

---

---

**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*

ISO/TR 31700-2:2023

<https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-4041-9aa4-c7388fc05c52/iso-tr-31700-2-2023>



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-31700-2-2023>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by 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 at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

# Contents

Page

|   |           |
|---|-----------|
| Foreword.....   | iv        |
| Introduction.....   | v         |
| <b>1 Scope.....</b>   | <b>1</b>  |
| <b>2 Normative references.....</b>                                      | <b>1</b>  |
| <b>3 Terms and definitions.....</b>                                     | <b>1</b>  |
| <b>4 Abbreviated terms.....</b>   | <b>2</b>  |
| <b>5 Overview of ISO 31700-1 requirements and related concepts.....</b> | <b>2</b>  |
| 5.1 ISO 31700-1 Requirements.....                                       | 2         |
| 5.2 Related concepts.....   | 3         |
| 5.3 Viewpoints in the use cases.....                                    | 6         |
| 5.3.1 General.....  | 6         |
| 5.3.2 Consumer product viewpoint.....                                   | 6         |
| 5.3.3 Engineering framework viewpoint.....                              | 7         |
| 5.3.4 Ecosystem viewpoint.....  | 7         |
| <b>6 Use case analysis.....</b>   | <b>7</b>  |
| 6.1 General.....  | 7         |
| 6.2 Use case template.....  | 7         |
| <b>7 Use cases.....</b>   | <b>8</b>  |
| 7.1 General.....  | 8         |
| 7.2 On-line retailing.....  | 9         |
| 7.2.1 On-line retailing use case main description.....                  | 9         |
| 7.2.2 On-line retailing consumer communication.....                     | 11        |
| 7.2.3 On-line retailing summary.....                                    | 12        |
| 7.2.4 On-line retailing general requirements.....                       | 13        |
| 7.2.5 On-line retailing risk management.....                            | 14        |
| 7.2.6 On-line retailing development, deployment and operation.....      | 15        |
| 7.2.7 On-line retailing end of PII lifecycle.....                       | 16        |
| 7.3 Fitness company.....  | 17        |
| 7.3.1 Fitness company use case main description.....                    | 17        |
| 7.3.2 Fitness company risk management of health application.....        | 19        |
| 7.3.3 Fitness company consumer communication.....                       | 20        |
| 7.4 Smart locks for homes front doors.....                              | 21        |
| 7.4.1 Smart locks product line main description.....                    | 21        |
| 7.4.2 Smart locks basic configuration.....                              | 24        |
| 7.4.3 Smart locks colocation configuration.....                         | 25        |
| 7.4.4 Smart locks family configuration.....                             | 26        |
| 7.4.5 Smart locks risk management.....                                  | 27        |
| 7.4.6 Smart locks consumer communication.....                           | 28        |
| 7.4.7 Smart locks development, deployment and operation.....            | 29        |
| <b>Bibliography.....</b>  | <b>31</b> |

## 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](http://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](http://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](http://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*.

ISO/TR 31700-2:2023

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](http://www.iso.org/members.html).

## Introduction

ISO 31700-1<sup>[1]</sup> 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<sup>[2]</sup> 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/TR 31700-2:2023](https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-4041-9aa4-c7388fc05c52/iso-tr-31700-2-2023)

<https://standards.iteh.ai/catalog/standards/sist/a0196826-4dff-4041-9aa4-c7388fc05c52/iso-tr-31700-2-2023>



# 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, 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

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 <http://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, 3.5]

#### 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, of systems.

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

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

**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<sup>[1]</sup> 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);
- 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                |



**Table 1 (continued)**

| Category  | ISO 31700-1 section number and requirement   |
|---|--|
| 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  |
| End of PII lifecycle requirements                     | 7.9 Operate privacy controls for the processes and products that the product in scope depends upon through the PII lifecycle |
|   | 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,<sup>[5]</sup> as shown in [Table 3](#);
- NIST Privacy framework functions,<sup>[7]</sup> as shown in [Table 4](#);
- NIST privacy engineering objectives as shown in [Table 5](#).

The resulting relations are shown in [Table 6](#).

**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<br>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  |
| Intervenability | Property that ensures that PII principals, PII controllers, PII processors and supervisory authorities can intervene in all privacy-relevant data processing <sup>[12]</sup>   |

**Table 4 — NIST Privacy Framework functions**

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

**Table 4 (continued)**

|               |  |
|---------------|--|
| 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   | 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<br>Transparency | Control-P, Communicate-P         | Predictability<br>Manageability     |
|                         | 4.3 Develop capability to determine consumer privacy preferences            | Product design and development | Intervenability<br>Transparency | Control-P, Communicate-P         | Predictability                      |
|                         | 4.4 Design human computer interface (HCI) for privacy                       | Product design and development | Transparency                    | Communicate-P                    | Predictability<br>Manageability     |
|                         | 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<br>Disassociability   |
|                         | 4.9 Documented information management                                       | Organisation policies          | -                               | Govern-P                         | Manageability                       |

Table 6 (continued)

| Category of requirement             | ISO 31700-1 Requirement  | Lifecycle processes            | Privacy protection goals                         | NIST Privacy Framework functions     | NIST privacy engineering objectives                 |
|-------------------------------------|--|--------------------------------|--|--------------------------------------|---|
| 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<br>Manageability                     |
|                                     | 5.4 Responding to consumer inquiries and complaints                        | Product use                    | Transparency                                     | Communicate-P                        | Predictability<br>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<br>Manageability<br>Disassociability |
|                                     | 6.3 Assess privacy capabilities of third parties                           | Product design and development | Unlinkability                                    | Identify-P, Protect-P                | Predictability<br>Manageability<br>Disassociability |
|                                     | 6.4 Establish and document requirements for privacy controls               | Product design and development | Unlinkability<br>Intervenability<br>Transparency | Identify-P, Control-P, Communicate-P | Predictability<br>Manageability<br>Disassociability |
|                                     | 6.5 Monitor and update risk assessment                                     | Product design and development | Unlinkability                                    | Identify-P, Govern-P                 | Predictability<br>Manageability<br>Disassociability |
|                                     | 6.6 Include privacy risks in cybersecurity resilience design               | Organisation policies          | Unlinkability                                    | Identify-P, Protect-P                | -   |

**Table 6 (continued)**

| Category of requirement                               | ISO 31700-1 Requirement  | Lifecycle processes            | Privacy protection goals                         | NIST Privacy Framework functions | NIST privacy engineering objectives                 |
|---|--|--------------------------------|--|----------------------------------|---|
| Develop, deploy and operate designed privacy controls | 7.2 Integrate the design and operation of privacy controls into the products development and management life-cycles          | Organisation policies          | Unlinkability<br>Intervenability<br>Transparency | Protect-P                        | Predictability<br>Manageability<br>Disassociability |
|   | 7.3 Design privacy controls  | Product design and development | Unlinkability<br>Intervenability<br>Transparency | Protect-P                        | Predictability<br>Manageability<br>Disassociability |
|   | 7.4 Implement privacy controls   | Product design and development | Unlinkability<br>Intervenability<br>Transparency | Protect-P                        | Predictability<br>Manageability<br>Disassociability |
|   | 7.5 Design privacy control testing   | Product design and development | Unlinkability<br>Intervenability<br>Transparency | Protect-P                        | Predictability<br>Manageability<br>Disassociability |
|   | 7.6 Manage the transition of privacy controls  | Organisation policies          | Intervenability<br>Transparency                  | Control-P, Communicate-P         | Predictability<br>Manageability<br>Disassociability |
|   | 7.7 Manage the operation of privacy controls   | Organisation policies          | Intervenability<br>Transparency                  | Control-P, Communicate-P         | Predictability<br>Manageability<br>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<br>Manageability<br>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 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