ISO/IEC JTC 1/WG 7
Working Group on Sensor Networks

Document Number:	N049
Date:	2010-07-05
Replace:	
Document Type:	Liaison Organization Contribution
Document Title:	Liaison Statement from JTC 1/SC 27/WG 5 to JTC 1/WG 7 on the ISO/IEC 4th CD 29100
Document Source:	JTC 1/SC 27/WG 5
Document Status:	For consideration at the 2nd WG 7 meeting in US.
Action ID:	FYI
Due Date:	
No. of Pages:	34

ISO/IEC JTC 1/WG 7 Convenor:
Dr. Yongjin Kim, Modacom Co., Ltd (Email: cap@modacom.co.kr)
ISO/IEC JTC 1/WG 7 Secretariat:
Ms. Jooran Lee, Korean Standards Association (Email: jooran@kisi.or.kr)

Committee Draft **ISO/IEC 4th CD 29100**	Reference number: ISO/IEC JTC 1/SC 27 **N8806**
Date: **2010-06-10**	Supersedes document SC 27 N8162
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.	
ISO/IEC JTC 1/SC27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: **2010-09-10** Please submit your votes and comments via the online balloting application by the due date indicated.

ISO/IEC 4th CD 29100

Title: Information technology -- Security techniques – Privacy framework

Project: 1.27.54 (29100)

Explanatory Report

Status	**SC 27 Decision**	**Reference documents**	
		Input	**Output**
Study Period (SP)	Resolution 30 of 17th SC 27 Plenary (N4599), Apr. 2005	JTC 1 Recommend. (JTC1N7552) to assign responsib. to SC 27 in the area of privacy technologies	Call f. Contr. (N4616)
	Recommend. of Ad Hoc on Privacy (N4880), Nov. 2005	SoContr (N4723)	Report of Ad Hoc Nov. 2005 (N4880)
NWIP	Recommend. of Ad Hoc on Privacy (N5186rev1), May 2006 and Resolut. 33 of 18th SC 27 Plenary (N5199), May 2006	Report on Ad Hoc, Nov. 2005 (N4880rev1) & May 2006 (N5186rev1); Report of teleconf. (N4953rev1); DE NWIP (N5064)	Text f. NWIP (N5211)
For details regarding project development at the Working Draft stage please see on the 2nd page.			
1st CD 29100	6th WG 5 meeting, Oct. 2008, resolutions 1, 10 (N7097rev1).	SoCom. (N7006); FIDIS (N7060); FR com (N7083); UKcom. (N6979).	DoC (N7238); Text f. 1st CD (N7239).
2nd CD 29100	7th WG 5 meeting, May 2009, resolutions 1, P4 (N7724); 21st Plenary, May 2009, resolution 8 (N7777); Deleg. of Auth. f. FCD resolution 16 (N7777).	SoV (N7544); FIDIS com. (N7541).	DoC (N7750); Text f. 2nd CD (N7751); JTC 1 notification on extension of limit dates (N8049).
3rd CD 29100	8th WG 5 meeting Nov. 2009, resolutions 1, 8 (N8138)	EU DP Auth. letter (N7980); SC37 com (N8045), SoV (N8048)	Liaisons to Art. 29 DP WP (N8155), to SC 31 (N8140) to SC 37 (N8141), DoC (N8161); Text f. 3rd CD (N8162).
4th CD 29100	9th WG 5 meeting, April 2010, reolutions 3, 7, P4, (N8828rev)	SoV (N8567); SC 37.comm. (N8562); TAS3 comm. (N8563)	Liaison statements to SC 37 (N8847); TAS3 (N8841); DoC (N8805); Text for 4th CD (N8806).

4th CD Consideration

In accordance with resolution P4 (in SC 27 N8828rev) of the 9th SC 27/WG 5 meeting held in Melaka (Malaysia), 19th – 23rd April 2010, the attached document is hereby circulated for a 3-month 4th CD LB closing by

2010-09-10

Secretariat, ISO/IEC JTC 1/SC27 -
DIN Deutsches Institut fuer Normung e.V., Burggrafenstr. 6, 10772 Berlin , Germany
Telephone: + 49 2601-2652; Facsimile: + 49 2601-1723; E-Mail: krystyna.passia@din.de, http://www.jtc1sc27.din.de/en

Explanatory Report			
Status	**SC 27 Decision**	**Reference documents**	
		Input	**Output**
1st WD 29100	Resolution 6 of 1st WG 5 meeting (N5513), Nov. 2006	SoV (N5288); SoContr. (N5332);	DoC (N5520); Report (N5565); Text f. 1st WD (N5519).
2nd WD 29100	2nd WG 5 meeting, May 2007, Resolutions 1 & 6 (N5873) & 19th Plenary, May 2007, resolutions 18 (N5939).	SoCom (N5667)	DoC (N5880draft); Text for 2nd WD (N5881).
3rd WD 29100	3rd WG 5 meeting, October 2007, resolutions 1, 8 (N6251)	SoCom. (N6021rev1);UK com. (N6058); FIDIS com. (N6107); Proposed DoC (N6120);NZ priv. infrastr. (N6269).	DoC (N6257); Text f. 3rd WD (N6258).
4th WD 29100	5th WG 5 meeting, April 2008, resolutions 1, 8 & P 3 (N6726) & 20th Plenary, April 2008, resolut. 2 (N6799); Deleg. of Auth. for 1st CD resolut. 14 (N6799).	SoCom. (N6522); FIDIS (N6503); Proposed DoC (N6585).	DoC (N6733); Text f. 4th WD (N6734).

© ISO/IEC 2010 – All rights reserved

ISO/IEC JTC 1/SC 27 N8806

ISO/IEC CD 29100.4

ISO/IEC JTC 1/SC 27/WG 5

Secretariat: DIN

Information technology — Security techniques — Privacy framework

Élément introductif — Élément central — Élément complémentaire

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

Secretariat ISO/IEC JTC 1/SC27
DIN German Institute for Standardization
10772 Berlin
Tel. + 49 30 2601 2652
Fax + 49 30 2601 1723

E-mail krystyna.passia@din.de
Web http://www.jtc1sc27.din.de/en (public web site)
http://isotc.iso.org/livelink/livelink/open/jtc1sc27 (SC27 documents)

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

© ISO/IEC 2010 – All rights reserved

Contents

Page

© ISO/IEC 2010 – All rights reserved

Figures

Tables

 © ISO/IEC 2010 – All rights reserved

Foreword

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

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

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

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

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

© ISO/IEC 2010 – All rights reserved

Introduction

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

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

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

In some jurisdictions, the reference to the privacy safeguarding requirements shall be understood as being complementary to the requirements for the protection of personal data. Due to the increasing number of information and communication technologies that process PII, it is important to have international information security standards that provide a common understanding for the protection of PII. This International Standard has the intention to enhance existing security standards by adding a focus relevant to the processing of PII.

The increasing commercial use (and value) of PII, the sharing of PII across legal jurisdictions, and the growing complexity of ICT systems, make it extremely difficult for an organization to ensure privacy and to achieve compliance with various laws and regulations. Uncertainty and distrust can arise as a result of how an organization or other entity handles privacy matters and as a result of cases of PII misuse.

Use of this International Standard will:

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

The privacy framework provided within this International Standard can serve as a basis for desirable additional privacy standardization initiatives, for example for a technical reference architecture, for the implementation and use of specific privacy technologies and overall privacy management, for privacy controls for outsourced data processes, for privacy risk assessments or for specific engineering specifications.

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

© ISO/IEC 2010 – All rights reserved

Information technology — Security techniques — Privacy framework

1 Scope

1.1 Purpose

This International Standard covers the basic elements of a privacy framework that should guide individuals and organizations in the privacy safeguarding when processing PII. This International Standard may also apply to individuals or organizations who are involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating ICT systems or services where PII is processed and privacy safeguards are required. However, this International Standard is limited to the processing of PII in ICT systems.

This International Standard establishes:

- a common privacy terminology;
- a description of the actors and their roles,
- an understanding of privacy safeguarding requirements; and
- a reference to known privacy principles.

2 Terms and definitions

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

2.1
anonymity
condition which requires that a PII controller or any other party/entity is unable to directly or indirectly determine the identity of the PII principal

2.2
anonymization
process by which PII is irreversibly removed or altered in such a way that a PII principal can no longer be identified directly or indirectly neither by the PII controller alone nor in collaboration with any other party

2.3
anonymized PII
PII that has been subject to a process of anonymization and that can no longer be used to identify, or re-identify, a PII principal

2.4
consent
PII principal's freely given, specific and informed indication by which his agreement to the processing of his personally identifiable information is signified

© ISO/IEC 2010 – All rights reserved

2.5
entity
natural or legal person, a public authority or agency or any other body

NOTE In the context outside the scope of this International Standard, an entity may refer to a natural person, animal, organisation, active or passive object, device or group of such items that has an identity.

2.6
identifiability
the ability of personal characteristics such as name/identity, location, contact or others to be associated to a natural person

2.7
identification
recognition of a person in a particular domain by a set of his or her attributes

2.8
identity
set of attributes which make it possible to recognize, contact or locate the PII principal

2.9
opt-in
process or type of policy whereby the PII principal is required to take a separate action to express specific, explicit, prior consent for a specific type of processing

NOTE PII (and an associated opt-in) could also be collected by a PII processor acting on behalf of a PII controller.

2.10
opt-out
process or type of policy whereby the PII principal is required to take a separate action in order to withhold or withdraw consent for a specific type of processing

NOTE In the case of opt-out, implied consent exists for the PII controller to process PII unless the individual explicitly denies or withdraws permission. Opt-out is also a process provided by a PII controller for a PII principal to deny or withdraw permission to perform a specific type of processing.

2.11
personally identifiable information
PII
any information (a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains, (b) from which identification or contact information of an individual person can be derived, or (c) that is or might be directly or indirectly linked to a natural person.

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

2.12
PII controller
entity (or entities) that determines the purposes and means for processing PII but does not include individual persons who use data for personal purposes

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

2.13

PII disclosure
release, transfer, access provisioning, or divulgation of PII in any form to a third party

2.14
PII principal
individual person to whom the PII relates

© ISO/IEC 2010 – All rights reserved

NOTE Depending on the jurisdiction and the particular data protection and privacy legislation, the concept of a 'PII principal' is also be defined as a 'PII owner', 'data owner', or 'data subject'. In some jurisdictions, the 'data owner' is the individual whose PII is processed by someone and who continues to hold ownership to his/her own PII. In other jurisdictions, the 'data owner' is not a PII principal but is a person or entity who received the right to process PII from an individual.

2.15
PII processor
entity that processes PII on behalf of and in accordance with the instructions of a PII controller

2.16
privacy breach
situation where PII is processed in an unlawful manner or in violation of one or more relevant privacy policies

2.17
privacy control
technical and organisational measures aimed at mitigating risks that could result in privacy breaches

NOTE 1 Privacy controls include policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature.

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

2.18
privacy enhancing technology
PET
coherent system of ICT measures that protect privacy by eliminating or reducing PII or by preventing unnecessary and/or undesired processing of PII; all without losing the functionality of the data system

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

2.19
privacy policy
specification of objectives, rules, obligations and privacy controls with regard to the processing of PII in a particular setting

2.20
privacy preferences
specific or implied choices made by an individual about how his/her PII should be processed

2.21
privacy principles
set of shared values governing the privacy protection of the PII when processed in ICT systems

2.22
privacy risk assessment
analysis of the risks of privacy breach involved in an envisaged processing operation

NOTE This analysis, also known as privacy impact assessment, is achieved to (a) ensure processing conforms to applicable legal, regulatory, and policy requirements regarding privacy, (b) determine the risks and effects of processing PII, and (c) examine and evaluate privacy controls and alternative processes for handling PII to mitigate identified privacy risks.

2.23
privacy safeguarding requirements
criteria to be fulfilled when implementing privacy controls designed to help mitigate risks of privacy breaches

2.24
processing of PII
any operation or set of operations performed upon PII

© ISO/IEC 2010 – All rights reserved

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

2.25
profile
a set of automatically generated data characterising a category of individuals that is intended to be applied to an individual, namely for the purpose of analysing or predicting personal preferences, behaviours and attitudes

2.26
pseudonymization
process applied to PII which replaces identity information with an alias

NOTE Pseudonymization allows, for example, a PII principal to use a resource or service without disclosing his or her identity, while still being held accountable for that use. After pseudonymization, it may still be possible to determine the PII principal's identity based on the alias and/or to link the PII principal's actions to one another and as a consequence, to the PII principal.

2.27
secondary use
processing of PII for a purpose different than the purpose(s) for which it was collected

2.28
sensitive PII
category of PII that affect the PII principal's most intimate sphere, or likely to give rise, in case of misuse, to unlawful or arbitrary discrimination or to a substantial harm or risk to the PII principal

NOTE: In some jurisdictions or in specific contracts, sensitive PII are defined in reference to the nature of the PII and may consist of PII revealing the racial origin, political opinions or religious or other beliefs, as well as personal data on health, sex life or criminal convictions, as well as other PII that may be defined as sensitive.

NOTE Harm should be taken to include monetary and non-monetary damages.

2.29
third party
any natural or legal person, public authority, agency or any other body other than the PII principal, the PII controller and the PII processor, and the persons who are authorized to process the data under the direct authority of the PII controller or the PII processor

© ISO/IEC 2010 – All rights reserved

3 Symbols and abbreviated terms

The following abbreviations are common to ISO/IEC 29100:

ICT Information and Communication Technology

PET Privacy Enhancing Technology

PII Personally Identifiable Information

© ISO/IEC 2010 – All rights reserved

4 Basic elements of the privacy framework

4.1 Overview of the privacy framework

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

- actors and their roles,
- interactions between the actors when processing PII,
- aspects for recognizing PII,
- privacy safeguarding requirements, and
- privacy principles.

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

4.2 Actors and roles

For the purposes of this standard, there are four main types of actors who can be involved in the processing of PII: PII principals, PII controllers, PII processors and third parties.

A PII principal is any natural person to whom the PII relates. Examples include an employee listed in the Human Resources system of a company, the consumer mentioned in a credit report, the patient listed in an electronic health record. It is not always necessary that the individual is identified directly by name in order to be considered a PII principal. If the person to whom the PII relates can be identified indirectly (e.g. through an account identifier, social security number, or even through the combination of available attributes), he or she is also considered to be a PII principal.

A PII controller is an entity who, alone or together with others, determines the purposes and means of the processing. A PII controller determines why (purpose) and how (means) the processing of PII takes place. The PII controller is responsible for ensuring adherence to the privacy principles during the processing of PII under its control (e.g. by implementing the necessary privacy controls). It is also possible that there is more than one PII controller for the same PII set or set of operations performed upon PII. In this case the different PII controllers must work together and make the necessary arrangements to ensure the privacy principles are adhered to during the processing of PII.

A PII controller may also decide to have a whole or a part of the processing operations carried out by a different entity on its behalf. A PII processor is an entity who performs processing operations on behalf of a PII controller. The PII processor must execute the processing of PII in accordance with the instructions of the PII controller. In some jurisdictions the PII processor should be bound by a legal contract requiring that it only act in accordance with the instructions of the PII controller and to observe the stipulated privacy requirements and implement the corresponding privacy controls.

A third party is any natural or legal person, public authority, agency or any other body other than the PII principal, the PII controller or the PII processor (or the persons who process PII under the direct authority of either the PII controller or the PII processor). The third party might receive PII from a PII controller or PII processor, but is not considered a PII processor because it does not process PII on behalf of the PII controller. In many instances the third party will become a PII controller in its own right once it has received the PII in question.

For the purposes of this standard, there are always at least two actors involved in the processing of PII, namely a PII principal and a PII controller.

© ISO/IEC 2010 – All rights reserved

4.3 Interactions

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

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

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

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

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

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

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

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

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

	PII principal	**PII controller**	**PII processor**
Scenario a)	PII provider	PII recipient	-
Scenario b)	-	PII provider	PII recipient
Scenario c)	PII provider	-	PII recipient
Scenario d)	PII recipient	PII provider	-
Scenario e)	PII recipient	-	PII provider
Scenario f)	-	PII recipient	PII provider

The PII processor has a specific role in these scenarios. He executes the processing of PII but does so, on behalf of and in accordance with the instructions of the PII controller.

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

© ISO/IEC 2010 – All rights reserved

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

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

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

The roles of the PII controller and a third party in these scenarios are illustrated in Table 2.

Table 2 – Possible flows of PII between the PII controller and a third party and their roles

	PII controller	**PII processor**	**Third party**
Scenario g)	PII provider	-	PII recipient
Scenario b)	-	PII provider	PII recipient

4.4 Recognizing PII

Any information that is in some way associated or associable with an individual that is either directly or indirectly identifiable is considered to be PII. To determine whether or not an individual should be considered identifiable, several factors need to be taken into account. In particular, account should be taken of all the means which can reasonably be used by the entity holding the data, or by any other party with access to the data, to identify that individual. The following subsections provide additional clarification on how to determine whether or not a PII principal should be considered identifiable.

4.4.1 Numeric identifiers

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

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

4.4.2 Other distinguishing characteristic(s)

The identifiability of a PII principal is equivalent to the ability of determining to which individual a given set of PII relates. Therefore, information does not necessarily need to be associated with a numeric identifier in order to be considered PII. Information will also be considered PII if it contains or is associated with a characteristic which distinguishes an individual from other individuals (e.g., biometric data).

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

© ISO/IEC 2010 – All rights reserved

In addition, there may also be situations in which an individual is identifiable even if there is no single attribute which uniquely identifies him or her. This is the case where a combination of several attributes taken together distinguishes this individual from other individuals. For example, the combination of the attributes “enterprise” and “salary” may be sufficient to identify an individual in certain instances. Both attributes contained directly in the information in question and attributes that can be easily linked to this information (e.g., by using a search engine or cross-referencing with other databases) should be taken into account when determining whether or not the information relates to an identifiable person.

Whether or not an individual is identifiable on the basis of a combination of attributes may also be dependent on the context of use. For instance the combination of the attributes “female”, “45” and “lawyer” may be sufficient to identify an individual within a particular company, but will often be insufficient to identify that individual outside of that company. Table 3 provides some examples of attributes that could be PII, depending on the circumstances. These examples are intended solely to be illustrative.

Table 3 – Examples of attributes that may constitute PII

Examples
National identifiers (e.g. passport number)
Customer number
Biometric identifier
Bank account or credit card number
Name
Gender
Date of birth
Home address
Personal telephone number
Personal e-mail address
IP address
Photograph or video identifiable to an individual
Trade-union membership
Sexual orientation
Criminal convictions or committed offences
Financial profile
Personal identification numbers (PIN) and passwords for financial accounts
Any information collected during health services
Disabilities
Racial or ethnic origin
Religious or philosophical beliefs
Age or special needs of vulnerable individuals
Personal or behavioural profile
Employees’ salaries and human resources files
Any PII identified as such
Location derived from telecommunications systems
Product and service preferences
Personal interests derived from tracking use of internet web sites

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

If the information in question does not directly or indirectly identify a PII principal, it should be determined whether the information is or can be linked to a PII principal. In first instance, information is considered to be linked to an individual if it refers to the identity, characteristics or behaviour of an individual. Examples include medical records, financial profiles, or the personal interests derived from tracking use of internet websites. But also simple attribute statements about a person such as age or gender of a person may qualify as PII.

Sometimes the link between the information and the individual is not immediately apparent. In some situations, the information conveyed concerns objects in the first instance, and not individuals (e.g. an IT account or credential). Nevertheless, if there is the relationship with an identifiable individual can be established, such information must also be treated as PII.

© ISO/IEC 2010 – All rights reserved

4.4.4 Pseudonymous data

Some PII can become pseudonymous when methods are applied to replace identity information with an alias. Conversely, pseudonymous data can become PII when it is correlated with specific PII of the individual. Information in an anonymous form is not considered to be PII. However, even in an anonymous set of data, the smaller the group within the anonymous set, the greater the likelihood of a PII principal being identifiable.

PII may be stored in an ICT system in such a way that it is not readily visible to system users, including the author, who may be the PII principal. Examples include the author's name stored as metadata in the properties of a document, and comments or tracked changes stored as metadata in a word processing document. The PII principal may not want this information to be distributed publicly. ICT systems should support mechanisms that will make the PII principal aware of such PII and provide the individual with appropriate control over the sharing of that information.

4.4.5 Unsolicited PII

PII may also be stored in an ICT system unsolicited by the PII controller or the PII processor. An example of unsolicited PII could include PII entered in a Web form by the PII principal that the PII recipient did not request nor seek to collect and PII stored in a cookie.

4.4.6 Sensitive PII

PII that affects the PII principal's most intimate sphere, or is likely to give rise, in case of misuse, to unlawful or arbitrary discrimination or to a substantial harm or risk to the PII Principal, are considered to be sensitive PII. In some jurisdictions, what constitutes sensitive PII is also defined explicitly in legislation. Examples include information revealing race, ethnic origin, religious or philosophical beliefs, political opinions, trade union memberships, sexual lifestyle or orientation, and the physical or mental health of the PII principal. In other jurisdictions, sensitive PII may include information that could facilitate identity theft or otherwise result in significant financial harm to the individual (e.g., credit card numbers, bank account information, or government-issued identifiers such as passport numbers, social security numbers or drivers' license numbers), and information that could be used to determine the PII principal's real time location.

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

The processing of sensitive PII requires special precautions and in many jurisdictions the requirements for the processing of sensitive PII is defined in laws or regulations. Some jurisdictions may require implementation of specific safeguards where certain types of sensitive PII are processed (e.g., a requirement to encrypt medical PII when transmitting it over a public network). PII controllers should carefully assess whether or not they are processing sensitive PII and install reasonable and appropriate privacy and security controls based on both the requirements set forth in the relevant jurisdiction as well as the potential adverse effects for PII principals in case of a privacy breach.

4.5 Privacy safeguarding requirements

The design of any ICT use case or procedure which involves the processing of PII should include the establishment of privacy safeguarding requirements. Privacy safeguarding requirements are the set of restrictions on the processing of PII which should be obeyed, and the privacy safeguards which should be implemented to protect the rights of PII principals and to privacy breaches, in accordance with the underlying privacy principles.

© ISO/IEC 2010 – All rights reserved

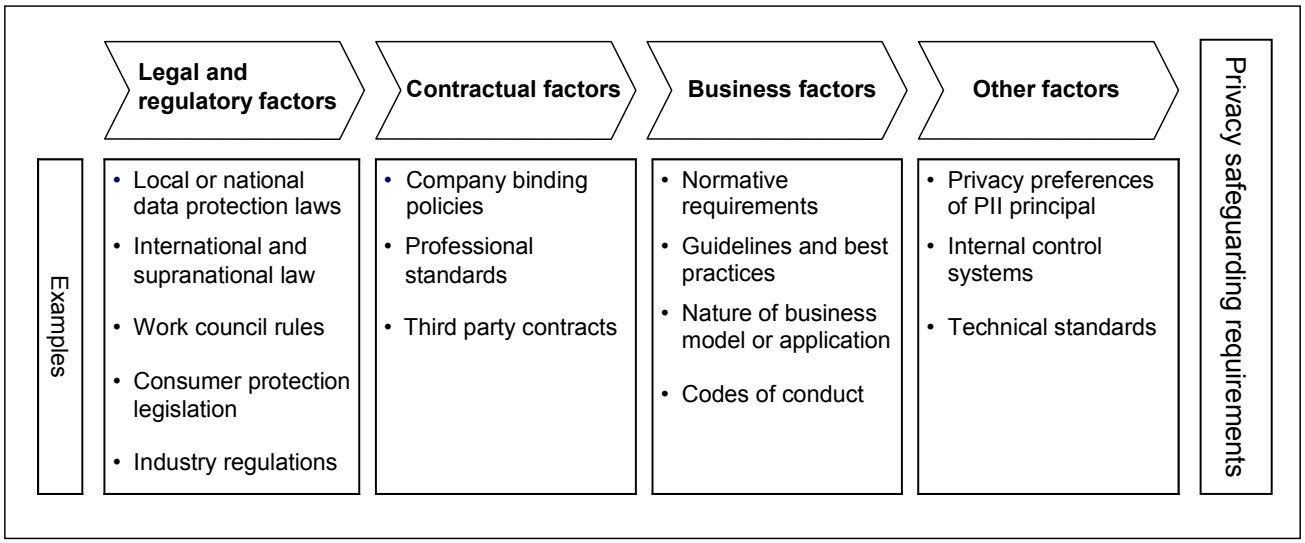

Figure 1 – Factors influencing privacy safeguarding requirements

Privacy safeguarding requirements are influenced by the following factors as depicted in Figure 1 above and described below:

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

4.5.1 Legal and regulatory factors

Privacy safeguarding requirements for designing ICT systems are often reflected in international, national, and local laws, regulations and judicial decisions, and agreements with works councils or other labour organizations. Some examples of local and national laws include data protection laws, consumer protection laws, breach notification laws, data retention laws, and employment laws. Relevant international law might contain rules affecting cross-border transfer of PII. PII controllers should coordinate closely with legal experts to ensure they are aware of all PII processing requirements. It is the responsibility of the PII controller to comply with these additional requirements before processing PII.

4.5.2 Contractual factors

Contractual obligations can affect the design of ICT systems and the respective privacy controls that should be considered. These could be contractual obligations between and among the different actors, such as PII processors, PII controllers, and third parties. For example, an entity may require third parties to use specific privacy controls and agree to specific PII disposal requirements before PII is transferred to them. Privacy safeguarding requirements could also be the result of company policies that the entity has set out for itself, for example to protect its brand from negative publicity in the event of a privacy breach. In addition, any third parties that have access to PII should be made aware of their obligations by the respective PII controller in a formalized manner, for example by entering into third party agreements. In some jurisdictions, national and regional authorities have established legal and contractual instruments that enable the transfer of PII to third parties.

© ISO/IEC 2010 – All rights reserved

4.5.3 Business factors

Factors that influence the privacy safeguarding requirements from a business viewpoint can vary widely depending on the type of entity and type of business. Some examples of business factors are whether the PII principal will need to be contacted regularly, how information is used within an entity by employees, or how the specific business application processes PII in a specific use case context.

4.5.4 Other factors

Other factors can affect the design of ICT systems and the associated privacy safeguarding requirements. These factors include internal control systems and professional or technical standards, such as using a particular information security standard in order to process credit card data. Another significant factor is the privacy preferences of PII principals. The personal disposition of an individual towards privacy and what an individual considers to be sensitive PII can depend on a number of factors including the person's understanding of the technology used, their background, the information being provided, the purpose of the transaction, the person's past experience, and socio-psychological factors.

ICT system designers should attempt to understand the likely privacy concerns of PII principals whose information may be stored in the system. Just as a system developer or an application or service provider may study customer target groups for usage expectations and wants and needs, it is important to try to understand the expectations and preferences of relevant individuals with respect to privacy. Although it is not always possible for ICT systems designers to provide PII principals with choices that match their privacy preferences, it is an important design consideration.

Examples of privacy preferences could include a preference for anonymity, the ability to restrict who can access specific PII, or the ability to restrict how PII may be used. To the extent feasible, the PII principal should be given a choice of preferences for the processing of his data, for example whether the PII is used for secondary purposes such as marketing. Privacy preferences in ICT systems are often presented from a set of options, such as checkboxes and dropdown menus.

The use case may allow the processing of PII to be adjusted to the privacy preferences of the PII principals. In this case privacy preferences should be collected when the PII principals are asked for their consent to the desired PII processing. Insofar as an adjustment is not possible, the conflicting requirements should be made transparent to the PII principals enabling them to make an informed choice whether they want to participate in the given PII use case at all.

Consider authenticated subscription-based access to content as an example use case. Preferences which can be collected and observed in this use case may include pseudonymous access or the use of collected PII for secondary purposes, such as marketing. The ICT system may collect the privacy preferences by presenting a set of options through the display of checkboxes or dropdown menus, or by offering payment options which are compatible with the privacy preference to be observed. Here, as in any other use case, the methods used and the choices offered should be considered in the design of the system. This use case, however, does not allow for anonymity. Hence the individual can either forego her or his preference to remain anonymous, or forego the use of the subscription service.

© ISO/IEC 2010 – All rights reserved

5 The privacy principles of ISO/IEC 29100

5.1 Overview of privacy principles

The privacy principles described in this standard were derived from existing sets of principles developed by a number of international organizations that are referenced in WG5 SD2, but focus here on their implementation in ICT systems and the development of privacy management systems to be implemented within the organization's ICT systems. These privacy principles should be used to guide the design, development, and implementation of privacy policies and privacy controls. Additionally, they can assist in the monitoring and measurement of performance, benchmarking and auditing aspects of privacy management programs in an organization.

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

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

Table 4 – The privacy principles of ISO/IEC 29100

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

5.2 Consent and choice

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

- allowing PII principals prior to the processing of their PII to freely, and on a knowledgeable basis, choose whether or not to allow the processing of their PII except where the PII principal cannot freely withhold consent or where applicable law specifically allows the processing of PII without the individual's consent,
- providing PII principals with the opportunity to choose how their PII is handled, where possible,
- obtaining the explicit opt-in consent of the PII principal for collecting or otherwise processing sensitive PII except where prohibited,
- informing PII principals, before obtaining consent, about their rights under the individual participation and access principle, and
- providing PII principals, before obtaining consent, with the information indicated by the openness, transparency and notice principle.

Provisions should be made to allow a PII principal to withdraw his/her consent at some later date. The PII controller should provide the PII principal with user-friendly means to withdraw consent easily, free of charge and in due time. Even if consent is withdrawn, there may be need to retain certain PII

© ISO/IEC 2010 – All rights reserved

for a period of time in order to comply with legal or contractual obligations (e.g., data retention, accountability). Where the PII principal does not have the ability to effectively withdraw consent for certain PII processing, the PII principal should be notified thereof prior to initial consent wherever possible. Where the PII principal has chosen to withdraw consent, this PII must in any event be exempted from processing for any other purpose.

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

- providing PII principals with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice and to give consent in relation to the processing of their PII at the time of collection or first use or as soon as practicable thereafter,
- informing PII principals about the consequences, if any, of withholding their consent in whole or in part may have, and
- implementing the PII principal's preferences as expressed in his/her consent.

Consent should be based on a freely given choice and based on a reasonably clear explanation of the implications of the data processing. Moreover, additional provisions may be defined for processing PII other than consent (e.g., the performance of a contract, the vital interest of the PII principal, or compliance with the law). Applicable law in some instances may provide that the consent of the PII principal does not constitute a sufficient legal basis to process PII (e.g., the consent of an employee given to his/her employer). Moreover, additional requirements on transferring PII internationally are to be considered. It is the responsibility of the PII controller to comply with these additional provisions before processing or transferring data.

5.3 Purpose legitimacy and specification

For a PII controller, adhering to the purpose legitimacy and specification principle means:

- checking whether the purpose(s) complies with applicable law and relies on a permissible legal basis such as consent, a contractual obligation, or on another basis as provided in clause 5.2 above,
- communicating the purpose(s) to the PII principal at or before the time the information is collected or used for the first time for a new purpose, or as soon as practical thereafter,
- using language for this specification which is both clear and appropriately adapted to the circumstances, and
- if applicable, giving sufficient explanations for the need of processing sensitive PII.

With regard to sensitive PII, stricter rules may apply to the purpose of processing. To be lawful, a purpose may require a legal basis or a specific authorization by a regulator such as a Data Protection Authority. If the purpose(s) for processing PII do not comply with applicable law, processing should not take place.

The purpose for the processing of PII should be sufficiently detailed in order to allow the PII principal to understand:

- the type of data necessary for the purpose,
- the circumstances triggering or authorizing the processing of PII,
- which persons or types of persons will have legitimate access to the PII, and
- how long the information will be stored.

5.4 Collection limitation

For a PII controller, adhering to the collection limitation principle means

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

© ISO/IEC 2010 – All rights reserved

Organizations should not collect PII indiscriminately. Both the amount and the type of PII collected should be limited to that which is necessary to fulfil the purpose(s) identified. Organizations should specify the type of PII collected as part of their information-handling policies and practices. With the consent of the individual, additional information may be collected. The request for additional information should be optional for the individual.

5.5 Data minimization

Data minimization is closely linked to the principle of “collection limitation” but goes further than that. For a PII controller, adhering to the data minimization principle means designing data processing procedures and ICT systems in such a way as to minimize the PII which is processed. Whereas “collection limitation” refers to limited data being collected in relation to the specified purpose, “data minimization” strictly minimizes the collection of data regardless of the purpose. Implementing “data minimization” in data processing systems means that the design of programs, information technologies, and systems should consider non-identifiable interactions and transactions by default and, wherever possible, the identifiability, observability, and linkability of PII is minimized.

5.6 Use, retention and disclosure limitation

For a PII controller, adhering to the use, retention and disclosure limitation principle means:

- limiting the use, retention and disclosure (including transfer) of PII to that which is necessary in order to fulfil specific, explicit and legitimate purposes specified by the PII controller prior to collection, unless the secondary use is explicitly required or permitted by applicable law,
- limiting further use of PII to the purposes originally specified by the PII controller unless the new purpose is required by law or has been consented to by the PII principal prior to use,
- limiting use of the PII to the communicated, specified purpose(s),
- prohibiting secondary uses that are incompatible with the communicated, specified purpose(s), and
- retaining PII only as long as necessary to fulfil the stated purposes, and thereafter securely destroy or anonymize it, and
- locking (i.e. archiving and exempting from further usage) any PII when and as long as the stated purposes have expired, but where retention is required by applicable laws.

When PII is transferred internationally, additional requirements should be fulfilled by the PII controller, in particular the provisions of clause 5.10. The transferring of PII to countries that do not provide a sufficient level of protection may be prohibited or the PII controller may be required to implement reasonable and appropriate privacy safeguarding measures through contractual or other means such as mandatory internal PII processing rules.

When personal information that has been collected is to be processed for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be processed for that purpose.

5.7 Accuracy and quality

For a PII controller, adhering to the accuracy and quality principle means

- ensuring that PII they process is accurate, complete, up-to-date (unless there is a legitimate basis for keeping anterior data) and adequate and relevant for the purpose of use,
- ensuring the reliability of PII collected from another source than the PII principal before it is processed,
- verifying through appropriate means the identity of the PII principal where it is appropriate to do so,
- establishing PII collection procedures to help ensure accuracy and quality, and
- establishing control mechanisms to periodically check the accuracy and quality of collected and stored PII.

© ISO/IEC 2010 – All rights reserved

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

5.8 Openness, transparency and notice

For a PII controller, adhering to the openness, transparency and notice principle means:

- providing PII principals with clear and easily accessible information about their practices, policies and procedures with respect to the handling of PII,
- including in these statements the fact that PII is being processed, the purpose for which this is done, the types of entities to whom the PII might be disclosed, and the identity of the PII controller including information on how to contact the PII controller,
- furthermore, disclosing the choices and means the PII controller offers PII principals for limiting the processing of, and for accessing and correcting their information, and
- giving notice to the PII principals when major changes in the PII handling procedures occur.

Transparency to include general information on the logic underlying the PII processing may be required, particularly, if the processing involves a decision impacting the PII principal. Entities that process PII are well advised to make specific information about their policies and practices relating to the management of PII readily available to the public. All contractual obligations that impact PII processing should be documented and communicated internally as appropriate.

5.9 Individual participation and access

For a PII controller, adhering to the individual participation and access principle means:

- giving PII principals with the ability to access and review their PII, provided that they are first authenticated with an appropriate level of assurance (see Table A-1) and such access is not prohibited by applicable law,
- allowing PII principals to challenge the accuracy and completeness of the PII and have it amended, corrected or removed as appropriate and possible in the specific context,
- providing any amendment, correction or removal to PII processors and third parties to whom personal data had been disclosed, where they are known, and
- establishing procedures to enable PII principals to exercise these rights in a simple, fast and efficient way, which do not entail undue delay or cost nor any profit for the PII controller.

The PII controller should apply appropriate safeguards to ensure that the PII principal accesses strictly his own PII and not that of other PII principals. Applicable law may provide the individual with the right to access, review and object to the processing of PII under certain circumstances. When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge should be recorded by the organization. When appropriate, the existence of the unresolved challenge should be transmitted to third parties having access to the information in question.

5.10 Accountability

The processing of PII entails a duty of care for its protection. For a PII controller, adhering to the accountability principle means:

- documenting and communicating as appropriate accountability for all privacy-related policies, procedures and practices,
- assigning to a specified individual within the organization (who may in turn delegate to others in the organization as appropriate) the task of implementing the privacy-related policies, procedures and practices,

© ISO/IEC 2010 – All rights reserved

- seeking equivalent privacy protection through contractual or other means when transferring PII to third parties,
- verifying and demonstrating that the processing meets the requirements of accountability by periodically conducting audits by internal auditors or by trusted third-party auditors,
- having appropriate internal controls and independent supervision mechanisms in place that assure compliance with relevant law and with their security, data protection and privacy policies and procedures,
- developing and maintaining privacy risk assessments in order to evaluate whether program and service delivery initiatives involving PII processing comply with data protection and privacy requirements,
- resolving risks and vulnerabilities that are discovered through the audit process,
- providing suitable training for the personnel of the PII controller who will have access to PII,
- setting up an efficient internal complaint handling procedure for use by PII principals,
- establishing redress procedures in order to give PII principals effective means to exercise their right for privacy protection and report privacy violations,
- informing PII principals in due time about privacy breaches that may lead to substantial damage to them as well as the measures taken for resolution insofar as this can be achieved with means and effort proportionate to the risks resulting from the breach unless prohibited (e.g., while working with law enforcement),
- allowing an aggrieved PII principal access to appropriate and effective sanctions and/or remedies, such as rectification, expungement or restitution if a privacy breach has occurred,
- considering procedures for compensation for situations in which it will be difficult or impossible to bring the individual's privacy status back to a position as if nothing had occurred and
- defining expected outcomes and usable fall back procedures.

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

Where redress processes are in place, users may feel more confident entering into a transaction because the perceived risk for the individual with regard to the outcome is effectively reduced. For some services redress is easier to achieve (e.g., financial loss) than for others (e.g., a stolen identity, damage to the image or reputation of the individual), where the ability to quantify and compensate for the loss could be somewhat harder. Redress works best when based on transparency and honesty, as it is through provision of clear redress procedures that barriers to service use or adoption by the user could be lowered. Required types of redress measures may be governed by law.

5.11 Information security controls

For a PII controller, adhering to the security controls principle means:

- protecting PII under its control with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the PII, and protect it against risks such as loss or unauthorized access, destruction, use, modification or disclosure, or other misuses, throughout the whole of its life cycle,
- ensuring that PII processors acting on its behalf also implement appropriate controls as per the preceding item,
- basing these controls on applicable legal requirements, security standards, the results of systematic privacy risk assessments as described in ISO 31000, and the costs associated with the security controls,

© ISO/IEC 2010 – All rights reserved

- implementing controls in proportion to the likelihood and severity of the potential consequences, the sensitivity of the PII, the number of PII principals that might be affected, and the context in which it is held,
- including reasonable organisational, physical, and technical means in the controls,
- subjecting the controls to periodic review and reassessment in an ongoing privacy risk management process, and
- choosing PII processors that provide sufficient guarantees with regard to technical and organisational security controls for the processing of PII and ensuring compliance with these controls.

PII processors should take similar measures.

5.12 Compliance

For a PII controller, adhering to the compliance principle means

- ensuring compliance with relevant law and with their security, data protection and privacy policies and procedures, and
- resolving privacy issues as they arise.

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

© ISO/IEC 2010 – All rights reserved

Annex A
(informative)
Relating privacy principles to information security controls

While some privacy problems differ from security issues (e.g., the misuse of the individual's PII by the PII controller or PII processor), others have identical causes or are in fact based on the latter. Nearly all security incidents or events – regardless of whether they stem from attacks and mistakes – have direct impact on data, which can be destroyed, eavesdropped, stolen or altered.

In consequence, every implemented security control could not only protect corporate secrets but also PII stored within the protected system. Policies ensuring data integrity, averting intrusion or data loss are therefore privacy controls as well as security controls.

Sometimes requirements for privacy have objectives that contradict requirements for ICT security. For example, security controls that have the objective to protect an entity against fraud and need to control specific activities of employees may contradict the employees' right to privacy. Sometimes it is necessary to sacrifice privacy to achieve security outcomes. For example, security screening at airports is designed to maintain security but as a consequence privacy can be sacrificed. To give another example, logging to detect unauthorised access to systems (desirable from an ICT security point of view) can capture and create PII without the consent of the PII principal and conflicts with the data minimization principle and associated requirements. Similarly, backup arrangements to provide high availability can present problems associated with PII minimization and PII accuracy.

Table A.1 attempts to show the relationship of the privacy principles of ISO/IEC 29100 to information security controls:

Table A.1 – Privacy principles and their corresponding information security controls

Privacy principles	**Information security controls**	**ISO/IEC 27002:2007 section reference:**
Consent and choice	The consent and choice of the PII principal should be subject to confidentiality rules as these are agreed according to roles and responsibilities within the organization. The PII controller should determine and document the most reasonable and appropriate security measures that minimize interference with the respective privacy requirements. For example, where appropriate, authentication could be used to help ensure that the individual who provides the consent is actually who he claims to be.	6.1.5 r a), b), d) and f), among others.
Purpose legitimacy and specification	Not applicable.	Not applicable
Collection limitation	A general measure to reduce risks is to reduce the amount of confidential information and critical assets required to be protected. Limiting the collection of PII information to the absolute minimum required supports the overall information security objective.	4.2 a) and c)
Data minimization	While security standards usually call for the monitoring of all activities, log files and other documents might contain PII and, therefore, could contradict the privacy principle of 'data minimization'. In consequence, extensive retention of data – advisable from a security standpoint – might pose a threat to privacy. Implementing data classification procedures to achieve a separate handling of PII and a PII minimization strategy are advised. The use of pseudonymization and anonymization are also advised.	5.7.4, 5.7.5, 5.7.6 and 10.10
Use, retention and	Limiting disclosure can, among other things, be controlled by the proper use of confidentiality agreements, classification and	6.1.5, 7.2 and 11

© ISO/IEC 2010 – All rights reserved

disclosure limitation	access control.	
Accuracy and quality	Since accuracy and quality of data is fundamental in all areas, reasonable and appropriate controls should already be implemented in most organizations. These controls can be applied to PII without extensive modifications and help control PII as well.	12.2.4
Openness, transparency and notice	Fulfilling these objectives requires a high level of security since it involves making information accessible to the individual the PII involves and relates to – and only that individual (PII principal). Reasonable and appropriate controls and security measures that apply when exchanging and revealing information therefore also apply to meeting these objectives.	10.8.1, 10.8.4, 10.9.1 and 10.10.1.
Individual participation and access	Access control rules should exist in every organization. Taking into account authorization policies, they can be applied to requests by PII providers as well. The existing controls can be extended to include these requests without elaborate alterations.	10.8, 10.9 and 11
Accountability	The assignment of specific roles and responsibilities plays an integral part in every security framework. Accountability for privacy related policies and procedures should be regarded as such an assignment and be realized by means of existing controls.	7.1 and 8.1.1
Information security controls	Existing security standards such as ISO/IEC 27002:2007 provide comprehensive recommendations on security controls that should be implemented explicitly for ensuring data security. In particular, the following security controls should be implemented (the following list is not exhaustive): Access to data processing facilities should be prohibited for unauthorized persons Unauthorized persons should not be allowed to access computer systems Authorized persons should only be able to access PII within the scope of their access authority Physical and electronic transport or transmission of PII should be reasonably and appropriately secured against unauthorized access Logs should be kept to document any access to and alteration of PII, particularly sensitive PII The handling of PII by third party contractors should be covered by binding contractual terms PII should be secured against accidental or unauthorized disclosure, modification, loss, removal or destruction PII with different purpose specifications should be handled separately Propoer procedures for privacy breach management should be in place	7.2, 9.1, 9.2, 10, 11, and 12.3
Compliance	Compliance with security standards such as ISO/IEC 27002:2007 provides conformance with security control requirements for the protection of PII that is a prerequisite for enforcement of privacy policy.	

The given information security controls are meant to be illustrative examples of recommended security controls and are not normative in nature.

© ISO/IEC 2010 – All rights reserved

Annex B
(informative)
Illustrative examples

The following descriptions are informative in nature but may support the elements described in this International Standard and are intended to provide examples for an improved understanding of the respective topics.

B.1 Interdependent issues

PII is processed for many different purposes, in many different forms and in practically all information and communication technologies today. Therefore, it is difficult to cover all areas that are interrelated and interdependent with the data handling procedures described in this International Standard. The following topics, however, are an attempt to address areas that are of practical use and represent additional information that is directly related to this International Standard at the time of its development:

a) Data storage

b) Data mining

c) System development

Data storage controls are mainly focused on secure retention of PII. These controls could include the following:

- appropriate procedures for saving: PII should be saved in such a way that transparency and accountability for the data is ensured and access to any specific PII is controlled but not unnecessarily hindered;
- appropriate backup procedures: Redundancies should be created to safely and securely store PII and to ensure its continued availability during or after security incidents or hardware failures;
- appropriate safeguards: PII should be stored in a manner intended to protect PII from loss, misuse, and unauthorized access, disclosure, alteration or destruction. Appropriate safeguards can include encryption, access controls, and physical security;
- minimizing PII stored: PII storage should be minimized whenever possible. PII should be stored only as long as necessary. The ability to link stored PII with other data about the individuals should be minimized unless the consent of the PII principal was given or it is required by law; and
- pseudonymizing or anonymizing PII: PII can also be pseudonymized or anonymized to reduce the impact of a privacy breach.

While data mining is a common practice, certain data mining techniques could potentially contradict or violate privacy safeguarding requirements by exceeding the boundaries of the specified purpose or by using non-public PII without the consent of the individual.

Privacy should have an important and permanent part in the development life cycle of systems. If privacy requirements are viewed as a separate and independent piece of functionality that might be added later on, they will not address the risks associated with systems that hold an increasing amount of PII and are increasingly vulnerable to privacy breach. The implementation of security measures alone in information systems does not and cannot ensure that PII is used in an appropriate way or in a way consistent with privacy requirements. Security controls usually take the viewpoint of protecting data from external or internal threats but security controls do not ensure the proper handling of content such as PII. Therefore, system developers should not leave addressing privacy requirements until the end of the development cycle. Privacy should be an integral part of the system

© ISO/IEC 2010 – All rights reserved

development life cycle. Failure to incorporate “privacy by design” will mean the risks associated with systems handling increasing amounts of PII will not be adequately addressed.

B.2 Examples of privacy safeguarding requirements

The following list of privacy safeguarding requirements has been provided to further illustrate and explain the meaning of privacy safeguarding requirements. It is not intended to be an exhaustive list; nor will all items below be necessary in all scenarios. Privacy safeguarding requirements will vary depending on context (e.g., the reasons for collecting PII, the type of PII being collected, how the PII will be used, etc.).

a) Obtaining and recording the PII principal’s knowledgeable, free and specific consent

Unless otherwise authorized (e.g., specifically exempted by law or professional code of practice), PII controllers processing PII should:

- obtain the knowledgeable, free, and specific consent of each individual for the processing of his/her PII (which could be required by law);
- inform individuals about the potential implications of choices they have made, including directives for locking or masking PII;
- enable ICT systems to transmit these choices in a consistent form whenever they process the associated PII including the withholding, withdrawal or revocation of consent;
- process these consent directives before processing the associated data and block the PII processing where it would violate the directives and where no exception for such a processing is outlined in law; and
- enable the ICT system to log cases where the consent directives prohibit the PII processing.

b) Identifying and communicating the purpose(s) for processing PII

PII controllers processing PII should:

- identify all the purposes for which PII will be processed before the time PII is collected; and
- make a reasonable effort to inform persons of these purposes, in a readily understandable manner, prior to collecting their PII.

c) Limiting the collection of PII to the identified purposes (collection limitation)

PII controllers collecting PII should:

- collect only that PII which is necessary to fulfil the purposes that they have identified, except with the consent of the individual or as permitted or required by law; and
- not collect PII by misleading or deceiving individuals or other organizations about the purposes for which information is being collected.

© ISO/IEC 2010 – All rights reserved

d) Implementing data minimization procedures

PII controllers processing PII should carefully consider and document procedures that state clearly which PII is needed for which purpose and how they will ensure that all PII processing involves only the minimum PII necessary. Anonymizing PII where possible is a recommended best practice to extend the data collection principle to PII processing and use procedures.

e) Limiting the use, disclosure and retention of PII

Personal information should not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information should be retained only as long as necessary for the fulfilment of those purposes.

PII that is no longer required to fulfil the identified purposes should be securely destroyed, erased, or anonymized. PII controllers should develop guidelines and implement procedures to govern the secure destruction of PII.

f) Providing individuals with access to information related to PII processing

PII controllers processing PII should, upon request:

- inform an authenticated individual of the existence, use and disclosure of his/her PII and give the individual direct access to that PII where such access is not prohibited by legislation;
- respond to requests for access to an authenticated individual's PII within a reasonable time and make it available in a form that is generally understandable;
- allow an authenticated individual to challenge the accuracy and completeness of his/her PII and have it amended as appropriate; and
- provide the ability for the individual to withdraw his/her consent and/or delete his/her PII where such a function is not prohibited by legislation or the circumstances of the original transaction.

g) Checking the PII's accuracy and quality

PII controllers processing PII should take reasonable steps or make a reasonable effort to:

- ensure that PII is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used, including disclosures of PII to third parties;
- accurately authenticate a PII principal when accessing or modifying his/her PII;
- amend PII when permitting access to or modification of his/her PII;
- notify users that have accessed the information in question that the information has been amended when the amended information can reasonably be expected to have an effect on the individual;
- record the substance of any unresolved challenges when the organization disagrees with the individual's assessment of incompleteness or inaccuracy; and
- communicate the existence of an unresolved challenge to users accessing the information in question.

© ISO/IEC 2010 – All rights reserved

h) Limitation of the processing of sensitive PII

PII controllers should only process sensitive PII if one of the following conditions is fulfilled:

- the PII principal has given his explicit consent to the processing of sensitive PII, unless applicable law provides that the processing of sensitive PII is prohibited even with the PII principal's consent;
- processing is necessary for the purposes of carrying out the obligations and specific rights of the PII controller in an employment scenario;
- processing is necessary to protect the vital interests of the PII principal or of another person when the PII principal is physically or legally incapable of giving his consent;
- if not prohibited, processing is carried out in the course of its legitimate activities, with appropriate guarantees, by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it, in connection with its purposes, and that the PII is not disclosed to a third party without the consent of the PII principal;
- processing relates to sensitive PII which has been made public by the PII principal or is necessary for the establishment, exercise or defense of legal claims;
- processing is required for the purpose of providing medical treatment or health care services, and where those PII are processed by a health professional or other individual bound by confidentiality, such as an obligation of professional secrecy;
- processing is necessary for reasons of substantial public interest.

© ISO/IEC 2010 – All rights reserved

Annex C
Bibliography

This annex gives a list of some of the most generally available reference works related to privacy and data protection. This list is not intended to be exhaustive and the listed reference works may not apply to all scenarios.

C.1 ISO/IEC documents and standards

ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) -- *Official Privacy Documents References*

ISO/IEC 29101, *Information technology - Security techniques - Privacy reference architecture*

ISO Guide 73, *Risk management - Vocabulary*

ISO/IEC 27001:2005, *Information technology - Security techniques - Information security management systems - Requirements*

ISO/IEC 27002: 2005, *Information technology - Security techniques - Code of practice for information security management*

ISO/IEC 31000:2009, *Risk management - Principles and guidelines*

C.2 Privacy and data protection references

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

APEC Privacy Framework

C*onvention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* Council of Europe Convention108 (ETS No. 108)

© ISO/IEC 2010 – All rights reserved