DRAFT International Standard

ISO/IEC DIS 27701.2

Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

ICS: 35.030

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2024-07-02

Voting terminates on:
2024-08-27

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

IMPORTANT — Please use this updated version dated 2024-06-19, and discard any previous version of this DIS as VA relation has been added.

Reference number
ISO/IEC DIS 27701.2:2024(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27701:2019), which has been redrafted as a stand-alone management system.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

0.1 General

Almost every organization processes personally identifiable information (PII). Further, the quantity and types of PII processed is increasing, as is the number of situations where an organization needs to cooperate with other organizations regarding the processing of PII. Protection of privacy in the context of the processing of PII is a societal need, as well as the topic of dedicated legislation or regulation all over the world.

This document includes mapping to:

— the privacy framework and principles defined in ISO/IEC 29100;

— ISO/IEC 27018;

— ISO/IEC 29151; and

— the EU General Data Protection Regulation.

NOTE These can be interpreted to take into account local legislation or regulation.

This document can be used by PII controllers (including those that are joint PII controllers) and PII processors (including those using subcontracted PII processors and those processing PII as subcontractors to PII processors).

By complying with the requirements in this document, an organization can generate evidence of how it handles the processing of PII. Such evidence can be used to facilitate agreements with business partners where the processing of PII is mutually relevant. This can also assist in relationships with other interested parties. The use of this document can provide independent verification of this evidence.

This document was initially developed as ISO/IEC 27552.

0.2 Compatibility with other management system standards

This document applies the framework developed by ISO to improve alignment among its management system standards.

This document enables an organization to align or integrate its PIMS with the requirements of other management system standards, and in particular with the information security management system specified in ISO/IEC 27001.

Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

1 Scope

This document specifies requirements for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS).

Guidance is provided to assist in the implementation of the requirements in this document.

This document is intended for PII controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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, *Information technology — Security techniques — Privacy framework*

3 Terms, definitions and abbreviations

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.6)

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: If the organization is part of a larger entity, the term “organization” refers only to the part of the larger entity that is within the scope of the privacy information *management system* (3.4).

3.2
interested party (preferred term)
stakeholder (admitted term)

person or *organization* (3.1) that can affect, be affected by, or perceive itself to be affected by a decision or activity

3.3
top management
person or group of people who directs and controls an *organization* (3.1) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.4) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

3.4
management system
set of interrelated or interacting elements of an *organization* (3.1) to establish *policies* (3.5) and *objectives* (3.6), as well as *processes* (3.8) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The management system elements include the organization's structure, roles and responsibilities, planning and operation.

3.5
policy
intentions and direction of an *organization* (3.1) as formally expressed by its *top management* (3.3)

3.6
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as finance, health and safety, and environment). They can be, for example, organization-wide or specific to a project, product or *process* (3.8).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended result, as a purpose, as an operational criterion, as a privacy information objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of *privacy information management systems* (3.22), privacy information objectives are set by the *organization* (3.1), consistent with the privacy information *policy* (3.5), to achieve specific results.

3.7
risk
effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

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

Note 3 to entry: Risk is often characterized by reference to potential events (as defined in ISO Guide 73) and consequences (as defined in ISO Guide 73), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (as defined in ISO Guide 73) of occurrence.

3.8
process
set of interrelated or interacting activities that uses or transforms inputs to deliver a result

Note 1 to entry: Whether the result of a process is called an output, a product or a service depends on the context of the reference.

3.9
competence
ability to apply knowledge and skills to achieve intended results

3.10
documented information
information required to be controlled and maintained by an *organization* (3.1) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media and from any source.

Note 2 to entry: Documented information can refer to: – the *management system (*3.4), including related *processes* (3.8); – information created in order for the organization to operate (documentation); – evidence of results achieved (records).

3.11
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to managing activities, *processes* (3.8), products, services, systems or *organizations* (3.1).

3.12
continual improvement
recurring activity to enhance *performance* (3.11)

3.13
effectiveness
extent to which planned activities are realized and planned results are achieved

3.14
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: “Generally implied” means that it is custom or common practice for the *organization* (3.1) and *interested parties* (3.2) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, e.g. in *documented information* (3.10).

3.15
conformity
fulfilment of a *requirement* (3.14)

3.16
nonconformity
non-fulfilment of a *requirement* (3.14)

3.17
corrective action
action to eliminate the cause(s) of a *nonconformity* (3.16) and to prevent recurrence

3.18
audit
systematic and independent *process* (3.8) for obtaining evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the *organization* (3.1) itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

3.19
measurement
process (3.8) to determine a value

3.20
monitoring
determining the status of a system, a *process* (3.8) or an activity

Note 1 to entry: To determine the status, there can be a need to check, supervise or critically observe.

3.21
joint PII controller
PII controller that determines the purposes and means of the processing of PII jointly with one or more other PII controllers

3.22
customer
person or *organization* (3.1) that could or does receive a product or a service that is intended for or required by this person or *organization* (3.1)

EXAMPLE Consumer, client, end-user, retailer, receiver of product or service from an internal *process* (3.8), beneficiary and purchaser.

Note 1 to entry: A customer can be internal or external to the organization.

Note 2 to entry: A customer can be an *organization* (3.1) that has a contract with a PII controller, a PII controller who has a contract with a PII processor or a PII processor that has a contract with a subcontractor for PII processing (see 4.2 for further information).

3.23
privacy information management system
PIMS
management system (3.4) which addresses the protection of privacy as potentially affected by the processing of PII

3.24
information security programme
set of policies (3.5), objectives (3.6) and processes (3.8) designed to manage risks (3.7) to an organization's (3.1) assets, to ensure confidentiality, integrity and availability of information

Note 1 to entry: An information security programme can be, for example, an information security management system such as one based on ISO/IEC 27001.

3.25
statement of applicability
documentation of all necessary controls and justification for inclusion or exclusion of controls

Note 1 to entry: Organizations may not require all controls listed in Annex A or may even exceed the list in Annex A with additional controls established by the organization itself.

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its privacy information management system.

The organization shall determine whether climate change is a relevant issue.

The organization shall determine if it is acting as a PII controller (including as a joint PII controller) or as a PII processor.

The organization shall determine external and internal issues that are relevant to its context and that affect its ability to achieve the intended outcome(s) of its PIMS.

NOTE 1 External and internal issues can include but are not limited to:

— applicable privacy legislation;

— applicable regulations;

— applicable judicial decisions;

— applicable organizational context, governance, policies and procedures;

— applicable administrative decisions;

— applicable contractual requirements.

Where the organization acts in both roles (i.e. a PII controller and a PII processor), separate roles shall be determined, each of which is the subject of a separate set of controls.

NOTE 2 The role of the organization can be different for each instance of the processing of PII, since it depends on who determines the purposes and means of the processing.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

— the interested parties that are relevant to the privacy information management system;

— the relevant requirements of these interested parties;

— which of these requirements will be addressed through the privacy information management system.

NOTE 1 Relevant interested parties can have requirements related to climate change.

The organization shall include among its interested parties those parties having interests or responsibilities associated with the processing of PII, including the PII principals.

NOTE 2 Other interested parties can include customers (see 4.2), supervisory authorities, other PII controllers, PII processors and their subcontractors.

Depending on the role of the organization, "customer" can be understood as either:

a) an organization who has a contract with a PII controller (e.g. the customer of the PII controller, the case of an organization which is a joint PII controller);
b) a PII controller who has a contract with a PII processor (e.g. the customer of the PII processor); or
c) a PII processor who has a contract with a subcontractor for PII processing (e.g. the customer of the subcontracted PII processor).

NOTE 3 An individual person in a business to consumer relationship with an organization is referred to as a "PII principal" in this document.

NOTE 4 Requirements relevant to the processing of PII can be determined by legal and regulatory requirements, by contractual obligations and by self-imposed organizational objectives. The privacy principles set out in ISO/IEC 29100 provide guidance concerning the processing of PII.

NOTE 5 As an element to demonstrate compliance to the organization's obligations, some interested parties can expect that the organization is in conformity with specific standards, such as the management system specified in this document, or any relevant set of specifications. These parties can call for independently audited compliance to these standards.

4.3 Determining the scope of the privacy information management system

The organization shall determine the boundaries and applicability of the privacy information management system to establish its scope.

When determining this scope, the organization shall consider:

— the external and internal issues referred to in 4.1;

— the requirements referred to in 4.2.

The scope of the organization's privacy information system shall be available and be maintained as documented information.

When determining the scope of the PIMS, the organization shall include the processing of PII.

4.4 Privacy information management system

The organization shall establish, implement, maintain and continually improve a privacy information management system, including the processes needed and their interactions, in accordance with the requirements of this document.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the privacy information management system by:

- ensuring that the privacy policy (see 5.2) and privacy objectives (see 6.2) are established and are compatible with the strategic direction of the organization;
- ensuring the integration of the privacy information management system requirements into the organization's business processes;
- ensuring that the resources needed for the privacy information management system are available;
- communicating the importance of effective privacy information management and of conforming to the privacy information management system requirements;
- ensuring that the privacy information management system achieves its intended result(s);
- directing and supporting persons to contribute to the effectiveness of the privacy information management system;
- promoting continual improvement;
- supporting other relevant roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.2 Privacy Policy

Top management shall establish a privacy policy that:

a) is appropriate to the purpose of the organization;
b) provides a framework for setting privacy objectives;
c) includes a commitment to meet applicable requirements;
d) includes a commitment to continual improvement of the privacy information management system.

The privacy policy shall:

- be available as documented information;
- be communicated within the organization;
- be available to interested parties, as appropriate.

5.3 Roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the privacy information management system conforms to the requirements of this document;
b) reporting on the performance of the privacy information management system to top management.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the privacy information management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

— give assurance that the privacy information management system can achieve its intended result(s);

— prevent, or reduce undesired effects;

— achieve continual improvement.

The organization shall plan:

a) actions to address these risks and opportunities;
b) how to

— integrate and implement the actions into its privacy information management system processes;

— evaluate the effectiveness of these actions.

6.1.2 Privacy risk assessment

The organization shall define and apply a privacy risk assessment process that:

a) establishes and maintains privacy risk criteria that include:
   1) the risk acceptance criteria; and
   2) criteria for performing privacy risk assessments;
b) ensures that repeated privacy risk assessments produce consistent, valid and comparable results;
c) identifies the privacy risks:
   1) associated with the protection of privacy and information security risks within the scope of the privacy information management system; and
   2) that identify the risk owners;
d) analyses the privacy risks that:
   1) assess the potential consequences for both the organization and PII principals that would result if the risks identified in 6.1.2 c) 1) were to materialize;

2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and

3) determine the levels of risk;

e) evaluates the privacy risks that:

1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and

2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the privacy risk assessment process.

NOTE For further information on the privacy risk assessment process, see ISO/IEC 27557.

6.1.3 Privacy risk treatment

The organization shall define and apply a privacy risk treatment process to treat risks related to the processing of PII, including risks to PII principals, and including the security of PII, by:

a) selecting appropriate privacy risk treatment options, taking account of the risk assessment results;

b) determining all controls that are necessary to implement the privacy risk treatment option(s) chosen;

NOTE 1 Organizations can design controls as required, or identify them from any source.

c) identifying and documenting the information security programme implemented by the organization, including the appropriate security controls;

NOTE 2 ISO/IEC 27002 provides a list of possible information security controls. If the information security programme is based on ISO/IEC 27001, users of this document are directed to ISO/IEC 27002 to ensure that no necessary information security controls are overlooked.

d) comparing the controls determined in 6.1.3 b) above with those in Annex A and verifying that no necessary controls have been omitted;

NOTE 3 Annex A contains a list of possible privacy controls. Users of this document are directed to Annex A to ensure that no necessary privacy controls are overlooked.

NOTE 4 The privacy controls listed in Annex A are not exhaustive and additional privacy controls can be included if needed.

NOTE 5 Organizations can address security and privacy in an integrated manner when considering the security of PII processing, combining security and privacy risk assessments for example, or as separate entities with overlapping areas.

e) producing a statement of applicability that includes;

— the necessary controls (see 6.1.3 b), c) and d));

— justification for their inclusion;

— whether the necessary controls are implemented or not; and

— the justification for excluding any of the controls from Annex A.

Not all the controls listed in Annex A need to be included. Justification for exclusion of any control can include where the controls are not deemed necessary by the risk assessment, and where they are not required by (or are subject to exceptions under) the applicable legislation or regulation, including those applicable to the PII principal.

f) formulating a privacy risk treatment plan;

g) obtaining the privacy risk owners' approval of the privacy risk treatment plan and acceptance of the residual privacy risks; and

h) considering the guidance in Annex B for the implementation of controls determined in b) and c).

The organization shall retain documented information about the information privacy risk treatment process.

6.2 Privacy objectives and planning to achieve them

The organization shall establish privacy objectives at relevant functions and levels.

The privacy objectives shall:

a) be consistent with the privacy policy (see 5.2);
b) be measurable (if practicable);
c) take into account applicable requirements;
d) be monitored;
e) be communicated;
f) be updated as appropriate;
g) be available as documented information.

When planning how to achieve its privacy objectives, the organization shall determine:

— what will be done;
— what resources will be required;
— who will be responsible;
— when it will be completed;
— how the results will be evaluated.

6.3 Planning of changes

When the organization determines the need for changes to the privacy information management system, the changes shall be carried out in a planned manner.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the privacy information management system.

7.2 Competence

The organization shall:

— determine the necessary competence of person(s) doing work under its control that affects its privacy information performance;
— ensure that these persons are competent on the basis of appropriate education, training, or experience;
— where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken.

Appropriate documented information shall be available as evidence of competence.

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the re-assignment of currently employed persons; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

- the privacy policy (see 5.2);
- their contribution to the effectiveness of the privacy information management system, including the benefits of improved privacy performance;
- the implications of not conforming with the privacy information management system requirements.

7.4 Communication

The organization shall determine the internal and external communications relevant to the privacy information management system including:

— on what it will communicate;
— when to communicate;
— with whom to communicate;
— how to communicate.

7.5 Documented information

7.5.1 General

The organization's privacy information management system shall include:

a) documented information required by this document;
b) documented information determined by the organization as being necessary for the effectiveness of the privacy information management system.

NOTE The extent of documented information for a privacy information management system can differ from one organization to another due to:

— the size of organization and its type of activities, processes, products and services;

— the complexity of processes and their interactions;

— the competence of persons.

7.5.2 Creating and updating documented information

When creating and updating documented information, the organization shall ensure appropriate:

— identification and description (e.g. a title, date, author, or reference number);

— format (e.g. language, software version, graphics) and media (e.g. paper, electronic);
— review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the privacy information management system and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed;
b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

— distribution, access, retrieval and use;
— storage and preservation, including preservation of legibility;
— control of changes (e.g. version control);
— retention and disposition.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the privacy information management system shall be identified as appropriate and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information.

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

— establishing criteria for the processes;
— implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the privacy information management system are controlled.

8.2 Privacy risk assessment

The organization shall perform privacy risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the privacy risk assessments.

8.3 Privacy risk treatment

The organization shall implement the privacy risk treatment plan.

The organization shall retain documented information of the results of the privacy risk treatment.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

— what needs to be monitored and measured;
— the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
— when the monitoring and measuring shall be performed;
— when the results from monitoring and measurement shall be analysed and evaluated.

Documented information shall be available as evidence of the results.

The organization shall evaluate the privacy performance and the effectiveness of the privacy information management system.

9.2 Internal audit

9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the privacy information management system:

a) conforms to:
   - the organization's own requirements for its privacy information management system;
   - the requirements of this document;
b) is effectively implemented and maintained.

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain (an) audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

a) define the audit objectives, criteria and scope for each audit;
b) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;
c) ensure that the results of audits are reported to relevant managers.

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

9.3 Management review

9.3.1 General

Top management shall review the organization's privacy information management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

9.3.2 Management review inputs

The management review shall include:

a) the status of actions from previous management reviews;
b) changes in external and internal issues that are relevant to the privacy information management system;
c) changes in needs and expectations of interested parties that are relevant to the privacy information management system;
d) information on the privacy information management system performance, including trends in:
   - nonconformities and corrective actions;
   - monitoring and measurement results;
   - audit results;
d) opportunities for continual improvement.

9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any need for changes to the privacy information management system.

Documented information shall be available as evidence of the results of management reviews.

10 Improvement

10.1 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the privacy information management system.

10.2 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:
   - take action to control and correct it;
   - deal with the consequences;
b) evaluate the need for action to eliminate the cause(s) of the nonconformity, in order that it does not recur or occur elsewhere, by:
   - reviewing the nonconformity;
   - determining the causes of the nonconformity;
   - determining if similar nonconformities exist, or can potentially occur;
c) implement any action needed;
d) review the effectiveness of any corrective action taken;
e) make changes to the privacy information management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Documented information shall be available as evidence of:

— the nature of the nonconformities and any subsequent actions taken;
— the results of any corrective action.

11 Further information on Annexes

Annex A lists the PIMS reference control objectives and controls for an organization acting as a PII controller (whether it employs a PII processor or not, and whether acting jointly with another PII controller or not), or as a PII processor (whether it subcontracts the processing of PII to a separate PII processor or not, and including those processing PII as subcontractor to PII processors), or as a PII processor or both.

Annex B lists the PIMS implementation guidance fir the implementation of controls listed in Annex A.

Annex C contains a mapping to ISO/IEC 29100.

Annex D contains a mapping of the controls in this document to the European Union General Data Protection Regulation.

Annex E contains a mapping to ISO/IEC 27018 and ISO/IEC 29151.

Annex F shows the correspondence between the controls in this edition of ISO/IEC 27701 and the previous 2019 edition.

Annex A
(normative)

PIMS reference control objectives and controls for PII Controllers and PII Processors

This annex is intended to be used by organizations acting as PII controllers or PII processors, or both.

Not all the control objectives and controls listed in this annex need to be included in the PIMS implementation. A justification for excluding any control objectives shall be included in the statement of applicability (see 6.1.3 f)). Justification for exclusion can include where the controls are not deemed necessary by the risk assessment, and where they are not required by (or are subject to exceptions under) the applicable legislation or regulation.

Table A.1 is for PII controllers, Table A.2 is for PII processors and Table A.3 relates to security controls for both PII controllers and PII processors

NOTE The references under 'Control reference' in tables A.1, A.2 and A.3 refer to the equivalent clause numbers in Annex B (e.g. guidance for control A.1.2.2 can be found in B.1.2.2).

Table A.1 — Control objectives and controls for PII controllers

Conditions for collection and processing Objective: To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, with clearly defined and legitimate purposes.		
Control reference	Control title	Control
A.1.2.2	Identify and document purpose	The organization shall identify and document the specific purposes for which the PII will be processed.
A.1.2.3	Identify lawful basis	The organization shall determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.
A.1.2.4	Determine when and how consent is to be obtained	The organization shall determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals.
A.1.2.5	Obtain and record consent	The organization shall obtain and record consent from PII principals according to the documented processes.
A.1.2.6	Privacy impact assessment	The organization shall assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.
A.1.2.7	Contracts with PII processors	The organization shall have a written contract with any PII processor that it uses, and shall ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex A (see Table A.2).
A.1.2.8	Joint PII controller	The organization shall determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller.

A.1.2.9	Records related to processing PII	The organization shall determine and securely maintain the necessary records in support of its obligations for the processing of PII.
Obligations to PII principals Objective: To ensure that PII principals are provided with appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII.		
A.1.3.2	Determining and fulfilling obligations to PII principals	The organization shall determine and document their legal, regulatory and business obligations to PII principals related to the processing of their PII and provide the means to meet these obligations.
A.1.3.3	Determining information for PII principals	The organization shall determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision.
A.1.3.4	Providing information to PII principals	The organization shall provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII.
A.1.3.5	Providing mechanism to modify or withdraw consent	The organization shall provide a mechanism for PII principals to modify or withdraw their consent.
A.1.3.6	Providing mechanism to object to PII processing	The organization shall provide a mechanism for PII principals to object to the processing of their PII.
A.1.3.7	Access, correction or erasure	The organization shall implement policies, procedures or mechanisms to meet their obligations to PII principals to access, correct or erase their PII.
A.1.3.8	PII controllers' obligations to inform third parties	The organization shall inform third parties with whom PII has been shared of any modification, withdrawal or objections pertaining to the shared PII, and implement appropriate policies, procedures or mechanisms to do so.
A.1.3.9	Providing copy of PII processed	The organization shall be able to provide a copy of the PII that is processed when requested by the PII principal.
A.1.3.10	Handling requests	The organization shall define and document policies and procedures for handling and responding to legitimate requests from PII principals.
A.1.3.11	Automated decision making	The organization shall identify and address obligations, including legal obligations, to the PII principals resulting from decisions made by the organization which are related to the PII principal based solely on automated processing of PII.
Privacy by design and by privacy default Objective: To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.		
A.1.4.2	Limit collection	The organization shall limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes.
A.1.4.3	Limit processing	The organization shall limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes.

A.1.4.4	Accuracy and quality	The organization shall ensure and document that PII is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the PII.
A.1.4.5	PII minimization objectives	The organization shall define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives.
A.1.4.6	PII de-identification and deletion at the end of processing	The organization shall either delete PII or render it in a form which does not permit identification or re-identification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s).
A.1.4.7	Temporary files	The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.
A.1.4.8	Retention	The organization shall not retain PII for longer than is necessary for the purposes for which the PII is processed.
A.1.4.9	Disposal	The organization shall have documented policies, procedures or mechanisms for the disposal of PII.
A.1.4.10	PII transmission controls	The organization shall subject PII transmitted (e.g. sent to another organization) over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.
PII sharing, transfer and disclosure Objective: To determine whether and document when PII is shared, transferred to other jurisdictions or third parties or disclosed in accordance with applicable obligations.		
A.1.5.2	Identify basis for PII transfer between jurisdictions	The organization shall identify and document the relevant basis for transfers of PII between jurisdictions.
A.1.5.3	Countries and international organizations to which PII can be transferred	The organization shall specify and document the countries and international organizations to which PII can possibly be transferred.
A.1.5.4	Records of transfer of PII	The organization shall record transfers of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals.
A.1.5.5	Records of PII disclosures to third parties	The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time.

Table A.2 — Control objectives and controls for PII processors

Conditions for collection and processing Objective: To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.		
Control reference	Control title	Control

A.2.2.2	Customer agreement	The organization shall ensure, where relevant, that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations (taking into account the nature of processing and the information available to the organization).
A.2.2.3	Organization's purposes	The organization shall ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.
A.2.2.4	Marketing and advertising use	The organization shall not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The organization shall not make providing such consent a condition for receiving the service.
A.2.2.5	Infringing instruction	The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation or regulation.
A.2.2.6	Customer obligations	The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.
A.2.2.7	Records related to processing PII	The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer.
Obligations to PII principals Objective: To ensure that PII principals are provided with the appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII.		
A.2.3.2	Comply with obligations to PII principals	The organization shall provide the customer with the means to comply with its obligations related to PII principals.
Privacy by design and privacy by default Objective: To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.		
A.2.4.2	Temporary files	The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.
A.2.4.3	Return, transfer or disposal of PII	The organization shall provide the ability to return, transfer or disposal of PII in a secure manner. It shall also make its policy available to the customer.
A.2.4.4	PII transmission controls	The organization shall subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.
PII sharing, transfer and disclosure Objective: To determine whether and document when PII is shared, transferred to other jurisdictions or third parties or disclosed in accordance with applicable obligations.		

A.2.5.2	Basis for PII transfer between jurisdictions	The organization shall inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract.
A.2.5.3	Countries and international organizations to which PII can be transferred	The organization shall specify and document the countries and international organizations to which PII can possibly be transferred.
A.2.5.4	Records of PII disclosures to third parties	The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.
A.2.5.5	Notification of PII disclosure requests	The organization shall notify the customer of any legally binding requests for disclosure of PII.
A.2.5.6	Legally binding PII disclosures	The organization shall reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures and accepting any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.
A.2.5.7	Disclosure of subcontractors used to process PII	The organization shall disclose any use of subcontractors to process PII to the customer before use.
A.2.5.8	Engagement of a subcontractor to process PII	The organization shall only engage a subcontractor to process PII according to the customer contract.
A.2.5.9	Change of subcontractor to process PII	The organization shall, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.

Table A.3 — Control objectives and controls for PII controllers and PII processors

Security considerations for PII controllers and processors Objective: To ensure the security of PII processing.		
Control reference	Control title	Control
A.3.3	Policies for information security	Information security policies related to PII processin**g** shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
A.3.4	Information security roles and responsibilities	Information security roles and responsibilities related to PII processing shall be defined and allocated according to the organization needs.
A.3.5	Classification of information	Information shall be classified according to the information security needs of the organization, with consideration for PII, based on confidentiality, integrity, availability and relevant interested party requirements.

A.3.6	Labelling of information	An appropriate set of procedures for information labelling that considers PII shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
A.3.7	Information transfer	Information transfer rules, procedures, or agreements related to processing PII shall be in place for all types of transfer facilities within the organization and between the organization and other parties.
A.3.8	Identity management	The full life cycle of identities related to PII processing shall be managed.
A.3.9	Access Rights	Access rights to PII and other associated assets related to PII processing shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.
A.3.10	Addressing information security within supplier agreements	Relevant information security requirements related to PII processing shall be established and agreed with each supplier based on the type of supplier relationship.
A.3.11	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents related to PII processing by defining, establishing and communicating incident management processes, roles and responsibilities.
A.3.12	Response to information security incidents	Information security incidents related to PII processing shall be responded to in accordance with the documented procedures.
A.3.13	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security related to PII processing and the organization's approach to meet these requirements shall be identified, documented and kept up to date.
A.3.14	Protection of records	Records related to PII processing shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.
A.3.15	Independent review of information security	The organization's approach to managing information security related to PII processing and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.
A.3.16	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards related to PII processing shall be regularly reviewed.
A.3.17	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function, as they relate to PII processing.
A.3.18	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of PII shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.

A.3.19	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.
A.3.20	Storage media	Storage media with PII shall be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.
A.3.21	Secure disposal or re-use of equipment	Items of equipment containing storage media with PII shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
A.3.22	User endpoint devices	PII stored on, processed by or accessible via user endpoint devices shall be protected.
A.3.23	Secure authentication	Secure authentication technologies and procedures related to PII processing shall be implemented based on information access restrictions.
A.3.24	Information backup	Backup copies of PII, and software and systems related to PII processing shall be maintained and regularly tested.
A.3.25	Logging	Logs that record activities, exceptions, faults and other relevant events related to PII processing shall be produced, stored, protected and analysed.
A.3.26	Use of cryptography	Rules for the effective use of cryptography related to PII processing, including cryptographic key management, shall be defined and implemented.
A.3.27	Secure development life cycle	Rules for the secure development of software and systems related to PII processing shall be established and applied.
A.3.28	Application security requirements	Information security requirements related to PII processing shall be identified, specified and approved when developing or acquiring applications.
A.3.29	Secure system architecture and engineering principles	Principles for engineering secure systems related to processing PII shall be established, documented, maintained and applied to any information system development activities.
A.3.30	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced PII processing system development.
A.3.31	Test information	Test information related to PII processing shall be appropriately selected, protected and managed.

Annex B
(normative)

Implementation guidance for PII Controllers and PII processors

B.1 Implementation guidance for PII controllers

B.1.1 General

The additions in this clause create the PIMS guidance for PII controllers. The implementation guidance documented in this clause relates to the controls listed in Table A.1.

B.1.2 Conditions for collection and processing

B.1.2.1 Objective

To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.

B.1.2.2 Identify and document purpose

Control

The organization should identify and document the specific purposes for which the PII will be processed.

Implementation guidance

The organization should ensure that PII principals understand the purpose for which their PII is processed. It is the responsibility of the organization to clearly document and communicate this to PII principals. Without a clear statement of the purpose for processing, consent and choice cannot be adequately given.

Documentation of the purpose(s) for processing PII should be sufficiently clear and detailed to be usable in the required information to be provided to PII principals (see B.1.3.3). This includes information necessary to obtain consent (see B.1.2.4), as well as documented information of policies and procedures (see B.1.2.9).

Other information

In the deployment of cloud computing services, the taxonomy and definitions in ISO/IEC 19944 can be helpful in providing terms for describing the purpose of the processing of PII.

B.1.2.3 Identify lawful basis

Control

The organization should determine, document and comply with the relevant lawful basis for the processing of PII for the identified purposes.

Implementation guidance

Some jurisdictions require the organization to be able to demonstrate that the lawfulness of processing was duly established before the processing.

The legal basis for the processing of PII can include:

— consent from PII principals;

— performance of a contract;

— compliance with a legal obligation;

— protection of the vital interests of PII principals;

— performance of a task carried out in the public interest;

— legitimate interests of the PII controller.

The organization should document this basis for each PII processing activity (see B.1.2.9).

The legitimate interests of the organization can include, for instance, information security objectives, which should be balanced against the obligations to PII principals with regards to the protection of privacy.

Whenever special categories of PII are defined, either by the nature of the PII (e.g. health information) or by the PII principals concerned (e.g. PII relating to children) the organization should include those categories of PII in its classification schemes.

The classification of PII that falls into these categories can vary from one jurisdiction to another and can vary between different regulatory regimes that apply to different kinds of business, so the organization needs to be aware of the classification(s) that apply to the PII processing being performed.

The use of special categories of PII can also be subject to more stringent controls.

Changing or extending the purposes for the processing of PII can require updating or revision of the legal basis. It can also require additional consent to be obtained from the PII principal.

B.1.2.4 Determine when and how consent is to be obtained

Control

The organization should determine and document a process by which it can demonstrate if, when and how consent for the processing of PII was obtained from PII principals.

Implementation guidance

Consent can be required for processing of PII unless other lawful grounds apply. The organization should clearly document when consent needs to be obtained and the requirements for obtaining consent. It can be useful to correlate the purpose(s) for processing with information about if and how consent is obtained.

Some jurisdictions have specific requirements for how consent is collected and recorded (e.g. not bundled with other agreements). Additionally, certain types of data collection (for scientific research for example) and certain types of PII principals, such as children, can be subject to additional requirements. The organization should take into account such requirements and document how mechanisms for consent meet those requirements.

B.1.2.5 Obtain and record consent

Control

The organization should obtain and record consent from PII principals according to the documented processes.

Implementation guidance

The organization should obtain and record consent from PII principals in such a way that it can provide on request details of the consent provided (for example the time that consent was provided, the identification of the PII principal, and the consent statement).

The information delivered to the PII principal before the consent process should follow the guidance in B.1.3.4.

The consent should be:

— freely given;

— specific regarding the purpose for processing; and

— unambiguous and explicit.

B.1.2.6 Privacy impact assessment

Control

The organization should assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of PII or changes to existing processing of PII is planned.

Implementation guidance

PII processing generates risks for PII principals. These risks should be assessed through a privacy impact assessment. Some jurisdictions define cases for which a privacy impact assessment is mandated. Criteria can include automated decision making which produces legal effects on PII principals, large scale processing of special categories of PII (e.g. health-related information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data or biometric data), or systematic monitoring of a publicly accessible area on a large scale.

The organization should determine the elements that are necessary for the completion of a privacy impact assessment. These can include a list of the types of PII processed, where the PII is stored and where it can be transferred. Data flow diagrams and data maps can also be helpful in this context (see B.1.2.9 for details of documented information of the processing of PII that can inform a privacy impact or other risk assessment).

Other information

Guidance on privacy impact assessments related to the processing of PII can be found in ISO/IEC 29134.

B.1.2.7 Contracts with PII processors

Control

The organization should have a written contract with any PII processor that it uses, and should ensure that their contracts with PII processors address the implementation of the appropriate controls in Annex A (see Table A.2).

Implementation guidance

The contract between the organization and any PII processor processing PII on its behalf should require the PII processor to implement the appropriate controls specified in Annex A (see Table A.2), taking account of the information security risk assessment process (see 6.1.2) and the scope of the processing of PII performed by the PII processor. By default, all controls specified in Annex A (see Table A.2) should be assumed as relevant. If the organization decides to not require the PII processor to implement a control from Annex A (see Table A.2), it should justify its exclusion (see 6.1.3).

A contract can define the responsibilities of each party differently but, to be consistent with this document, all controls should be considered and included in the documented information.

B.1.2.8 Joint PII controller

Control

The organization should determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller.

Implementation guidance

Roles and responsibilities for the processing of PII should be determined in a transparent manner.

These roles and responsibilities should be documented in a contract or any similar binding document that contains the terms and conditions for the joint processing of PII. In some jurisdictions, such an agreement is called a data sharing agreement.

A joint PII controller agreement can include (this list is neither definitive nor exhaustive):

— purpose of PII sharing / joint PII controller relationship;

— identity of the organizations (PII controllers) that are part of the joint PII controller relationship;

— categories of PII to be shared or transferred and processed under the agreement;

— overview of the processing operations (e.g. transfer, use);

— description of the respective roles and responsibilities;

— responsibility for implementing technical and organizational security measures for PII protection;

— definition of responsibility in case of a PII breach (e.g. who will notify, when, mutual information);

— terms of retention or disposal of PII;

— liabilities for failure to comply with the agreement;

— how obligations to PII principals are met;

— how to provide PII principals with information covering the essence of the arrangement between the joint PII controllers;

— how PII principals can obtain other information they are entitled to receive; and

— a contact point for PII principals.

B.1.2.9 Records related to processing PII

Control

The organization should determine and securely maintain the necessary records in support of its obligations for the processing of PII.

Implementation guidance

A way to maintain documented information of the processing of PII is to have an inventory or list of the PII processing activities that the organization performs. Such an inventory can include:

— the type of processing;

— the purposes for the processing;

— a description of the categories of PII and PII principals (e.g. children);

— the categories of recipients to whom PII has been or will be disclosed, including recipients in third countries or international organizations;

— a general description of the technical and organizational security measures; and

— a privacy impact assessment report.

Such an inventory should have an owner who is responsible for its accuracy and completeness.

B.1.3 Obligations to PII principals

B.1.3.1 Objective

To ensure that PII principals are provided with appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII.

B.1.3.2 Determining and fulfilling obligations to PII principals

Control

The organization should determine and document their legal, regulatory and business obligations to PII principals related to the processing of their PII and provide the means to meet these obligations.

Implementation guidance

Obligations to PII principals and the means to support them vary from one jurisdiction to another.

The organization should ensure that they provide the appropriate means to meet the obligations to PII principals in an accessible and timely manner. Clear documentation should be provided to the PII principal describing the extent to which the obligations to them are fulfilled and how, along with an up-to-date contact point where they can address their requests.

The contact point should be provided in a similar way to that used to collect PII and consent (e.g. if PII are collected by email or a website, the contact point should be by email or the website, not an alternative such as phone or fax).

B.1.3.3 Determining information for PII principals

Control

The organization should determine and document the information to be provided to PII principals regarding the processing of their PII and the timing of such a provision.

Implementation guidance

The organization should determine the legal, regulatory or business requirements for when information is to be provided to the PII principal (e.g. prior to processing, within a certain time from when it is requested) and for the type of information to be provided.

Depending on the requirements, the information can take the form of a notice. Examples of types of information that can be provided to PII principals are:

— information about the purpose of the processing (see B.1.2.2);

— contact details for the PII controller or its representative;

— information about the lawful basis for the processing (see B.1.2.3);

— information on where the PII was obtained, if not obtained directly from the PII principal;

— information about whether the provision of PII is a statutory or contractual requirement, and where appropriate, the possible consequences of failure to provide PII;

— information on obligations to PII principals, as determined in B.1.3.2, and how PII principals can benefit from them, especially regarding accessing, amending, correcting, requesting erasure, receiving a copy of their PII and objecting to the processing;

— information on how the PII principal can withdraw consent (see B.1.3.5);

— information about transfers of PII;

— information about recipients or categories of recipients of PII;

— information about the period for which the PII will be retained;

— information about the use of automated decision making based on the automated processing of PII;

— information about the right to lodge a complaint and how to lodge such a complaint;

— information regarding the frequency with which information is provided (e.g. “just in time” notification, organization defined frequency).

The organization should provide updated information if the purposes for the processing of PII are changed or extended.

B.1.3.4 Providing information to PII principals

Control

The organization should provide PII principals with clear and easily accessible information identifying the PII controller and describing the processing of their PII.

Implementation guidance

The organization should provide the information detailed in B.1.3.3 to PII principals in a timely, concise, complete, transparent, intelligible and easily accessible form, using clear and plain language, as appropriate to the target audience.

Where appropriate, the information should be given at the time of PII collection. It should also be permanently accessible.

NOTE Icons and images can be helpful to the PII principal by giving a visual overview of the intended processing.

B.1.3.5 Providing mechanism to modify or withdraw consent

Control

The organization should provide a mechanism for PII principals to modify or withdraw their consent.

Implementation guidance

The organization should inform PII principals of their rights related to withdrawing consent (which may vary by jurisdiction) at any time, and provide the mechanism to do so. The mechanism used for withdrawal depends on the system; it should be consistent with the mechanisms used for obtaining consent when possible. For example, if the consent is collected by email or a website, the mechanism for withdrawing it should be the same, not an alternative solution such as phone or fax.

Modifying consent can include placing restrictions on the processing of PII, which can include restricting the PII controller from deleting the PII in some cases.

Some jurisdictions impose restrictions on when and how a PII principal can modify or withdraw their consent.

The organization should record any request to withdraw or change consent in a similar way to the recording of the consent itself.

Any change of consent should be disseminated, through appropriate systems, to authorized users and to relevant third parties.

The organization should define a response time and requests should be handled according to it.

Additional information

When consent for particular processing of PII is withdrawn, all the processing of PII performed before withdrawal should normally be considered as appropriate, but the results of such processing should not be used for new processing. For example, if a PII principal withdraws their consent for profiling, their profile should not be further used or consulted.

B.1.3.6 Providing mechanism to object to PII processing

Control

The organization should provide a mechanism for PII principals to object to the processing of their PII.

Implementation guidance

Some jurisdictions provide PII principals with a right to object to the processing of their PII. Organizations subject to the legislation or regulation of such jurisdictions should ensure that they retain records of PII principals exercising this right.

The organization should document the legal and regulatory requirements related to objections by the PII principals to processing (e.g. objection relating to the processing of PII for direct marketing purposes). The organization should provide information to principals regarding the ability to object in these situations. Mechanisms to object can vary, but should be consistent with the type of service provided (e.g. online services should provide this capability online).

B.1.3.7 Access, correction or erasure

Control

The organization should implement policies, procedures or mechanisms to meet their obligations to PII principals to access, correct or erase their PII.

Implementation guidance

The organization should implement policies, procedures or mechanisms for enabling PII principals to obtain access to, correct and erase of their PII, if requested and without undue delay.

The organization should define a response time and requests should be handled according to it.

Any corrections or erasures should be disseminated through the system or to authorized users, and should be passed to third parties (see B.1.3.8) to whom the PII has been transferred.

NOTE Documented information generated by the control specified in B.1.5.4 can help in this regard.

The organization should implement policies, procedures or mechanisms for use when there can be a dispute about the accuracy or correction of the data by the PII principal. These policies, procedures or mechanisms should include informing the PII principal of what changes were made, and of reasons why corrections cannot be made (where this is the case).

Some jurisdictions impose restrictions on when and how a PII principal can request correction or erasure of their PII. The organization should determine these restrictions as applicable and keep itself up-to-date about them.

B.1.3.8 PII controllers' obligations to inform third parties

Control

The organization should inform third parties with whom PII has been shared of any modification, withdrawal or objections pertaining to the shared PII, and implement appropriate policies, procedures or mechanisms to do so.

Implementation guidance

The organization should take appropriate steps, bearing in mind the available technology, to inform third parties of any modification or withdrawal of consent, or objections pertaining to the shared PII.

NOTE 1 Legal requirement can apply.

The organization should determine and maintain active communication channels with third parties. Related responsibilities can be assigned to individuals in charge of their operations and maintenance. When informing third parties, the organization should monitor their acknowledgement of receipt of the information.

NOTE 2 Changes resulting from the obligations to PII principals can include modification or withdrawal of consent, requests for correction, erasure, or restrictions on processing, or objections to the processing of PII as requested by the PII principal.

B.1.3.9 Providing copy of PII processed

Control

The organization should be able to provide a copy of the PII that is processed when requested by the PII principal.

Implementation guidance

The organization should provide a copy of the PII that is processed in a structured, commonly used, format accessible by the PII principal.

Some jurisdictions define cases where the organization should provide a copy of the PII processed in a format allowing portability to the PII principals or to recipient PII controllers (typically structured, commonly used and machine readable).

The organization should ensure that any copies of PII provided to a PII principal relate specifically to that PII principal.

Where the requested PII has already been deleted subject to the retention and disposal policy (as described in B.1.4.8), the PII controller should inform the PII principal that the requested PII has been deleted.

In cases where the organization is no longer able to identify the PII principal (e.g. as a result of a de-identification process), the organization should not seek to (re-)identify the PII principals for the sole reason of implementing this control. However, in some jurisdictions, legitimate requests can require that additional information should be requested from the PII principal to enable re-identification and subsequent disclosure.

Where technically feasible, it should be possible to transfer a copy of the PII from one organization directly to another organization, at the request of the PII principal.

B.1.3.10 Handling requests

Control

The organization should define and document policies and procedures for handling and responding to legitimate requests from PII principals.

Implementation guidance

Legitimate requests can include requests for a copy of PII processed, or requests to lodge a complaint.

Some jurisdictions allow the organization to charge a fee in certain cases (e.g. excessive or repetitive requests).

Requests should be handled within the appropriate defined response times.

Some jurisdictions define response times, depending on the complexity and number of the requests, as well as requirements to inform PII principals of any delay. The appropriate response times should be defined in the privacy policy.

B.1.3.11 Automated decision making

Control

The organization should identify and address obligations, including legal obligations, to the PII principals resulting from decisions made by the organization which are related to the PII principal based solely on automated processing of PII.

Implementation guidance

Some jurisdictions define specific obligations to PII principals when a decision based solely on automated processing of PII significantly affects them, such as notifying the existence of automated decision making, allowing for the PII principals to object to such decision making, or obtaining human intervention.

NOTE In some jurisdictions, some processing of PII cannot be fully automated.

Organizations operating in these jurisdictions should take compliance with these obligations into account.

B.1.4 Privacy by design and privacy by default

B.1.4.1 Objective

To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.

B.1.4.2 Limit collection

Control

The organization should limit the collection of PII to the minimum that is relevant, proportional and necessary for the identified purposes.

Implementation guidance

The organization should limit the collection of PII to what is adequate, relevant and necessary in relation to the identified purposes. This includes limiting the amount of PII that the organization collects indirectly (e.g. through web logs, system logs).

Privacy by default implies that, where any optionality in the collection and processing of PII exists, each option should be disabled by default and only enabled by explicit choice of the PII principal.

B.1.4.3 Limit processing

Control

The organization should limit the processing of PII to that which is adequate, relevant and necessary for the identified purposes.

Implementation guidance

Limiting the processing of PII should be managed through information security and privacy policies (see 5.2) along with documented procedures for their adoption and compliance.

Processing of PII, including:

— the disclosure;

— the period of PII storage; and

— who is able to access their PII;

should be limited by default to the minimum necessary relative to the identified purposes.

B.1.4.4 Accuracy and quality

Control

The organization should ensure and document that PII is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the PII.

Implementation guidance

The organization should implement policies, procedures or mechanisms to minimize inaccuracies in the PII it processes. There should also be policies, procedures or mechanisms to respond to instances of inaccurate PII. These policies, procedures or mechanisms should be included in the documented information (e.g. through technical system configurations) and should apply throughout the PII lifecycle.

Additional information

For further information on the PII processing life-cycle, see ISO/IEC 29101:2018, 6.2.

B.1.4.5 PII minimization objectives

Control

The organization should define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives.

Implementation guidance

Organizations should identify how the specific PII and amount of PII collected and processed is limited relative to the identified purposes. This can include the use of de-identification or other data minimization techniques.

The identified purpose (see B.1.2.2) can require the processing of PII that has not been de-identified, in which case the organization should be able to describe such processing.

In other cases, the identified purpose does not require the processing of the original PII, and the processing of PII which has been de-identified can suffice to achieve the identified purpose. In these cases, the organization should define and document the extent to which the PII needs to be associated with the PII principal, as well as the mechanisms and techniques designed to process PII, such that the de-identification and PII minimization objectives are achieved.

Mechanisms used to minimize PII vary depending on the type of processing and the systems used for the processing. The organization should document any mechanisms (technical system configurations, etc.) used to implement data minimization.

In cases where processing of de-identified data is sufficient for the purposes, the organization should document any mechanisms (technical system configurations, etc.) designed to implement de-identification objectives set by the organization in a timely manner. For instance, the removal of attributes associated with PII principals can be sufficient to allow the organization to achieve its identified purpose. In other cases, other de-identification techniques, such as generalization (e.g. rounding) or randomization techniques (e.g. noise addition) can be used to achieve an adequate level of de-identification.

NOTE 1 For further information on de-identification techniques, refer to ISO/IEC 20889.

NOTE 2 For cloud computing, ISO/IEC 19944 provides a definition of data identification qualifiers that can be used to classify the degree to which the data can identify a PII principal or associate a PII principal with a set of characteristics in the PII.

B.1.4.6 PII de-identification and deletion at the end of processing

Control

The organization should either delete PII or render it in a form which does not permit identification or re-identification of PII principals, as soon as the original PII is no longer necessary for the identified purpose(s).

Implementation guidance

The organization should have mechanisms to erase the PII when no further processing is anticipated. Alternatively, some de-identification techniques can be used as long as the resulting de-identified data cannot reasonably permit re-identification of PII principals.

B.1.4.7 Temporary files

Control

The organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.

Implementation guidance

The organization should perform periodic checks that unused temporary files are deleted within the identified time period.

Other information

Information systems can create temporary files in the normal course of their operation. Such files are specific to the system or application, but can include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed but there are circumstances in which they cannot be deleted. The length of time for which these files remain in use is not always deterministic but a “garbage collection” procedure should identify the relevant files and determine how long it has been since they were last used.

B.1.4.8 Retention

Control

The organization should not retain PII for longer than is necessary for the purposes for which the PII is processed.

Implementation guidance

The organization should develop and maintain retention schedules for information it retains, taking into account the requirement to retain PII for no longer than is necessary. Such schedules should take into account legal, regulatory and business requirements. Where such requirements conflict, a business decision needs to be taken (based on a risk assessment) and documented in the appropriate schedule.

B.1.4.9 Disposal

Control

The organization should have documented policies, procedures or mechanisms for the disposal of PII.

Implementation guidance

The choice of PII disposal techniques depends on a number of factors, as disposal techniques differ in their properties and outcomes (for example in the granularity of the resultant physical media, or the ability to recover deleted information on electronic media). Factors to consider when choosing an appropriate disposal technique include, but are not limited to, the nature and extent of the PII to be disposed of, whether or not there is metadata associated with the PII, and the physical characteristics of the media on which the PII is stored.

B.1.4.10 PII transmission controls

Control

The organization should subject PII transmitted (e.g. sent to another organization) over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.

Implementation guidance

Transmission of PII needs to be controlled, typically by ensuring that only authorized individuals have access to transmission systems, and by following the appropriate processes (including the retention of audit logs) to ensure that PII is transmitted without compromise to the correct recipients.

B.1.5 PII sharing, transfer and disclosure

B.1.5.1 Objective

To determine whether and document when PII is shared, transferred to other jurisdictions or third parties or disclosed in accordance with applicable obligations.

B.1.5.2 Identify basis for PII transfer between jurisdictions

Control

The organization should identify and document the relevant basis for transfers of PII between jurisdictions.

Implementation guidance

PII transfer can be subject to legislation or regulation depending on the jurisdiction or international organization to which data is to be transferred (and from where it originates). The organization should document compliance to such requirements as the basis for transfer.

Some jurisdictions can require that information transfer agreements be reviewed by a designated supervisory authority. Organizations operating in such jurisdictions should be aware of any such requirements.

NOTE Where transfers take place within a specific jurisdiction, the applicable legislation or regulation are the same for the sender and recipient.

B.1.5.3 Countries and international organizations to which PII can be transferred

Control

The organization should specify and document the countries and international organizations to which PII can possibly be transferred.

Implementation guidance

The identities of the countries and international organizations to which PII can possibly be transferred in normal operations should be made available to customers. The identities of the countries arising from the use of subcontracted PII processing should be included. The countries included should be considered in relation to B.1.5.2.

Outside of normal operations, there can be cases of transfer made at the request of a law enforcement authority, for which the identity of the countries cannot be specified in advance, or is prohibited by applicable jurisdictions to preserve the confidentiality of a law enforcement investigation (see B.1.5.2, B.2.5.5 and B.2.5.6).

B.1.5.4 Records of transfer of PII

Control

The organization should record transfers of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals.

Implementation guidance

Recording can include transfers from third parties of PII which has been modified as a result of PII controllers' managing their obligations, or transfers to third parties to implement legitimate requests from PII principals, including requests to erase PII (e.g. after consent withdrawal).

The organization should have a policy defining the retention period of these records.

The organization should apply the data minimization principle to the records of transfers by retaining only the strictly needed information.

B.1.5.5 Records of PII disclosure to third parties

Control

The organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time.

Implementation guidance

PII can be disclosed during the course of normal operations. These disclosures should be recorded. Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure and the source of the authority to make the disclosure.

B.2 Implementation guidance for PII processors

B.2.1 General

The additions in this clause create the PIMS guidance for PII processors. The implementation guidance documented in this clause relate to the controls listed in Table A.2.

B.2.2 Conditions for collection and processing

B.2.2.1 Objective

To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.

B.2.2.2 Customer agreement

Control

The organization should ensure, where relevant, that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations (taking into account the nature of processing and the information available to the organization).

Implementation guidance

The contract between the organization and the customer should include the following wherever relevant, and depending on the customer's role (PII controller or PII processor) (this list is neither definitive nor exhaustive):

— privacy by design and privacy by default (see B.1.4 and B.2.4);

— achieving security of processing;

— notification of breaches involving PII to a supervisory authority;

— notification of breaches involving PII to customers and PII principals;

— conducting privacy impact assessments (PIA); and

— the assurance of assistance by the PII processor if prior consultations with relevant PII protection authorities are needed.

Some jurisdictions require that the contract include the subject matter and duration of the processing, the nature and purpose of the processing, the type of PII and categories of PII principals.

B.2.2.3 Organization's purposes

Control

The organization should ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.

Implementation guidance

The contract between the organization and the customer should include, but not be limited to, the objective and time frame to be achieved by the service.

In order to achieve the customer's purpose, there can be technical reasons why it is appropriate for the organization to determine the method for processing PII, consistent with the general instructions of the customer but without the customer's express instruction. For example, in order to efficiently utilize network or processing capacity it can be necessary to allocate specific processing resources depending on certain characteristics of the PII principal.

The organization should allow the customer to verify their compliance with the purpose specification and limitation principles. This also ensures that no PII is processed by the organization or any of its subcontractors for other purposes than those expressed in the documented instructions of the customer.

B.2.2.4 Marketing and advertising use

Control

The organization should not use PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principal. The organization should not make providing such consent a condition for receiving the service.

Implementation guidance

Compliance of PII processors with the customer's contractual requirements should be documented, especially where marketing or advertising is planned.

Organizations should not insist on the inclusion of marketing or advertising uses where express consent has not been fairly obtained from PII principals.

NOTE This control is in addition to the more general control in B.2.2.3 and does not replace or otherwise supersede it.

B.2.2.5 Infringing instruction

Control

The organization should inform the customer if, in its opinion, a processing instruction infringes applicable legislation or regulation.

Implementation guidance

The organization’s ability to verify if the instruction infringes legislation or regulation can depend on the technological context, on the instruction itself, and on the contract between the organization and the customer.

B.2.2.6 Customer obligations

Control

The organization should provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.

Implementation guidance

The information needed by the customer can include whether the organization allows for and contributes to audits conducted by the customer or another auditor mandated or otherwise agreed by the customer.

B.2.2.7 Records related to processing PII

Control

The organization should determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer.

Implementation guidance

Some jurisdictions can require the organization to record information such as:

— categories of processing carried out on behalf of each customer;

— transfers to third countries or international organizations; and

— a general description of the technical and organizational security measures.

B.2.3 Obligations to PII principals

B.2.3.1 Objective

To ensure that PII principals are provided with the appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII.

B.2.3.2 Comply with obligations to PII principals

Control

The organization should provide the customer with the means to comply with its obligations related to PII principals.

Implementation guidance

A PII controller's obligations can be defined by legislation, by regulation or by contract. These obligations can include matters where the customer uses the services of the organization for implementation of these obligations. For example, this can include the correction or deletion of PII in a timely fashion.

Where a customer depends on the organization for information or technical measures to facilitate meeting the obligations to PII principals, the relevant information or technical measures should be specified in a contract.

B.2.4 Privacy by design and privacy by default

B.2.4.1 Objective

To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.

B.2.4.2 Temporary files

Control

The organization should ensure that temporary files created as a result of the processing of PII are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.

Implementation guidance

The organization should conduct periodic verification that unused temporary files are deleted within the identified time period.

Other information

Information systems can create temporary files in the normal course of their operation. Such files are specific to the system or application, but can include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed but there are circumstances in which they cannot be deleted. The length of time for which these files remain in use is not always deterministic but a “garbage collection” procedure should identify the relevant files and determine how long it has been since they were last used.

B.2.4.3 Return, transfer or disposal of PII

Control

The organization should provide the ability to return, transfer or disposal of PII in a secure manner. It should also make its policy available to the customer.

Implementation guidance

At some point in time, PII can need to be disposed of in some manner. This can involve returning the PII to the customer, transferring it to another organization or to a PII controller (e.g. as a result of a merger), deleting or otherwise destroying it, de-identifying it or archiving it. The capability for the return, transfer or disposal of PII should be managed in a secure manner.

The organization should provide the assurance necessary to allow the customer to ensure that PII processed under a contract is erased (by the organization and any of its subcontractors) from wherever they are stored, including for the purposes of backup and business continuity, as soon as they are no longer necessary for the identified purposes of the customer.

The organization should develop and implement a policy in respect to the disposal of PII and should make this policy available to customer when requested.

The policy should cover the retention period for PII before its disposal after termination of a contract, to protect the customer from losing PII through an accidental lapse of the contract.

NOTE This control and guidance is also relevant under the retention principle (see B.1.4.8).

B.2.4.4 PII transmission controls

Control

The organization should subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.

Implementation guidance

Transmission of PII needs to be controlled, typically by ensuring that only authorized individuals have access to transmission systems, and by following the appropriate processes (including the retention of audit data) to ensure that PII is transmitted without compromise to the correct recipients. Requirements for transmission controls can be included in the contract between the PII processor and the customer.

Where no contractual requirements related to transmission are in place, it can be appropriate to take advice from the customer prior to transmission.

B.2.5 PII sharing, transfer and disclosure

B.2.5.1 Objective

To determine whether and document when PII is shared, transferred to other jurisdictions or third parties or disclosed in accordance with applicable obligations.

B.2.5.2 Basis for PII transfer between jurisdictions

Control

The organization should inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract.

Implementation guidance

PII transfer between jurisdictions can be subject to legislation or regulation depending on the jurisdiction or organization to which PII is to be transferred (and from where it originates). The organization should document compliance with such requirements as the basis for transfer.

The organization should inform the customer of any transfer of PII, including transfers to:

— suppliers;

— other parties;

— other countries or international organizations.

In case of changes, the organization should inform the customer in advance, according to an agreed timeframe, so that the customer has the ability to object to such changes or to terminate the contract.

The agreement between the organization and the customer can have clauses where the organization can implement changes without informing the customer. In these cases, the limits of this allowance should be set (e.g. the organization can change suppliers without informing the customer, but cannot transfer PII to other countries).

In case of international transfer of PII, agreements such as Model Contract Clauses, Binding Corporate Rules or Cross Border Privacy Rules, the countries involved and the circumstances in which such agreements apply, should be identified.

B.2.5.3 Countries and international organizations to which PII can be transferred

Control

The organization should specify and document the countries and international organizations to which PII can possibly be transferred.

Implementation guidance

The identities of the countries and international organizations to which PII can possibly be transferred in normal operations should be made available to customers. The identities of the countries arising from the use of subcontracted PII processing should be included. The countries included should be considered in relation to B.2.5.2.

Outside of normal operations, there can be cases of transfer made at the request of a law enforcement authority, for which the identity of the countries cannot be specified in advance, or is prohibited by applicable jurisdictions to preserve the confidentiality of a law enforcement investigation (see B.1.5.2, B.2.5.5 and B.2.5.6).

B.2.5.4 Records of PII disclosures to third parties

Control

The organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.

Implementation guidance

PII can be disclosed during the course of normal operations. These disclosures should be recorded. Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure and the source of the authority to make the disclosure.

B.2.5.5 Notification of PII disclosure requests

Control

The organization should notify the customer of any legally binding requests for disclosure of PII.

Implementation guidance

The organization can receive legally binding requests for disclosure of PII (e.g. from law enforcement authorities). In these cases, the organization should notify the customer of any such request within agreed timeframes and according to an agreed procedure (which can be included in the customer contract).

In some cases, the legally binding requests include the requirement for the organization not to notify anyone about the event (an example of a possible prohibition on disclosure would be a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

B.2.5.6 Legally binding PII disclosures

Control

The organization should reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures and accepting any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.

Implementation guidance

Details relevant to the implementation of the control can be included in the customer contract.

Such requests can originate from several sources, including courts, tribunals and administrative authorities. They can arise from any jurisdiction.

B.2.5.7 Disclosure of subcontractors used to process PII

Control

The organization should disclose any use of subcontractors to process PII to the customer before use.

Implementation guidance

Provisions for the use of subcontractors to process PII should be included in the customer contract.

Information disclosed should cover the fact that subcontracting is used and the names of relevant subcontractors. The information disclosed should also include the countries and international organizations to which subcontractors can transfer data (see B.2.5.3) and the means by which subcontractors are obliged to meet or exceed the obligations of the organization (see B.2.5.8).

Where public disclosure of subcontractor information is assessed to increase security risk beyond acceptable limits, disclosure should be made under a non-disclosure agreement or on the request of the customer. The customer should be made aware that the information is available.

This does not concern the list of countries where the PII can be transferred. This list should be disclosed to the customer in all cases in a way that allows them to inform the appropriate PII principals.

B.2.5.8 Engagement of a subcontractor to process PII

Control

The organization should only engage a subcontractor to process PII according to the customer contract.

Implementation guidance

Where the organization subcontracts some or all of the processing of that PII to another organization, a written authorization from the customer is required prior to the PII processed by the subcontractor. This can be in the form of appropriate clauses in the customer contract, or can be a specific "one-off" agreement.

The organization should have a written contract with any subcontractors that it uses for PII processing on its behalf, and should ensure that their contracts with subcontractors address the implementation of the appropriate controls in Annex A (see Table A.2).

The contract between the organization and any subcontractor processing PII on its behalf should require the subcontractor to implement the appropriate controls specified in Annex A (see Table A.2), taking account of the information security risk assessment process (see 6.1.2) and the scope of the

processing of PII performed by the PII processor. By default, all controls specified in Annex A (see Table A.2) should be assumed as relevant. If the organization decides to not require the subcontractor to implement a control from Annex A (see Table A.2), it should justify its exclusion.

A contract can define the responsibilities of each party differently but, to be consistent with this document, all controls should be considered and included in the documented information.

B.2.5.9 Change of subcontractor to process PII

Control

The organization should, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.

Implementation guidance

Where the organization changes the organization with which it subcontracts some or all of the processing of that PII, then written authorization from the customer is required for the change, prior to the PII processed by the new subcontractor. This can be in the form of appropriate clauses in the customer contract, or can be a specific "one-off" agreement.

B.3 Implementation guidance for PII controllers and PII processors

B.3.1 Objective

To ensure the security of PII processing.

B.3.2 General

The additions in this clause create the PIMS guidance for PII controllers and PII processors. The implementation guidance documented in this clause relate to the controls listed in Table A.3. Unless otherwise stated by specific provisions in Table A.3, or determined by the organization according to applicable jurisdictions, the same guidance applies for PII controllers and PII processors.

B.3.3 Policies for information security

Control

Information security policies related to PII processing should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Implementation guidance

Either by the development of separate privacy policies, or by the augmentation of information security policies, the organization should produce a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation or regulation and with the contractual terms agreed between the organization and its partners, its subcontractors and its applicable third parties (customers, suppliers etc.), which should clearly allocate responsibilities between them.

Any organization that processes PII, whether a PII controller or a PII processor, should consider applicable PII protection legislation or regulation during the development and maintenance of information security policies.

B.3.4 Information security roles and responsibilities

Control

Information security roles and responsibilities related to PII processing should be defined and allocated according to the organization needs.

Implementation guidance

The organization should designate a point of contact for use by the customer regarding the processing of PII. When the organization is a PII controller, designate a point of contact for PII principals regarding the processing of their PII (see B.1.3.4).

The organization should appoint one or more persons responsible for developing, implementing, maintaining and monitoring an organization-wide governance and privacy programme, to ensure compliance with all applicable laws and regulations regarding the processing of PII.

The responsible person should, where appropriate:

— be independent and report directly to the appropriate management level of the organization in order to ensure effective management of privacy risks;

— be involved in the management of all issues which relate to the processing of PII;

— be expert in data protection legislation, regulation and practice;

— act as a contact point for supervisory authorities;

— inform top-level management and employees of the organization of their obligations with respect to the processing of PII;

— provide advice in respect of privacy impact assessments conducted by the organization.

NOTE Such a person is called a data protection officer in some jurisdictions, which define when such a position is required, along with their position and role. This position can be fulfilled by a staff member or outsourced.

B.3.5 Classification of information

Control

Information should be classified according to the information security needs of the organization, with consideration for PII, based on confidentiality, integrity, availability and relevant interested party requirements.

Implementation guidance

The organization's information classification scheme should explicitly consider PII as part of the scheme it implements. Considering PII within the overall classification scheme is integral to understanding what PII the organization processes (e.g. type, special categories), where such PII is stored and the systems through which it can flow.

B.3.6 Labelling of information

Control

An appropriate set of procedures for information labelling that considers PII should be developed and implemented in accordance with the information classification scheme adopted by the organization.

Implementation guidance

The organization should ensure that people under its control are made aware of the definition of PII and how to recognize information that is PII.

B.3.7 Information transfer

Control

Information transfer rules, procedures, or agreements related to processing PII should be in place for all types of transfer facilities within the organization and between the organization and other parties.

Implementation guidance

The organization should consider procedures for ensuring that rules related to the processing of PII are enforced throughout and outside of the system, where applicable.

B.3.8 Identity management

Control

The full life cycle of identities related to PII processing should be managed.

Implementation guidance

Procedures for registration and de-registration of users who administer or operate systems and services that process PII should address the situation where user access control for those users is compromised, such as the corruption or compromise of passwords or other user registration data (e.g. as a result of inadvertent disclosure).

The organization should not reissue to users any de-activated or expired user IDs for systems and services that process PII.

In the case where the organization is providing PII processing as a service, the customer can be responsible for some or all aspects of user ID management. Such cases should be included in the documented information.

Some jurisdictions impose specific requirements regarding the frequency of checks for unused authentication credentials related to systems that process PII. Organizations operating in these jurisdictions should take compliance with these requirements into account.

B.3.9 Access rights

Control

Access rights to PII and other associated assets related to PII processing should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.

Implementation guidance

The organization should maintain an accurate, up-to-date record of the user profiles created for users who have authorized access to the information system and the PII contained therein. Each profile comprises the set of data about the user, including user ID, necessary to implement the identified technical controls providing authorized access.

Implementing individual user access IDs enables appropriately configured systems to identify who accessed PII and what additions, deletions or changes they made. As well as protecting the organization, users are also protected as they can identify what they have processed and what they have not processed.

In the case where the organization is providing PII processing as a service, the customer can be responsible for some or all aspects of access management. Where appropriate, the organization should provide the customer the means to perform access management, such as by providing administrative rights to manage or terminate access. Such cases should be included in the documented information.

B.3.10 Addressing information security within supplier agreements

Control

Relevant information security requirements related to PII processing should be established and agreed with each supplier based on the type of supplier relationship.

Implementation guidance

The organization should specify in agreements with suppliers whether PII is processed and the minimum technical and organizational measures that the supplier needs to meet in order for the organization to meet its information security and PII protection obligations (see B.1.2.7 and B.2.2.2).

Supplier agreements should clearly allocate responsibilities between the organization, its partners, its suppliers and its relevant third parties (customers, suppliers, etc.) taking into account the type of PII processed.

The agreements between the organization and its suppliers should provide a mechanism for ensuring the organization supports and manages compliance with all applicable legislation or regulation. The agreements should call for independently audited compliance, acceptable to the customer.

NOTE For such audit purposes, compliance with relevant and applicable security standards such as ISO/IEC 27001 can be considered.

Where the role of the organization is a PII processor, the organization should specify in contracts with any suppliers that PII is only processed on its instructions.

B.3.11 Information security incident management planning and preparation

Control

The organization should plan and prepare for managing information security incidents related to PII processing by defining, establishing and communicating incident management processes, roles and responsibilities.

Implementation guidance

As part of the overall information security incident management process, the organization should establish responsibilities and procedures for identifying and recording breaches of PII. Additionally, the organization should establish responsibilities and procedures related to notification to relevant parties of PII breaches (including the timing of such notifications) and the disclosure to authorities, taking into account the applicable legislation or regulation.

Some jurisdictions impose specific regulations regarding breach responses, including notification. Organizations operating in these jurisdictions should ensure that they can demonstrate compliance with these regulations.

B.3.12 Response to information security incidents

Control

Information security incidents related to PII processing should be responded to in accordance with the documented procedures.

Implementation guidance for PII controllers

An incident that involves PII should trigger a review by the organization, as part of its information security incident management process, to determine if a breach involving PII that requires a response has taken place.

An event does not necessarily trigger such a review.

NOTE 1 An information security event does not necessarily result in actual, or the significant probability of, unauthorized access to PII or to any of the organization's equipment or facilities storing PII. These can include, but are not limited to, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks and packet sniffing.

When a breach of PII has occurred, response procedures should include relevant notifications and records.

Some jurisdictions define cases when the breach should be notified to the supervisory authority, and when it should be notified to PII principals.

Notifications should be clear.

NOTE 2 Notification can contain details such as:

— a contact point where more information can be obtained;

— a description of and the likely consequences of the breach;

— a description of the breach including the number of individuals concerned as well as the number of records concerned;

— measures taken or planned to be taken.

NOTE 3 Information on the management of security incidents can be found in the ISO/IEC 27035 series.

Where a breach involving PII has occurred, a record should be maintained with sufficient information to provide a report for regulatory or forensic purposes, such as:

— a description of the incident;

— the time period;

— the consequences of the incident;

— the name of the reporter;

— to whom the incident was reported;

— the steps taken to resolve the incident (including the person in charge and the data recovered);

— the fact that the incident resulted in unavailability, loss, disclosure or alteration of PII.

In the event that a breach involving PII has occurred, the record should also include a description of the PII compromised, if known; and if notifications were performed, the steps taken to notify PII principals, regulatory agencies or customers.

Implementation guidance for PII processors

Provisions covering the notification of a breach involving PII should form part of the contract between the organization and the customer. The contract should specify how the organization will provide the information necessary for the customer to fulfil their obligation to notify relevant authorities. This notification obligation does not extend to a breach caused by the customer or PII principal or within system components for which they are responsible. The contract should also define expected and externally mandated limits for notification response times.

In some jurisdictions, the PII processor should notify the PII controller of the existence of a breach without undue delay (i.e. as soon as possible), preferably, as soon as it is discovered so that the PII controller can take the appropriate actions.

Where a breach involving PII has occurred, a record should be maintained with sufficient information to provide a report for regulatory or forensic purposes, such as:

— a description of the incident;

— the time period;

— the consequences of the incident;

— the name of the reporter;

— to whom the incident was reported;

— the steps taken to resolve the incident (including the person in charge and the data recovered);

— the fact that the incident resulted in unavailability, loss, disclosure or alteration of PII.

In the event that a breach involving PII has occurred, the record should also include a description of the PII compromised, if known; and if notifications were performed, the steps taken to notify the customer or the regulatory agencies.

In some jurisdictions, applicable legislation or regulation can require the organization to directly notify appropriate regulatory authorities (e.g. a PII protection authority) of a breach involving PII.

B.3.13 Legal, statutory, regulatory and contractual requirements

Control

Legal, statutory, regulatory and contractual requirements relevant to information security related to PII processing and the organization's approach to meet these requirements should be identified, documented and kept up to date.

Implementation guidance

The organization should identify any potential legal sanctions (which can result from some obligations being missed) related to the processing of PII, including substantial fines directly from the local supervisory authority.

In some jurisdictions, International Standards such as this document can be used to form the basis for a contract between the organization and the customer, outlining their respective security, privacy and PII protection responsibilities. The terms of the contract can provide a basis for contractual sanctions in the event of a breach of those responsibilities.

B.3.14 Protection of records

Control

Records related to PII processing should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

Implementation guidance

Review of current and historical policies and procedures can be required (e.g. in the cases of customer dispute resolution and investigation by a supervisory authority).

The organization should retain copies of its privacy policies and associated procedures for a period as specified in its retention schedule (see B.1.4.8). This includes retention of previous versions of these documents when they are updated.

B.3.15 Independent review of information security

Control

The organization's approach to managing information security related to PII processing and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.

Implementation guidance

Where an organization is acting as a PII processor, and where individual customer audits are impractical or can increase risks to security, the organization should make available to customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and operated in accordance with the organization's policies and procedures. A relevant independent audit, as selected by the organization, should normally be an acceptable method for fulfilling the customer's interest in reviewing the organization's processing operations, if it covers the needs of anticipated users and if results are provided in a sufficient transparent manner.

B.3.16 Compliance with policies, rules and standards for information security

Control

Compliance with the organization's information security policy, topic-specific policies, rules and standards related to PII processing should be regularly reviewed.

Implementation guidance

As part of technical reviews of compliance with security policies and standards, the organization should include methods of reviewing tools and components related to processing PII. This can include:

— ongoing monitoring to verify that only permitted processing is taking place; or

— specific penetration or vulnerability tests (for example, de-identified datasets can be subject to a motivated intruder test to validate that de-identification methods are compliant with organizational requirements).

B.3.17 Information security awareness, education and training

Control

Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function, as they relate to PII processing.

Implementation guidance

Measures should be put in place, including awareness of incident reporting, to ensure that relevant staff are aware of the possible consequences to the organization (e.g. legal consequences, loss of business and brand or reputational damage), to the staff member (e.g. disciplinary consequences) and to the PII principal (e.g. physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the handling of PII.

NOTE Such measures can include the use of appropriate periodic training for personnel having access to PII.

B.3.18 Confidentiality or non-disclosure agreements

Control

Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of PII should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.

Implementation guidance

The organization should ensure that individuals operating under its control with access to PII are subject to a confidentiality obligation. The confidentiality agreement, whether part of a contract or separate, should specify the length of time the obligations should be adhered to.

When the organization is a PII processor, a confidentiality agreement, in whatever form, between the organization, its employees and its agents should ensure that employees and agents comply with the policy and procedures concerning data handling and protection.

B.3.19 Clear desk and clear screen

Control

Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.

Implementation guidance

The organization should restrict the creation of hardcopy material including PII to the minimum needed to fulfil the identified processing purpose.

B.3.20 Storage media

Control

Storage media with PII should be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.

Implementation guidance

The organization should document any use of removable media or devices for the storage of PII. Wherever feasible, the organization should use removable physical media or devices that permit encryption when storing PII. Unencrypted media should only be used where unavoidable, and in instances where unencrypted media or devices are used, the organization should implement procedures and compensating controls (e.g. tamper-evident packaging) to mitigate risks to the PII.

Where removable media on which PII is stored is disposed of, secure disposal procedures should be included in the documented information and implemented to ensure that previously stored PII will not be accessible.

If physical media is used for information transfer, a system should be put in place to record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender, the authorized recipients, the date and time, and the number of physical media. Where possible, additional measures such as encryption should be implemented to ensure that the data can only be accessed at the point of destination and not in transit.

The organization should subject physical media containing PII before leaving its premises to an authorization procedure and ensure the PII is not accessible to anyone other than authorized personnel.

NOTE One possible measure to ensure PII on physical media leaving the organization's premises is not generally accessible is to encrypt the PII concerned and restrict decryption capabilities to authorized personnel.

Removable media which is taken outside the physical confines of the organization is prone to loss, damage and inappropriate access. Encrypting removable media adds a level of protection for PII which reduces security and privacy risks should the removable media be compromised.

B.3.21 Secure disposal or re-use of equipment

Control

Items of equipment containing storage media with PII should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Implementation guidance

The organization should ensure that, whenever storage space is re-assigned, any PII previously residing on that storage space is not accessible.

On deletion of PII held in an information system, performance issues can mean that explicit erasure of that PII is impractical. This creates the risk that another user can access the PII. Such risk should be avoided by specific technical measures.

For secure disposal or re-use, equipment containing storage media that can possibly contain PII should be treated as though it does contain PII.

B.3.22 User endpoint devices

Control

PII stored on, processed by or accessible via user endpoint devices should be protected.

Implementation guidance

The organization should ensure that the use of mobile devices does not lead to a compromise of PII.

B.3.23 Secure authentication

Control

Secure authentication technologies and procedures related to PII processing should be implemented based on information access restrictions.

Implementation guidance

Where required by the customer, the organization should provide the capability for secure log-on procedures for any user accounts under the customer's control.

B.3.24 Information backup

Control

Backup copies of PII, and software and systems related to PII processing should be maintained and regularly tested.

Implementation guidance

The organization should have a policy which addresses the requirements for backup, recovery and restoration of PII (which can be part of an overall information backup policy) and any further requirements (e.g. contractual or legal requirements) for the erasure of PII contained in information held for backup requirements.

PII-specific responsibilities in this respect can depend on the customer. The organization should ensure that the customer has been informed of the limits of the service regarding backup.

Where the organization explicitly provides backup and restore services to customers, the organization should provide them with clear information about their capabilities with respect to backup and restoration of PII.

Some jurisdictions impose specific requirements regarding the frequency of backups of PII, the frequency of reviews and tests of backup, or regarding the recovery procedures for PII. Organizations operating in these jurisdictions should demonstrate compliance with these requirements.

There can be occasions where PII needs to be restored, perhaps due to a system malfunction, attack or disaster. When PII is restored (typically from backup media), processes need to be in place to ensure that the PII is restored into a state where the integrity of PII can be assured, or where PII inaccuracy or incompleteness is identified and processes put in place to resolve them (which can involve the PII principal).

The organization should have a procedure for, and a log of, PII restoration efforts. At a minimum, the log of the PII restoration efforts should contain:

— the name of the person responsible for the restoration;

— a description of the restored PII.

Some jurisdictions prescribe the content of the logs of PII restoration efforts. Organizations should be able to document compliance with any applicable jurisdiction-specific requirements for restoration log content. The conclusions of such deliberations should be included in documented information.

The use of subcontractors to store replicated or backup copies of PII processed is covered by the controls in this document applying to subcontracted PII processing (see B.3.10, B.3.20). Where physical media transfers take place related to backups and restoration, this is also covered by controls in this document (B.3.7).

B.3.25 Logging

Control

Logs that record activities, exceptions, faults and other relevant events related to PII processing should be produced, stored, protected and analysed.

Implementation guidance

A process should be put in place to review event logs using continuous, automated monitoring and alerting processes, or else manually where such review should be performed with a specified, documented periodicity, to identify irregularities and propose remediation efforts.

Where possible, event logs should record access to PII, including by whom, when, which PII principal's PII was accessed, and what (if any) changes were made (additions, modifications or deletions) as a result of the event.

Where multiple service providers are involved in providing services, there can be varied or shared roles in implementing this guidance. These roles should be clearly defined and included in the documented information, and agreement on any log access between providers should be addressed.

Log information recorded for, for example, security monitoring and operational diagnostics, can contain PII. Measures such as controlling access should be put in place to ensure that logged information is only used as intended.

A procedure, preferably automatic, should be put in place to ensure that logged information is either deleted or de-identified as specified in the retention schedule (see B.1.4.8).

Implementation guidance for PII processors:

The organization should define criteria regarding if, when and how log information can be made available to or usable by the customer. These criteria should be made available to the customer.

Where the organization permits its customers to access log records controlled by the organization, the organization should implement appropriate controls to ensure that the customer can only access records that relate to that customer’s activities, cannot access any log records which relate to the activities of other customers, and cannot amend the logs in any way.

B.3.26 Use of cryptography

Control

Rules for the effective use of cryptography related to PII processing, including cryptographic key management, should be defined and implemented.

Implementation guidance

Some jurisdictions can require the use of cryptography to protect particular kinds of PII, such as health data, resident registration numbers, passport numbers and driver's licence numbers.

The organization should provide information to the customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The organization should also provide information to the customer about any capabilities it provides that can assist the customer in applying their own cryptographic protection.

B.3.27 Secure development life cycle

Control

Rules for the secure development of software and systems related to PII processing should be established and applied.

Implementation guidance

Policies for system development and design should include guidance for the organization’s processing of PII needs, based on obligations to PII principals or any applicable legislation or regulation and the types of processing performed by the organization. Annexes A and B provide control considerations for processing of PII, which can be useful in developing policies for privacy in systems design.

Policies that contribute to privacy by design and privacy by default should consider the following aspects:

a) guidance on PII protection and the implementation of the privacy principles (see ISO/IEC 29100) in the software development lifecycle;

b) privacy and PII protection requirements in the design phase, which can be based on the output from a privacy risk assessment or a privacy impact assessment (see B.1.2.6);

c) PII protection checkpoints within project milestones;

d) required privacy and PII protection knowledge;

e) by default minimize processing of PII.

B.3.28 Application security requirements

Control

Information security requirements related to PII processing should be identified, specified and approved when developing or acquiring applications.

Implementation guidance

The organization should ensure that PII that is transmitted over untrusted data transmission networks is encrypted for transmission.

Untrusted networks can include the public internet and other facilities outside of the operational control of the organization.

NOTE In some cases (e.g. the exchange of e-mail) the inherent characteristics of untrusted data transmission network systems can require that some header or traffic data be exposed for effective transmission.

B.3.29 Secure system architecture and engineering principles

Control

Principles for engineering secure systems related to processing PII should be established, documented, maintained and applied to any information system development activities.

Implementation guidance

Systems or components related to the processing of PII should be designed following the principles of privacy by design and privacy by default, and to anticipate and facilitate the implementation of relevant controls (as described in B.1 and B.2 for PII controllers and PII processors respectively), in particular such that the collection and processing of PII in those systems is limited to what is necessary for the identified purposes of the processing of PII (see B.1.2.2).

For example, an organization that processes PII should ensure that, based on the relevant jurisdiction, it disposes of PII after a specified period. The system that processes that PII should be designed in a way to facilitate this deletion requirement.

B.3.30 Outsourced development

Control

The organization should direct, monitor and review the activities related to outsourced PII processing system development.

Implementation guidance

The same principles (see B.3.29) of privacy by design and privacy by default should be applied, if applicable, to outsourced information systems.

B.3.31 Test information

Control

Test information related to PII processing should be appropriately selected, protected and managed.

Implementation guidance

PII should not be used for testing purposes; false or synthetic PII should be used. Where the use of PII for testing purposes cannot be avoided, technical and organizational measures equivalent to those used in the production environment should be implemented to minimize the risks. Where such equivalent measures are not feasible, a risk assessment should be undertaken and used to identify the selection of appropriate mitigating controls.

Annex C
(informative)

Mapping to ISO/IEC 29100

Table C.1 and C.2 give an indicative mapping between provisions of this document and the privacy principles from ISO/IEC 29100. It shows in a purely indicative manner how compliance to requirements and controls of this document relates to the general privacy principles specified in ISO/IEC 29100.

Table C.1 — Mapping of controls for PII controllers and ISO/IEC 29100

Privacy principles of ISO/IEC 29100	Related controls for PII controllers
1. Consent and Choice	A.1.2.2 Identify and document purpose A.1.2.3 Identify lawful basis A.1.2.4 Determine when and how consent is to be obtained A.1.2.5 Obtain and record consent A.1.2.6 Privacy impact assessment A.1.3.5 Providing mechanism to modify or withdraw consent A.1.3.6 Providing mechanism to object to PII processing A.1.3.8 PII controllers' obligations to inform third parties
2. Purpose legitimacy and specification	A.1.2.2 Identify and document purpose A.1.2.3 Identify lawful basis A.1.2.6 Privacy impact assessment A.1.3.3 Determining information for PII principals A.1.3.4 Providing information to PII principals A.1.3.11 Automated decision making
3. Collection limitation	A.1.2.6 Privacy impact assessment A.1.4.2 Limit collection
4. Data minimization	A.1.4.3 Limit processing A.1.4.5 PII minimization objectives A.1.4.6 PII de-identification and deletion at the end of processing
5. Use, retention and disclosure limitation	A.1.4.5 PII minimization objectives A.1.4.6 PII de-identification and deletion at the end of processing A.1.4.7 Temporary files A.1.4.8 Retention A.1.4.9 Disposal A.1.5.2 Identify basis for PII transfer between jurisdictions A.1.5.5 Records of PII disclosure to third parties

Privacy principles of ISO/IEC 29100	Related controls for PII controllers
6. Accuracy and quality	A.1.4.4 Accuracy and quality
7. Openness, transparency and notice	A.1.3.3 Determining information for PII principals A.1.3.4 Providing information to PII principals
8. Individual participation and access	A.1.3.2 Determining and fulfilling obligations to PII principals A.1.3.4 Providing information to PII principals A.1.3.7 Access, correction or erasure A.1.3.9 Providing copy of PII processed A.1.3.10 Handling requests
9. Accountability	A.1.2.7 Contracts with PII processors A.1.2.8 Joint PII controller A.1.2.9 Records related to processing PII A.1.3.10 Handling requests A.1.5.2 Identify basis for PII transfer between jurisdictions A.1.5.3 Countries and international organizations to which PII can be transferred A.1.5.4 Records of transfer of PII
10. Information Security	A.1.2.7 Contracts with PII processors A.1.4.10 PII transmission controls
11. Privacy compliance	A.1.2.6 Privacy impact assessment

Table C.2 — Mapping of controls for PII processors and ISO/IEC 29100

Privacy principles of ISO/IEC 29100	Related controls for PII processors
1. Consent and choice	A.2.2.6 Customer obligations
2. Purpose legitimacy and specification	A.2.2.2 Customer agreement A.2.2.3 Organization's purposes A.2.2.4 Marketing and advertising use A.2.2.5 Infringing instruction A.2.3.2 Comply with obligations to PII principals
3. Collection limitation	N/A
4. Data minimization	A.2.4.2 Temporary files
5. Use, retention and disclosure limitation	A.2.5.4 Records of PII disclosure to third parties A.2.5.5 Notification of PII disclosure requests A.2.5.6 Legally binding PII disclosures
6. Accuracy and quality	N/A
7. Openness, transparency and notice	A.2.5.7 Disclosure of subcontractors used to process PII A.2.5.8 Engagement of a subcontractor to process PII A.2.5.9 Change of subcontractor to process PII

Privacy principles of ISO/IEC 29100	Related controls for PII processors
8. Individual participation and access	A.2.3.2 Comply with obligations to PII principals
9. Accountability	A.2.2.7 Records related to processing PII A.2.4.3 Return, transfer or disposal of PII A.2.5.2 Basis for PII transfer between jurisdictions A.2.5.3 Countries and international organizations to which PII can be transferred
10. Information security	A.2.4.4 PII transmission controls
11. Privacy compliance	A.2.2.6 Customer obligations

Annex D
(informative)

Mapping to the General Data Protection Regulation

This annex gives an indicative mapping between provisions of this document and Articles 5 to 49 except 43 of the General Data Protection Regulation of the European Union. It shows how compliance to requirements and controls of this document can be relevant to fulfil obligations of GDPR.

However, it is purely indicative and as per this document, it is the organizations responsibility to assess its legal obligations and decide how to comply with them.

Table D.1 — Mapping of ISO/IEC 27701 structure to GDPR articles

Subclause of this document	GDPR article
4.1	(24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
4.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
4.3	(32)(2)
4.4	(32)(2)
6.1.2	(32)(1)(b), (32)(2)
6.1.3	(32)(1)(b), (32)(2)
5.2	(24)(2)
5.3	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
B.3.5	(5)(1)(f), (32)(2)
B.3.6	(5)(1)(f)
B.3.7	(5)(1)(f)
B.1.3.7	(5)(1)(f)
B.3.9	(5)(1)(f)
B.3.10	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e), (28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
B.3.11	(5)(1)(f), (33)(1), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2), (34)(3)(a), (34)(3)(b), (34)(3)(c), (34)(4)
B.3.12	(33)(1), (33)(2), (33)(3)(a), (33)(3)(b), (33)(3)(c), (33)(3)(d), (33)(4), (33)(5), (34)(1), (34)(2)
B.3.13	(5)(1)(f), (28)(1), (28)(3)(a), (28)(3)(b), (28)(3)(c), (28)(3)(d), (28)(3)(e),

Subclause of this document	GDPR article
	(28)(3)(f), (28)(3)(g), (28)(3)(h), (30)(2)(d), (32)(1)(b)
B.3.14	(5)(2), (24)(2)
B.3.15	(32)(1)(d), (32)(2)
B.3.16	(32)(1)(d), (32)(2)
B.3.17	(39)(1)(b)
B.3.18	(5)(1)(f), (28)(3)(b), (38)(5)
B.3.19	(5)(1)(f)
B.3.20	(5)(1)(f), (32)(1)(a)
B.3.21	(5)(1)(f)
B.3.22	(5)(1)(f)
B.3.23	(5)(1)(f)
B.3.24	(5)(1)(f), (32)(1)(c)
B.3.25	(5)(1)(f)
B.3.26	(32)(1)(a)
B.3.27	(25)(1)
B.3.28	(5)(1)(f), (32)(1)(a)
B.3.29	(25)(1)
B.3.31	(5)(1)(f)
B.1.2.2	(5)(1)(b), (32)(4)
B.1.2.3	(10), (5)(1)(a), (6)(1)(a), (6)(1)(b), (6)(1)(c), (6)(1)(d), (6)(1)(e), (6)(1)(f), (6)(2), (6)(3), (6)(4)(a), (6)(4)(b), (6)(4)(c), (6)(4)(d), (6)(4)(e), (8)(3), (9)(1), (9)(2)(b), (9)(2)(c), (9)(2)(d), (9)(2)(e), (9)(2)(f), (9)(2)(g), (9)(2)(h), (9)(2)(i), (9)(2)(j), (9)(3), (9)(4), (17)(3)(a), (17)(3)(b), (17)(3)(c), (17)(3)(d), (17)(3)(e), (18)(2), (22)(2)(a), (22)(2)(b), (22)(2)(c), (22)(4)
B.1.2.4	(8)(1), (8)(2)
B.1.2.5	(7)(1), (7)(2), (9)(2)(a)
B.1.2.6	(35)(1), (35)(2), (35)(3)(a), (35)(3)(b), (35)(3)(c), (35)(4), (35)(5), (35)(7)(a), (35)(7)(b), (35)(7)(c), (35)(7)(d), (35)(8), (35)(9), (35)(10), (35)(11), (36)(1), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
B.1.2.7	(5)(2), (28)(3)(e), (28)(9)
B.1.2.8	(26)(1), (26)(2), (26)(3)
B.1.2.9	(5)(2), (24)(1), (30)(1)(a), (30)(1)(b), (30)(1)(c), (30)(1)(d), (30)(1)(f), (30)(1)(g), (30)(3), (30)(4), (30)(5)
B.1.3.2	(12)(2)
B.1.3.3	(11)(2), (13)(3), (13)(1)(a), (13)(1)(b), (13)(1)(c), (13)(1)(d), (13)(1)(e), (13)(1)(f), (13)(2)(c), (13)(2)(d), (13)(2)(e), (13)(4), (14)(1)(a), (14)(1)(b), (14)(1)(c), (14)(1)(d), (14)(1)(e), (14)(1)(f), (14)(2)(b), (14)(2)(e), (14)(2)(f), (14)(3)(a), (14)(3)(b), (14)(3)(c), (14)(4), (14)(5)(a), (14)(5)(b), (14)(5)(c), (14)(5)(d), (15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (15)(2), (18)(3), (21)(4)

Subclause of this document	GDPR article
B.1.3.4	(11)(2), (12)(1), (12)(7), (13)(3), (21)(4)
B.1.3.5	(7)(3), (13)(2)(c), (14)(2)(d), (18)(1)(a), (18)(1)(b), (18)(1)(c), (18)(1)(d)
B.1.3.6	(13)(2)(b), (14)(2)(c), (21)(1), (21)(2), (21)(3), (21)(5), (21)(6)
B.1.3.7	(5)(1)(d), (13)(2)(b), (14)(2)(c), (16), (17)(1)(a), (17)(1)(b), (17)(1)(c), (17)(1)(d), (17)(1)(e), (17)(1)(f), (17)(2)
B.1.3.8	(19)
B.1.3.9	(15)(3), (15)(4), (20)(1), (20)(2), (20)(3), (20)(4)
B.1.3.10	(15)(1)(a), (15)(1)(b), (15)(1)(c), (15)(1)(d), (15)(1)(e), (15)(1)(f), (15)(1)(g), (15)(1)(h), (12)(3), (12)(4), (12)(5), (12)(6)
B.1.3.11	(13)(2)(f), (14)(2)(g), (22)(1), (22)(3)
B.1.4.2	(5)(1)(b), (5)(1)(c)
B.1.4.3	(25)(2)
B.1.4.4	(5)(1)(d)
B.1.4.5	(5)(1)(c), (5)(1)(e)
B.1.4.6	(5)(1)(c), (5)(1)(e), (6)(4)(e), (11)(1), (32)(1)(a)
B.1.4.7	(5)(1)(c)
B.1.4.8	(13)(2)(a), (14)(2)(a)
B.1.4.9	(5)(1)(f)
B.1.4.10	(5)(1)(f)
B.1.5.2	(15)(2), (44), (45)(1), (45)(2)(a), (45)(2)(b), (45)(2)(c), (45)(3), (45)(4), (45)(5), (45)(6), (45)(7), (45)(8), (45)(9), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (46)(4), (46)(5), (47)(1)(a), (47)(1)(b), (47)(1)(c), (47)(2)(a), (47)(2)(b), (47)(2)(c), (47)(2)(d), (47)(2)(e), (47)(2)(f), (47)(2)(g), (47)(2)(h), (47)(2)(i), (47)(2)(j), (47)(2)(k), (47)(2)(l), (47)(2)(m), (47)(2)(n), (47)(3), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6), (30)(1)(e), (48)
B.1.5.3	(15)(2), (30)(1)(e)
B.1.5.4	(30)(1)(e)
B.1.5.5	(30)(1)(d)
B.2.2.2	(28)(3)(f), (28)(3)(e), (28)(9), (35)(1)
B.2.2.3	(5)(1)(a), (5)(1)(b), (28)(3)(a), (29), (32)(4)
B.2.2.4	(7)(4)
B.2.2.5	(28)(3)(h)
B.2.2.6	(28)(3)(h)
B.2.2.7	(30)(3), (30)(4), (30)(5), (30)(2)(a), (30)(2)(b)
B.2.3.2	(15)(3), (17)(2), (28)(3)(e)
B.2.4.2	(5)(1)(c)
B.2.4.3	(28)(3)(g), (30)(1)(f)

Subclause of this document	GDPR article
B.2.4.4	(5)(1)(f)
B.2.5.2	(44), (46)(1), (46)(2)(a), (46)(2)(b), (46)(2)(c), (46)(2)(d), (46)(2)(e), (46)(2)(f), (46)(3)(a), (46)(3)(b), (48), (49)(1)(a), (49)(1)(b), (49)(1)(c), (49)(1)(d), (49)(1)(e), (49)(1)(f), (49)(1)(g), (49)(2), (49)(3), (49)(4), (49)(5), (49)(6)
B.2.5.3	(30)(2)(c)
B.2.5.4	(30)(1)(d)
B.2.5.5	(28)(3)(a)
B.2.5.6	(48)
B.2.5.7	(28)(2), (28)(4)
B.2.5.8	(28)(2), (28)(3)(d)
B.2.5.9	(28)(2)

Annex E
(informative)

Mapping to ISO/IEC 27018 and ISO/IEC 29151

ISO/IEC 27018 gives further information for organizations acting as PII processors and providing public cloud services. ISO/IEC 29151 gives additional controls and guidance for the processing of PII by PII controllers.

Table E.1 gives an indicative mapping between provisions of this document and provisions from ISO/IEC 27018 and ISO/IEC 29151. It shows how requirements and controls of this document can have some correspondence with provisions from ISO/IEC 27018 or ISO/IEC 29151.

It is purely indicative and it should not be assumed that a given link between provisions means equivalence.

Table E.1 — Mapping of ISO/IEC 27701 to ISO/IEC 27018 and ISO/IEC 29151

Subclause in this document	Subclause in ISO/IEC 27018	Subclause in ISO/IEC 29151
4	N/A	N/A
5	N/A	N/A
6	N/A	4.2
7	N/A	7.2.3
8	N/A	N/A
9	N/A	N/A
10	N/A	N/A
B.3.2	N/A	N/A
B.3.3, B.3.4, B.3.5, B.3.6, B.3.7, B.3.8, B.3.9, B.3.10, B.3.11, B.3.12, B.3.13, B.3.14, B.3.15, B.3.16	5.1.1, 6.1.1, 9.2.1, 16.1.1, 18.2.1, A.10.1, A.10.2, A.11.6, A.11.8, A,11,9, A.11.10 , A.11.11	5, 8.1, 8.2, 9.2, 9.3, 18.2
B.3.17, B.3.18	7.2.2	N/A
B.3.19, B.3.20, B.3.21	11.2.7, A.11.2, A.11.4, A.11.5, A.11.13,	8.3, 11.1
B.3.22, B.3.23, B.3.24, B.3.25, B.3.26, B.3.27, B.3.28, B.3.29, B.3.30, B.3.31	7.2.2, 9.4.2, 10.1.1, 12.1.4, 12.4.1, 12.4.2, 13.2.1, A.11.1	9.4, 12.1, 12.2, 12.3, 12.4, 13.1, 13.2
B.1.2.2	N/A	A.4
B.1.2.3	N/A	A.4.1
B.1.2.4	N/A	N/A
B.1.2.5	N/A	A.3.1
B.1.2.6	N/A	A.11.2

Subclause in this document	Subclause in ISO/IEC 27018	Subclause in ISO/IEC 29151
B.1.2.7	N/A	A.11.3
B.1.2.8	N/A	N/A
B.1.2.9	N/A	N/A
B.1.3.2	N/A	A.10
B.1.3.3	N/A	N/A
B.1.3.4	N/A	A.9
B.1.3.5	N/A	N/A
B.1.3.6	N/A	N/A
B.1.3.7	N/A	A.10.1
B.1.3.8	N/A	N/A
B.1.3.9	N/A	N/A
B.1.3.10	N/A	N/A
B.1.3.11	N/A	N/A
B.1.4.2	N/A	A.5
B.1.4.3	N/A	N/A
B.1.4.4	N/A	A.8
B.1.4.5	N/A	N/A
B.1.4.6	N/A	A.7.1
B.1.4.7	N/A	A.7.2
B.1.4.8	N/A	A.7.1
B.1.4.9	N/A	N/A
B.1.4.10	N/A	N/A
B.1.5.2	N/A	A.13.2
B.1.5.3	N/A	A.13.2
B.1.5.4	N/A	A.13.2
B.1.5.5	N/A	A.7.4
B.2.2.2	N/A	N/A
B.2.2.3	A.3.1	N/A
B.2.2.4	A.3.2	N/A
B.2.2.5	N/A	N/A
B.2.2.6	N/A	N/A
B.2.2.7	N/A	N/A
B.2.3.2	A.2.1	N/A
B.2.4.2	A.5.1	N/A
B.2.4.3	A.10.3	N/A
B.2.4.4	A.12.2	N/A

Subclause in this document	Subclause in ISO/IEC 27018	Subclause in ISO/IEC 29151
B.2.5.2	N/A	N/A
B.2.5.3	A.12.1	N/A
B.2.5.4	A.6.2	N/A
B.2.5.5	A.6.1	N/A
B.2.5.6	A.6.1	N/A
B.2.5.7	A.8.1	A.7.5
B.2.5.8	A.8.1	N/A
B.2.5.9	A.8.1	N/A

Annex F
(informative)

Correspondence with ISO/IEC 27701:2019

The purpose of this annex is to provide backwards compatibility with ISO/IEC 27701:2019 for organizations that are currently using that document and now wish to transition to this edition.

Table F.1 provides the correspondence of the controls specified in Annex A with those in ISO/IEC 27701:2019. 'N/A' in the first column identifies those controls not included in this document. 'New' in the second column identifies controls not included in ISO/IEC 27701:2019.

Table F.1 — Correspondence between controls in this document and controls in ISO/IEC 27701:2019

ISO/IEC 27701 control identifier	ISO/IEC 27701: 2019 control identifier	Control name
A.3.3	6.2.1.1, 6.2.1.2	Policies for information security
A.3.4	6.3.1.1	Information security roles and responsibilities
N/A	6.3.1.2	Segregation of duties
N/A	6.4.2.1	Management responsibilities
N/A	6.3.1.3	Contact with authorities
N/A	6.3.1.4	Contact with special interest groups
N/A	New	Threat intelligence
N/A	6.3.1.5, 6.11.1.1	Information security in project management
N/A	6.5.1.1, 6.5.1.2	Inventory of information and other associated assets
N/A	6.5.1.3, 6.5.2.3	Acceptable use of information and other associated assets
N/A	6.5.1.4	Return of assets
A.3.5	6.5.2.1	Classification of information
A.3.6	6.5.2.2	Labelling of information
A.3.7	6.10.2.1, 6.10.2.2, 6.10.2.3	Information transfer
N/A	6.6.1.1, 6.6.1.2	Access control
A.3.8	6.6.2.1	Identity management
N/A	6.6.2.4, 6.6.3.1, 6.6.4.3	Authentication information
A.3.9	6.6.2.2, 6.6.2.5, 6.6.2.6	Access rights

A.3.10	6.12.1.1 6.12.1.2	Addressing information security within supplier agreements
N/A	6.12.1.3	Managing information security in the ICT supply chain
N/A	6.12.2.1, 6.12.2.2	Monitoring, review and change management of supplier services
N/A	New	Information security for use of cloud services
N/A	6.13.1.1	Information security incident management planning and preparation
A.3.11	6.13.1.4	Assessment and decision on information security events
A.3.12	6.13.1.5	Response to information security incidents
N/A	6.13.1.6	Learning from information security incidents
N/A	6.13.1.7	Collection of evidence
N/A	6.14.1.1, 6.14.1.2, 6.14.1.3	Information security during disruption
N/A	New	ICT readiness for business continuity
A.3.13	6.15.1.1, 6.15.1.5	Legal, statutory, regulatory and contractual requirements
N/A	6.15.1.2	Intellectual property rights
A.3.14	6.15.1.3	Protection of records
N/A	6.15.1.4	Privacy and protection of PII
A.3.15	6.15.2.1	Independent review of information security
A.3.16	6.15.2.2, 6.15.2.3	Compliance with policies, rules and standards for information security
N/A	6.9.1.1	Documented operating procedures
N/A	6.4.1.1	Screening
N/A	6.4.1.2	Terms and conditions of employment
A.3.17	6.4.2.2	Information security awareness, education and training
N/A	6.4.2.3	Disciplinary procedures
N/A	6.4.3.1	Responsibilities after termination or change of employment
A.3.18	6.10.2.4	Confidentiality or non-disclosure agreements
N/A	6.3.2.2	Remote working
N/A	6.13.1.2, 6.13.1.3	Information security event reporting
N/A	6.8.1.1	Physical security perimeter
N/A	6.8.1.2, 6.8.1.6	Physical entry

N/A	6.8.1.3	Securing offices, rooms and facilities
N/A	New	Physical security monitoring
N/A	6.8.1.4	Protecting against physical and environmental threats
N/A	6.8.1.5	Working in secure areas
A.3.19	6.8.2.9	Clear desk and clear screen
N/A	6.8.2.1	Equipment siting and protection
N/A	6.8.2.6	Security of assets off-premises
A.3.20	6.5.3.1, 6.5.3.2, 6.5.3.3, 6.8.2.5	Storage media
N/A	6.8.2.2	Supporting utilities
N/A	6.8.2.3	Cabling security
N/A	6.8.2.4	Equipment maintenance
A.3.21	6.8.2.7	Secure disposal or re-use of equipment
A.3.22	6.3.2.1, 6.8.2.8	User endpoint devices
N/A	6.6.2.3	Privileged access rights
N/A	6.6.4.1	Information access restriction
N/A	6.6.4.5	Access to source code
A.3.23	6.6.4.2	Secure authentication
N/A	6.9.1.3	Capacity management
N/A	6.9.2.1	Protection against malware
N/A	6.9.6.1	Management of technical vulnerabilities
N/A	New	Configuration management
N/A	New	Information deletion
N/A	New	Data masking
N/A	New	Data leakage prevention
A3.24	6.9.3.1	Information backup
N/A	6.14.2.1	Redundancy of information processing facilities
A.3.25	6.9.4.1, 6.9.4.2, 6.9.4.3	Logging
N/A	New	Monitoring activities
N/A	6.9.4.4	Clock synchronization
N/A	6.6.4.4	Use of privileged utility programme(s)
N/A	6.9.5.1, 6.9.6.2	Installation of software on operational systems
N/A	6.10.1.1	Network security

N/A	6.10.1.2	Security of network services
N/A	6.10.1.3	Segregation of networks
N/A	New	Web filtering
A.3.26	6.7.1.1, 6.7.1.2	Use of cryptography
A.3.27	6.11.2.1	Secure development life cycle
A.3.28	6.11.1.2, 6.11.1.3	Application security requirements
A.3.29	6.11.2.5	Secure system architecture and engineering principles
N/A	New	Secure coding
N/A	6.11.2.8, 6.11.2.9	Security testing in development and acceptance
A.3.30	6.11.2.7	Outsourced development
N/A	6.9.1.4, 6.11.2.6	Separation of development, testing and production environments
N/A	6.9.1.2, 6.11.2.2, 6.11.2.3, 6.11.2.4	Change management
A.3.31	6.11.3.1	Test information
N/A	6.9.7.1	Protection of information systems during audit testing

Table F.2 provides the correspondence of the controls specified in clause 6 in ISO/IEC 27701:2019 with those in this document. 'N/A' in the second column identifies those controls not included in this document.

Table F.2 — Correspondence between controls in ISO/IEC 27701:2019 and controls in this document

ISO/IEC 27701: 2019 control identifier	ISO/IEC 27701 control identifier	Control name according to ISO/IEC 27701:2019
6.2.1.1	A.3.3	Policies for information security
6.2.1.2	A.3.3	Review of policies for information security
6.3.1.1	A.3.4	Internal security roles and responsibilities
6.3.1.2	N/A	Segregation of duties
6.3.1.3	N/A	Contact with authorities
6.3.1.4	N/A	Contact with special interest groups
6.3.1.5	N/A	Information security in project management
6.3.2.1	A.3.22	Mobile device policy

6.3.2.2	N/A	Teleworking
6.4.1.1	N/A	Screening
6.4.1.2	N/A	Terms and conditions of employment
6.4.2.1	N/A	Management responsibilities
6.4.2.2	A.3.17	Information security awareness, education and training
6.4.2.3	N/A	Disciplinary procedures
6.4.3.1	N/A	Termination or change of employment responsibilities
6.5.1.1	N/A	Inventory of assets
6.5.1.2	N/A	Ownership of assets
6.5.1.3	N/A	Acceptable use of assets
6.5.1.4	N/A	Return of assets
6.5.2.1	A.3.5	Classification of information
6.5.2.2	A.3.6	Labelling of information
6.5.2.3	N/A	Handling of assets
6.5.3.1	A.3.20	Management of removable media
6.5.3.2	A.3.20	Disposal of media
6.5.3.3	A.3.20	Physical media transfer
6.6.1.1	N/A	Access control policy
6.6.1.2	N/A	Access to networks and network services
6.6.2.1	A.3.8	User registration and de-registration
6.6.2.2	A.3.9	User access provisioning
6.6.2.3	N/A	Management of privileged access rights
6.6.2.4	N/A	Management of secret authentication information of users
6.6.2.5	A.3.9	Review of user access rights
6.6.2.6	A.3.9	Removal or adjustment of access rights
6.6.3.1	N/A	Use of secret authentication information
6.6.4.1	N/A	Information access restriction
6.6.4.2	A.3.23	Secure log-on procedures
6.6.4.3	N/A	Password management system
6.6.4.4	N/A	Use of privileged utility programme(s)
6.6.4.5	N/A	Access control to program source code
6.7.1.1	A.3.26	Policy on the use of cryptographic controls
6.7.1.2	A.3.26	Key management
6.8.1.1	N/A	Physical security perimeter

6.8.1.2	N/A	Physical entry controls
6.8.1.3	N/A	Securing offices, rooms and facilities
6.8.1.4	N/A	Protecting against external and environmental threats
6.8.1.5	N/A	Working in secure areas
6.8.1.6	N/A	Delivery and loading areas
6.8.2.1	N/A	Equipment siting and protection
6.8.2.2	N/A	Supporting utilities
6.8.2.3	N/A	Cabling security
6.8.2.4	N/A	Equipment maintenance
6.8.2.5	N/A	Removal of assets
6.8.2.6	N/A	Security of equipment and assets off-premises
6.8.2.7	A.3.21	Secure disposal or re-use of equipment
6.8.2.8	A.3.22	Unattended user equipment
6.8.2.9	A.3.19	Clear desk and clear screen policy
6.9.1.1	N/A	Documenting operating procedures
6.9.1.2	N/A	Change management
6.9.1.3	N/A	Capacity management
6.9.1.4	N/A	Separation of development, testing and operational environments
6.9.2.1	N/A	Controls against malware
6.9.3.1	A.3.24	Information backup
6.9.4.1	A.3.25	Event logging
6.9.4.2	A.3.25	Protection of log information
6.9.4.3	A.3.25	Administrator and operator logs
6.9.4.4	N/A	Clock synchronization
6.9.5.1	N/A	Installation of software on operational systems
6.9.6.1	N/A	Management of technical vulnerabilities
6.9.6.2	N/A	Restriction on software installation
6.9.7.1	N/A	Information systems audit controls
6.10.1.1	N/A	Network controls
6.10.1.2	N/A	Security in network services
6.10.1.3	N/A	Segregation in networks
6.10.2.1	A.3.7	Information transfer policies and procedures
6.10.2.2	A.3.7	Agreements for information transfer

6.10.2.3	A.3.7	Electronic messaging
6.10.2.4	A.3.18	Confidentiality or non-disclosure agreements
6.11.1.1	N/A	Information security requirements analysis and specification
6.11.1.2	A.3.28	Securing application services on public networks
6.11.1.3	A.3.28	Protecting application services transactions
6.11.2.1	A.3.27	Secure development policy
6.11.2.2	N/A	System change control procedures
6.11.2.3	N/A	Technical review of applications after operating platform changes
6.11.2.4	N/A	Restrictions of changes to software packages
6.11.2.5	A.3.29	Secure systems engineering principles
6.11.2.6	N/A	Secure development environment
6.11.2.7	A.3.30	Outsourced development
6.11.2.8	N/A	System security testing
6.11.2.9	N/A	System acceptance testing
6.11.3.1	A.3.30	Protection of test data
6.12.1.1	A.3.10	Information security policy for supplier relationships
6.12.1.2	A.3.10	Addressing security within supplier agreements
6.12.1.3	N/A	Information and communication technology supply chain
6.12.2.1	N/A	Monitoring and review of supplier services
6.12.2.2	N/A	Managing changes to supplier services
6.13.1.1	N/A	Responsibilities and procedures
6.13.1.2	N/A	Reporting information security events
6.13.1.3	N/A	Reporting information security weaknesses
6.13.1.4	A.3.11	Assessment and decisions on information security events
6.13.1.5	A.3.12	Response to information security incidents
6.13.1.6	N/A	Learning from information security incidents
6.13.1.7	N/A	Collection of evidence
6.14.1.1	N/A	Planning information security continuity
6.14.1.2	N/A	Implementing information security continuity
6.14.1.3	N/A	Verify, renew and evaluate information security continuity
6.14.2.1	N/A	Availability of information processing facilities
6.15.1.1	A.3.13	Identification of applicable legislation and contractual requirements

6.15.1.2	N/A	Intellectual property rights
6.15.1.3	A.3.14	Protection of records
6.15.1.4	N/A	Privacy and protection of personally identifiable information
6.15.1.5	A.3.13	Regulation of cryptographic controls
6.15.2.1	A.3.15	Independent review of information security
6.15.2.2	A.3.16	Compliance with security policies and standards
6.15.2.3	A.3.16	Technical compliance review

Bibliography

[1] ISO/IEC 19944-1, *Cloud computing and distributed platforms — Data flow, data categories and data use —Part 1: Fundamentals*

[2] ISO/IEC 19944-2, *Cloud computing and distributed platforms — Data flow, data categories and data use —Part 2: Guidance on application and extensibility*

[3] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*

[4] ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[5] ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

[6] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing Information security risks*

[7] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[8] ISO/IEC 27035-1, *Information technology — Information security incident management — Part 1: Principles and process*

[9] ISO/IEC 27035-2, *Information technology — Information security incident management — Part 2: Guidance to plan and prepare for incident response*

[10] ISO/IEC 27557, *Information security, cybersecurity and privacy protection — Application of ISO 31000:2018 for organizational privacy risk management*

[11] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[12 ISO/IEC 29134, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[13] ISO/IEC 29151, *Information technology — Security techniques — Code of practice for personally identifiable information protection*

[14] ISO/IEC 29184, *Information technology — Online privacy notices and consent*

[15] ISO 31000, *Risk management — Guidelines*