Technical Report

ISO/IEC TR 31700-2

Second edition
2026-07

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

Part 2: Use cases

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

Partie 2: Cas d'usage

Reference number
ISO/IEC TR 31700-2:2026(en)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 44, *Consumer protection in the field of privacy by design*.

This second edition cancels and replaces the first edition (ISO/TR 31700-2:2023), which has been technically revised.

The main changes are as follows:

— the list of high-level requirements (Table 1) has been updated to align with ISO 31700-1 [1];

— editorial corrections have been made to figures.

A list of all parts in the ISO/IEC 31700 series can be found on the ISO and IEC websites.

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

Introduction

ISO 31700-1 [1] provides high-level requirements and recommendations for organizations using privacy by design in the development, maintenance and operation of consumer goods and services. These are grounded in a consumer-focused approach, in which consumer privacy rights and preferences are placed at the heart of product development and operation.

Use cases help to identify, clarify and organize system requirements related to a set of goals, by illustrating a series of possible sequences of interactions between stakeholder(s) and system(s) in a particular ecosystem.

The use cases in this document use a template that is based on IEC 62559-2 [2] while enabling a focus on privacy by design challenges.

Although a wide range of use cases exist, this document focuses on three sample use cases to illustrate the implementation of ISO 31700-1 [1]: online retailing, a fitness company and smart locks.

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

Part 2: Use cases

1 Scope

This document provides illustrative use cases, with associated analysis, to assist in understanding the requirements of ISO 31700-1 [1].

The intended audience includes engineers and practitioners who are involved in the development, implementation or operation of digitally-enabled consumer goods and services.

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
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 that involve processing of personally identifiable information, including product retirement and the eventual deletion of any associated personally identifiable information

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

[SOURCE: ISO 31700-1:2023 [3], 3.5]

3.2
use case
description of a sequence of interactions of a consumer and a consumer product used to help identify, clarify and organize requirements to support a specific business goal

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

Note 2 to entry: Systems of interest in this document are consumer goods systems or service systems.

[SOURCE: ISO 31700-1:2023 [3], 3.22, modified — Note 2 to entry has been added.]

4 Abbreviated terms

HCI human computer interface

NIST National Institute of Standards and Technology

PII personally identifiable information

5 Overview of ISO 31700-1 [1] requirements and related concepts

5.1 ISO 31700-1 [1] requirements

Table 1 lists the subclauses containing requirements from ISO 31700-1 [1], categorized as:

— general (ISO 31700-1:2023 [3], Clause 4);

— consumer communication requirements (ISO 31700-1:2023 [3], Clause 5);

— risk management requirements (ISO 31700-1:2023 [3], Clause 6);

— developing, deploying and operating designed privacy controls (ISO 31700-1:2023 [3], Clause 7);

— end of PII lifecycle requirements (ISO 31700-1:2023 [3], Clause 8).

Table 1 — ISO 31700-1 requirements

Category	ISO 31700-1:2023 subclause number
General	4.2 Designing capabilities to enable consumers to enforce their privacy rights
	4.3 Developing capability to determine consumer privacy preferences
	4.4 Designing human computer interface (HCI) for privacy
	4.5 Assigning relevant roles and authorities
	4.6 Establishing multi-functional responsibilities
	4.7 Developing privacy knowledge, skill and ability
	4.8 Ensuring knowledge of privacy controls
	4.9 Documentation and information management
Consumer communication requirements	5.2 Provision of privacy information
	5.3 Accountability for providing privacy information
	5.4 Responding to consumer inquiries and complaints
	5.5 Communicating to diverse consumer population
	5.6 Prepare data breach communications
Risk management requirements	6.2 Conducting a privacy risk assessment
	6.3 Assessing privacy capabilities of third parties
	6.4 Establishing and documenting requirements for privacy controls
	6.5 Monitoring and updating risk assessment
	6.6 Including privacy risks in cybersecurity resilience design

Table 1 *(continued)*

Category	ISO 31700-1:2023 subclause number
Developing, deploying and operating designed privacy controls	7.2 Integrating the design and operation of privacy controls into the products development and management lifecycles
	7.3 Designing privacy controls
	7.4 Implementing privacy controls
	7.5 Designing privacy control testing
	7.6 Managing the transition of privacy controls
	7.7 Managing the operation of privacy controls
	7.8 Preparing for and managing a privacy breach
	7.9 Operating privacy controls for the processes and products upon which the product in scope depends upon throughout the PII lifecycle
End of PII lifecycle requirements	8.2 Designing privacy controls for retirement and end of use

5.2 Related concepts

The tables in this subclause illustrate the relationships between the requirements of ISO 31700-1 [1] and related privacy engineering concepts, categorized as follows:

— lifecycle processes (Table 2);

— privacy protection goals, see ISO/IEC TR 27550 [4] (Table 3;)

— NIST Privacy Framework functions,[5] (Table 4);

— NIST privacy engineering objectives (Table 5).

The resulting relations are shown in Table 6.

Table 2 — Lifecycle processes

Organization policies	Activities carried out by the organization to define and maintain policies related to privacy by design.
Product design and development	Activities carried out by the organization to design and develop consumer goods or services.
Product use	Activities carried out by the organization to manage privacy when consumer goods or services are in use.

Table 3 — Privacy protection goals

Unlinkability	Property that privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context. NOTE This ensures that a PII principal can make multiple uses of resources or services without others being able to link these uses together.
Transparency	Property that ensures that all privacy-relevant data processing, including the legal, technical and organizational setting, can be understood as documented or stated.
Intervenability	Property that ensures that PII principals, PII controllers, PII processors and supervisory authorities can intervene in all privacy-relevant data processing.[6]

Table 4 — NIST Privacy Framework functions

Identify-P	Develop the organizational understanding to manage privacy riskarising from data processing for individuals.
Govern-P	Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.
Control-P	Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.
Communicate-P	Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.
Protect-P	Develop and implement appropriate data processing safeguards.

Table 5 — NIST privacy engineering objectives

Predictability	Enabling reliable assumptions by individuals, owners and operators about data and their processing by a system, product or service.
Manageability	Providing the capability for granular administration of data, including alteration, deletion and selective disclosure.
Disassociability	Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system.

Table 6 — ISO 31700-1 requirements relationship with associated concepts

Category of requirement	ISO 31700-1 requirement location	Lifecycle processes	Privacy protection goals	NIST Privacy Framework functions	NIST privacy engineering objectives
General	4.2 Designing capabilities to enable consumers to enforce their privacy rights	Product design and development	Intervenability Transparency	Control-P, Communicate-P	Predictability Manageability
	4.3 Developing capability to determine consumer privacy preferences	Product design and development	Intervenability Transparency	Control-P, Communicate-P	Predictability
	4.4 Designing human computer interface (HCI) for privacy	Product design and development	Transparency	Communicate-P	Predictability Manageability
	4.5 Assigning relevant roles and authorities	Organization policies	-	Govern-p	Manageability
	4.6 Establishing multi-functional responsibilities	Organization policies	-	Govern-P	Manageability
	4.7 Developing privacy knowledge, skill and ability	Organization policies	-	Govern-P	Manageability
	4.8 Ensuring knowledge of privacy controls	Organization policies	-	Govern-P	Manageability Disassociability
	4.9 Documentation and information management	Organization policies	-	Govern-P	Manageability

Table 6 *(continued)*

Category of requirement	ISO 31700-1 requirement location	Lifecycle processes	Privacy protection goals	NIST Privacy Framework functions	NIST privacy engineering objectives
Consumer communication requirements	5.2 Provision of privacy information	Organization policies	Transparency	Communicate-P	Predictability
	5.3 Accountability for providing privacy information	Organization policies	Transparency	Govern-P Communicate-P	Predictability Manageability
	5.4 Responding to consumer inquiries and complaints	Product use	Transparency	Communicate-P	Predictability Manageability
	5.5 Communicating to diverse consumer population	Product use	Transparency	Communicate-P	Predictability
	5.6 Prepare data breach communications	Product use	Transparency	Communicate-P	Predictability
Risk management requirements	6.2 Conducting a privacy risk assessment	Product design and development	Unlinkability	Identify-P	Predictability Manageability Disassociability
	6.3 Assessing privacy capabilities of third parties	Product design and development	Unlinkability	Identify-P, Protect-P	Predictability Manageability Disassociability
	6.4 Establishing and documenting requirements for privacy controls	Product design and development	Unlinkability Intervenability Transparency	Identify-P, Control-P, Communicate-P	Predictability Manageability Disassociability
	6.5 Monitoring and updating risk assessment	Product design and development	Unlinkability	Identify-P, Govern-P	Predictability Manageability Disassociability
	6.6 Including privacy risks in cybersecurity resilience design	Organization policies	Unlinkability	Identify-P, Protect-P	-

Table 6 *(continued)*

Category of requirement	ISO 31700-1 requirement location	Lifecycle processes	Privacy protection goals	NIST Privacy Framework functions	NIST privacy engineering objectives
Developing, deploying and operating designed privacy controls	7.2 Integrating the design and operation of privacy controls into the products development and management lifecycles	Organization policies	Unlinkability Intervenability Transparency	Protect-P	Predictability Manageability Disassociability
	7.3 Designing privacy controls	Product design and development	Unlinkability Intervenability Transparency	Protect-P	Predictability Manageability Disassociability
	7.4 Implementing privacy controls	Product design and development	Unlinkability Intervenability Transparency	Protect-P	Predictability Manageability Disassociability
	7.5 Designing privacy control testing	Product design and development	Unlinkability Intervenability Transparency	Protect-P	Predictability Manageability Disassociability
	7.6 Managing the transition of privacy controls	Organization policies	Intervenability Transparency	Control-P, Communicate-P	Predictability Manageability Disassociability
	7.7 Managing the operation of privacy controls	Organization policies	Intervenability Transparency	Control-P, Communicate-P	Predictability Manageability Disassociability
	7.8 Preparing for and managing a privacy breach	Organization policies	-	Protect-P, Control-P	-
	7.9 Operating privacy controls for the processes and products upon which the product in scope depends upon throughout the PII lifecycle	Product use	-	Control-P, Communicate-P	-
End of PII lifecycle requirements	8.2 Designing privacy controls for retirement and end of use	Product design and development	-	Control-P, Communicate-P	Predictability Manageability Disassociability

5.3 Viewpoints in the use cases

5.3.1 General

The viewpoints presented here are shown in the sequence diagrams of the use cases in Clause 7.

5.3.2 Consumer product viewpoint

Consumer products and associated organizational practices protect consumers' privacy when the product is in use and throughout the PII lifecycle, while the PII is under the organization's purview.

During product development, considering how a product is likely to be used in practice can require a number of different contexts and situations to be evaluated. Different users with different capabilities need to be catered for. This is particularly relevent given that the product, once in the possession of a consumer, is operated in unconstrained circumstances where the consumers' understanding and abilities can, and often