SLOVENSKI STANDARD
SIST ISO 31700-1:2024

01-maj-2024

Varstvo potrošnikov - Vgrajena zasebnost za potrošniško blago in storitve - 1. del: Zahteve na visoki ravni

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

Ta slovenski standard je istoveten z: **ISO 31700-1:2023**

ICS:

03.080.30	Storitve za potrošnike	Services for consumers
03.100.01	Organizacija in vodenje podjetja na splošno	Company organization and management in general

SIST ISO 31700-1:2024 **en**

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.