INTERNATIONAL STANDARD

**ISO 31700-1**

First edition
2023-01

# Consumer protection — Privacy by design for consumer goods and services —

## Part 1: High-level requirements

*Protection des consommateurs — Respect de la vie privée assuré dès la conception des biens de consommation et services aux consommateurs*

*Partie 1: Exigences de haut niveau*



Reference number
ISO 31700-1:2023(E)



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) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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.

This document was prepared by Project Committee ISO/PC 317, *Consumer protection: privacy by design for consumer goods and services*.

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.

# Introduction

Consumers' trust and how well individual privacy needs are met are defining concerns for the digital economy. This includes how consumers' personally identifiable information (PII) and other data are processed (collected, used, accessed, stored, and deleted) — or intentionally not collected or processed — by the organization and by the digital goods and services within that digital economy. If PII has been compromised because of lax, outdated, or non-existent privacy practices, the consequences for the individual can be severe. In addition, consumers' trust of the digital product can be damaged with potentially legal or reputational impacts to the organization providing that consumer product.

"Privacy by Design" was originally used by the Information and Privacy Commissioner of Ontario, Canada. with the goal that the individual need not bear the burden of striving for protection when using a consumer product.

Privacy by design refers to several methodologies for product, process, system, software and service development, e.g. References [1], [2], [3], [4], [5] and [6]. These methodologies take into account the privacy of a consumer throughout the design and development of a product, considering the entire product lifecycle - from before it is placed on the market, through purchase and use by consumers, to the expected time when all instances of that product finally stop being used. It means that a product has default consumer-oriented privacy controls and settings that provide appropriate levels of privacy, without placing undue burden on the consumer.

NOTE This document provides references in the bibliography to other existing standards and resources, that provide more detailed requirements and guidance on privacy (e.g. identification of PII, PII access and privacy controls, consumer consent, notification of privacy breach, secure disposal of PII, interactions with third party processors) for common functions within the organization (e.g. Corporate Governance; Data and Privacy Governance; IT Operations and IT Services Management; Security and Security Management; Data Management and Database Administration; Marketing, Product Management; Web and mobile application development, systems development; Systems administration, network administration).

In this document, the benefits of privacy by design can be viewed through three guiding principles as outlined below.

**Empowerment and transparency**

There is growing demand for accurate privacy assertions, systematic methods of privacy due diligence, and greater transparency and accountability in the design and operation of consumer products that process PII. The goal is to promote wider adoption of privacy-aware design, earn consumer trust and satisfy consumer needs for robust privacy and data protection. In addition, the intent is to create and promote innovative solutions that protect and manage consumers' privacy: a) by analysing and implementing privacy controls based on the consumer's perspective, context, and needs, and b) by succinctly documenting and communicating directly to consumers how privacy considerations were approached.

**Institutionalization and responsibility**

In today's digital world of shared platforms, interconnected devices, cloud applications and personalization, it is increasingly important to delineate and distinguish the responsibilities and perspectives of the consumer of the products that process PII from those of product design, business and other stakeholders in the ecosystems in which the product operates.

Privacy by design focuses on the consumer perspective when institutionalizing robust privacy norms throughout the ecosystem including privacy protection and data handling practices. With privacy by design, the consumer's behavioural engagement with the product(s) and their privacy needs are considered early and throughout the product lifecycle process. This way, decisions concerning consumer privacy needs will be more consistent and systematic and become a functional requirement alongside the interests of product design, business and other stakeholders.

Privacy by design also focuses on accountability, responsibility, and leadership. These aspects are essential to successfully operationalizing and institutionalizing the privacy by design process.

A demonstrated leadership commitment to privacy by design is essential to operationalize and institutionalize privacy in the product design process of an organization.

**Ecosystem and lifecycle**

A privacy by design approach can be applied to the broader information ecosystems in which both technologies and organizations operate and function. Privacy and consumer protection benefit from taking a holistic, integrative approach that considers as many contextual factors as possible (e.g. the type of consumer, their goal and intent in using a product, and the data the product will process for that consumer) – even (or especially) when these factors lie outside the direct control of any particular actor, organization, or component in the system. [see 5.5.3 a)].

Privacy by design applies to all products that use PII, whether physical goods, or intangible services such as software as a service, or a mixture of both. It is intended to be scalable to the needs of all types of organizations in different countries and different sectors, regardless of organization size or maturity.

It is possible that additional privacy issues and a need for related controls are identified at any point in the product lifecycle, including during development or after use by consumers. Privacy by design methodologies support iterative approaches to product development, with supplementary privacy enhancements designed and deployed long after the initial design phase.

**Audience for this document**

The primary audiences for this document are those staff of organizations and third parties, who are responsible for the concept, design, manufacturing, management, testing, operation, service, maintenance and disposal of consumer goods and services.

# Consumer protection — Privacy by design for consumer goods and services —

## Part 1: High-level requirements

## 1 Scope

This document establishes high-level requirements for privacy by design to protect privacy throughout the lifecycle of a consumer product, including data processed by the consumer.

This document does not contain specific requirements for the privacy assurances and commitments that organizations can offer consumers nor does it specify particular methodologies that an organization can adopt to design and-implement privacy controls, nor the technology that can be used to operate such controls.

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

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

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

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

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

**3.1**
**consumer**
individual member of the general public purchasing or using property, products for private purposes

Note 1 to entry: "Consumer" (including elderly, children, and persons with disabilities) covers both consumers and potential consumers. Consumer products can be one-time purchases or long-term contracts or obligations.

Note 2 to entry: This term only applies to natural persons, not legal entities.

Note 3 to entry: *Property, products or services* (3.3) purchased or used by consumers can be used for professional purposes and not only private ones (e.g. Bring Your Own Device).

[SOURCE: ISO/IEC Guide 14:2018, 3.2, modified — "or serviced" has been removed from the definition, Note 1 to entry has been modified, Notes 2 and 3 to entry have been added.]

**3.2**
**personally identifiable information**
**PII**
**personal information**
information that a) can be used to establish a link between the information and the natural person to whom such information relates or b) is or can be directly or indirectly linked to a natural person

Note 1 to entry: To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

Note 2 to entry: A public cloud *PII processor* (3.18) is typically not in a position to know explicitly whether information it processes falls into any specified category unless this is made transparent by the cloud service customer.

[SOURCE: ISO/IEC 19944-1:2020, 3.3.1, modified — The admitted term has been deleted, Note 1 to entry and Note 2 to entry have been shortened.]

**3.3**
**privacy breach**
situation where *personally identifiable information* (3.2) is processed in violation of one or more relevant privacy safeguarding *requirements* (3.9)

[SOURCE: ISO/IEC 29100:2011, 2.13]

**3.4**
**service**
output of an organization with at least one activity necessarily performed between the organization and the *consumer* (3.1)

Note 1 to entry: The dominant elements of a service are generally intangible.

Note 2 to entry: A service often involves activities at the interface with the consumer to establish consumer *requirements* (3.9) as well as upon delivery of the service and can involve a continuing relationship such as banks, accountancies or public organizations, e.g. schools or hospitals.

Note 3 to entry: Provision of a service can involve, for example, the following:

— an activity performed on a consumer-supplied tangible product (e.g. a car to be repaired);

— an activity performed on a consumer-supplied intangible product (e.g. the income statement needed to prepare a tax return);

— the delivery of an intangible product (e.g. the delivery of information in the context of knowledge transmission);

— the creation of ambience for the customer (e.g. in hotels and restaurants).

Note 4 to entry: A service is generally experienced by the consumer.

[SOURCE: ISO 9000:2015, 3.7.7, modified — “customer” has been replaced with “consumer”.]

**3.5**
**privacy by design**
design methodologies in which privacy is considered and integrated into the initial design stage and throughout the complete lifecycle of products, processes or *services* (3.3) that involve processing of *personally identifiable information* (3.2), including product *retirement* (3.15) and the eventual *deletion* (3.26) of any associated *personally identifiable information* (3.2)

Note 1 to entry: The lifecycle also includes changes or updates.

**3.6**
**interested party**
**stakeholder**
person, group of people or organization (3.2.1) that has an interest in, can affect, be affected by, or perceive itself to be affected by a decision or activity

**3.7**
**consumer-configurable privacy setting**
**consumer privacy setting**
consumer privacy control
specific choices made by a *personally identifiable information* (3.2) principal about how their *personally identifiable information* is processed for a particular purpose

[SOURCE: ISO/IEC 29100:2011, 2.17, modified — Preferred term deleted, new preferred and admitted terms added.]

**3.8**
**processing of personally identifiable information**
**processing of PII**
operation or set of operations performed upon *personally identifiable information* (3.2)

Note 1 to entry: Examples of processing operations of *personally identifiable information* include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of *personally identifiable information*.

[SOURCE: ISO/IEC 29100:2011, 2.23]

**3.9**
**requirement**
statement that translates or expresses a need and its associated *constraints* (3.7) and *conditions* (3.10) in an unambiguous manner

Note 1 to entry: Requirements exist at different levels in the system structure.

Note 2 to entry: A requirement always relates to a system, software or *service* (3.4), or other item of interest.

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.19, modified – "in an unambiguous manner" has been added to the definition, Note 2 to entry has been deleted and Note 3 to entry is now Note 2 to entry.]

**3.10**
**condition**
measurable qualitative or quantitative *attribute* (3.11) that is stipulated for a *requirement* (3.9**)** and that indicates a circumstance or event under which a requirement applies

[SOURCE: ISO/IEC/IEEE 29148:2018, 3.1.6]

**3.11**
**attribute**
inherent property or characteristic of an entity that can be distinguished quantitatively or qualitatively by human or automated means

Note 1 to entry: ISO 9000 distinguishes two types of attributes: a permanent characteristic existing inherently in something; and an assigned characteristic of a product, process, or system (e.g. the price of a product, the owner of a product). The assigned characteristic is not an inherent quality characteristic of that product, process or system.

[SOURCE: ISO/IEC 25000:2014, 4.1, modified — Note 1 to entry has been removed; Note 2 to entry has become Note 1 to entry.]

**3.12**
**third party**
person or body that is independent of the *organization* (3.1)

Note 1 to entry: All business associates are third parties, but not all third parties are business associates.

Note 2 to entry: A third party can be a *personally identifiable information controller* (3.19) or a *personally identifiable information processor* (3.20) or both, depending on context.

**3.13**
**consumer product**
good or service designed and produced primarily for, but not limited to, personal or household use, including its components, parts accessories, instructions and packaging

[SOURCE: ISO 10377:2013, 2.2, modified]

**3.14**
**personally identifiable information lifecycle**
**PII lifecycle**
sequence of events from creation or origination, collection, through storage, use and transfer to eventual disposal (e.g. secure destruction) of *personally identifiable information* (3.2).

**3.15**
**retirement**
withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system

Note 1 to entry: This can include decommissioning, cessation of marketing, selling, or provision of parts, services or software updates for the product.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.39, modified — Note 1 to entry added.]

**3.16**
**privacy control**
measure that treats *privacy risks* (3.18) by reducing their likelihood or their consequences

Note 1 to entry: Privacy controls include organizational, physical and technical measures, e.g. policies, procedures, guidelines, legal contracts, management practices, data-minimizing protocols and techniques or organizational structures.

Note 2 to entry: Control is also used as a synonym for safeguard or countermeasure.

[SOURCE: ISO/IEC 29100:2011, modified — Note 1 to entry modified.]

**3.17**
**information security**
preservation of confidentiality, integrity and availability of information

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

[SOURCE: ISO/IEC 27000:2018, 3.28]

**3.18**
**privacy risk**
effect of uncertainty on privacy

Note 1 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 2 to entry: a privacy risk can be *personally identifiable information* (3.2) misuse or the risk that *consumers* (3.1) will experience adverse consequences resulting from personally identifiable information processing.

[SOURCE: ISO/IEC 29100:2011, 2.19, modified — Note 1 to entry has been deleted, Note 2 to entry has been added.]

**3.19**
**personally identifiable information controller**
**PII controller**
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information* (3.2) other than natural persons who use data for personal purposes

[SOURCE: ISO/IEC 29100:2011, 2.10, modified — Note to entry has been removed.]

**3.20**
**personally identifiable information processor**
**PII processor**
privacy stakeholder that processes *personally identifiable information* (3.2) on behalf of and in accordance with the instruction of a *PII controller* (3.19)

[SOURCE: ISO/IEC 29100:2011, 2.12]

**3.21**
**human-centred design**
approach to system design and development that aims to make interactive systems more usable by focusing on the use of the system by human beings; applying human factors, ergonomics and usability knowledge and techniques

Note 1 to entry: The term "human-centred design" is used rather than "consumer-centred design" to emphasize that design impacts a number of stakeholders, not just those typically considered as *consumer* (3.1). However, in practice, they are often used synonymously.

Note 2 to entry: Usable systems can provide a number of benefits including improved productivity, enhanced consumer wellbeing, avoidance of stress, increased accessibility, and reduced risk of harm.

[SOURCE: ISO/IEC 25063:2014, 3.6, modified — Note 1 to entry has been modified.]

**3.22**
**use case**
description of a sequence of interactions of a *consumer* (3.1) and a consumer product used to help identify, clarify, and organize *requirements* (3.9) to support a specific business goal

Note 1 to entry: Consumer can be users, engineers, systems.

[SOURCE: ISO/TR 14872:2019, 3.9, modified — "user" has been changed to "consumer", "system" has been changed to "consumer product" and Note to entry has been added.]

**3.23**
**consumer vulnerability**
state in which an individual can be placed at a disadvantage, or at risk of detriment, during his/her interaction with a service provider due to the presence of personal, situational and market environment factors

Note 1 to entry: Anyone can be vulnerable at any time. Vulnerability can be temporary or permanent.

Note 2 to entry: Factors that contribute to consumer vulnerability can be personal (e.g. health, illness, injuries, disability, impairment) or situational (e.g. job loss, bereavement, low-level of literacy).

Note 3 to entry: An organization's processes and procedures can reduce or exacerbate consumer vulnerability.

Note 4 to entry: A consumer when vulnerable can:

— be at higher risk of experiencing negative outcomes when interacting with service providers;

— have limited ability to maximize his/her wellbeing;

— have difficulty in obtaining or assimilating information;

— be less able to buy, choose or access suitable services;

— be more susceptible to certain marketing practices

Note 5 to entry: Market environment factors include but are not limited to: demographic factors, ecological factors. economic factors, socio-cultural factors, political and legal factors, international environments, technological factors

[SOURCE: ISO/IEC Guide 76:2020, 3.14, modified — Note 5 to entry has been added.]

**3.24**
**accountable person**
designated person for the correct and thorough completion of a specified deliverable or task, who ensures the prerequisites of the task are met, who delegates the work to the *responsible party* (3.25) and signs off (approves) work of the responsible party

**3.25**
**responsible party**
person or persons who complete a delegated task or specified deliverable

Note 1 to entry: The responsible party can be one role or a shared role, although others may be delegated to assist in the work required.

**3.26**
**deletion**
process by which *personally identifiable information* (*PII)* (3.2) is changed in a manner so that it is no longer present, recognizable or usable and can only be reconstructed with excessive effort

Note 1 to entry: The term "deletion" covers the following: disposition mechanism, erasure, destruction, destruction of data storage media.

Note 2 to entry: The term "deletion" refers to the elimination of the bit patterns or comparable practices, not simply marking or moving the data to be hidden. As a result, excessive effort for PII reconstruction will be required, considering all the means likely reasonably to be used, e. g. available state of the art of technology, human and technical resources, costs and time.

Note 3 to entry: For selecting the methods for deletion, a risk-based approach shall be taken into account, including sensitivity of PII and potential use of forensic tools. Required measures may change during time depending on the state of the art of technology and other factors.

Note 4 to entry: PII can also be changed by applying irreversible de-identification techniques. Such data often fall out of privacy legislation.

Note 5 to entry: De-identification techniques can be found in ISO/IEC 20889.

**3.27**
**privacy risk assessment**
overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment and mitigation with regard to the processing of *personally identifiable information* (3.2), framed within an organization's broader risk management framework

Note 1 to entry: This process can be documented in various ways, including with a privacy impact assessment.

[SOURCE: ISO/IEC 29100:2011/Amd.1:2018, 2.20, modified — The admitted term "privacy impact assessment" has been removed and Note 1 to entry has been added.]

**3.28**
**documented information**
artefact
information required to be controlled and maintained by an organization 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, including related processes;

— information created in order for the organization to operate (documentation);

— evidence of results achieved (records).

[SOURCE: ISO/IEC 27000:2018, 3.19]

**3.29**
**information security management**
managing the preservation of confidentiality, integrity and availability of information

[SOURCE: ISO/IEC TR 27016:2014, 3.12]

**3.30**
**vulnerable consumer**
*consumer* (3.1) who could be at greater risk of harm from products due, for example, to their age, level of literacy (including technological literacy), physical condition or limitations, or inability to access product safety information and who could be permanently or temporarily unable to represent their own interests for example, through a mental, emotional, societal or physical cause that may limit their capacity to make voluntary and informed decisions

**3.31**
**change management**
judicious use of means to effect a change or a proposed change, to a product or service

[SOURCE: ISO/IEC/IEEE 24765:2017]

**3.32**
**personally identifiable information principal**
**PII principal**
natural person to whom the personally identifiable information relates

[SOURCE: ISO/IEC 29100:2011, modified — Note to entry deleted.]

**3.33**
**end of use**
status of a product that is no longer utilized by a consumer

Note 1 to entry: End of use can occur for a multitude of reasons, including but not limited to: product is broken, it no longer functions properly, it no longer satisfies the *consumer's* (3.1) *requirement* (3.9), the consumer is deceased or incapacitated, the product has been recycled or destroyed, or the consumer passed the product to other consumers through gifts or second-hand markets.

**3.34**
**cybersecurity**
protection of an IT-system from attacks or damage to its hardware, software or information, as well as from disruption or misdirection of the *services* (3.3) it provides

[SOURCE: ISO/TR 22100-4:2018, 3.10, modified — The preferred term "Information Technology security" has been deleted.]

**3.35**
**risk**
effect of uncertainty on objectives

[SOURCE: ISO/IEC Guide 73:2009, 1.1, modified — Notes to entry have been delete.]

# 4 General

## 4.1 Overview

In order to implement and adhere to privacy by design for consumer products, there are requirements to be met by those involved in or contributing to designing, selling, or managing consumer products that process PII throughout their lifecycle. Consumer privacy rights and preferences can play an important and informative role when defining privacy requirements for the consumer product.

PII has a lifecycle, from creation or origination, collection, through storage, use and transfer to its eventual disposal (e.g. secure destruction). The value of PII and related risks to the consumer can vary during the PII lifecycle, but protection of the consumer remains important at all stages and in all contexts of its lifecycle.

Information systems also have lifecycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained, and eventually retired from service and disposed of. PII protection can also be taken into account at each of these stages. New system developments and changes to existing systems present opportunities for organizations to update and improve privacy and the associated security controls. This can be achieved by taking into account current and projected privacy and information security risks and actual incidents should they arise[7].

As illustrated in Figure 1, the PII lifecycle and the product lifecycle are not one and the same. The product lifecycle starts with the inception or ideation of a product and ends with product destruction or disposal. This can occur even after support for the product has ended and after the consumer has retired the product. The arc of the PII lifecycle extends from the creation or collection of PII by a product to its destruction or disposal. Sometimes the PII lifecycle extends beyond the product lifecycle. For a product to be designed with privacy in mind, its designers need to understand both lifecycles for the product being designed and the requirements for both that protect the privacy and the PII of the consumers of the product and those who interact with it throughout both lifecycles.

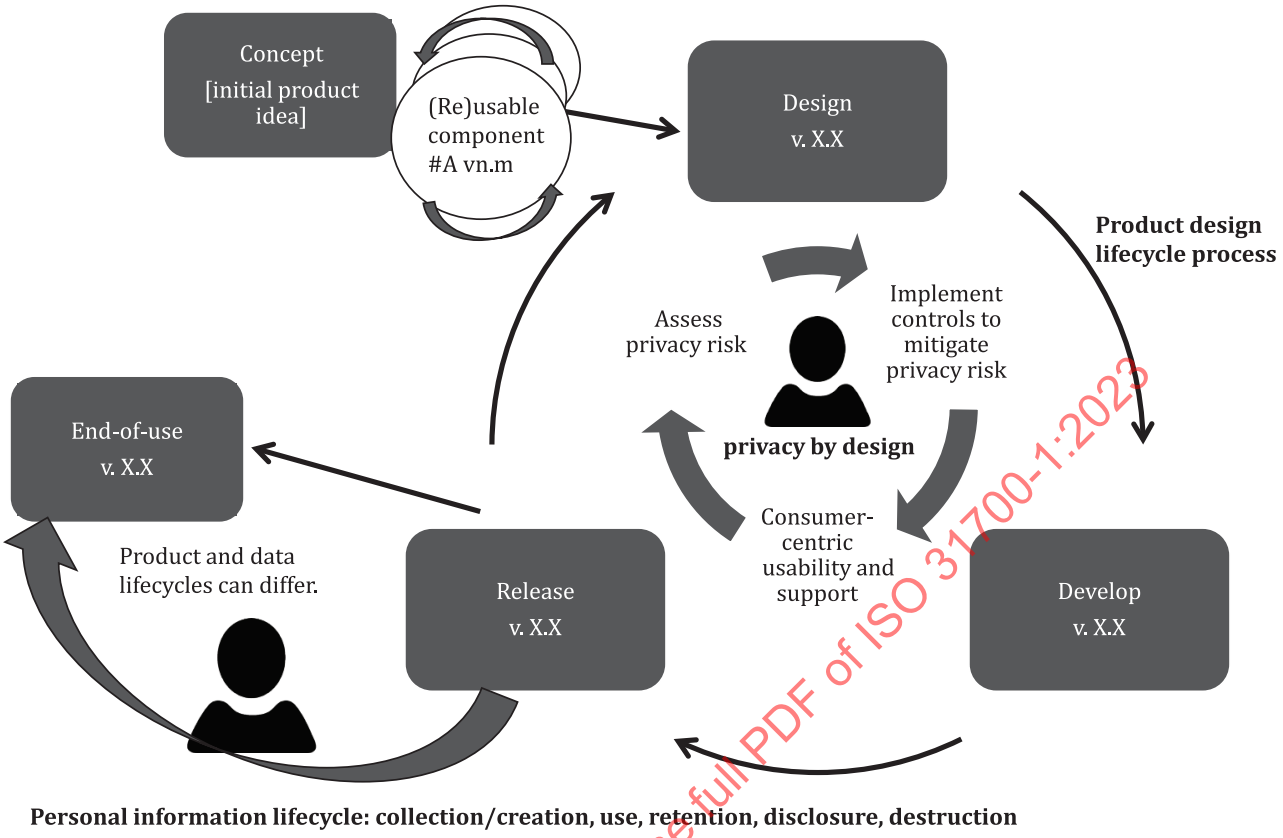


**Figure 1 — Personally identifiable information and product lifecycles**

## 4.2 Designing capabilities to enable consumers to enforce their privacy rights

### 4.2.1 Requirement

The organization shall implement the means by which the consumer can exercise their privacy rights and prerogatives.

Note 1 The means can include, but are not limited to: the design, the features, the operation of the controls, the proven effectiveness of the product.

Note 2 It is presupposed that it is done in compliance with the relevant regulations and requirements where the consumer product is sold or distributed.

### 4.2.2 Explanation

Many decisions regarding consumer PII do not rest solely with the organization. Decisions about PII are governed by law or regulation, by cultural norms, by unilateral policy, by contract, by economics, or by technical controls that implement individual consent and personal preferences (see 4.3.1)[8][9][10][11][12][13][14].

The use of the product by consumers will also place obligations on the organization to respect consumer privacy rights. Privacy rights include, for example, individual control of PII; consent provision or revocation; receipt of information through privacy notices, explanatory text, or other documentation; access to PII; portability; rights for data erasure and correction. These obligations can be onerous for the organization or can be designed to be relatively effortless. Unless the organization understands the consumer's role in the organization's fulfilment of these obligations, the organization can waste considerable resources, while not meeting its obligations.

Due to their effect or potential effect on the organization's ability to consistently provide products that meet consumer and applicable statutory and regulatory requirements, it is important to include privacy needs of consumers into the organization's process of examining those of interested parties. Consumer empowerment involves the ability to play a participatory role and to exercise effective privacy rights throughout the lifecycle of their own PII that is processed by the product.

### 4.2.3 Guidance

a) The organization should follow a privacy information management system.

NOTE ISO/IEC 27701 and the NIST Privacy Framework provide more explanation on privacy management[15][16].

b) The organization should identify the factors impacting their products related to consumers' privacy rights. Such factors can include legal requirements, cultural norms, unilateral policy, contracts, economics, and available technology. In doing so the organization should involve subject-matter-experts.

c) The organization should determine if it falls under any codified role (e.g. personally identifiable information controller or personally identifiable information processor) because such roles can impose specific legal obligations with respect to the consumer.

d) The organisation should implement supply chain privacy and security best practices and measures to allow consumers to exercise their rights and prerogatives.

e) Access to PII, including collection and processing, should be granted only to authorized staff with an organizational need for the data as determined by privacy policies.

f) The organization should consider usability and the overall consumer experience when determining both product features and privacy by design frameworks and protections.

g) The organization should provide a genuinely informative privacy statement explaining in clear simple terms, among other things, how the consumer can exercise their privacy rights before the applicable product collects the consumer's personal information, see ISO/IEC 29184 [17].

h) A consumer product should access, collect, use, disclose, transfer or store only the minimum information required to provision, operate or maintain the product; to meet identified organization purposes.

i) Company commitments (e.g. privacy policy or public statements) should be reviewed when configuring consumer privacy settings in new or modified products and updated. It is presupposed that this review is to ensure there are no violations of company commitments to consumers or applicable statutory and regulatory requirements.

j) When the consumer makes a request, the organization should be able to locate all of a consumer's relevant PII and perform the necessary actions (e.g. hard delete, export, restrict, correct) in a scalable, timely and secure manner.

k) After product retirement, the organization should process only the minimum PII required to meet identified organization purposes and should promptly and securely delete all PII that is not needed to uphold those requirements[59]. It is presupposed that these purposes are consistent with applicable legal or contractual requirements.

## 4.3 Developing capability to determine consumer privacy preferences

### 4.3.1 Requirement

The organization shall determine consumer needs related to processing of their PII by products designed and developed for consumers.

### 4.3.2 Explanation

PII processing enables the product to function and the organization to support the consumer during the product's lifecycle. Unless the organization has a clear view about consumers' privacy preferences, it will be difficult to design the product to address these preferences in a way that both protects the consumer's privacy and enables the organization to meet its other obligations. In addition, IP addresses, MAC addresses and other types of information that was once considered machine data or telemetry data are now considered PII in many jurisdictions if such information can be reasonably linked to a consumer's device. Consumers can have very different levels of insight into the existing and emerging interconnectedness of 'networks' (communication, social, personal. etc.), information communication technologies (ICTs) and other digital components of products with which a consumer interacts. Advances in computing therefore impact consumers privacy expectations: for example but not limited to, a set of information that appears not to identify a consumer, when linked with other sets of information, could allow the identification of the consumer, could reveal personal information about the consumer (for example, their behaviour, personal history, relationships or location) or could distort personal information about the consumer through adding false details. Consumers have a range of capabilities and vulnerabilities[18][19][20][21] that will affect how they interact with the product and its privacy controls. Unless the organization understands its consumers well, it cannot be certain that the design of those privacy controls that require consumer action or inaction will operate as designed.

NOTE For further information on consumer vulnerability and vulnerable situation refer to ISO 22458[18] and ISO/IEC Guide 76[19].

### 4.3.3 Guidance

a) Consumer privacy preferences and needs should play an important and informative role when defining privacy requirements for the consumer product (see 4.4.1).

b) Consumers' views and preferences should be sought as part of the product design process to ensure that the product's privacy controls will operate as designed, in a way that provides a beneficial user experience for consumers that respects the sensitivity of their data and their privacy rights and needs[21].

c) The organization should understand how the consumer uses privacy controls so that the product's privacy controls can remain effective notwithstanding the actions or inactions of consumers

d) The organization should consider its existing and future consumers as a key resource in the product lifecycle. This can take the form of a formal approach to engage with consumers for example, from the simple provision of careful analysis of inputs from easy-to-use feedback mechanisms to the most thorough (and expensive) user research by professional privacy-literate user researchers deploying rigorous privacy research methodologies.

e) If the product has privacy controls that can be operated by the consumer, the consumer should be advised how to operate them, in order to prevent errors, either knowingly or unknowingly. These errors can include but are not limited to data processing that goes against a consumer's wishes if the consumer: unknowingly clicked the wrong option; did not understand the effect or implication of enabling or disabling a particular setting or control on the further handling of their personal information; or their location unknowingly being tracked by default by the product.

f) The organization should have a clear view about consumers' privacy preferences. If it does not, it will be difficult to design the product to address these preferences in a way that both protects the consumer privacy and enables the organization to meet its other obligations.

## 4.4 Designing human computer interface (HCI) for privacy

### 4.4.1 Requirement

The organization shall design consumer-configurable privacy settings and privacy management measures taking account of the capabilities of consumers and their potential disabilities.

### 4.4.2 Explanation

Using human-centred design benefits not only the consumer but has substantial economic value for organizations. Highly usable systems, services and goods tend to be more successful both technically and commercially.

Empowering consumers to manage their own data as well as privacy controls and preferences is a critical check against abuses and misuses of PII. Consumer understanding of how and in what context their PII is being processed by the product – and giving them some level of control – is a fundamental underpinning for transparency and trust.

Where a consumer operates privacy controls over the product, these need to be defined, documented in the use cases[22][72], and designed to take into account consumer experience, human factors, and the wide range of potential consumers capabilities, experiences and disabilities as they relate to the product's capabilities.

Use cases[23] describe the use of the product by the consumer and influence the analysis of privacy risks to consumers. Defining the central use cases allows the product designers to explore the peripheral use cases and those that represent abuse and misuse cases. Use cases can be used to identify consumer privacy needs that arise from consumer interactions and known technical and consumer vulnerabilities.

### 4.4.3 Guidance

a) Consumer control and choice should be clear and evident in the design of consumer-configurable privacy setting.

b) Designing consumer-configurable privacy settings should adopt privacy engineering techniques[21].

c) Product design can convey the context for processing of PII. Product development teams should avoid design practices that have the potential to impede transparency, exploit ambiguity and create a negative consumer experience as it relates to use of PII. This requires careful consideration of privacy controls in all product development stages, including consumer experience and systems design, to ensure consumers do not unwittingly share PII, prevents them from managing how their PII might be processed or results in unexpected uses of their PII.

## 4.5 Assigning relevant roles and authorities

### 4.5.1 Requirement

The organization shall assign and maintain roles and responsibilities, including at least one accountable person for the overview of the entire PII and product lifecycle with responsibility for ensuring the management of privacy risks and controls for the PII throughout the PII lifecycle.

### 4.5.2 Explanation

Roles and authorities over a consumer product's lifecycle and its PII lifecycle, inform risk management and provide accountability for the privacy controls associated with the product.

### 4.5.3 Guidance

a) The accountable person's role should include the privacy status, which can include but is not limited to the current status of processing or use of the data, the identifiability state of the data (raw, pseudonymized/de-identified, anonymized), the intended deletion date of the PII associated with a product. This role can contribute to a product's lifecycle and the lifecycle of the PII it processes, to ensure the effectiveness of all the product's privacy controls. An accountable person can include but is not limited to: incident response coordinators, production manager and consumer communication.

b) Accountability and responsibilities should be clearly defined, adequately resourced, and periodically reviewed for efficacy.

## 4.6 Establishing multi-functional responsibilities

### 4.6.1 Requirement

The organization shall designate an accountable person for each function or organization that contributes to the design or operation of privacy controls or manages the processing of the PII by the product.

### 4.6.2 Explanation

While the accountable person is responsible for the overall effectiveness of the product's privacy controls, the design and operation often require the contribution of expertise from multiple functions, and from multiple organizations. Sometimes teams are formed by combining multiple functional teams into one. These multi-functional teams are composed of experts from various functional areas and work cooperatively towards some organizational goal.

Ensuring that privacy is an integral part of the design process requires multi-functional expertise. Integrated design teams expose engineers to other non-technical perspectives (e.g. legal, consumer) and vice versa, thereby helping to embed strong privacy norms among the technical specialists whose focus is generally on security.

Multifunctional development teams can include both security and privacy experts when designing privacy into consumer products given that privacy risks arise not only from cybersecurity related incidents but also from authorized PII processing.

Nonetheless, privacy and information security are both integral together as a coherent control mechanism. Privacy principles include information security and requirements for reasonable safeguards for PII, that include, but are not limited to: controls, mechanisms and technical protections. Privacy helps to safeguard important values such as human autonomy and dignity. Guiding decisions can result from robust ethical norms, principles, practices, and organizational policies. Governance mechanisms can uphold, maintain, and evolve those norms, principles, and practices. Information security seeks to enable and protect activities and assets of both people and enterprises from a loss of confidentiality, integrity, and availability[25][26].

### 4.6.3 Guidance

a) Senior roles within each function and organization that contribute expertise to the design or operation of privacy controls should be designated to represent and take responsibility for those contributions.

b) The roles should be sufficiently senior to ensure that the importance of privacy can be appropriately included alongside other operational priorities.

## 4.7 Developing privacy knowledge, skill and ability

### 4.7.1 Requirement

Persons with the responsibility or accountability for the design and operation of privacy controls shall ensure necessary training is available to help ensure teams have the knowledge, skills, and capabilities to carry out their roles effectively.

### 4.7.2 Explanation

Knowledge of privacy by design and the ability to apply it to systems, components, products, and services are important skills for privacy staff, including the accountable person and responsible party[27][28].

### 4.7.3 Guidance

a) The organization should tailor the approach to training the accountable person and responsible party in privacy by design in accordance with the objectives of the training.

b) The organization should monitor the impact of the training to establish its long-term effectiveness, and review and revise the training to keep it up to date.

c) Training should address all aspects of the PII lifecycle, and, for example, scope of PII, types and classification of data processed; use cases; policies around data at employee devices, tools to share data, data at company supplied tools (e.g. email, chat); and how to contact the privacy team for follow-up questions.

d) Staff engaged in data processing should receive privacy awareness education and training to carry out privacy-related duties and responsibilities consistent with the organization's policies, processes, procedures, and privacy values.

e) Staff who operate processes for the organization to discharge its obligations to consumers, such as enabling consumers to exercise their privacy rights or preferences, should also be trained and sufficiently capable.

f) Staff contributing to the design and execution of the product should be made aware of their privacy responsibilities and those who provide specialist contributions trained in how to do this effectively.

g) Knowledge, skills and capability in privacy by design, should also be incorporated into contracts and service level agreements with third parties including those to whom PII is transferred.

h) Training should include sharing of good practice and extend to those who contribute from third parties including those to whom PII is transferred.

## 4.8 Ensuring knowledge of privacy controls

### 4.8.1 Requirement

Persons with the responsibility or accountability for the design and operation of privacy controls shall ensure necessary training is available to help ensure teams are adequately knowledgeable in both the privacy requirements of the product and the organization’s privacy policies and procedures.

### 4.8.2 Explanation

The organization will need to have privacy expertise available if it is to lead efforts in disseminating knowledge to staff involved in the design and development of products and its data lifecycle. This expertise can reside in-house or can be external to the organization. The dissemination of knowledge[29] of the privacy controls for the product and the organization’s privacy policies needs to occur prior to and during a project to allow staff to integrate this knowledge with their core skills. This will allow them to identify the best means for implementing privacy controls as part of the product development and ensure they align with the organization’s privacy objectives. Appropriate resources should be made available to staff to ensure questions can be addressed as required throughout the product development stages and in the ongoing product and PII lifecycles.

Below, by category of control, are lists of controls the accountable person can be knowledgeable of and ensure their teams have sufficient skill and knowledge of.

Compliance and administrative controls include, for example, privacy awareness and training, privacy impact assessments, governance and privacy program, records of processing activities, consent text, data processing agreement, binding corporate rules, 3rd party controls or agreements

Technical controls include, for example, physical device controls, Time to Live (TTL, a mechanism that limits the lifespan of data in a computer or network), PII encryption (in transit and at rest), de-identification and anonymization, access controls, other privacy enhancing technologies.

Privacy enhancing services can include but are not limited to a consent toolkit or framework, PII deletion service, PII export service, PII encryption service, de-identification or anonymization tools, up-to-date PII inventory, consumer PII locator.

The accountable person is supported by various privacy specialists that support accomplishing the following tasks:

— recommendations on compliance controls based on legal, policies, requirements and privacy risk assessments;

— recommendations on and standardizing technical controls, tools and other supports during the implementation of controls, identification of privacy gaps in platforms, and leading platform controls;

— maintaining the overall privacy program and privacy projects across the organization;

— ensuring technical controls are tracked, prioritized, so that progress is made and implemented across the organization, for example, data retention across the organization, data inventory projects, data export or deletion projects.

### 4.8.3 Guidance

a) Each responsible party that contributes expertise should be trained in privacy to ensure that good practice is incorporated into the product in a structured, transparent way.

b) Each responsible party that contributes expertise should have appropriate privacy expertise and understanding of the process to ensure that good privacy practices are incorporated into the product in a structured way.

c) Legal and regulatory obligations associated with the product together with the voluntary privacy policies that the organization chooses to adopt for its product should constitute the source of the privacy control objectives for the product. These are the objectives that will guide designers and developers in the design of privacy controls.

## 4.9 Documentation and information management

### 4.9.1 Requirement

The organization shall create and maintain documented information to demonstrate that the design and operation of privacy controls are effective.

### 4.9.2 Explanation

If the design and operation of a product's privacy controls are going to be embedded into the product's lifecycle, then documentation from the design stage will capture the key information that will be used by staff of the organization and third parties later in the lifecycle. Documented information often takes the form of a living document that is updated with details of the design of the privacy controls, information on their testing, and their operation later in the lifecycle.

The organization maintains documented information (e.g. policies, procedures, instructions to follow) and stores records for tracking the performed activities. This helps when employees carry on the activities (because they need to know the policies, procedures and instructions and to review the

records of the previous tasks or of similar activities). Documented information for the privacy by design for consumer products can include[30] the following:

— privacy risk assessment;

— PII / data flow or map;

— functional and non-functional privacy requirements of the product and service;

— privacy controls to be implemented in the product and service;

— test results, acceptance decisions and authorizations for the delivery;

— communication to the consumers with regards to privacy.

### 4.9.3 Guidance

a) The organization should manage documented information that is approved by relevant authorities; and is readable by and made available to all intended recipients.

NOTE For more information regarding documented information using a Privacy Information Management system or Information Security Management system, refer to ISO/IEC 27701, ISO/IEC 27001 and ISO/IEC 27002.

b) Documented information should be controlled to ensure that it is available and suitable for use, where and when it is needed, and is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

c) For the control of documented information, the organization should address the following activities, as applicable:

— distribution, access, retrieval and use;

— storage and preservation, including the preservation of legibility;

— control of changes (e.g. version control);

— retention and disposition.

d) Documented information of external origin, determined by the organization to be necessary for the planning and operation of privacy controls, should be identified as appropriate, and controlled.

## 5 Consumer communication requirements

### 5.1 Overview

Consumers of products that process PII expect information at the point of collection or when a privacy impacting decision can be made, that contains clear, concise, accessible, meaningful, and verifiable explanations and commitments about how and why a product will or will not process PII and manage privacy. The objective is to facilitate confident, informed decision-making by the consumer prior to acquisition or use. Consumers of products that process PII also want to know when incidents or errors in how their PII is processed puts them or their PII at risk, or when there are changes in the purposes for which their PII will be processed.

Transparency and consumer communications support accountability. They enable consumers and others to compare actual processing details with such explanations and commitments and take action (i.e. file a complaint or stop using the product) and challenge the accountable person when warranted. They take many forms from consumer-interfaces, help files, and product documentation through packaging, marketing content, and consumer service scripts to FAQs, notices, and policies.

Opportunities for transparency and consumer communications present themselves throughout the consumer facing elements of the product's lifecycle and its ecosystem. The accountable person can have consumer-facing responsibilities for creating privacy focused communications, notices and documentation about the product. The responsible party that creates create consumer privacy focused communications, notices and documentation about the product can be one in the same with the accountable person (see 4.6.1).

## 5.2 Provision of privacy information

### 5.2.1 Requirement

The organization shall inform users about the product's consumer-configurable privacy settings. The organization shall maintain and make available information on the product's privacy settings or features to other users so that they can configure the product according to their privacy objectives.

### 5.2.2 Explanation

Once the product is released to consumers, the organization's ability to change its controls can be limited. Unless the pre-release process of testing the operation of the product's controls is robust, products can be released that fail to manage their privacy risks appropriately.

Consumers need to be aware of how a product processes PII in order to make informed decisions to use or acquire products that process PII. Usually, this transparency and communication takes the form of a manual on the product's privacy settings or features, privacy notices[17] and/or product documentation that explains aspects of how the product processes PII; contracts and SLAs; instructions for requiring support or sending complaints; it also takes the form of user-interface labels, packaging, and marketing statements.

NOTE Further information on contents of online privacy notices is provided by ISO/IEC 29184.

During the product support period, keeping the consumer informed of changes to privacy risks helps them to be empowered to manage those risks effectively. Unless this communication is designed to be effective, consumers can find that the product exposes them to significant residual privacy risks.

Support can include technical fixes to software or hardware that change the privacy controls built into the product during development.

Consumers will often need support to understand how to install, setup and operate a product and if they have issues or complaints. Consumer products often involve services that are supplied by different providers and this needs to be made clear to the consumer so that they know who to contact and who is responsible. Ensuring that consumers are aware of where to get support and that the support activities will act to protect their privacy is necessary to maintain consumer trust and confidence in third parties.

### 5.2.3 Guidance

a) The source information for privacy focused communications, notices, and documentation should include the following:

   — brief, coherent overview of the product's privacy settings or features, including the consequences of re-configuring them from their default privacy protective settings;

   — privacy notices and/or product documentation that explain aspect of how the product processes PII; this will include PII processed, purposes for which the PII is processed; with whom the data is shared (and for what purposes);

   — contracts and SLAs;

   — instructions for requesting support or sending complaints and how the consumer can exercise available privacy rights;

- controls that are enabled as part of the product design to protect the PII and the consumer from unfair and unauthorized access and use of the PII;
- machine learning transparency, for example but not limited to: in models where it is clear which version of the model is in use; what the model is intended to do and who created the model for which purposes; in datasets where it is clear how the PII was collected whether it was cleaned or not and whether it was checked for bias; in traceability, to find which model (including the version) and which datasets and PII were used during an algorithmic decision;
- entity that is responsible for deciding how the PII will be processed and for incident and privacy breach management notification responses.

b) Business models should be identified when data is collected and passed to third parties for commercial, i.e. profit, purposes.

c) The communication strategy should not only consider the sensitive nature of the data collected by the product used by people with disabilities and the diversity of consumers' needs (e.g. auditory, visual or haptic), but also incorporate such considerations when developing privacy disclosures, notices, and other controls within the product.

d) The organization should appoint appropriate roles for the maintenance of such documentation.

e) The public point of contact should include the organization's identity, geographical address, and contact information, and information on when a consumer can expect to receive a response.

f) The organization should plan for, design and operate controls over consumers' digital legacy[31] where a consumer dies, and communicate these to consumers.

g) The organization should ensure communication outlines how they plan, design, and operate privacy controls over users' digital legacy[31] and guidance on how consumers can implement these controls.

h) The multi-functional team should determine a pre-withdrawal period during which consumers will be notified of the planned retirement of the product.

i) Product end of life withdrawal consumer information should include the following:

- best before dates/shelf lives for physical products[32];
- consumer options if they are to continue using the product[32];
- any consumer alternative products;
- consumer feedback mechanisms if product end of life actions present unanticipated difficulties for consumers;
- the fact that the organization will continue to retain/process PII;
- purpose of retaining/processing PII after product end of life;
- types of PII;
- retention (or the criteria used to determine the retention period).

## 5.3 Accountability for providing privacy information

### 5.3.1 Requirement

The accountable person shall ensure that the consumer-facing responsible party provides privacy notices or documentation so consumers understand how their PII will be processed throughout the PII lifecycle.

### 5.3.2 Explanation

This ensures that products that process PII are designed with consideration and ensures that consumers of such products will have access to information on how their PII is processed in such products. In some cases, the accountable person with consumer-facing responsibilities will be one in the same with the party that is responsible for designing the product (or iterations/upgrades of the product).

### 5.3.3 Guidance

a) These communications, notices, or documentation should be available to consumers prior to sale or license of the product and throughout product and its PII lifecycle.

b) The multi-functional team should notify consumers, sales and support of privacy protecting actions that they might need to take as a result of ceasing sales, support or organizational processing of product data.

NOTE ISO/IEC 29184 provides more explanations on good practices to follow for providing notices.

## 5.4 Responding to consumer inquiries and complaints

### 5.4.1 Requirement

The accountable person shall provide the consumer-facing responsible party both the resources and means of escalation for effectively responding to consumer inquiries and complaints about the processing of their PII[33][34][35][36][37].

### 5.4.2 Explanation

As issues arise and need clarification, the accountable person has an obligation to support the consumer facing responsible party.

### 5.4.3 Guidance

a) Such resources should include the following:

— training and documentation for consumer and technical support activity instructions (including maintaining privacy during support operations);

— FAQ on technical issues and consumer use issues related to privacy controls within the product;

— independent alternative mechanisms available to consumers where complaints cannot be resolved directly;

— instructions on where and how a consumer can go for assistance.

## 5.5 Communicating to diverse consumer population

### 5.5.1 Requirement

The organization shall communicate with consumers through a range of channels, media and languages in the markets for which the product is designed, in a way that does not restrict consumers understanding the product, its privacy settings, and how their PII is processed.

### 5.5.2 Explanation

Ensuring that consumers receive documentation that they can understand and are aware of where to get support and that the support activities will act to their needs.

As part of privacy by design, the organization that designed the product, has a responsibility to ensure consumers who purchase or use the product have a mechanism through which they can communicate with the re-seller or manufacturing organization regarding privacy questions or complaints up to and including after product retirement, the nominal end of life or termination of support.

### 5.5.3 Guidance

a) Privacy settings and privacy management measures should take into account the characteristics of the target consumers including vulnerable consumers in the target group. In particular, it is important to consider minors, elderly, and people with low IT-literacy.

b) The organization should ensure by contract (if it is a third party) or internal SLA (if it is a member of the same organization), that the consumer-facing responsible party provides consumers of the product a means of asking questions, filing complaints, seeking support, or having their privacy rights addressed.

c) Clear and easily understandable documentation should be written and made easily accessible to relevant consumers, including considerations for vulnerable consumers and the language of countries where the product or service is promoted. Documentation can include: documents related to privacy settings and controls, PII processing, the purpose and relevant protections to reduce privacy-related harm of PII processing.

d) Communications with consumers should be enabled through a diverse set of communication channels, enabling comments, questions for resolution, and complaints.

e) The effectiveness of these channels should be monitored, reviewed, and revised to ensure that they provide an acceptable consumer experience for consumers of the product.

## 5.6 Prepare data breach communications

### 5.6.1 Requirement

The organization shall create, test, and maintain resilient arrangements for communications with stakeholders after a privacy breach.

### 5.6.2 Explanation

Communication with product consumers in the event of a privacy breach is critical to ensuring that those affected are empowered to manage any residual privacy risks.[36][37] In addition, regulators can also set deadlines for organizations to report privacy breaches.

NOTE Refer to ISO/IEC 27035-1 and ISO/IEC 27035-2.

### 5.6.3 Guidance

a) The organization should consider including, among others, the following:

- what content is covered in the communication (e.g. cause, type of data breached, what actions a consumer can take, what actions were taken by the organization, contact for further information);
- what communication channel they use to communicate to affected individuals (e.g. email);
- what if the organization does not possess contact info;
- who sends the notification and when;
- in what languages notification is prepared;
- who signs off the communication

b) This communication should be prepared in advance and form part of the preparations for privacy breach management.

# 6 Risk management requirements

## 6.1 Overview

Like other operational risks, PII processing benefits from a risk management approach.[38][39] Proactively and effectively managing and mitigating privacy risks in an effort to prevent a privacy breach or adverse consequences reflects privacy by design. The purpose of risk management in this context is to control the privacy risks to which the consumers are exposed in relation to the consumer products in question.

Information about the ecosystem in which the product is designed and operates can inform the scope and scale of potential privacy risk. For example, the acceptance criteria against which the organization can evaluate the significance of privacy risks identified in the risk assessment in order to make decisions regarding risk acceptance or treatment. Organizations can communicate the criteria with PII principals and other stakeholders. Where direct communication is infeasible, transparency and feedback mechanisms can be employed.

The privacy risks associated with consumer products can take into consideration privacy events as potential problems individuals can experience, arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete lifecycle, from data collection through disposal[16].

For sources of privacy risks to consider during an assessment, organizations can reference internal risk registers if used by the organization, and external resources[43].

Any use of consumers' PII that is associated with a consumer product, whether or not a consumer directly uses the product, can incorporate privacy by design.

Privacy risk management guidance and resources[39][41][42][45][46][47] occur globally in a number of documents and standards and can be mandated by various data protection authorities[41].

## 6.2 Conducting a privacy risk assessment

### 6.2.1 Requirement

The organization shall take a structured approach to privacy risk assessment that demonstrates that privacy risks have been sufficiently taken into account in the design and operation of privacy controls throughout the PII lifecycle.

### 6.2.2 Explanation

Privacy risk assessments help an organization identify privacy risks engendered by the product, prioritize them, and determine appropriate risk management approaches to accept, avoid, mitigate, treat or transfer each risk. Risk treatment (including risk reduction) or acceptance decisions are made based on established risk criteria. Some identified risks can be escalated or delegated to others for decision-making outside of the accountable person due to lack or authority or resources. This process can be documented in various ways, including with a privacy impact assessment[44][45][46].

There are a variety of inputs that are useful for conducting a privacy risk assessment. These include understanding the ecosystem in which the product will operate, establishing risk criteria, and selecting a risk assessment methodology as well as more tangible inputs such as a data map, product use cases, and a set of privacy requirements relevant to the product.

Documented information provides the foundation of context, process, and boundaries for an informed privacy risk assessment, and supports continuous risk management. Documented information includes

explicit documentation of functional and non-functional privacy requirements. Examples of documented information representations include, for example, spreadsheet documentation of compliance tasks and processes, those components of consumer stories, use cases, misuse cases, interface design, data flow diagram, sequence diagrams or activity diagrams that clearly show embedding of privacy requirements, business model diagrams that show PII flows across technology platforms, and diagrams of privacy architectures. Organizational privacy-related documentation (e.g. privacy policies, privacy training materials, documentation of go-to personnel for privacy consultations) can form part of a larger, organization-wide privacy information management approach.

### 6.2.3 Guidance

a) Privacy risk assessments should produce a prioritized set of risks to help organizations to weigh the benefits of the PII processing against the risks and to individuals and determine the appropriate response (e.g. risk treatment or acceptance determinations based on the organization's risk tolerance).

b) The organization should conduct a privacy risk assessment prior to the production or release of the consumer product.

c) A data map or records of processing activities should be produced. These can be a useful input because they illustrate the context and flow of PII processing, including potential unanticipated consequences of a particular proposed flow, such as the unexpected joining of logs data through a common identifier, or unintended commingling of data in a shared storage container, can be illustrated in different ways, and can contain varying levels of detail based on organizational needs. Data maps can include the operating environment, the owners or operators of these components, specific type of processing across the PII lifecycle, and specific elements of PII being processed across the lifecycle of the consumer product.

d) Privacy requirements relevant to the product should be derived initially, from a variety of sources, including legal environment (e.g. laws, regulations, contracts), organizational policies or cultural values, relevant standards, and privacy principles. The more sensitive the information or the higher the risk to rights of individuals, the greater the obligation on the organization to take measures to protect data and to show this is considered and effected at the time of design. These requirements are updated or expanded upon based on the results of privacy risk assessments.

e) The organization should assess privacy risks introduced by the use of third parties including those to whom PII is transferred in the product lifecycle.

f) Retirement privacy risks should be considered for the product and PII throughout the product's ecosystem.

g) The organization should assess risks of retaining PII associated with the product after retirement and after consumer end of use (see Clause 8).

h) The potential privacy risks inherent in the technology used should also be an input in the privacy risk assessment, especially when incorporating new technologies into the product.

i) Consumer privacy needs can be useful inputs to privacy risk assessments. Organizations should consider what is known about the privacy interests of individuals as useful inputs to the privacy risk assessment process.

## 6.3 Assessing privacy capabilities of third parties

### 6.3.1 Requirement

The organization shall take into account the privacy risk management capabilities of those third-parties that process PII, design or operate privacy controls.

### 6.3.2 Explanation

A consumer product's use of PII can be complex, particularly when multiple stakeholders and requirements are involved. For example, a 'virtual assistant' can involve products or systems running in the home (home equipment) as well as systems running externally (organizational servers) with each component operating across multiple lifecycles. Beyond the physical entity lifecycle of the consumer product, other lifecycles can be involved such as the PII lifecycle, the organizational server lifecycles, the system development lifecycle, etc. Each lifecycle can involve multi-functional collaboration on activities such as quality checking and certification that affect other development or operational components of the product. The operation of a consumer product can therefore involve a complex network of stakeholders and requirements, creating a need to identify, align and coordinate the roles and responsibilities of the stakeholders in the ecosystem.

Where third parties process PII in support of the product lifecycle, their processing can be taken into account in establishing the PII lifecycle and relevant privacy controls. This can mean that the PII lifecycle is extended due to third parties processing PII before the start or after the end of the product lifecycle including those to whom PII is transferred.

### 6.3.3 Guidance

a) The privacy capabilities of third-parties should be assessed through appropriate due diligence, risk assessment and agreements setting out obligations, accountabilities and review of their performance, including audits and reviews.

b) The role of third parties in this process is central. They can pose particular privacy risks and provide particular privacy controls that can significantly impact on the privacy risks posed by the product. Therefore, the third parties should provide information that will allow the organization to clarify these risks. This sharing of information should form part of any contract or service level agreement with the third party, including those to whom PII is transferred.

c) The organization should implement third-party governance technical mechanisms and operating processes to govern data sharing and privacy risks.

d) The organization's relationships with third parties including those to whom PII is transferred should be based on contracts or other measures.

e) The organization should include clauses in contracts with third parties that define third-party obligations if a consumer exercises any rights to personal information or if the product is retired.

f) The performance of third parties including those to whom PII is transferred should be periodically evaluated with appropriate means (e.g. review of reports, audits) and followed by appropriate actions.

g) Unacceptable performance should be reviewed with the third party and remediated as required.

## 6.4 Establishing and documenting requirements for privacy controls

### 6.4.1 Requirement:

The organization shall establish and document the privacy requirements that will determine the design and operation of privacy controls throughout the PII lifecycle.

### 6.4.2 Explanation

Privacy requirements provide the foundation for designing or selecting privacy controls. Engineering activities involve identifying requirements for the developments and implementation of privacy controls to meet their desired privacy outcomes. This requirement focuses on the latter.

The controls (i.e. the means) an organization selects to manage privacy risks will vary. Because of this, consumers generally need access to the information that explains how privacy in the product is

managed and how to operate the privacy controls to which they have access in a given product up to and including retirement.

Many other management, technology, quality, safety, and other information-related standards include privacy controls. Privacy controls that come from any relevant source can be incorporated into the product's design process

### 6.4.3 Guidance

a) Requirements should be established based on privacy risk assessment results.

b) Results of the privacy risk assessment can lead to changes to the initial set of privacy controls relevant to the product.

c) Privacy controls associated with any product that the product in scope depends upon should be reviewed for consistency with the intended purpose.

d) The output from a risk assessment should inform an updated set of documented requirements for privacy controls.

e) The assessed privacy needs and preferences of consumers should also be considered when establishing requirements for privacy controls.

f) The multi-functional team should identify any consumer use of organizational processing resources that continues after product sales or support ceases.

## 6.5 Monitoring and updating risk assessment

### 6.5.1 Requirement

Following product release to the market, the organization shall monitor the privacy risks associated with the product in use and update the design and operation of privacy controls, where necessary, to continuously meet privacy requirements.

### 6.5.2 Explanation

Changes to the product or organizational context can give rise to new privacy risks or necessitate updates to documented information, privacy risk assessment, privacy requirements and implemented controls as part of privacy risk management. The updates can be: a) updated inputs for privacy risk assessment; b) updated privacy risks and risk response treatment or acceptance determinations; c) updated privacy control implementation, including re-evaluation of the suitability of privacy controls and the possibility for including or developing new privacy controls. When applying the design process to the retirement phase of the product lifecycle, the possibilities can include that the consumer deliberately and permanently stops using the product; passes the product on for reuse as a gift or via a second-hand market, or dies.

### 6.5.3 Guidance

a) The organization should model the use of the product during the design phase, including post-release and post-retirement, and assess whether, when the product fails, it continues to meet privacy requirements.

b) Updates to documented information, privacy risk assessment, privacy requirements, and privacy control operation should be iterative during the product lifecycle.

c) The organization should ensure that each release, and the totality of all releases for the product, ensure that the privacy risks are managed in a way that prevents privacy controls from losing effectiveness.

d) Monitoring can involve changes to the product and associated PII processing directly, or can be external to the product, such as organizational objectives or the legal and regulatory environment. Post-release product updates can necessitate new or updated communication with consumers. The organization should ensure that new or emerging privacy risks are assessed including any consumer feedback and complaints.

e) The organization should ensure that any changes to product functionality or other settings do not lead to a loss of effectiveness in the operation of privacy controls in a way that increases residual privacy risks, without consideration of additional or new compensating controls or control improvements.

## 6.6 Including privacy risks in cybersecurity resilience design

### 6.6.1 Requirement

The organization shall consider the risk to PII in its information security policies and procedures.

NOTE Among considerations is the impact of disruptions to the resilience of privacy controls.

### 6.6.2 Explanation

Organizational resilience is the ability of an organization to absorb and adapt in a changing environment. Organizations' operations and product supply chains can be subject to day-to-day disruptions. If controls are to be operated continuously, preparations will need to be made to prevent, detect, recover, and resume from disruptions that impact PII.

Composability is a system design principle that deals with the inter-relationships of components. For example, privacy protections are not necessarily preserved because a system can be embedded within the product and sometimes the product is used as a component of a larger system. Therefore, understanding privacy risks within the system as well as a component of other systems is essential when designing cybersecurity resilience plans.

### 6.6.3 Guidance

Guidance on organizational resilience can be found in ISO 22316[48].

# 7 Developing, deploying and operating designed privacy controls

## 7.1 Overview

Privacy controls are designed, developed, deployed, managed and operated over a product's lifecycle to ensure they achieve (and continue to achieve) the intended privacy objectives within the product and that these controls do not degrade or operate in unintended ways.

Evolving privacy requirements or evolving consumer privacy needs or preferences can also trigger the need to design and implement new privacy controls over the lifecycle of a consumer product[49].

Taking a coordinated approach to the design, development, deployment, management, operation and evolution of a product's privacy controls contributes to the efficiency, effectiveness, and continued privacy by design.

The opportunity for greater effectiveness and efficiency grows if the development, deployment, management, and operation of privacy controls is integrated into an organization's overall approach to developing, deploying, managing, operating, evolving controls.

The management of these controls can be part of an organization's service management systems (SMS) as specified in ISO 20000-1[50].

NOTE ISO 20000-1 specifies requirements for an organization to establish, implement, maintain and continually improve a SMS. The requirements include the planning, design, transition, delivery and improvement of services to meet the service requirements and deliver value.

## 7.2 Integrating the design and operation of privacy controls into the product development and management lifecycles

### 7.2.1 Requirement

The organization shall integrate the design and operation of the privacy controls for the consumer product into the product's development and management lifecycle.

### 7.2.2 Explanation

The design and operation of privacy controls realizes the intended privacy design of the product and the associated governing practices, processes and policies required to achieve the product's privacy goals. The specific development and management approach and the engineering of the controls will vary based on the nature of the product and the context in which it is designed to be used. The process requirements for designing, building, deploying and operating new or changed privacy controls can be documented as follows[54]:

— Privacy requirements and controls description;

— Management information systems and tools that support the organization's lifecycle documentation and management of requirements and controls;

— Privacy control technology architectures;

— Administrative and other management processes that support the privacy controls;

— Measurement methods and metrics describing the developed controls, their deployment and performance in operation.

### 7.2.3 Guidance

a) The organization should maintain a single source of consistent and accurate information on all privacy controls that is widely available to those authorized to access it.

b) The organization should ensure that all current and planned privacy controls are delivered to meet the privacy requirements. This is accomplished through a constant cycle of negotiating, agreeing, monitoring, reporting on and reviewing privacy controls against the privacy requirements and through the instigation of actions to correct or improve the operation of privacy controls.

c) The organization should ensure the continuous operation of privacy controls by managing the risks that can affect those services and thereby ensure minimum continuity-related service levels (see Clause 6.)

d) The organization should ensure that the security (e.g. confidentiality, integrity and availability) of the privacy controls align with the identified privacy protection goals.

e) The organization should ensure that all contracts and agreements with third parties support the privacy requirements of the product and that all third parties show evidence of their contractual commitments.

f) The organization should liaise closely with those who contribute their expertise from third parties to ensure that their participation is maintained across the PII lifecycle.

g) Third parties should provide information that will allow the organization to clarify privacy issues as they arise, and this sharing of information should form part of the contract and service level agreement with the third party.

## 7.3 Designing privacy controls

### 7.3.1 Requirement

The organization shall design the privacy controls to meet the requirements that result from a privacy risk assessment.

### 7.3.2 Explanation

Requirements are met by operating controls. How the control is designed is based on the risk and the desired outcome or the objective of implementing the control. The implemented controls combine to create privacy capabilities.

Privacy controls for the product and associated PII processing include but are not limited to the following:

— Privacy controls resulting from the organization's existing knowledge, including knowledge derived from consent management and privacy preference management;

— Privacy controls that meet requirements and/or address risks identified during the privacy risk assessment.

### 7.3.3 Guidance

a) The organization should design privacy controls to meet the consumers' privacy requirements and needs throughout the PII lifecycle[24][51][52][53].

b) The organization should design privacy controls to meet its requirements and address risks identified during the privacy risk assessment.

## 7.4 Implementing privacy controls

### 7.4.1 Requirement

The organization shall engineer, develop, test, validate, and implement the privacy controls to meet the privacy requirements and monitor their effectiveness throughout the PII lifecycle.

### 7.4.2 Explanation

Engineering, development, testing and validation of privacy controls ensures that the product, its associated PII processing and the realized privacy controls meet the organization's privacy goals and requirements.

### 7.4.3 Guidance

a) The organization should implement controls to meet the requirements throughout the products lifecycle and the PII lifecycle[24][51][52][53].

b) Privacy control implementation should be consistent with the organization's enterprise architecture and associated security and privacy architectures.

c) The organization should use best practices when implementing controls, including privacy engineering methodologies, concepts and principles.

NOTE Documents such as References [53][54][55] provide more information on best practices.

d) Risk assessments should guide and inform decisions regarding the cost, benefit, and risk trade-offs in using different technologies or policies for control implementation[56].

e) Privacy controls should be tested to ensure that they meet privacy requirements.

f) The viability of implementing proposed privacy controls should be included as part of any product options appraisal process for potential new products. Where the viability assessment suggests that the product cannot meet privacy requirements, the product can be reviewed or abandoned.

g) The output should be a set of implemented privacy controls that meet established requirements that are ready for transition to service.

## 7.5 Designing privacy control testing

### 7.5.1 Requirement

The organization shall undertake control tests, and set control acceptance criteria that demonstrate the intended operational effectiveness of the privacy controls throughout the PII lifecycle.

### 7.5.2 Explanation

Assurance about the effectiveness of privacy controls requires the comprehensive testing of the design and anticipated operation of each privacy control to be tested (e.g. use and misuse cases and regression tests). The design of a control will be tested while the product is being developed, and the operation of the control will be tested before release and throughout the support period to retirement, and in some cases, during the post-retirement period.

### 7.5.3 Guidance

a) All tests of the design and operation of privacy controls should be designed in advance so that they are tested for soundness according to a pre-determined plan and approved at an appropriate level of management.

b) Acceptance criteria should also be designed and approved in advance.

c) Development of acceptance criteria should follow a clear methodology, for example: definition of the expected result of the privacy by design process (i.e. effective protection of the assessed risks); definition of the privacy requirements to be implemented to provide effective risk protection (e.g. purpose limitation, data minimization, transparency, etc.); and determination of the technologies or processes that effectively realize the design principles (e.g. data anonymization, accessible user interface design, etc.).

d) The testing should meet acceptance criteria, if the control needs to be considered to be effective.

e) A testing method should be defined to assure that each of the criteria are met effectively (e.g. differential privacy to assure data minimization, user experience design methods to assure usability of visual interface).

f) Where testing shows that a control is not effective, its design or its operation should be reviewed, revised, and re-tested before it is considered to be effective at managing privacy risks.

g) The organization should undertake privacy threat modelling based on privacy and data risk relevant test scenarios; consider augmenting existing development security threat modelling processes if possible.

h) The organization should review privacy control test plans annually to ensure viability and relevance.

i) Tests should be repeated in case of changes that can have impacts on privacy controls.