ISO 31700-1:2022(E)

2022-06-2908-10

ISO/PC 317 N270

Secretariat: BSI

Consumer protection – Privacy by design for consumer goods and services — Part 1: High-level requirements

ISO copyright office

CP 401 • Ch. de Blandonnet 8

CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11

Fax: +41 22 749 09 47

Email: copyright@iso.org

Website: www.iso.org

Published in Switzerland

Contents

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] that takes]. 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 1. 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'~~consumers' privacy: ~~i~~a) by analysing and implementing privacy controls based on the consumer's perspective, context, and needs, and~~; ii)~~ b) by succinctly documenting and communicating to consumers directly 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 S. 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.

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* (3.6 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 — to replace "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.~~13~~15) and the eventual *deletion* (3.~~24~~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

~~[SOURCE: ISO 22886:2020(en), modified to include non-organized persons such as vulnerable population and groups that have aligned responsibilities but may not have direct impact.]~~

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* ~~may be~~is processed for a particular purpose

[SOURCE: ISO/IEC 29100:2011, 2.17, modified ~~to address consumer-enabled control~~— 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~~(en)~~], 2.23]

3.9
requirement
statement that translates or expresses a need and its associated *constraints* (3.7) and *conditions* (3.~~8~~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.~~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.~~6~~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 — ~~The original~~ 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 ~~*PII*~~*personally identifiable information controller* (3.~~17~~19) or a ~~*PII*~~*personally identifiable information processor* (3.~~18~~20) or both, depending on context.

~~[SOURCE: ISO: 37301: 2021, 3.3, modified – Note 2 to entry added.]~~

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

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

3.14
~~personal~~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~~(en),~~ 4.1.39, modified — Note 1 to entry added.]

3.16
privacy control
measure that treats *privacy risks* (3.~~16~~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 text added], 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, 2.333.28]

3.18
privacy risk
effect of uncertainty on privacy

Note 1 to entry: — Risk is defined as the "effect of uncertainty on objectives" in and .

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 2 to entry: a privacy risk can be PII*personally identifiable information* (3.2) misuse or the risk that *consumers* (3.1) will experience adverse consequences resulting from PIIpersonally 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 Note 3].]

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 to delete, modified — Note 1]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* (3.1719)

[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.~~6~~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", ~~Notes1~~"system" has been changed to "consumer product" and Note to entry has been added~~. Note 2 deleted~~].]

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 ~~(3.1)~~ 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 ~~maximise~~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 added~~, 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 ~~must sign~~signs off (approve) work of the responsible party~~.~~

3.25
responsible party
person or persons who complete a delegated task or specified deliverable ~~(see accountable person (3.24))~~

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: ~~In this document~~ The term "deletion" covers the following: disposition mechanism, erasure, destruction, destruction of data storage media.

Note 2 to entry: ~~In this document,~~ 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 ~~preferred~~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: