~~Reference number of document:~~ ISO-/TR 31700-2:2023(E)

~~Committee identification:~~ ISO PC 317

Secretariat: BSI

Privacy by design for consumer goods and services — Use cases

Ingénierie respectueuse de la protection de la vie privée pour les biens de consommation et services – cas d'usage

iTeh STANDARD PREVIEW
(standards.iteh.ai)

~~Publication stage~~

ISO/PRF TR 31700-2
https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-404[illegible]9aa4-c7388fc05c52/iso-[illegible]

~~Warning for WDs and CDs~~

~~This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.~~

~~Recipients of this draft are invited to submit, with their comments, notification of any relevant patent~~

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 31700-2
https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-4041-9aa4-c7388fc05c52/iso-prf-tr-31700-2

© ISO/IEC 2022 – All rights reserved

© ISO 2023

All rights ~~of which they are aware and to provide supporting documentation.~~

~~*A model manuscript of a draft International Standard (known as "The Rice Model") is available at https://www.iso.org/iso/model_document-rice_model.pdf*~~

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 31700-2
https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-4041-9aa4-c7388fc05c52/iso-prf-tr-31700-2

Formatted: Font: 12 pt

Copyright Notice

This ISO document is a working draftreserved. Unless otherwise specified, or committee draft and is copyright protected by ISO. While required in the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from itcontext of its implementation, no part of this publication may be reproduced, stored or utilized otherwise in any form or transmitted in any form for any other purposeby any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO.

Requests for permission to reproduce this document for at the purpose of selling it should be addressed as shownaddress below or to ISO's ISO's member body in the country of the requester:.

Secretariat of ISO PC317, BSI, Jean Stride: Jean.Stride@bsigroup.com

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

ISO Copyright Office
CP 401 • CH-1214 Vernier, Geneva
Phone: + 41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org
Published in Switzerland.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 31700-2
https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-4041-9aa4-c7388fc05c52/iso-prf-tr-31700-2

Formatted: Tab stops: Not at 304.8 pt

Formatted: Font: 12 pt, Bold

Contents

Formatted: Tab stops: Not at 460.7 pt

~~© ISO/IEC 2022 – All rights reserved~~

© ISO 2023 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/FDIS TR 31700-2
https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-404f-9aa4-c7388fc05c52/iso-fdis-tr-31700-2

Formatted: Font: 12 pt

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Formatted: Tab stops: Not at 304.8 pt

Formatted: Font: 12 pt, Bold

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~~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~~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.

iTeh STANDARD PREVIEW

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~~www.iso.org/iso/foreword.html.

(standards.iteh.ai)

This document was prepared by Project Committee 317 Consumer Protection – privacy by design for consumer goods and services.

ISO/PRF TR 31700-2
https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-4041-9aa4-c7388fc05c52/iso-prf-tr-31700-2

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~~www.iso.org/members.html.

Formatted: Tab stops: Not at 460.7 pt

~~© ISO/IEC 2022 – All rights reserved~~

© ISO 2023 – All rights reserved

Formatted: Font: 12 pt

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 case 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 and on the ISO 31700-1 requirements.

Although there are a wide range of use cases, this document provides three sample use cases to help further understand the implementation of ISO 31700-1: -on-line retailing, a fitness company-, and smart locks.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 31700-2
https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-4041-9aa4-c7388fc05c52/iso-prf-tr-31700-2

Formatted: Tab stops: Not at 304.8 pt

Privacy by design for Consumer Goods and Services — Use cases

1 Scope

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

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

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

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

ISO/PRF TR 31700-2
https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-4041-9aa4-c7388fc05c52/iso-tr-31700-2

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

~~associated personally identifiable information~~

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

[SOURCE ISO 31700-1:2023, 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~~Consumers can be users, engineers, of systems.

Note 2 to entry: ~~a~~A system of interest in this document is a consumer goods or service.

[SOURCE: ISO 31700-1:2023, 3.22, modified — note 2 added]

© ISO 2023 – All rights reserved

Formatted: Font: 12 pt, Bold

4 Abbreviated terms

NIST National Institute of Standards and Technology

PII Personally identifiable information

5 Overview of ISO 31700-1 requirements and related concepts

5.1 ISO 31700-1 Requirements

Table 1 lists ISO 31700-1:2023[1] requirements, categorised as:

— general (ISO 31700-1:2023, clause 4);

— consumer communication requirements (ISO 31700-1:2023, clause 5);

— risk management requirements (ISO 31700-1:2023, clause 6);

— develop, deploy and operated privacy controls (ISO 31700-1:2023, clause 7); and

— end of PII lifecycle requirements (ISO 31700-1:2023, clause 8).

Table 1 — ISO 31700-1 requirements

Category	ISO 31700-1 section number and requirement
General	4.2 Design capabilities to enable consumers to enforce their privacy rights
	4.3 Develop capability to determine consumer privacy preferences
	4.4 Design human computer interface (HCI) for privacy
	4.5 Assign relevant roles and authorities
	4.6 Establish multi-disciplinary responsibilities
	4.7 Develop privacy knowledge, skill and ability
	4.8 Ensure knowledge of privacy controls
	4.9 Documented information management
Consumer communication requirements	5.2 Provision of privacy information
	5.3 Accountability of responsible persons to 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 Conduct a privacy risk assessment
	6.3 Assess privacy capabilities of third parties
	6.4 Establish and document requirements for privacy controls
	6.5 Monitor and update risk assessment
	6.6 Include privacy risks in cybersecurity resilience design

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 31700-2
https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-4041-9aa4-c7388fc05c52/iso-tr-31700-2

Formatted: Footer

© ISO/IEC 2022 – All rights reserved

© ISO 2023 – All rights reserved

Formatted: Font: 12 pt, Bold

Develop, deploy and operate designed privacy controls	7.2 Integrate the design and operation of privacy controls into the products development and management lifecycles
	7.3 Design privacy controls
	7.4 Implement privacy controls
	7.5 Design privacy control testing
	7.6 Manage the transition of privacy controls
	7.7 Manage the operation of privacy controls
	7.8 Prepare breach management
	7.9 Operate privacy controls for the processes and products that the product in scope depends upon through the PII lifecycle
End of PII lifecycle requirements	8.2 Design privacy controls for retirement and end of use

5.2 Related concepts

The tables in this clause illustrate the relationships between the requirements of ISO 31700-1 and related privacy engineering concepts:

— lifecycle processes as shown in Table 2;

— privacy protection goals ~~[5],~~ as shown in Table 3.

— NIST Privacy framework functions ~~[7],~~ as shown in Table 4; ~~and~~

— NIST privacy engineering objectives as shown in Table 5.

The resulting relations are shown in Table 6.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 31700-2
https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-4041-9aa4-c7388fc05c52/iso-prf-tr-31700-2

Table 2 — Lifecycle processes

Organisation policies	Activities carried out by the organisation to define and maintain policies related to privacy by design
Product design and development	Activities carried out by the organisation to design and develop consumer goods or services
Product use	Activities carried out by the organisation 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 It 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

Formatted: Footer

© ISO 2023 – All rights reserved

Formatted: Font: 12 pt, Bold

Intervenability	Property that ensures that PII principals, PII controllers, PII processors and supervisory authorities can intervene in all privacy-relevant data processing.[12]

Table 4 — NIST Privacy Framework functions

Identify-P	Develop the organizational understanding to manage privacy risk for individuals arising from data processing
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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TR 31700-2:2023
https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-4041-9aa4-c7388fc05c52/iso-tr-31700-2

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

Category of requirement	ISO 31700-1 Requirement	Lifecycle processes	Privacy protection goals	NIST Privacy Framework functions	NIST privacy engineering objectives
General	4.2 Design capabilities to enable consumers to enforce their privacy rights	Product design and development	Intervenability Transparency	Control-P, Communicate-P	Predictablity Manageability
	4.3 Develop capability to determine consumer privacy preferences	Product design and development	Intervenability Transparency	Control-P, Communicate-P	Predictability
	4.4 Design human computer interface (HCI) for privacy	Product design and development	Transparency	Communicate-P	Predictablity Manageability

© ISO/IEC 2022 – All rights reserved

Formatted: Footer

© ISO 2023 – All rights reserved

Formatted: Font: 12 pt, Bold

	4.5 Assign relevant roles and authorities	Organisation policies	-	Govern-p	Manageability
	4.6 Establish multi-disciplinary responsibilities	Organisation policies	-	Govern-P	Manageability
	4.7 Develop privacy knowledge, skill and ability	Organisation policies	-	Govern-P	Manageability
	4.8 Ensure knowledge of privacy controls	Organisation policies	-	Govern-P	Manageability Disassociability
	4.9 Documented information management	Organisation policies	-	Govern-P	Manageability
Consumer communication requirements	5.2 Provision of privacy information	Organisation policies	Transparency	Communicate-P	Predictability
	5.3 Accountability of responsible persons to providing privacy information	Organisation 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 Conduct a privacy risk assessment	Product design and development	Unlinkability	Identify-P	Predictability Manageability Disassociability
	6.3 Assess privacy capabilities of third parties	Product design and development	Unlinkability	Identify-P, Protect-P	Predictability Manageability Disassociability
	6.4 Establish and document requirements for privacy controls	Product design and development	Unlinkability Intervenability Transparency	Identify-P, Control-P, Communicate-P	Predictability Manageability Disassociability

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 31700-2
https://standards.iteh.ai/catalog/standards/sist/a019682e-4dff-4041-9aa4-c7388fc05c52/iso-prf-tr-31700-2

© ISO/IEC 2022 – All rights reserved

Formatted: Footer

© ISO 2023 – All rights reserved

Formatted: Font: 12 pt, Bold

	6.5 Monitor and update risk assessment	Product design and development	Unlinkability	Identify-P, Govern-P	Predictability Manageability Disassociability
	6.6 Include privacy risks in cybersecurity resilience design	Organisation policies	Unlinkability	Identify-P, Protect-P	-
Develop, deploy and operate designed privacy controls	7.2 Integrate the design and operation of privacy controls into the products development and management lifecycles	Organisation policies	Unlinkability Intervenability Transparency	Protect-P	Predictability Manageability Disassociability
	7.3 Design privacy controls	Product design and development	Unlinkability Intervenability Transparency	Protect-P	Predictability Manageability Disassociability
	7.4 Implement privacy controls	Product design and development	Unlinkability Intervenability Transparency	Protect-P	Predictability Manageability Disassociability
	7.5 Design privacy control testing	Product design and development	Unlinkability Intervenability Transparency	Protect-P	Predictability Manageability Disassociability
	7.6 Manage the transition of privacy controls	Organisation policies	Intervenability Transparency	Control-P, Communicate-P	Predictability Manageability Disassociability
	7.7 Manage the operation of privacy controls	Organisation policies	Intervenability Transparency	Control-P, Communicate-P	Predictability Manageability Disassociability
	7.8 Prepare breach management	Organisation policies	-	Protect-P, Control-P	-
	7.9 Operate privacy controls for the processes and products that the product in scope depends upon through the PII lifecycle	Product use	-	Control-P, Communicate-P	-
End of PII lifecycle requirements	8.2 Design privacy controls for retirement and end of use	Product design and development	-	Control-P, Communicate-P	Predictability Manageability Disassociability

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/a019682...9aa4-c7388fc05c52/iso-prf-tr-31700-2

© ISO/IEC 2022 – All rights reserved

Formatted: Footer

© ISO 2023 – All rights reserved

Formatted: Font: 12 pt, Bold

5.3 Viewpoints in the use cases

5.3.1 General

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

5.3.2 Consumer product viewpoint

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

Considering how a product is likely to be used in practice, during product development, can require a number of different contexts and situations to be evaluated. Different users with different capabilities are catered for. This applies as the product, once in the possession of a consumer user, is operated in unconstrained circumstances where the consumer's understanding and abilities can, and often do, vary considerably.

For each type of use the precise definition of use is coupled with an accurate description of how the product and any associated organisational processes would operate so as to protect privacy.

Finally, consumer use can change over time and vary between cultures or demographic groups.

5.3.3 Engineering framework viewpoint

The development and management of privacy controls is an essential part of the engineering of consumers products. The resulting engineering framework combines:

— processes based on standards such as ISO/IEC/IEEE 15288 ~~— System life cycle processes~~ [3];

— extensions of such processes that integrate privacy engineering. These extensions can be based on ISO/IEC TR 27550 ~~– Privacy engineering for system life cycle processes~~ [5], with the support of frameworks such as the NIST Privacy Framework ~~[7]~~, the use of OASIS PMRM [6] to operationalize privacy principles~~, and~~;

— the integration of the consumer product viewpoint, which is supported by ISO 31700-1 [1].

NOTE An additional reference ~~o~~to OASIS PMRM is under development: ISO/IEC 27561, Information technology — Privacy operationalisation model and method for engineers — POMME

5.3.4 Ecosystem viewpoint

Consumer products involve two ecosystems:

— the supply chain, i.e., the ecosystem associated with the system lifecycle process. This involves organisation and contractual activities on the privacy capabilities provided by third parties; ~~and~~

— the data space, i.e., the ecosystem associated with users and providers of data. This involves organisation and contractual activities on data sharing.

6 Use case analysis

6.1 General

A use case template was developed to help illustrate, in a consistent manner, the use case examples. The template is structured to provide the information that illustrates the use of ISO 31700-1~~:~~.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/PRF TR 31700-2
https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-4041-9aa4-c7388fc05c52/iso-prf-tr-31700-2

Formatted: Footer

© ISO/IEC 2022 – All rights reserved

© ISO 2023 – All rights reserved