TECHNICAL REPORT

ISO/TR 31700-2

First edition
2023-01

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/TR 31700-2:2023(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

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.

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[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);

— 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
	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;

— 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 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[12]

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 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
	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

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 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
	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	-

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 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

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

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[3];

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

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

NOTE An additional reference 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;

— 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.

— The entries for the main narrative are general. They include ID: use case name; description of product, service or process; privacy protection goal; ecosystem and systems of interest; users, stakeholders; PII; purpose; and use case narrative.

— The entries for the extended narratives follow the requirements of ISO 31700-1: general requirements; consumer communication requirements; risk management requirements; development, deployment and operations of designed privacy controls; and end of PII lifecycle requirements.

6.2 Use case template

Table 7 provides a template for the main narrative of a use case.

Table 7 — Template for main narrative

Entry	Entry description
ID	Unique identification

Table 7 *(continued)*

Entry	Entry description
Use case name	Meaningful name
Description of product, service or process	Short description of product
Privacy protection goal	Short description of privacy protection goals
Ecosystem and systems of interest	Describe systems of interest
Users	Describe users
Stakeholders	Describe stakeholders
PII	Describe PII collected
Purpose	Describe purpose of PII collection
Main narrative	Short narrative on consumer goods and services (possibly with a sequence diagram)

Table 8 provides a template for the extended narratives of a use case.

Table 8 — Template for extended narratives

Entry	Entry description
ID	Unique identification
Use case name	Meaningful name
Additional narrative	Narrative describing a specific variation, or focusing on the use of requirements in a specific clause of ISO 31700-1. When possible, a sequence diagram is provided. Table 9 lists possible categories of narratives.

Table 9 lists proposed categories of extended narratives. They match categories of ISO 31700-1 requirements.

Table 9 — Categories of extended narratives

Category of extended narratives	Relationship with ISO 31700-1
General requirements	Focus on ISO 31700-1:2023, 4.2 to 4.9
Consumer communication requirements	Focus on ISO 31700-1:2023, 5.2 to 5.6
Risk management requirements	Focus on ISO 31700-1:2023, 6.2 to 6.6
Development, deployment and operation of designed privacy controls	Focus on ISO 31700-1;2023, 7.2 to 7.9
End of PII lifecycle requirements	Focus on ISO 31700-1:2023, 8.2

7 Use cases

7.1 General

Three use cases are described: on-line retailing, a fitness company and smart locks. These use cases cover ISO 31700-1 requirements as shown in Table 10.

NOTE A sequence diagram is provided for each narrative. The codes for the sequence diagrams in Figure 1 to Figure 16 are available at: https://standards.iso.org/iso/tr/31700/-2/ed-1/en/.

Table 10 — Use cases requirement coverage

Category of requirement	ISO 31700-1 Requirement		On-line retailing	Fitness compa-ny	Smart locks
General	4.2	Design capabilities to enable consumers to enforce their privacy rights	X		
	4.3	Develop capability to determine consumer privacy preferences	X		
	4.4	Design human computer interface (HCI) for privacy	X		
	4.5	Assign relevant roles and authorities	X		
	4.6	Establish multi-disciplinary responsibilities	X		
	4.7	Develop privacy knowledge, skill and ability	X		
	4.8	Ensure knowledge of privacy controls	X		
	4.9	Documented information management	X		
Consumer communication requirements	5.2	Provision of privacy information		X	X
	5.3	Accountability of responsible persons to providing privacy information		X	X
	5.4	Responding to consumer inquiries and complaints	X	X	X
	5.5	Communicating to diverse consumer population	X	X	X
	5.6	Prepare data breach communications	X		X
Risk management requirements	6.2	Conduct a privacy risk assessment	X	X	X
	6.3	Assess privacy capabilities of third parties	X	X	X
	6.4	Establish and document requirements for privacy controls	X	X	X
	6.5	Monitor and update risk assessment	X	X	X
	6.6	Include privacy risks in cybersecurity resilience design			X
Develop, deploy and operate designed privacy controls	7.2	Integrate the design and operation of privacy controls into the products development and management lifecycles			X
	7.3	Design privacy controls	X		X
	7.4	Implement privacy controls	X		X
	7.5	Design privacy control testing			X
	7.6	Manage the transition of privacy controls			X
	7.7	Manage the operation of privacy controls	X		X
	7.8	Prepare breach management	X		X
	7.9	Operate privacy controls for the processes and products that the product in scope depends upon through the PII lifecycle	X		X
End of PII lifecycle requirements	8.2	Design privacy controls for retirement and end of use	X		

7.2 On-line retailing

7.2.1 On-line retailing use case main description

ID	Unique identification	UC 31700-01a
Use case name	Meaningful name	On line retailing

Description of product, service or process	Short description of product	A service that allows the customers to search, select and purchase the products, services and information remotely over the Internet
Privacy protection goal	Short description of privacy protection goals	Data and PII provided to or collected by the retailer is limited to information used to complete the sale, delivery, provide a receipt, enable product or service improvement, and provide customer support.
Ecosystem and systems of interest	Describe systems of interest	Customer Privacy Expectation Customer post purchase privacy expectation Online retailers' transaction system Online retailers' order fulfilment information system Online retailers' delivery system Internet service provider information system
Users	Describe users	Any consumer placing order, including vulnerable persons (e.g., seniors, minors, disabled)
Stakeholders	Describe stakeholders	Retailer fulfilment and delivery staff Order processing system Delivery system Payment system Return system Marketing and tracking system Consumer device (e.g., tablet, smart phone, laptop)
PII	Describe PII processed	Client name, address, email and phone. Credit card information for payment for processing of order.
Product use purpose	Describe purpose of PII processing	The PII is collected by the seller to fulfil the order and enable product development and service improvement.
Main narrative	Short narrative on consumer goods and services (possibly with a diagram)	A consumer goes online to find toys for the grandchildren. The consumer visits several websites, including initiating orders that the consumer does not complete. The consumer finds an online retailer and completes an order for 2 items. To fulfil the order, the consumer provides contact information including delivery address and payment method. For the purposes of shipping and order he provides his contact information and address. In order to process payment he enters his credit card. The online retailer asks if he wants to set up an account. He declines. The online retailer asks if he wants them to retain the contact information after delivery for future purchases or returns. The client declines to allow this except related to the right of return. The online retailer asks some questions regarding family size, ages and income. The client declines to answer and declines to receive any information related to new products.

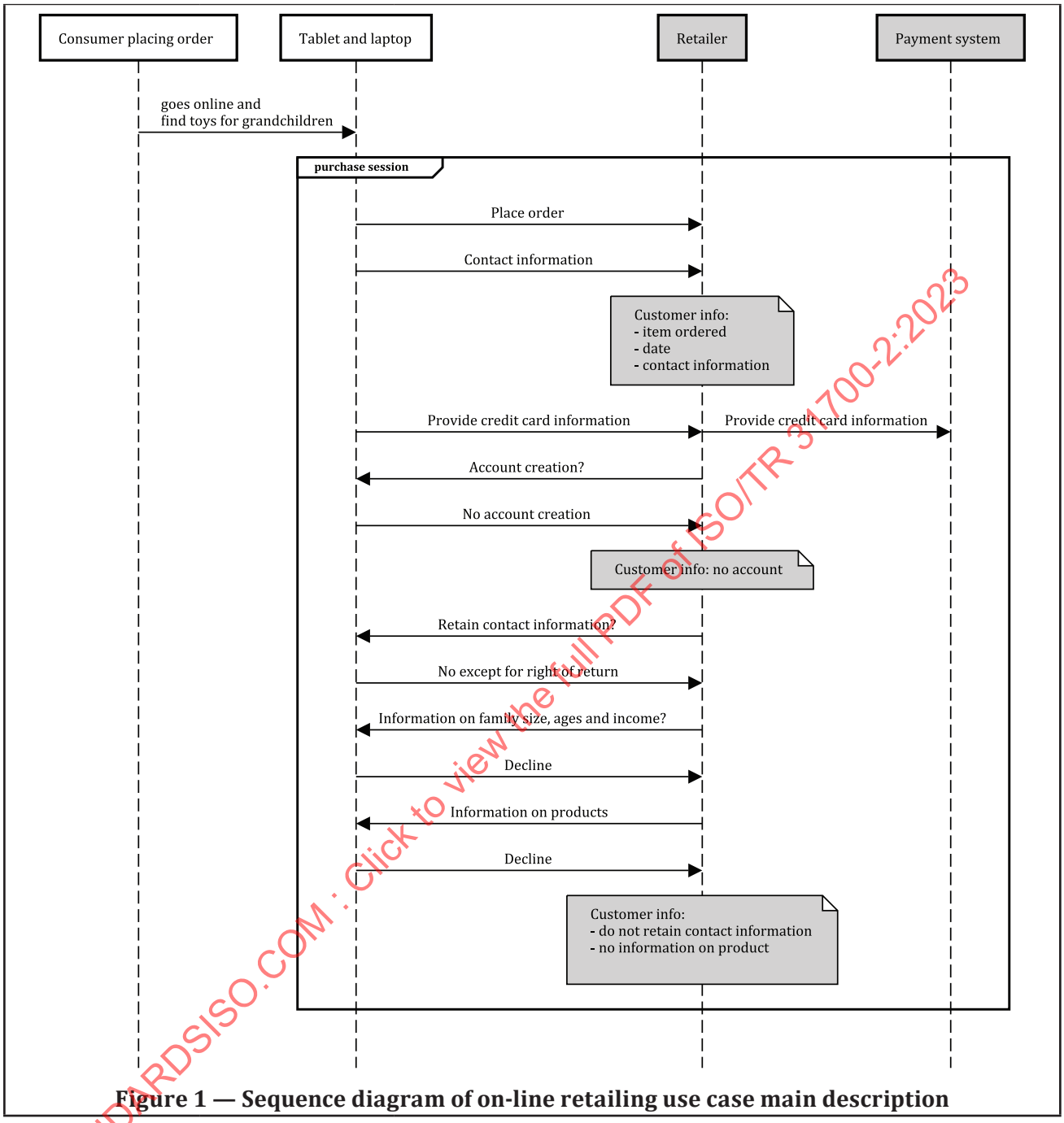

Figure 1 — Sequence diagram of on-line retailing use case main description

7.2.2 On-line retailing consumer communication

ID	Unique identification	UC 31700-01b
Use case name	Meaningful name	On line retailing

Narrative on consumer communication	Describe how requirements for consumer communication can help (possibly with a diagram)	The information system of the retailer company is subject to a cybersecurity attack, causing the system to be stopped for several hours. The organisation activates its consumer support program. It makes a privacy announcement on the web which confirms that there has been no privacy breach. The customer makes a specific inquiry on his purchase and gets customised information reassuring the customer that their order was not impacted nor their payment or other PII

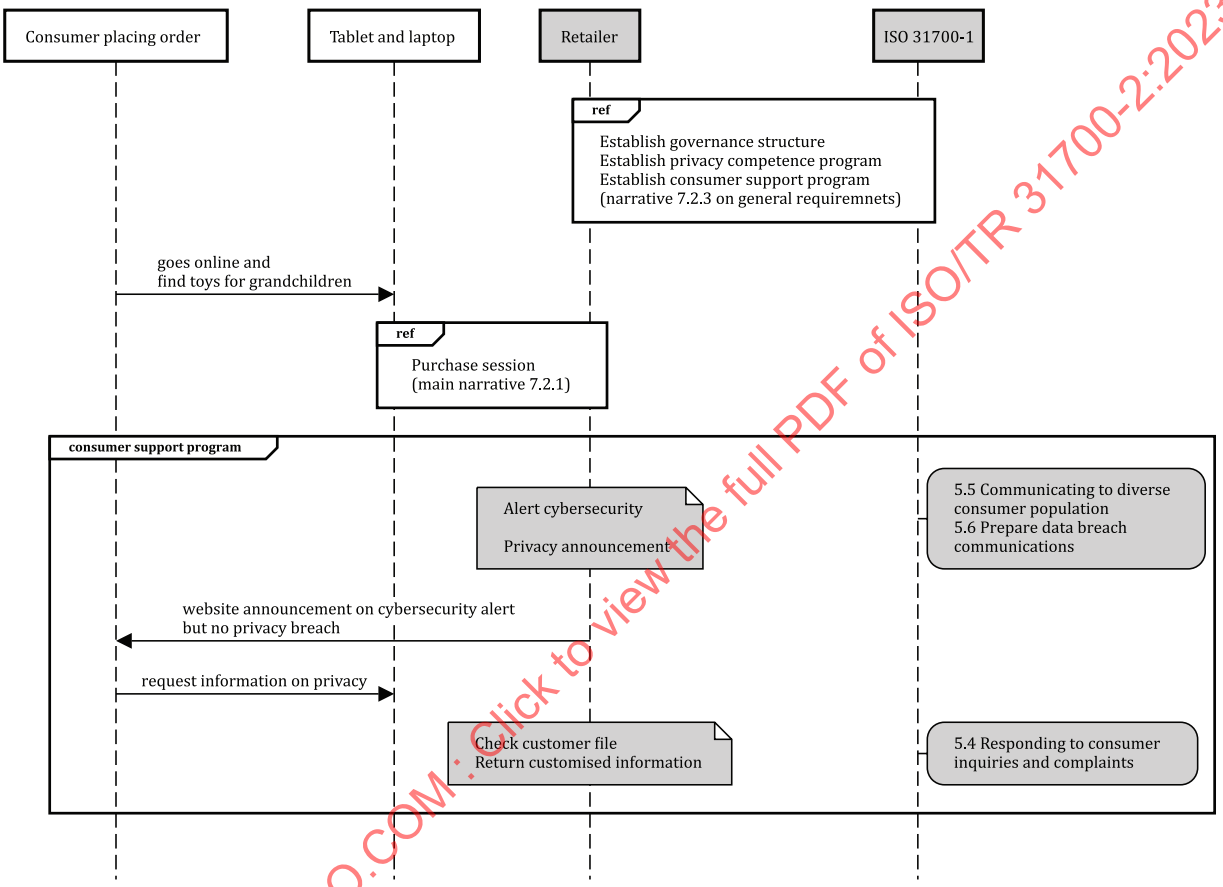

Figure 2 — Sequence diagram of on-line retailing consumer communication

7.2.3 On-line retailing summary

ID	Unique identification	UC 31700-01c
Use case name	Meaningful name	On line retailing

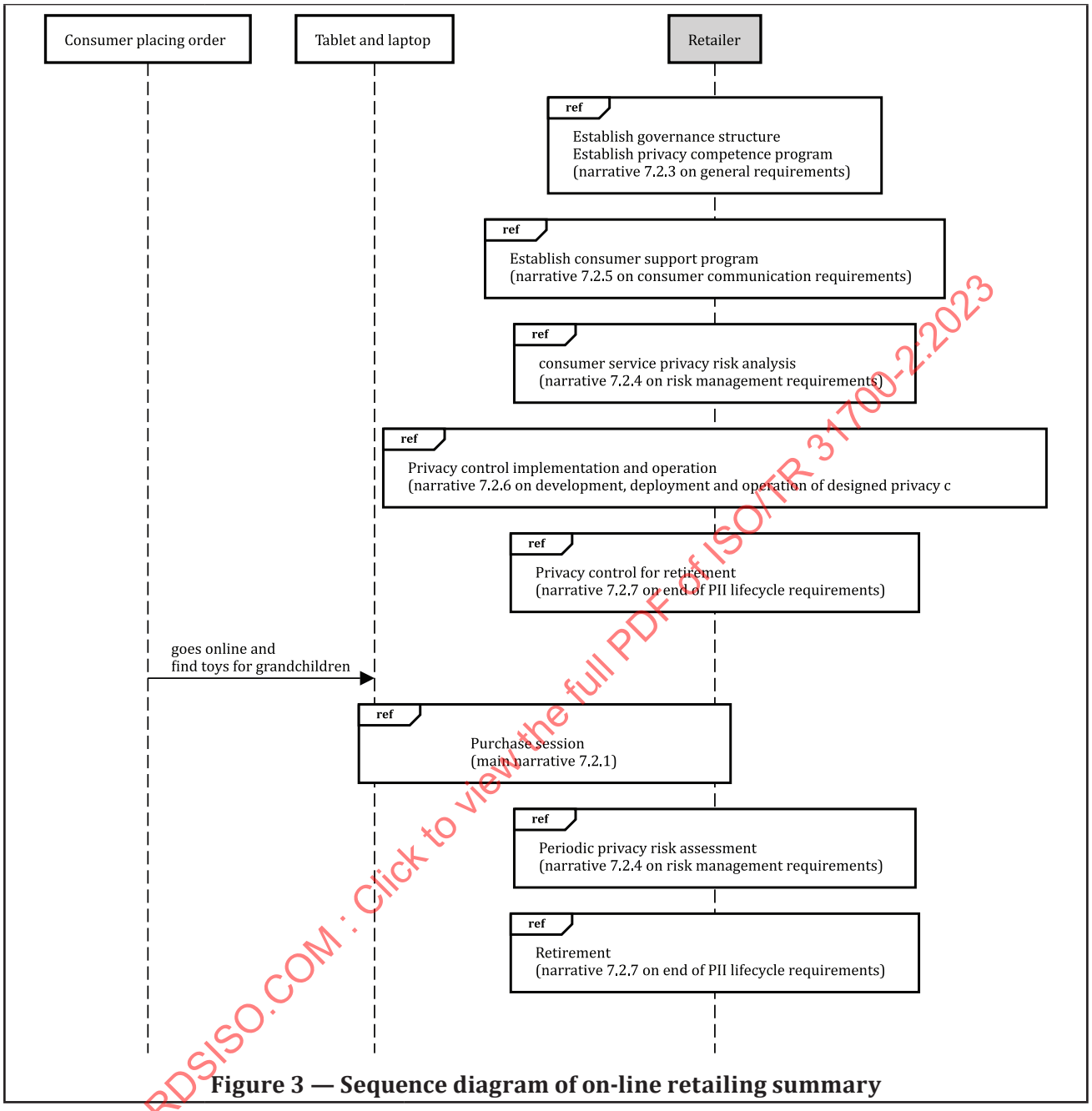

Figure 3 — Sequence diagram of on-line retailing summary

7.2.4 On-line retailing general requirements

ID	Unique identification	UC 31700-01d
Use case name	Meaningful name	On line retailing

Narrative on general requirements	Describe how general requirements can help (possibly with a diagram)	A company wants to create an online retail business. It establishes a governance structure to deal with privacy compliance and consumer communication. It further establishes a privacy competence program for employees engaged throughout the data processing ecosystem. This includes knowledge on regulation and on privacy enhancing technologies. A consumer support program is created. This includes capabilities and communications for consumers to indicate privacy preferences, understand privacy controls available to them, and to enact their privacy rights, as well as the planning for interactions with consumers.

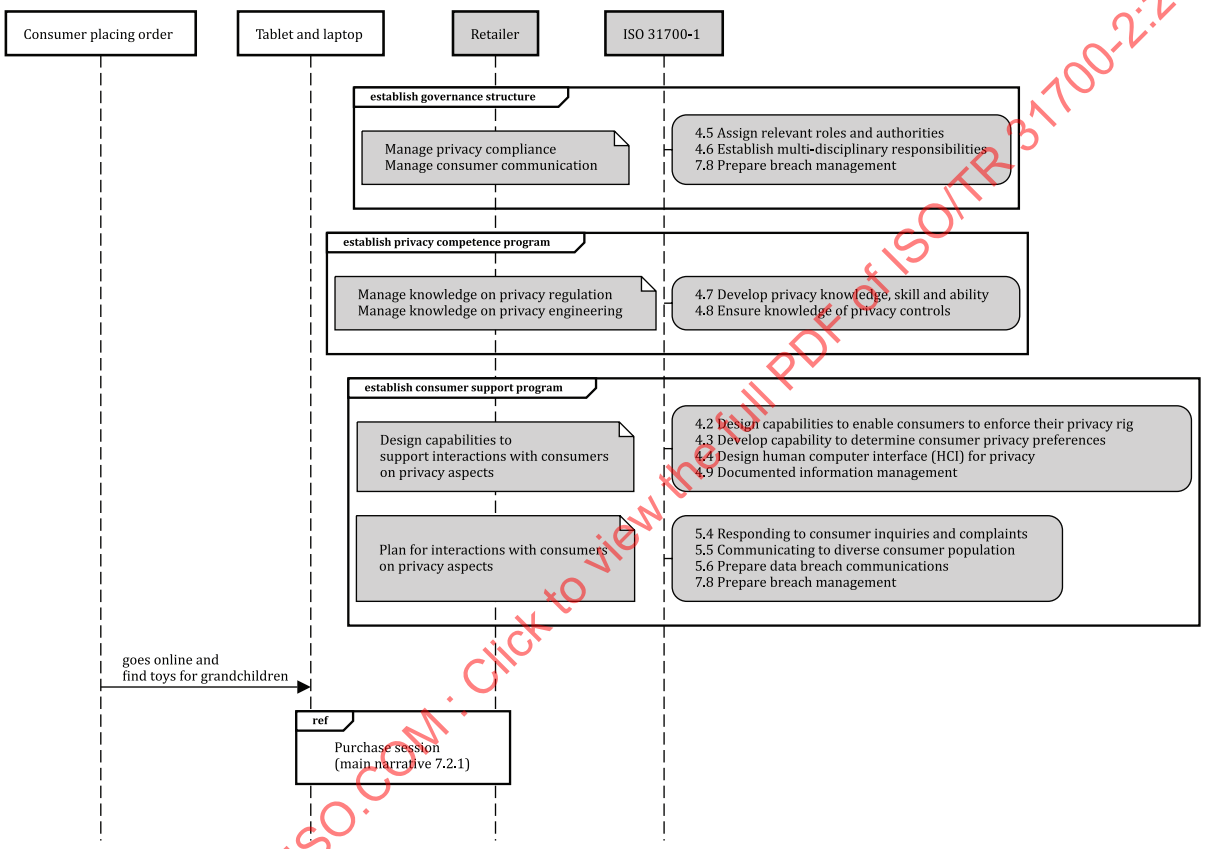

Figure 4 — Sequence diagram of on-line retailing general requirements

7.2.5 On-line retailing risk management

ID	Unique identification	UC 31700-01e
Use case name	Meaningful name	On line retailing
Narrative on risk management	Describe how requirements on risk management can help (possibly with a diagram)	The product management team of the retailer performs an initial consumer service privacy risk analysis which leads to requirements on consumer support, and requirements on protection of data storage. An assessment of supplier providing data storage protection leads to a selected implementation. A periodic privacy risk assessment is carried out. The impact of the cybersecurity alert on data protection is evaluated. The consumer support program is also evaluated. They lead to some minor adjustments

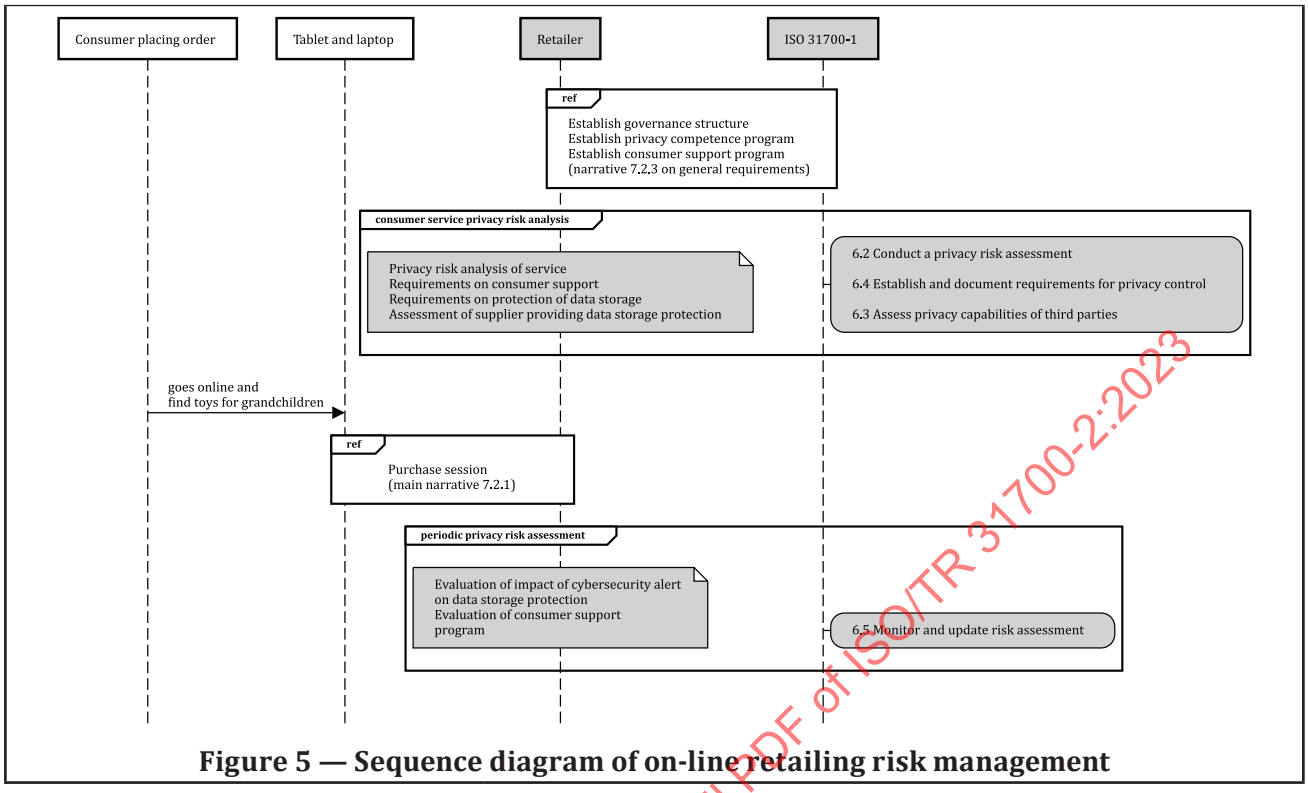

Figure 5 — Sequence diagram of on-line retailing risk management

7.2.6 On-line retailing development, deployment and operation

ID	Unique identification	UC 31700-01f
Use case name	Meaningful name	On-line retailing
Narrative on development, deployment and operation	Describe how requirements for privacy controls can help (possibly with a diagram)	Further to the consumer service privacy risk analysis, the development team is mandated to implement a privacy control concerning consumer accounts which includes an access control policy enforcement and monitoring mechanism, as well as associated organisation measures concerning rules on which employees can access data.

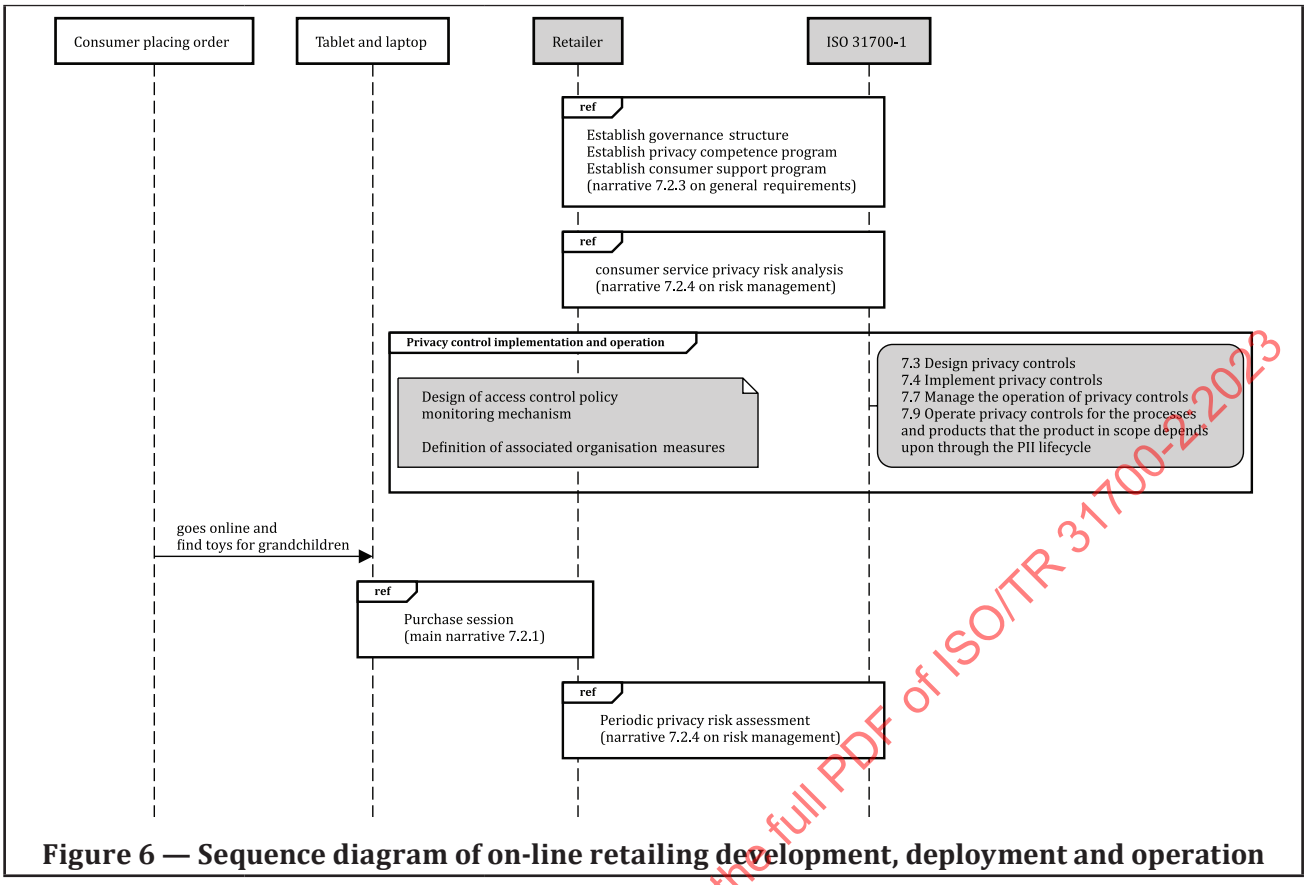

Figure 6 — Sequence diagram of on-line retailing development, deployment and operation

7.2.7 On-line retailing end of PII lifecycle

ID	Unique identification	UC 31700-01g
Use case name	Meaningful name	On line retailing
Narrative on end of PII lifecycle	Describe how requirements for end of PII lifecycle can help (possibly with a diagram)	Further to the consumer service privacy risk analysis, the development team is mandated to implement a privacy control for retirement of the service which includes a mechanism to keep track of all PII. Upon retirement, the mechanism is used to securely delete all PII that is no longer used or is at the end of the data retention lifecycle

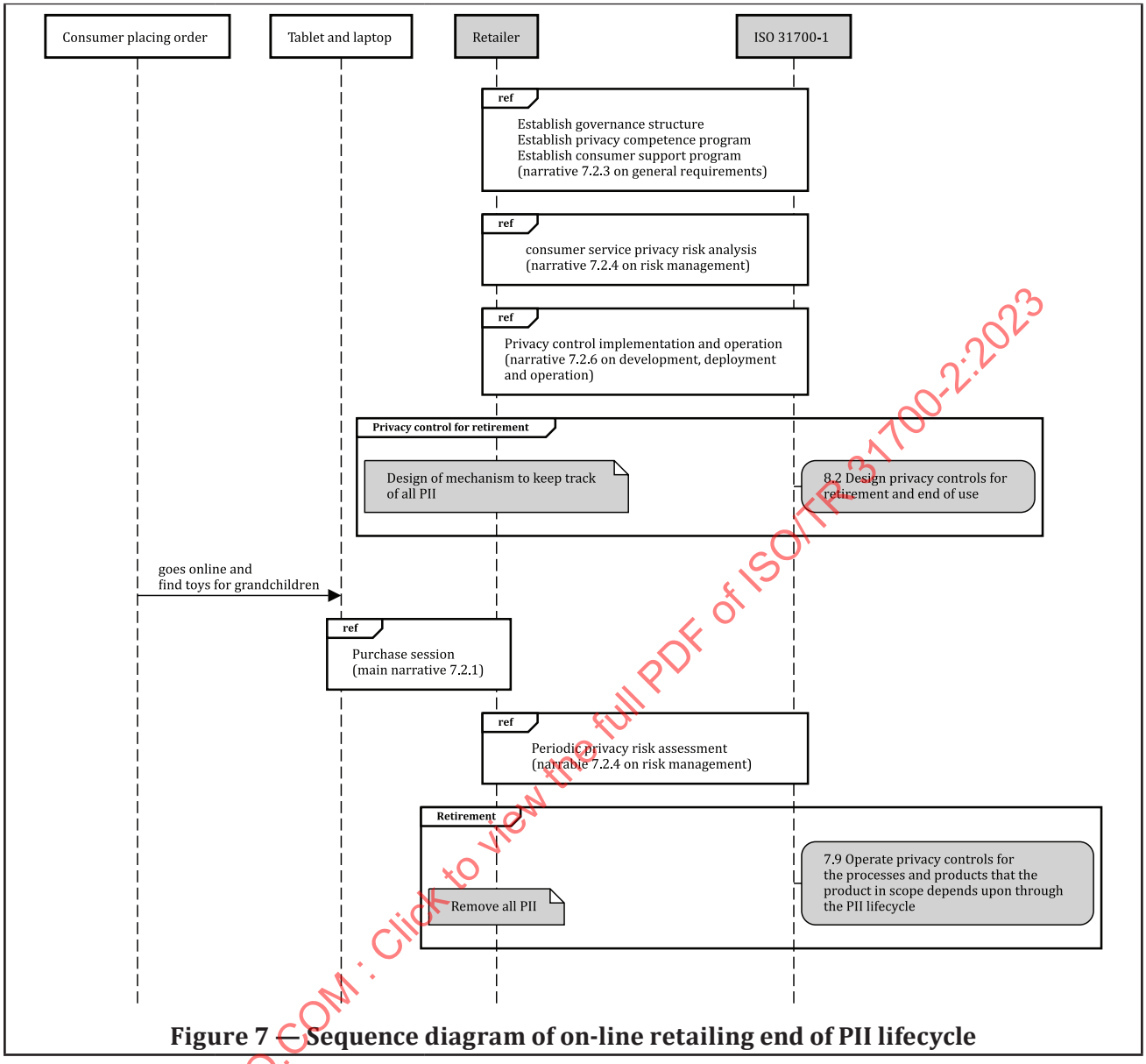

Figure 7 — Sequence diagram of on-line retailing end of PII lifecycle

7.3 Fitness company

7.3.1 Fitness company use case main description

ID	Unique identification	UC 31700-02a
Use case name	Meaningful name	Fitness centre
Description of product, service or process	Short description of product	A combined service that allows customers to practice physical activities in an external place and track their health info on their mobile phone.
Privacy protection goal	Short description of privacy protection goals	Ensure security of health info access on a mobile phone through biometric verification.
Ecosystem and systems of interest	Describe systems of interest	Fitness centre information system. Smart phone application. Smart watch with sensors.

Users	Describe users	Clients
Stakeholders	Describe stakeholders	Fitness company (FC) as data controller Health application provider (HAP) as data processor
PII	Describe PII processed	Health data in the smart phone Access data Data on location and time Client payment information Client name, address, email and phone
Product use purpose	Describe purpose of PII processing	Provide information on personal health (e.g., fitness, diet, health indicators).
Main narrative	Short narrative on consumer goods and services (possibly with a diagram)	A consumer goes to a fitness centre to get a membership. He provides his contact information and address. In order to process payment, he enters his credit card. The fitness centre asks the client if he wants to receive newsletters or become member of loyalty program. He declines. The fitness centre proposes the use of a smart health application with an additional subscription cost. The application can receive information provided by various sensors used in the fitness centre. The data is only collected in a protected zone of the smart phone and protected through a combination of password and biometric authentication. He accepts. The consumer can then practice activities in the fitness centre. It can then access collected health info. The heath info is not accessible by the fitness company nor by any other organisations

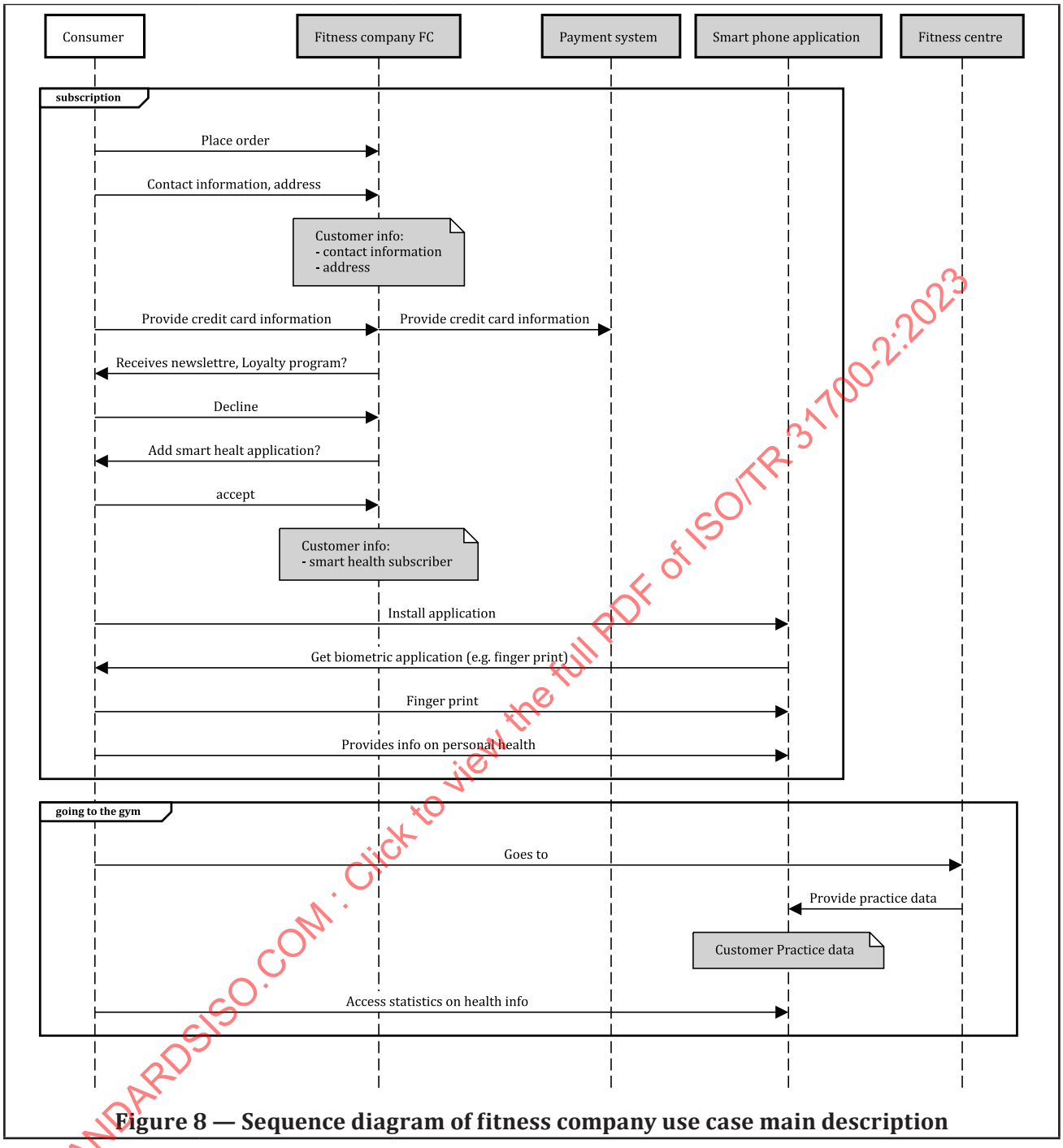

Figure 8 — Sequence diagram of fitness company use case main description

7.3.2 Fitness company risk management of health application

ID	Unique identification	UC 31700-02b
Use case name	Meaningful name	Fitness company

Narrative on risk management requirements	Describe how requirements on risk management can help (possibly with a diagram)	The fitness company FC undertakes with the help of the data protection officer, privacy consultants the development of an application that collects information on fitness practice and health data and helps consumers monitors their health. They contact a health application provider HAP, and start to carry out jointly a consumer service privacy risk analysis It includes assessment of the privacy capabilities of HAP that determines that HAP has the experience and competence to act as data processor. FC and HAP then work jointly on the requirements for privacy controls and agree to mandate the processing and storing data in a protected area in the smart phone. An assessment of the risk or non-authorised access leads to the use of the smart phone biometrics authentication for access. A periodic privacy risk assessment is carried out. The consumer support program is also evaluated. They can lead to some adjustments

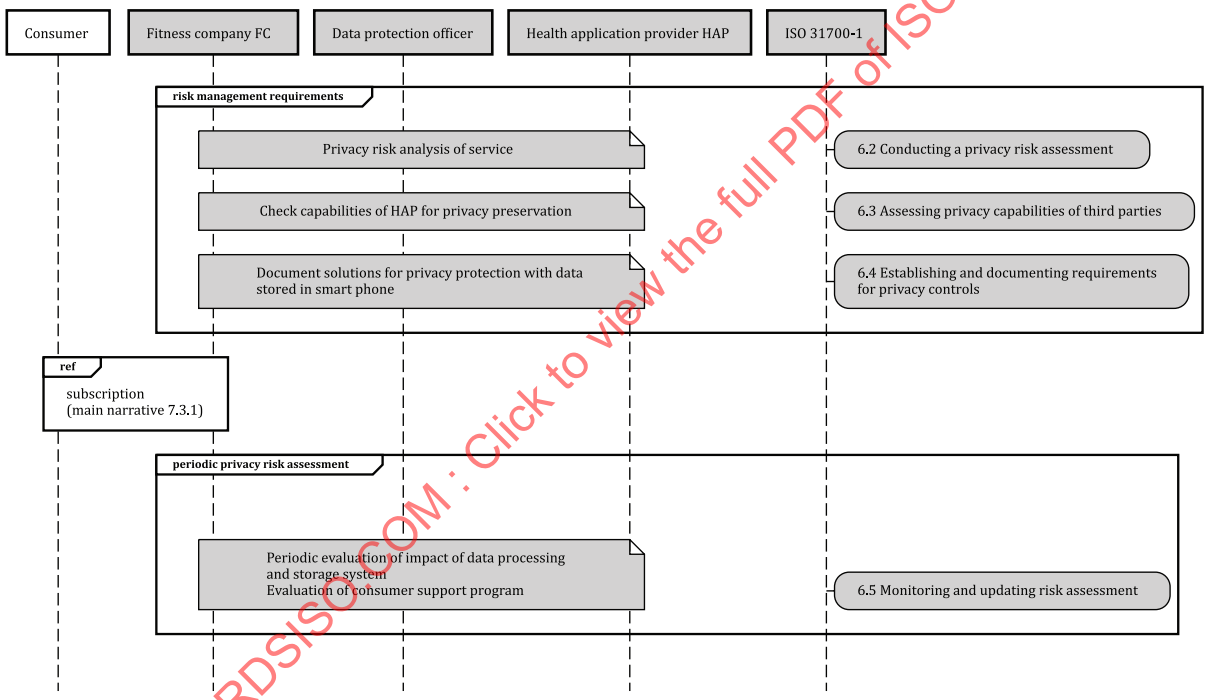

Figure 9 — Sequence diagram of fitness company risk management of health application

7.3.3 Fitness company consumer communication

ID	Unique identification	UC 31700-02c
Use case name	Meaningful name	Fitness company

Narrative on consumer communication requirements	Describe how requirements on consumer communication management can help (possibly with a diagram)	The Fitness company communicates on the features it is making available to ease access to its customers. With the help of the company data protection officer, it nominates a privacy communication manager who undertakes the creation of communication material on the privacy of the smart phone application. A customer is interested to take a membership. Further to an exchange with the customer enquiry service, it selects the health application option. A few months later, the press is reporting a privacy vulnerability in another health tracking smart phone application. The Fitness company undertakes an information campaign to its subscribers.

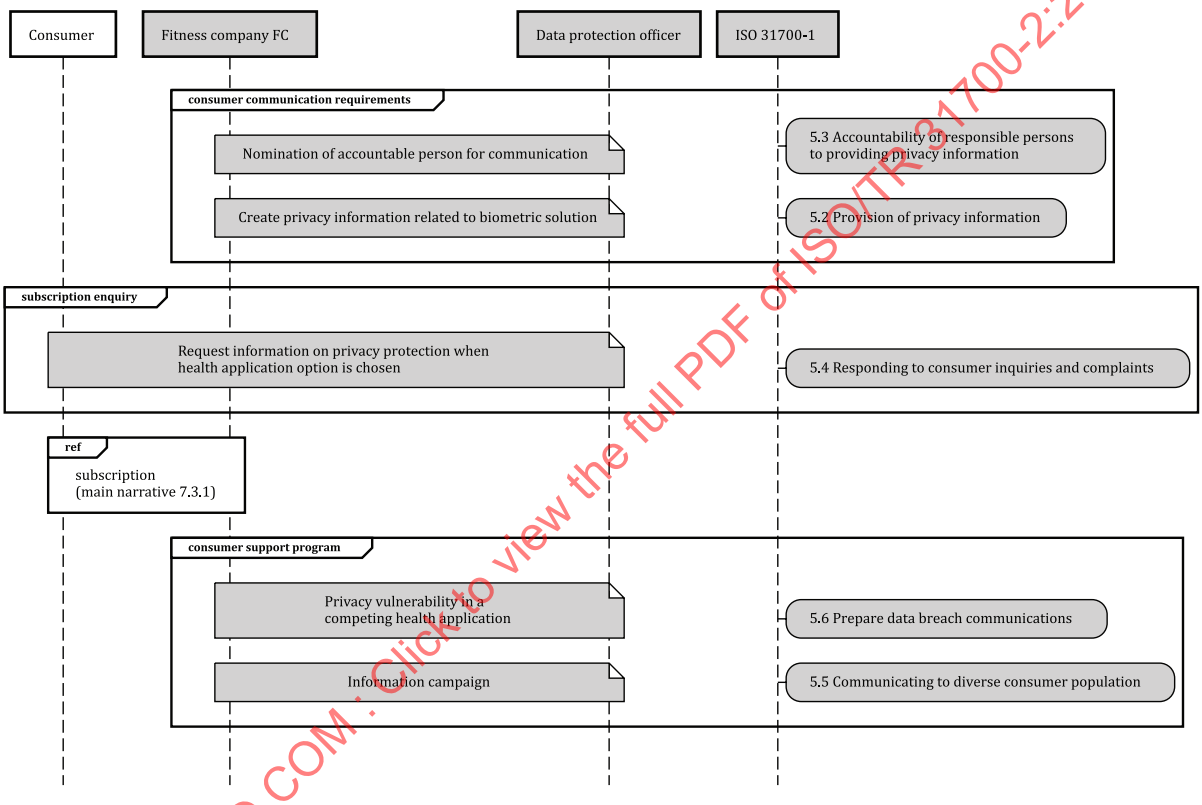

Figure 10 — Sequence diagram of fitness company consumer communication

7.4 Smart locks for homes front doors

7.4.1 Smart locks product line main description

ID	Unique identification	UC 31700-03a
Use case name	Meaningful name	Smart locks product line
		The smart locks product line includes the following components and functions:

Description of product, service or process	Short description of product	— connected lock: home Wi-Fi and Internet connected lock with control software to remotely open and close lock on receiving valid control instructions via Wi-Fi as well as opening and closing under manual control with lock status monitoring too; — smart lock application: application on smartphone providing ability to open and close the lock as well as monitor the condition of the lock open, closed, deadlocked, and physical integrity impacted; — unique smart key: domestic users have a unique smart key that they control, identified as an initial requirement from known potential for abusive use; — recording capability: household recording of smart lock use by occupants only available for each individual and their own records and no records access for other adult household members; — sharing data: option for householders to share their data re use of the smart lock with the others in the household; and — access to children record: the smart lock use record can be accessible by parents or guardians. Three use scenarios are considered in this use case: — basic use: existing smart lock registered householder enters home from outside using remote control facility; — colocation use e.g., flat sharing: lock use records shared; and — family use: data re children's use of the lock available to parents.
Privacy protection goal	Short description of privacy protection goals	Ensure privacy of access rights to the home. Ensure privacy and security of any use logs and records.
Ecosystem and systems of interest	Describe systems of interest	Other products that interwork with the smart lock are: — smart phones; — home Wi-Fi routers; and — internet service. The ecosystem includes organisations in the associated supply chain in order to ensure that the lifecycle of the used capabilities is aligned with the smart lock product lifecycle.
Users	Describe users	— Consumer users — Householder (entering home) — Other householders (for lock status update)
Stakeholders	Describe stakeholders	Stakeholders who use the smart lock technology Stakeholders who develop the technology
		Purpose 1 Basic use - Personal access control data: it is assumed that the designers have used the smartphone security capability to verify access to the phone itself. The data types are:

PII	Describe PII processed	— touch screen digital code entry to smartphone; — API data valid access to phone; — smart lock associated personal identification (e.g., Pat, Pete, Phyllis, Petra); and — unique smart key tokens. Purpose 2 secure storage of smart key data The data types are: — cyber-protected smart lock associated personal identification; and — cyber-protected unique smart key tokens. Purpose 3 Open lock remotely to enter the home: it ensures secure transmission of 'open' instruction to smart lock. The instruction is processed within the lock, resulting in the activation of the lock to open. The data types are: — smart lock IP address for routing instruction to the smart lock; — cyber-protected smart lock identification to link householders use to the correct lock; and — cyber-protected smart lock 'open' instruction data. Purpose 4 status of lock update: when a user enters and closes the door, the smart lock registers the change of status and communicates that to the smart lock householders. The data types are: — cyber-protected 'door closed' status data; and — smart lock App identification and IP addresses to route lock status update data to householders.
Product use purpose	Describe purpose of PII processing	Three scenarios: — basic opening: entry to home by one of its occupants; — co-location use: sharing of lock use information between householders; — family use: parental monitoring of children's use of the lock.
Main narrative on product line	Short narrative on consumer goods and services (possibly with a diagram)	Smart locks are an example of a consumer household product with a number of different users in the household. Further locks can be used by a number of different types of households. As in this example, many consumers choose household products that do not use cloud type services as part of their functionality, and so their use of the product involves only processing undertaken on consumer equipment. Even if not processed in the 'cloud', near field communications (e.g., Bluetooth or WIFI enabled communications) involving PII requires both privacy and therefore security of data transmission, processing and storage. Smart locks support a number of use scenarios to be examined for determination of privacy and security requirements and risk assessment. The following illustrates some of the different household privacy contexts and use of the product.

		— Adding a single occupant to smart lock use — Removing a single occupant from smart lock use — Child use of smart lock — Parental monitoring of child use — *Known unknown (at this point in time) adolescent circumvention of children monitoring* — Change of whole household occupancy — Landlord access to rented accommodation — Change of ownership of dwelling — Loss of 'smart key' assumed to be app on smartphone — Unauthorised return of previous occupant who has retained smart key — Use of stolen smart key capability — Malicious household Wi-Fi monitoring to gain smart lock access control or use information — Malicious use of smart lock in abusive relationships — Temporary access for friends and family to 'keep an eye on the home' while occupants away — Software update of product — Mechanical forcing or circumvention of lock — Locksmith services – installation, forced opening and or repair — Product use when product manufacturer support no longer available — Disposal of smart lock typically after replacement by new lock (several extra scenarios re second hand markets, recycling and disposal as waste) Security aspects: in addition to the security protection of stored PII and transmitted data the use cases integrate careful consideration of security access controls functionally designed into the product. If the product is going to be offered for use generically, then the security access controls for many types of household use is typically considered.

7.4.2 Smart locks basic configuration

ID	Unique identification	UC 31700-03b
Use case name	Meaningful name	Smart locks opening basic