII given to each processor to reduce the risk of collusion among the processors. The PII controller keeps a registry of PII processors and their respective pseudonymization keys. Additionally, each occurrence of PII disclosure should be logged by both sides of the disclosure transaction – the ICT systems of both the PII controller and the PII processor.

PII processor. The ICT system of the PII processor can perform pseudonymization, if instructed to do so by the PII controller.

8.2.3.5 PII anonymization

General. The anonymization process takes PII and removes all personal identifiers or otherwise irreversibly alters it 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.

Examples of anonymization techniques include:

a. generalizing the PII, making information less precise, such as grouping continuous values or replacing categorical values with broader terms;

b. suppressing the PII—deleting an entire record or certain parts of records that would render it identifiable;

c. introducing noise into the PII—adding small amounts of variation into selected information fields such as weight, height or age;

d. swapping the PII—exchanging certain PII fields of one record with the same PII fields of another similar record (e.g., swapping the postal codes of two records); and

e. replacing PII with the average value—replacing each value of PII within clustered records with the average value for the entire group of PII.

There exist techniques that leave a possibility of re-identifying the PII principal associated with the data. Such techniques are not suitable for application in this component. Furthermore, there exist anonymization techniques that may accidentally transform PII so that it identifies a different PII principal. The quality of the anonymization technique used should be evaluated before including it in the design of the ICT system.

PII can be anonymized by the ICT system of any privacy stakeholder before transfer to the ICT systems of other privacy stakeholders.

8.2.3.6 Secret sharing

General. Secret sharing is a technique for distributing PII values into shares that individually reveal no information about the original value. Secret sharing can be used for PII collection to reduce the risk of a privacy breach. Secret sharing provides better privacy when performed at the ICT system of the PII principal and used in conjunction with secure multiparty computation.

Secret sharing can be used to reduce the risk of insider attacks, as a party with access to a share of a PII value cannot learn the original value from it. This makes insider attacks significantly more complex. For optimal results, secret sharing requires that there is more than one instance of each actor in the system. Each instance should store and process a limited number of shares.

PII principal. The ICT system of the PII principal can perform secret sharing on the PII collected from PII principals. The resulting shares are then transmitted to the PII controllers.

PII controller. The ICT system of the PII controller can use secret sharing to process secret-shared PII received from the ICT system of the PII principal or to perform secret sharing on plain PII before it is transmitted to the ICT system of the PII processor.

PII processor. The ICT system of the PII processor can use secret sharing for one of two purposes. The first is to store or load secret-shared PII before processing. In this case, the PII is stored in secret-shared form, but it is reconstructed before processing. The second is to use it in conjunction with secure multiparty computation. In that case, it is possible to perform computations directly on secret-shared PII.

8.2.3.7 PII encryption

General. PII encryption components should provide mechanisms for encrypting PII before it is stored. The design of an ICT system should include defining which stored PII needs to be encrypted. Depending on the privacy safeguarding requirements, the encryption keys can be shared between ICT systems so each of them can decrypt the PII and access it appropriately. If a secure computation technique that is capable of processing encrypted PII is used, the information does not have to be decrypted in order to be processed.

The component services include key management, encryption of PII within databases and encryption of stored PII such as backup files and archives.

PII encryption can be used for protecting stored PII. This can be done for two purposes. Firstly, one can store encrypted PII to prevent unauthorized access to it. If it needs to be processed, it is decrypted with the respective decryption key. Encrypting PII reduces the security risk of data breach from backups. The keys used for encryption should be stored separately from the encrypted PII.

Additionally, PII can be encrypted to prepare it for processing in encrypted form using secure computation techniques such as homomorphic encryption.

In all cases, suitable key-lengths should be defined such that current and near-future computational resources cannot break that key.

8.2.3.8 PII use

General. In order to use PII in computations or analyses, the ICT system of the actor should implement a PII use component. This component implements the business logic of the PII processing. Note that some PII use scenarios could be implemented using secure computation to reduce the risk of leaking PII.

8.2.3.9 Secure computation

PII controller and PII processor. Secure computation can be used to let PII controllers and PII processors process PII without having access to the raw input values. Instead, secure computation techniques perform computations on PII that has been transformed by PETs such as encryption or secret sharing.

A subset of secure computation techniques known as secure multiparty computation is a technique whereby multiple parties can jointly compute some value based on individually held secret parts of information without revealing those secrets to one another in the process. For optimal protection against privacy breaches, secure multiparty computation should involve several PII controllers or PII processors and their ICT systems, each with their respective secret information

Secure computation can reduce the risk of PII leaks from the ICT system of the actor, as PII is not provided to the processing party in a clear form.

8.2.3.10 Query management

General. The query management component of the ICT system of the PII controller and/or PII processor is deployed for filtering incoming queries. For example, a service can refuse to respond to a statistical query if there are not enough inputs for that query. While the refusal to reply to a query still provides some information to the privacy stakeholder making the query, the technique should still be considered in certain scenarios.

Query management is a specific technique used in data mining applications for minimizing PII processing. This technique facilitates the provision of PII analysis services while not risking the misuse of PII and not jeopardizing the precision of the data mining algorithms. The query management process should be used to ensure that a only sufficient PII for the processes involved is processed.

Methods of query management include restricting the size of query results, controlling the overlap amongst successive queries, keeping audit trails of all answered queries and constantly checking for possible compromises, suppression of PII cells of small sizes and clustering entities into mutually exclusive atomic populations.

8.2.3.11 PII inventory

General. The PII inventory component provides an overview of the PII stored in the ICT system. Information from the PII categorization system should be used to categorize the PII values stored in the system. The identity management system should be used to determine the PII principal related to a particular item of PII. The PII inventory component should be capable of providing the privacy stakeholder using the ICT system with at least the following metrics:

a. the amount of PII in the system (number of records, metadata about the records); and

b. the number of PII principals who have provided information.

Depending on the privacy safeguarding requirements, this component can provide additional information such as the list of PII principals.

The PII inventory component has a similar function in all the actors – to provide an overview of how much PII is kept locally and who are the respective PII principals. The ICT system of the PII controller should extend this functionality by keeping records of the PII processing undertaken by the ICT systems of the PII processors. This should be done in collaboration with the respective PII management and archival components in the ICT system of the PII processor.

8.2.3.12 PII disclosure

PII controller. The PII disclosure component is responsible for managing any disclosure of PII by the PII controller. This may include preparing PII before it leaves the ICT system of the PII controller. For example, the PII controller can pseudonymize or anonymized PII using the respective component before sending it to a PII processor. PII disclosure often requires the use of the PII transfer component.

If pseudonymization is used during PII disclosure, the log should also contain a description of the pseudonymization function used to disclose the PII. In this case, different pseudonymization functions should be used during disclosures as this reduces the feasibility of linking together disclosed databases, as the same identifier will not be mapped to the same pseudonym.

PII processor. PII can be disclosed by the ICT system of the PII processor in a similar manner as in the ICT system of the PII controller. Any such disclosure should be performed according to the directions of the PII controller.

8.2.3.13 PII archiving and retention

General. When PII is not in active use and is scheduled to be archived, it should be prepared for archiving. The archiving and retention component should ensure that the archive is sufficiently protected and that archiving and retention procedures are followed. Encryption, secret sharing and pseudonymization can be used to protect archived PII from unauthorized processing. It is important to know which encryption key, secret sharing scheme or pseudonymization scheme was used during the process in order to recover PII later.

If the PII retention period has passed, this component should schedule the anonymization or secure removal of the PII from the system.

8.2.3.14 Audit logging

The audit logging component should log each transaction performed on PII. This component should be integrated with every other component so that it can log all relevant activities.

The identity of the actor or actors who access PII, initiate PII transactions or receive PII resulting from PII transactions should be recorded in the transaction log. This will entail the integration of audit logging with the authentication, authorization and PII layer modules. Secure logging techniques should be used to prevent tampering with the log entries.

8.2.3.15 Relationship between privacy principles and the components in the PII layer

Table 3 shows an example mapping from the privacy principles of ISO/IEC 29100 to the components of the PII layer. An 'X' in the table indicates a relationship between a component of the layer and a principle. This relationship, however, is only shown as an example.

Table 3 — Example of the relationship between privacy principles and the components in the PII layer

Components \ Principles	Consent and choice	Purpose legitimacy and specification	Collection limitation	Data minimization	Use, retention and disclosure limitation	Accuracy and quality	Openness, transparency and notice	Individual participation and access	Accountability	Information security controls	Compliance
PII management	X	X	X	X	X		X	X			
PII transfer	X	X		X	X		X	X			
PII validation						X					
PII pseudonymization				X						X	
PII anonymization				X						X	
Secret sharing				X						X	
PII encryption				X						X	
PII use	X	X		X	X	X	X				
Secure computation				X						X	
Query management				X	X					X	
PII inventory				X	X		X		X		
PII disclosure	X	X		X	X		X				
PII archiving and retention	X	X		X	X		X				
Audit logging									X	X	

8.3 Actor view

The actor view illustrates how the components in the ISO/IEC 29101 architecture framework are deployed into the ICT systems of a particular privacy stakeholder. For each actor, the view gives a subset of components that are suitable for deployment in the ICT system of that actor. The developer uses this view to decide which components should be included in the architecture of the ICT system of a privacy stakeholder.

This view does not make any component mandatory in the ICT system of a particular privacy stakeholder.

8.3.1 ICT system of the PII principal

The ICT system of the PII principal focuses on but is not limited to, communicating the privacy policy, handling consent management and PII collection.

Since the PII principal is the party that provides PII to the overall system, the ICT system in use by the PII principal should contain components for securing PII during collection. These techniques may include, but are not limited to, pseudonymization, anonymization, encryption and secret sharing.

The architecture for the ICT system of the PII principal is presented in Figure 3.

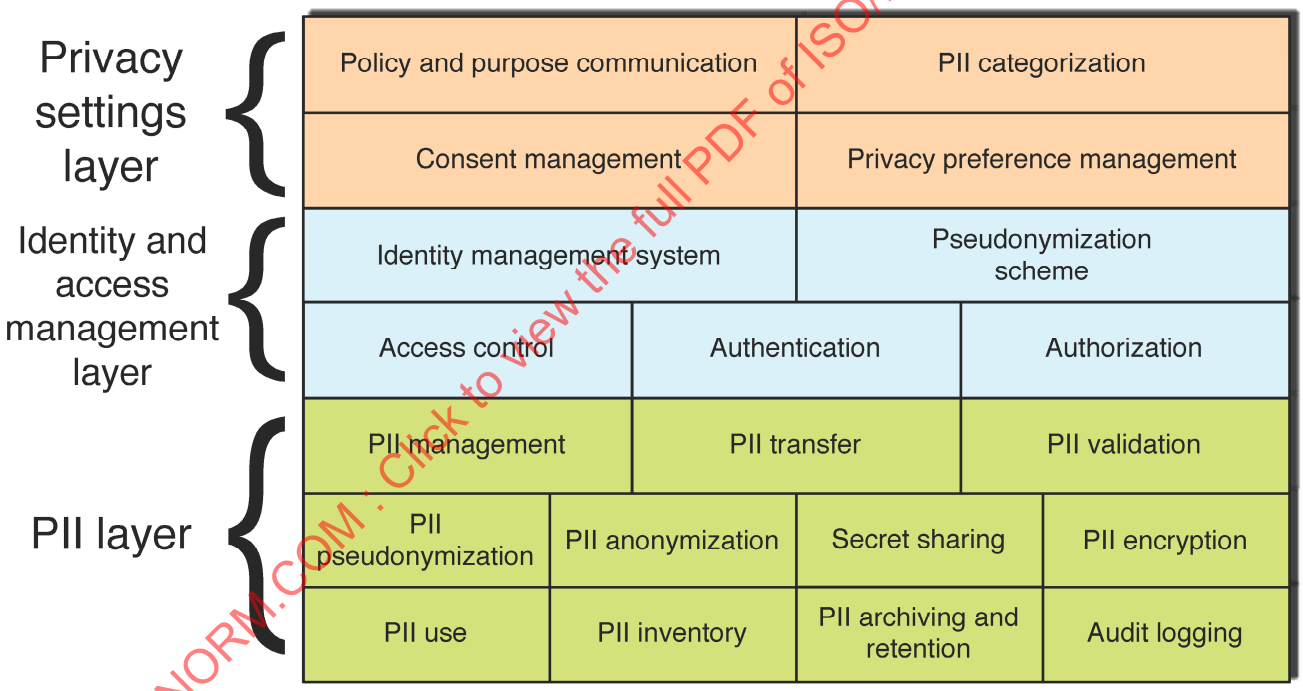

Figure 3 — The architecture of the ICT system of the PII principal

8.3.2 ICT system of the PII controller

The ICT system of the PII controller should communicate the privacy policy to all other participants. Additionally, the PII controller should manage the collection and processing of all PII. The ICT system of the PII controller should process PII based on the latest privacy policy, privacy safeguarding requirements and any privacy preferences that have been collected from the PII principal. The PII controller should make sure that the privacy settings components contain up-to-date information about policy and purpose at all times.

Additionally, the PII controller manages the processing of PII by PII processors. This includes oversight and responsibility for enforcement of the applicable privacy policies and any consent limitations and privacy preferences that have been collected from the PII principal. This requires the PII controller to communicate

this information to the PII processors, monitor their behaviour and take remedial action if the limitations and preferences are not complied with.

Furthermore, the controller may apply privacy enhancing technologies such as pseudonymization, anonymization or secret sharing to further reduce the chance that the ICT system of the PII processor can determine the PII principal associated with PII. Figure 4 shows the components for the ICT system of the PII controller.

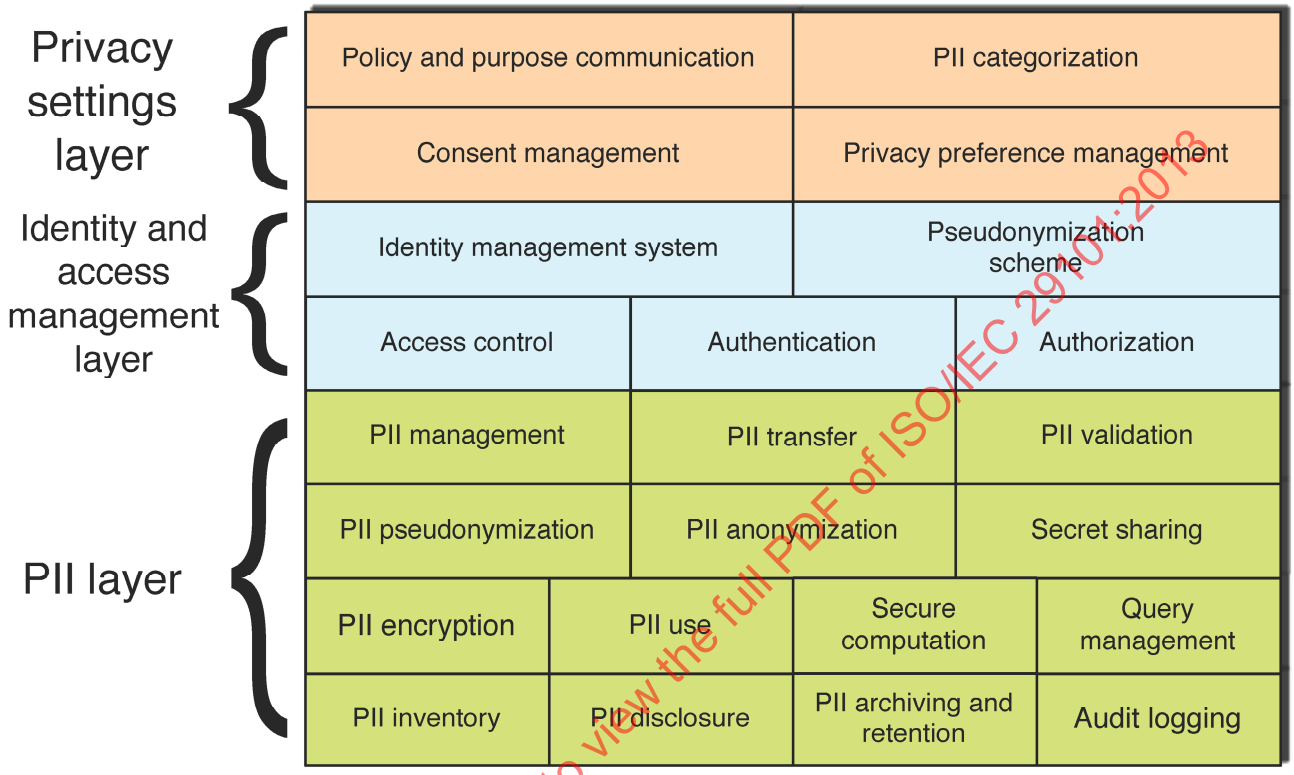

Figure 4 — The architecture of the ICT system of the PII controller

8.3.3 ICT system of the PII processor

The PII processor uses its ICT system for processing PII in accordance with its agreement with the PII controller. The ICT system of the PII controller passes on the policy and privacy preference information associated with the PII and necessary for its processing. Additionally, the ICT system of the PII processor should be capable of supporting PII transformed by privacy-enhancing technologies.

If a PET that does not change the PII representation (for example, pseudonymization or anonymization) is used to protect PII, the ICT system of the PII processor does not have to contain special processing technologies. However, if cryptographic techniques such as secret sharing or PII encryption are used, the ICT system of the PII processor will need to employ secure multiparty computation or PII decryption to be able to work with the PII. Secure multiparty computation may offer a reduced risk of privacy breaches during processing. Refer to Figure 5 for the architecture of the ICT system of the PII processor.

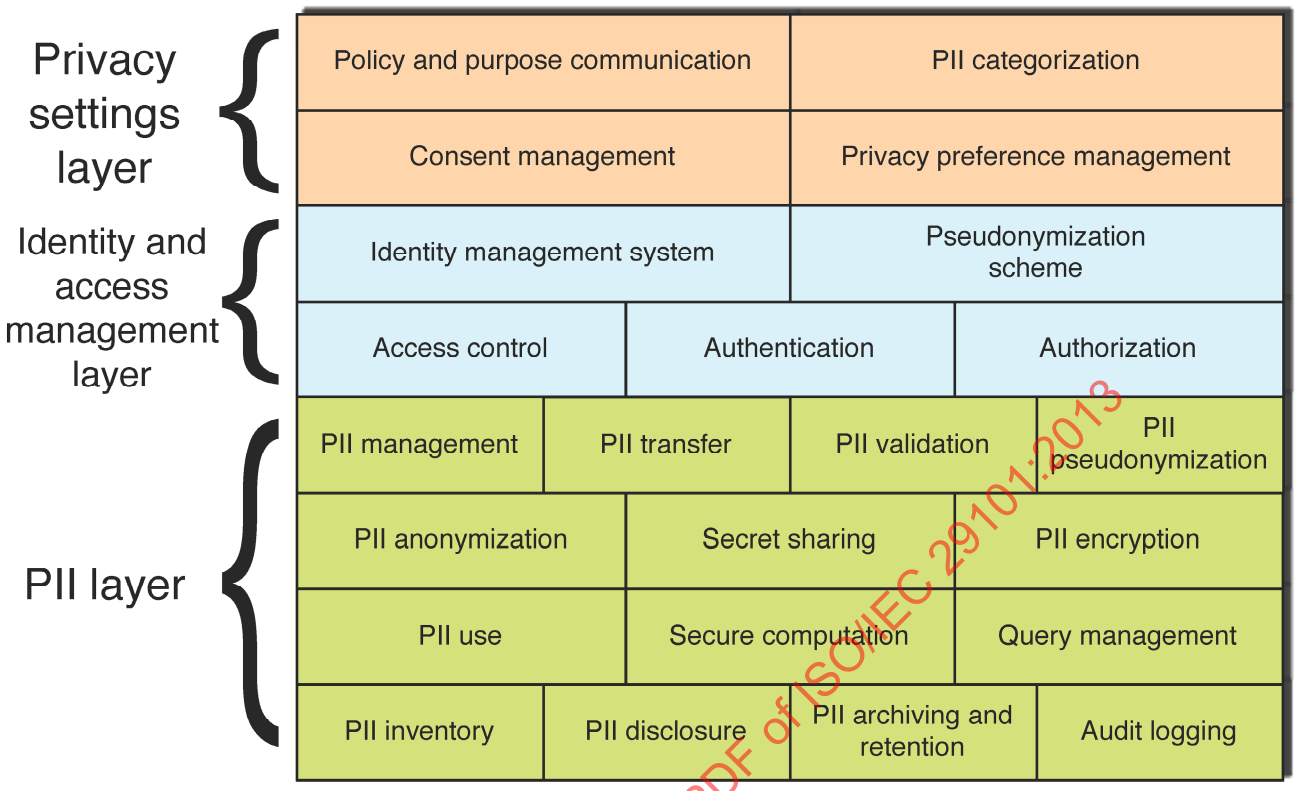

Figure 5 — The architecture of the ICT system of the PII processor

8.4 Interaction view

The interaction view describes how the components deployed in the ICT systems of different privacy stakeholders interact. The majority of components described in this architecture framework require information sharing or communication among actors. This clause describes which components may benefit from sharing PII or metadata among the actors. The developer of an ICT system can use this view to design the interactions between the ICT systems of individual actors.

A figure is presented for each layer of architectural components. This figure shows the span of components among actors. If a single component covers multiple actors, the data or program code of this component should be shared among the respective actors. Note that this does not mean that all the PII should be shared. Information should only be distributed following the principle of least privilege – if an actor does not require certain information to perform its duties, it should not have access to this information.

For example, even though the ICT system of the PII processor requires access to the privacy preferences of the PII principal in order to respect them, it should only have access to the preferences for those principals for which it has been provided PII. The PII controller may have PII from multiple PII principals, but if the controller has not delegated processing on behalf of a particular PII principal to a PII processor, it does not have to share the respective privacy preferences. On the other hand, if PII is transferred from the controller to the processor, the privacy preferences of the respective PII principals should be made available to the ICT system of the PII processor.

8.4.1 Privacy settings layer

The privacy settings layer covers services and information governing all aspects of PII processing. Therefore, it should be present throughout the processing of PII. Figure 6 illustrates the span of privacy settings components over the actors.

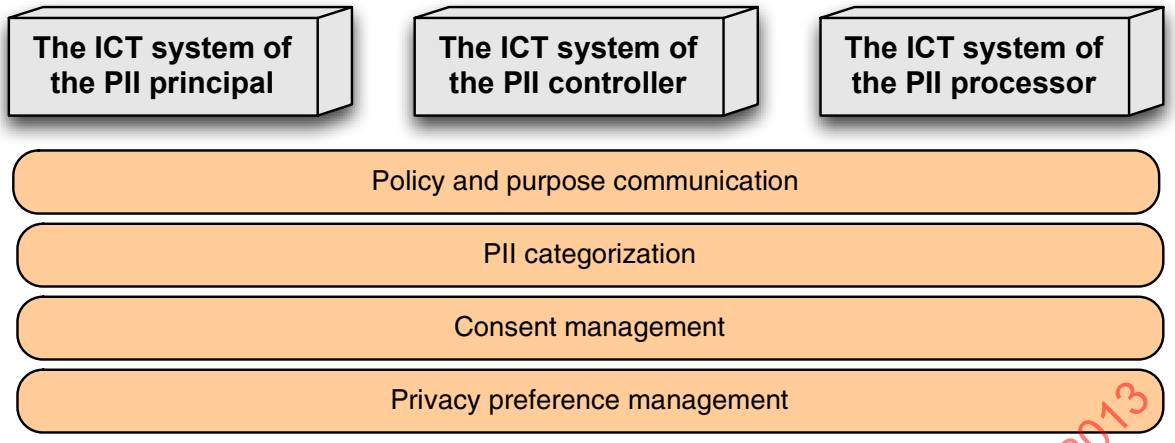

Figure 6 — The deployment of components in the privacy settings layer

8.4.2 Identity and access management layer

Some identity management services are generic and are used by all actors. However, this does not mean that all the actors should share all the identity information. The principle of least privilege should be followed and each ICT system should only have access to identity information it requires. Figure 7 shows the deployment of identity management services.

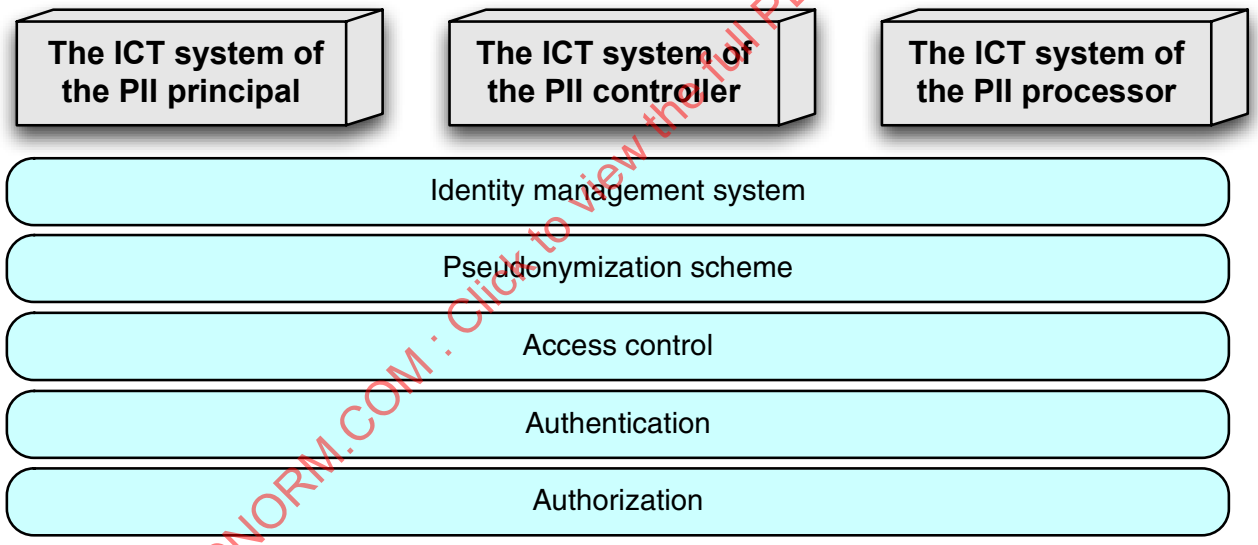

Figure 7 — The deployment of components in the identity and access management layer

8.4.3 PII layer

The PII layer also contains globally used services such as general PII management and PII inventory. However, it should be noted that there are services in this layer that can be deployed for any actor, but depending on the design of the system, it may be beneficial to deploy them for only some actors. For example, secret sharing gives the greatest effect when deployed directly in the ICT system of the PII principal. However, it can also be performed by the ICT system of the PII controller before passing PII to the ICT system of the PII processor. Figure 8 shows how the PII-related components can be deployed.

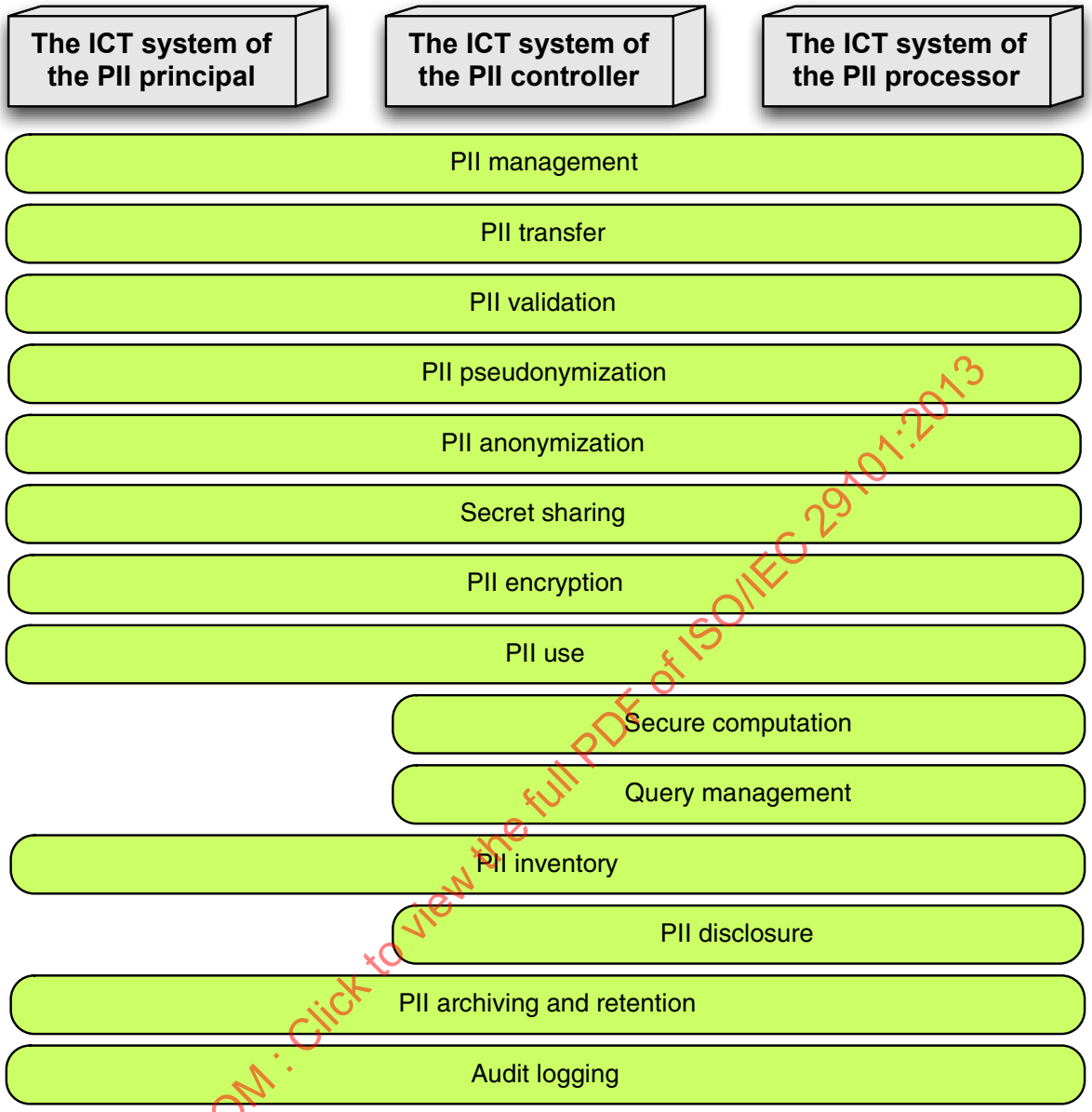

Figure 8 — The deployment of components in the PII layer

Annex A
(informative)

Examples of the PII-related concerns of an ICT system

A.1 Introduction

The following are examples of PII-related concerns for the architecture of an ICT system. The concerns are linked to architectural components with each component being mapped to one or more concerns. Developers should identify specific concerns for their application and ensure that the ICT system architecture design includes components that address the concerns.

In the example below the high level concerns are split into a number of sub-concerns. The sub-concerns described here are provided as an illustration and are not necessarily complete. Developers should determine the appropriate concerns and sub-concerns for their application through a process of analysis.

A.2 Obtaining and communicating consent

Consent by the PII principal to the processing of his/her PII is an important aspect of the management of that PII. Consequently, the architecture of the ICT system should include elements that enable management of that consent, in addition to those that ensure that the limits of such consent are respected.

Consent is specific to the declared purposes of use and should be voluntarily obtained from the PII principal on the basis of information provided by the PII controller about those purposes and all the entities (PII controller and PII processor(s)) that will process it, including the legal jurisdictions that apply to them.

In some cases, applicable law may define exceptions where the processing of PII without the PII principal's consent may be allowed (e.g., in connection with a lawful investigation). The relevant legislation should be consulted to identify all such exceptions and the associated consent provisions.

Consent may also be provided by a legally authorized proxy (e.g. parent, guardian, attorney), if the PII principal is not legally competent (e.g., the PII principal is a child). A proxy will provide the PII of the PII principal instead of the PII principal themselves and will determine and provide relevant consent information and limitations on the use and transfer of the PII to other parties on behalf of the PII principal. The PII and the associated consent and usage information should be held in confidence by the proxy.

Proxies should be trustworthy persons who act in the best interests of their clients. In the event of a perceived breach of trust by a proxy, legal sanctions may be quite limited particularly in the case of proxies who have a close relationship with the PII principal (e.g. parent or guardian) . In cases where proxies are professionals (e.g. attorneys) who are appointed to act on behalf of PII principals there may be recourse to legal and professional sanctions to deal with proxies who fail to uphold their duty of trust.

Some of the related concerns are:

a. obtaining consent from the PII principal or proxy;

b. securely transferring and recording consent information;

c. allowing the withdrawal or modification of consent;

d. associating consent information with PII;

e. recording the application of consent; and

f. reacting to the withdrawal and modification of previously given consent.

In cases where the PII principal does not give consent for their PII to be collected and processed, it may be necessary to make alternative arrangements that do not involve PII. Where alternative arrangements are not available it may be necessary to prohibit the PII principal from using the service.

A.3 Communicating the purpose of PII collection

PII controllers collect PII for a particular purpose. Information about these purposes should be presented to the PII principal during interactions when consent is required.

Information about the purpose of processing should be communicated to PII controllers or PII processors whenever PII is transferred (e.g., by tagging the PII with its purpose before transfer). This way, all PII controllers and PII processors know the purpose and limits of authorized processing.

Keeping processing within the limits of the original purpose can be achieved by organizational means. Alternatively, PETs like query management can be used to enforce limits on the processing of PII.

Some of the related concerns for an ICT system maintaining and communicating information about the purpose of PII collection are:

a. entering and updating information describing the purpose(s) for the collection, use and transfer of PII;

b. transferring and presenting information describing the purpose(s) of PII collection within the ICT system;

c. associating information about the purpose(s) of collection with the corresponding PII; and

d. ensuring that all further processing stays within the purpose provided.

A.4 Secure PII processing

ICT system developers should take the nature and extent of authorized access to the PII into consideration. The more often that PII is accessed and the more people that have access rights to PII, the more likely are privacy breaches.

Another factor to be considered is the level of direct control a PII controller or PII processor has over the PII being processed. For example, if PII in the ICT system of the PII controller or PII processor is accessed remotely, that actor should assign a higher risk level to the PII.

Concerns for PII transfer and storage processes should cover at least the following categories:

a. collection and modification of PII;

b. authorization of PII transmissions;

c. authenticated and confidential transmission of PII;

d. storing PII;

e. controlling access to PII;

f. ensuring the accuracy of PII; and

g. deploying additional privacy controls and PETs as recommended by the privacy safeguarding requirements.

A.5 Classification and control of PII

PII processing flow models should be developed as an integral component of a privacy risk assessment. The PII processing flow diagram should not only show the areas where PII is collected, transferred, used, stored or disposed of but should also show areas where sensitive PII is processed and, as a consequence, requires the implementation of stronger safeguarding measures.

Classifying data into PII and non-PII is the minimum requirement where sensitive PII (e.g. personal data on health, ethnicity etc.) is processed. Such data should be subject to more rigorous protective measures in accordance with relevant legislation.

Classification and control concerns within an ICT system should include:

a. determining which data is PII and classifying PII;

b. quantifying the number of PII actors;

c. quantifying the amount and sensitivity of the PII; and

d. controlling transfers and internal copies of PII.

A.6 Accounting and Audit of PII operations

Transactions involving PII should be accounted for in a PII transaction database. Accounting should include a record of all PII processing and any errors that occurred which could have led to a compromise of the confidentiality or integrity of the PII. The accounting records should be subject to periodic independent audits to check for potential breaches of confidentiality, integrity or any unauthorized access or other unauthorized behaviour.

Concerns related to the auditability to PII operations include:

a. logging the granting, modification and revocation of consent;

b. logging storage and transfer of the PII;

c. logging processing of sensitive PII; and

d. logging transfers of PII.

A.7 Archiving and disposal of PII

When PII is not required anymore, it should be disposed of. Disposal procedures should ensure that it is not possible to recover PII from the media used for its storage.

Concerns related to the correct archiving and disposal of PII include:

a. secure backup of PII; and

b. secure PII disposal techniques.

Table A.1, Table A.2 and Table A.3 show a correspondence mapping between the example concerns and components of the layers in the ISO/IEC 29101 architecture. An ‘X’ in the table indicates a relationship between a component of the layer and a principle. This relationship, however, is only shown as an example.

Table A.1 — Examples of the relationship between concerns and the components in the privacy settings layer

Components \ Concerns	Obtaining and handling consent	Maintaining purpose information	Secure PII storage and transfer	Secure PII processing	Classification and control of PII	Auditability of PII operations	Archiving and disposal of PII
Policy and purpose communication	X	X	X	X		X	
PII categorization			X	X	X	X	X
Consent management	X				X	X	
Privacy preference management	X	X	X	X		X	X

Table A.2 — Examples of the relationship between concerns and the components in the identity and access management layer

Components \ Concerns	Obtaining and handling consent	Maintaining purpose information	Secure PII storage and transfer	Secure PII processing	Classification and control of PII	Auditability of PII operations	Archiving and disposal of PII
Identity management system	X		X		X	X	X
Pseudonymization scheme			X				
Access control			X	X		X	
Authentication			X	X		X	
Authorization			X	X		X	

Table A.3 — Examples of the relationship between concerns and the components in the PII layer

Components \ Concerns	Obtaining and handling consent	Maintaining purpose information	Secure PII storage and transfer	Secure PII processing	Classification and control of PII	Auditability of PII operations	Archiving and disposal of PII
PII management			X		X		X
PII transfer			X		X		
PII validation				X			
PII pseudonymization			X			X	
PII anonymization			X			X	
Secret sharing			X				
PII encryption			X				X
PII use				X			
Secure computation				X			
Query management				X			
PII inventory					X	X	X
PII disclosure					X	X	
PII archiving and retention			X				X
Audit logging					X	X	X

A.8 Relationship with privacy principles

Table A.4 shows a correspondence mapping between the privacy principles of ISO/IEC 29100 and the high-level concerns in this Annex.

Table A.4 — Examples of the relationship between privacy principles and the high-level concerns

Principles / Concerns	Consent and choice	Purpose legitimacy and specification	Collection limitation	Data minimization	Use, retention and disclosure limitation	Accuracy and quality	Openness, transparency and notice	Individual participation and access	Accountability	Information security controls	Compliance
Obtaining and communicating consent	X				X						X
Communicating the purpose of PII collection		X					X				X
Secure PII processing			X	X	X	X	X	X		X	X
Classification and control of PII									X	X	X
Auditability of PII operations									X	X	X
Archiving and disposal of PII					X					X	X

Annex B
(informative)

A PII aggregation system with secure computation

B.1 Introduction

This clause presents an example architecture derived from the general architecture framework. The architecture makes use of PETs for minimizing PII disclosure. Note that this example is for illustrative purposes only. Any application will need an architecture based on a proper assessment of the goals and associated requirements of the application in question.

This example describes a system that collects PII from PII principals securely over secure channels. The PII controller then uses secret sharing to transform PII into non-PII. The resulting non-PII is then transferred to three PII processors who use secure computation to process the secret-shared PII without being able to link the values with the individual PII principals. The PII processor nodes that are engaged in secure computation will get a secret-shared result and transfer it to the data analyst who can reconstruct the result from the shares.

B.2 Purpose, actors and deployment

The purpose of the ICT system will be to collect personal information from a number of PII principals. The collection is organized by an organization conducting a statistical study. However, since the organization itself does not have the knowledge for statistical analysis, it outsources the actual study design and data analysis to a data analysis bureau.

Secret sharing and secure multiparty computation (SMC) are used to further protect PII. The use of secret sharing and secure multiparty computation in this scenario requires at least three organizations to participate in the secure processing of PII. These organizations will become secure multiparty computation nodes and their role is to store secret shared PII and perform secure multiparty computation on it.

If no organization hosting an SMC node publishes its share database, it is impossible for other SMC nodes to reconstruct the original PII. SMC nodes are typically selected to be non-colluding representatives of the stakeholders.

The actors of the application are:

a. the individuals providing PII are the PII principals;

b. the study coordinator acts as the PII controller; and

c. the SMC nodes and the data analyst are the PII processors.

The ICT system is deployed as shown in Figure B.1;

a. the ICT system of the PII principal is a web application running in the PII principal's web browser. It is hosted in the PII controller's web server;

b. the ICT system of the PII controller is a web application hosted in the PII controller's web server; and

c. the ICT system of the PII processor is a specialized application with a connected secure computation system for storing the secret shared data that has been sent for processing.

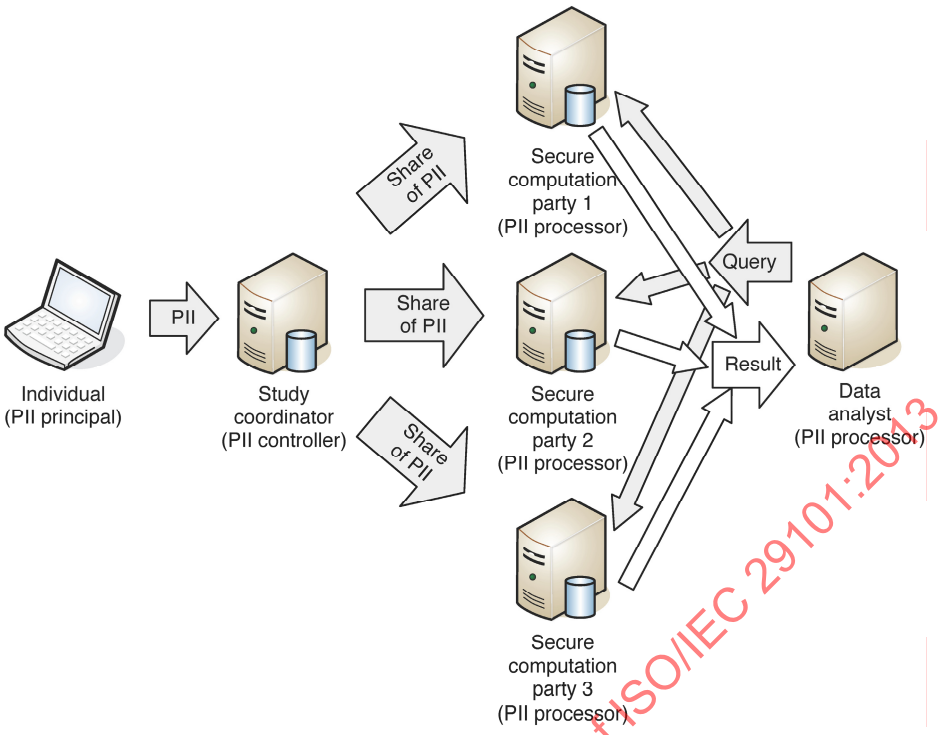

Figure B.1 — Deployment of the secure computation system

B.3 Architecture for the PII entry application

The study coordinator prepares the ICT system of the PII principal. However, it still contains all three layers of the ISO/IEC 29101 architecture framework. Figure B.2 shows the architecture for the PII entry application.

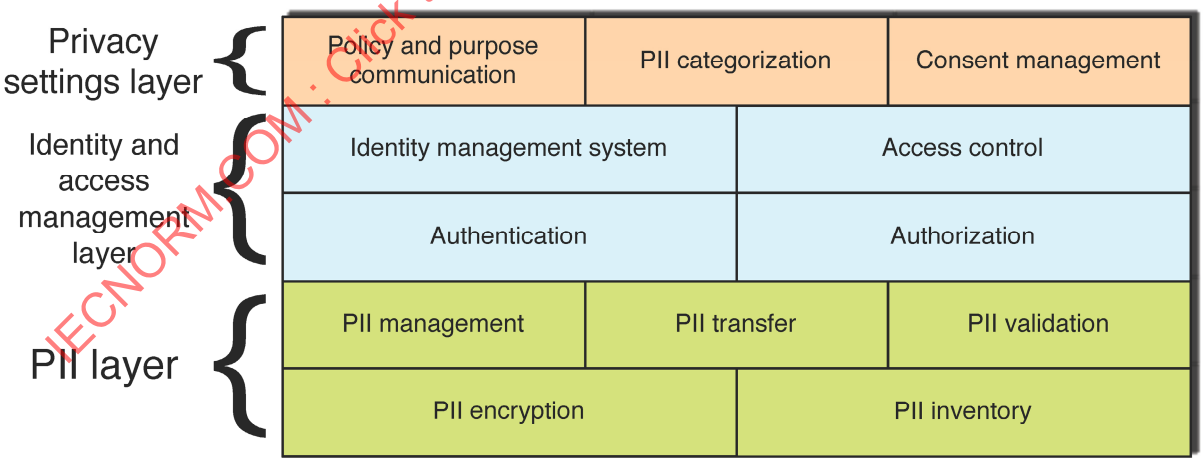

Figure B.2 — The architecture for the PII entry ICT system

The components can be implemented as follows:

Privacy settings layer:

a. **PII categorization**: since the PII principal is asked for sensitive PII, all the PII entered is automatically considered sensitive, except for the fact and time of consent;

b. **consent management**: the PII entry application, after presenting the policy and purpose, explicitly asks the PII principal for consent before presenting the PII entry form. The consent decision and its date are also transferred to the ICT system of the PII controller. A random value is generated by the ICT system of the PII principal and transferred to the ICT system of the PII controller along with the consent to allow modification or withdrawal of consent. To modify or withdraw consent, the PII principal contacts the study coordinator and presents the random value, which can be used to look up the previously provided PII and mark it for modification or removal; and

c. **policy and purpose communication**: the privacy policy and purpose of PII collection are delivered to the PII principal within the PII entry application as it is downloaded from the web server.

Identity and access management layer:

a. **identity management system**: the PII principals are not identified as the data entry is anonymous. The PII controller's identity is communicated through the PII entry application; and

b. **access control, authentication and authorization**: access to the PII entry application is limited by restricting its delivery from the PII controller's server. PII principals are not authenticated to maintain their anonymity (no group authentication method is used either). The PII principal authenticates the PII controller servers through the standard secure HTTP connection.

PII layer:

a. **PII management:** the PII entry application does not provide local storage in the PII principal's web browser. It transfers the PII directly to the PII controller;

b. **PII transfer:** secure HTTP is used to send the PII to the PII controller servers;

c. **PII validation:** the fields in the PII entry form are assigned metadata values that are used to validate that the entered values conform to the correct format;

d. **PII encryption:** encryption of PII (and the rest of the messages between the PII principal and PII controller) is handled by the secure HTTP connection; and

e. **PII inventory:** after filling out the form, the PII entry application allows the PII principal to review the answers and save or print a copy of the PII with the name of the PII controller's and PII processors' organizations and the random value sent with the consent.

B.4 Architecture for the study control application

The PII controller also uses a web-based ICT system with some extra capabilities for handling the PII collected from several principals, transferring it to PII processors and running more thorough audits. The architecture is presented in Figure B.3.

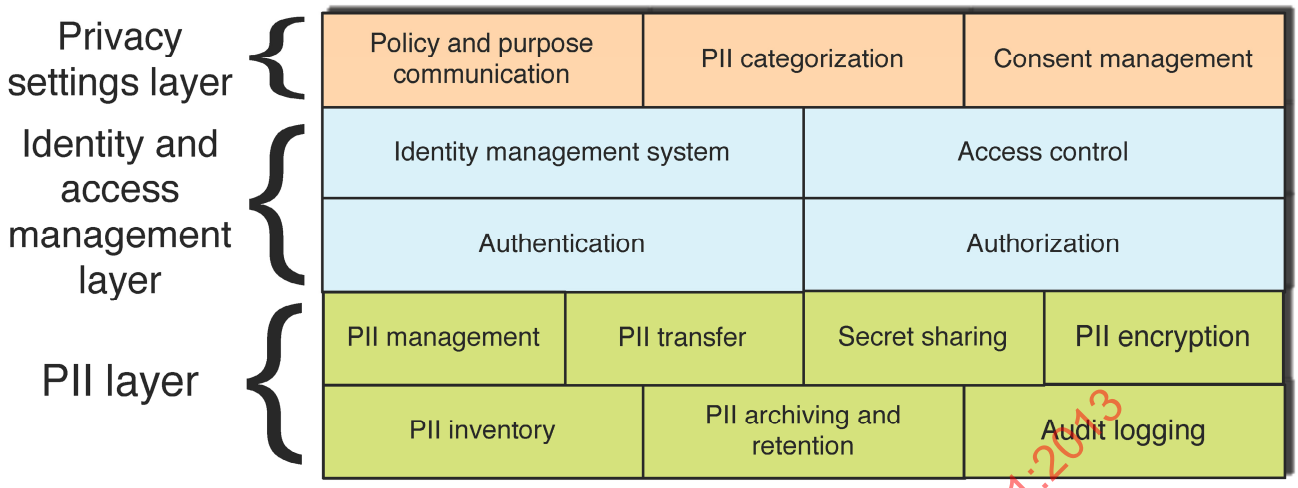

Figure B.3 — The architecture for the study coordinator ICT system

The components can be implemented as follows:

Privacy settings layer:

a. **policy and purpose communication**: the PII controller communicates the policy and purpose to the PII principal by preparing and delivering the PII entry application. The PII controller communicates the policy to PII processors through contractual agreements;

b. **PII categorization**: the ICT system of the PII controller contains built-in rules for classifying PII from the PII principals as sensitive PII (with the exception of consent information); and

c. **consent management**: the PII controller receives consent information from the PII entry application and stores it together with the PII. The associated random value can later be used to perform consent modification or withdrawal.

Identity and access management layer:

a. **identity management system**: no identity information about PII principals is stored. The ICT system of the PII controller additionally stores information about the SMC nodes and the data analyst; and

b. **access control, authentication and authorization**: access to the PII entry application is controlled by enabling or disabling its delivery and disabling the PII collection service. Standard techniques (a smartcard, biometrics, passwords etc.) are used to authorize access to the ICT system of the PII controller.

PII layer:

a. **PII management**: the ICT system of the study coordinator receives PII from the PII entry applications and stores it in a database. The ICT system is capable of transferring the PII to the ICT system of the PII processor;

b. **PII transfer**: the ICT system can receive secure HTTP requests from the PII entry application. It can also open secure channels to the PII processor's systems to transfer shares of PII;

c. **secret sharing**: to transfer PII to the secure computation system, the ICT system uses secret sharing to divide the individual values into shares. Each share alone reveals no information about the input values;

d. **PII encryption**: encryption is used when transferring PII from the PII entry application. In addition, shares of PII are encrypted in transit to the PII processors. Note that since secret sharing ensures the confidentiality of PII during storage, the shares need not be encrypted;

e. **PII inventory**: the ICT system can provide the number of PII principals that have provided PII for the study;

f. **PII archiving and retention**: after the completion of the study, the contents of the study database are securely archived. The specific tools of the database management system are used for making the backup; and

g. **audit logging**: the ICT systems logs each received PII entry, each action performed by the PII controller using its ICT system and each transfer of PII to the PII processors.

B.5 Architecture for the secure PII analysis application

The data analyst's ICT system is a distributed system consisting of the secure storage and secure multiparty computation system and a client application for making queries to the secure computation system. The following architecture covers the whole distributed system. Note, that in the following architecture description, an SMC node means the secure computation system software run by the organizations hosting the SMC system. Figure B.4 illustrates the architecture.

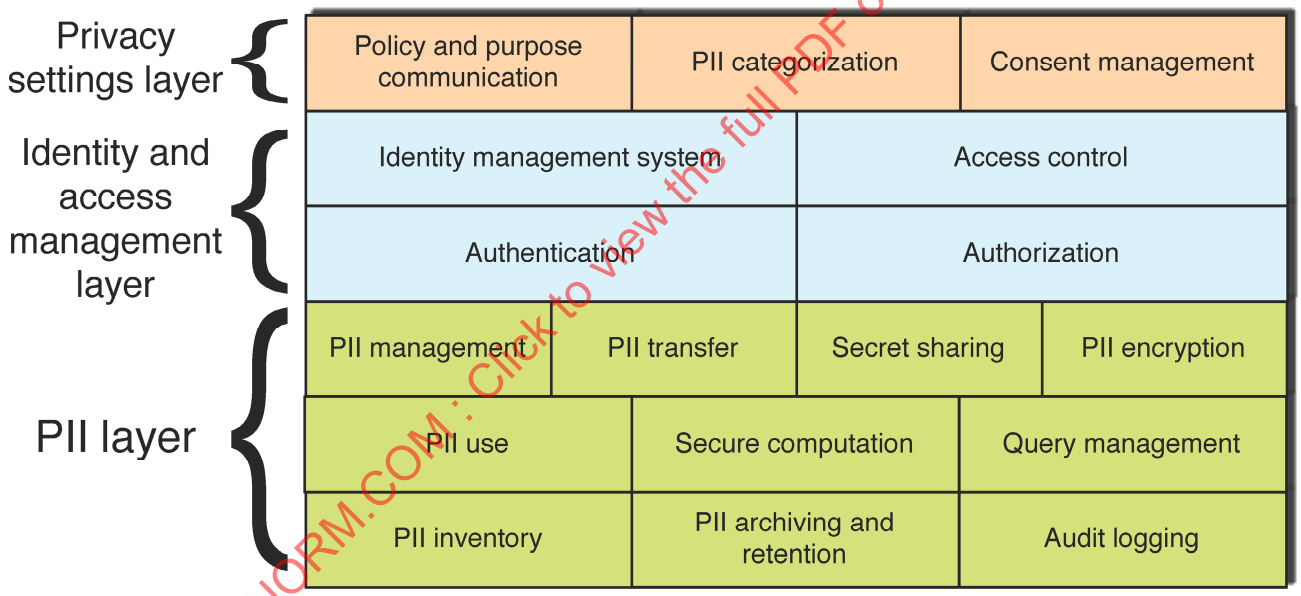

Figure B.4 — The architecture for the secure data analysis application

The components can be implemented as follows:

Privacy settings layer:

a. **policy and purpose communication**: the data analyst and the SMC nodes receive the policy and purpose with the analysis contract from the PII controller;

b. **PII categorization**: the information stored using secret sharing is categorized as sensitive PII and it is processed using secure multiparty computation. Non-PII, if any, is processed using standard methods; and

c. **consent management**: the study coordinator ensures that it passes only PII from consenting principals to the PII processors. If a PII principal modifies or withdraws consent, the study coordinator notifies the data analyst and the SMC nodes who should then remove the respective shares from their systems.

Identity and access management layer:

a. **identity management system**: the security of secure multiparty computation depends on SMC nodes knowing the identity of each other and the privacy stakeholders using the system (the study coordinator ICT system providing the PII and the data analysis ICT system giving queries). Similarly, the data analyst's ICT system should know the identities of the SMC nodes and the study coordinator; and

b. **access control, authentication and authorization**: the SMC nodes authenticate and authorize the study coordinator's ICT system before accepting PII from it. Similarly, the SMC nodes authenticate and authorize the data analyst's ICT system before accepting queries. The ICT system of the data analyst uses standard techniques for authenticating and authorizing the PII processor.

PII layer:

a. **PII management**: the SMC nodes store the PII in secret-shared form. The data analyst's ICT system should have the capability to store queries and their results;

b. **PII inventory**: the SMC nodes can provide information about the number of records in their secret-shared database;

c. **PII use**: the data analyst crafts queries and sends them to the SMC nodes. The SMC nodes process PII while preserving privacy and return the query results to the data analyst. The data analyst constructs reports for the study coordinator;

d. **PII transfer**: SMC nodes use secure channels to receive secret-shared PII and queries and also to perform secure multiparty computation. The study results are transferred from the data analyst to the study coordinator using encrypted e-mail messages;

e. **secret sharing**: secret sharing is used within the secure multiparty computation system to store PII and within the secure computation protocols;

f. **PII encryption**: encryption is used in the transfer or PII, secret-shared PII, queries and results. Optionally, study results are transferred in an encrypted form;

g. **query management**: the SMC nodes refuse to answer queries, if there are less than a predefined number of PII records. Also, they provide the data analyst with only the final results of the statistical algorithms. Intermediate values are kept in secret-shared form. Only previously agreed on statistical procedures are used;

h. **secure computation**: this system uses secure multiparty computation with three nodes;

i. **PII archiving and retention**: in this application, the SMC nodes should archive their databases in the same secret-shared form or dispose of the PII securely. The data analyst securely archives the study results. The access and query logs should be archived by both the SMC nodes and the data analyst's ICT system; and

j. **audit logging**: the SMC nodes should keep a log of all the following events: 1) PII received from the study coordinator, 2) queries received from the data analyst, 3) results returned to the data analyst. The data analyst's ICT system should keep a log of all queries made and all results received.