International Standard

ISO/IEC 27561

First edition
2024-03

Information security, cybersecurity and privacy protection — Privacy operationalisation model and method for engineering (POMME)

Sécurité de l'information, cybersécurité et protection de la vie privée — Méthode et modèle d'opérationnalisation de la confidentialité pour l'ingénierie (POMME)

Reference number
ISO/IEC 27561:2024(en)

COPYRIGHT PROTECTED DOCUMENT

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 ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Symbols and abbreviated terms ... **7**

5 Context of privacy operationalization ... **7**
5.1 General ... 7
5.2 Privacy engineering viewpoint ... 7
5.3 Privacy engineering operationalization model ... 8
5.4 Privacy engineering operationalization method ... 8
5.5 POMME processes overview ... 8
5.6 Privacy and security ... 9

6 Initial information inventory process ... **10**
6.1 Purpose ... 10
6.2 Outcomes ... 10
6.3 Define and describe the TOA ... 10
6.4 Participant and information source identification ... 11
6.5 Systems and processes identification ... 11
6.6 Domains and domain owners identification ... 11
6.7 Intra-domain roles and responsibilities identification ... 12
6.8 Touch points identification ... 12
6.9 Data flows identification ... 12
6.10 PII identification ... 12

7 Privacy controls, privacy control requirements, capabilities, risk assessment and iteration process ... **13**
7.1 Purpose ... 13
7.2 Outcomes ... 13
7.3 Privacy control specification ... 14
7.4 Privacy control requirement specification ... 14
7.5 Capabilities specification ... 14
7.6 Risk assessment ... 15
7.7 Iteration ... 15

8 Privacy capabilities ... **16**
8.1 Capabilities overview ... 16
8.2 Capability details and associated functions ... 17
8.2.1 Core policy capabilities ... 17
8.2.2 Privacy assurance capabilities ... 18
8.2.3 Presentation and lifecycle capabilities ... 18

Annex A (informative) **Mapping of the privacy principles from ISO/IEC 29100 to POMME capabilities** ... **19**

Annex B (informative) **Lifecycle process example involving a PII controller and a solution provider** ... **20**

Annex C (informative) **POMME capability functions and mechanisms in a consumer application use case** ... **23**

Bibliography ... **28**

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 27, *Information security, cybersecurity and privacy protection*.

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

Privacy principles and associated privacy control requirements face a number of challenges arising from the need to comply with consumer expectations and global regulations for privacy which are continually evolving, as well as the complex and rapidly changing ecosystem of devices, networks and applications through which personally identifiable information (PII) flows. To face these challenges, privacy principles and associated privacy control requirements are expected to be operationalized into sets of capability functions and mechanisms. The privacy operationalization model and method for engineering (POMME) addresses these challenges, particularly in interconnected and interdependent applications and rapid lifecycle development processes.

Achieving effective operationalization in this environment is a critical responsibility of privacy engineers and the developers and solution providers who support them. They should not only understand the technology interfaces and interdependencies among components as they design these systems, but also ensure that the appropriate privacy controls are selected and implemented across the entire data flow landscape relevant to their analysis.

POMME provides a structured and extensible analytic model and method to accomplish these objectives. It is based on the OASIS Privacy Management Reference Model and Methodology (PMRM),[1] and it reflects findings expressed in ISO/IEC TR 27550, which provides extensive information on privacy engineering that organizations can use to integrate privacy engineering into system lifecycle processes. It also describes the relationship between privacy engineering and other engineering viewpoints (system engineering, security engineering, and risk management).

POMME supports the operationalization of privacy as it is defined in ISO/IEC 29100, utilizing a process following ISO/IEC/IEEE 24774. The primary focus of POMME is on the functional architecture and implementation details of privacy engineering, rather than the “policy” aspects of privacy, such as privacy principles, privacy impact assessments (PIAs) and privacy control statements. These policy elements are essential inputs into the engineering process and are already addressed by existing standards, codes of practice, and guidance listed in the Bibliography. POMME utilizes these elements to support the functional role of the privacy engineer.

Through the use of POMME, a privacy engineer can define the domain boundaries of a target of analysis (TOA) and research, document, and organize the information (e.g. standards, privacy policies, and technical data). By doing so, the capabilities necessary to implement privacy control requirements can be identified. This enables the privacy engineer to:

a) determine the functions needed to implement privacy control requirements;

b) understand the relationship among controls, particularly when controls are interdependent or networked or cloud-based;

c) select the specific implementation mechanisms (such as code or product configurations) that deliver the required privacy controls in their operational state.

An additional benefit of POMME is that its structured processes support improved usage and integration of privacy management tools, such as privacy-specific open source software.

Figure 1 and Table 1 illustrate the POMME operationalization model and method.

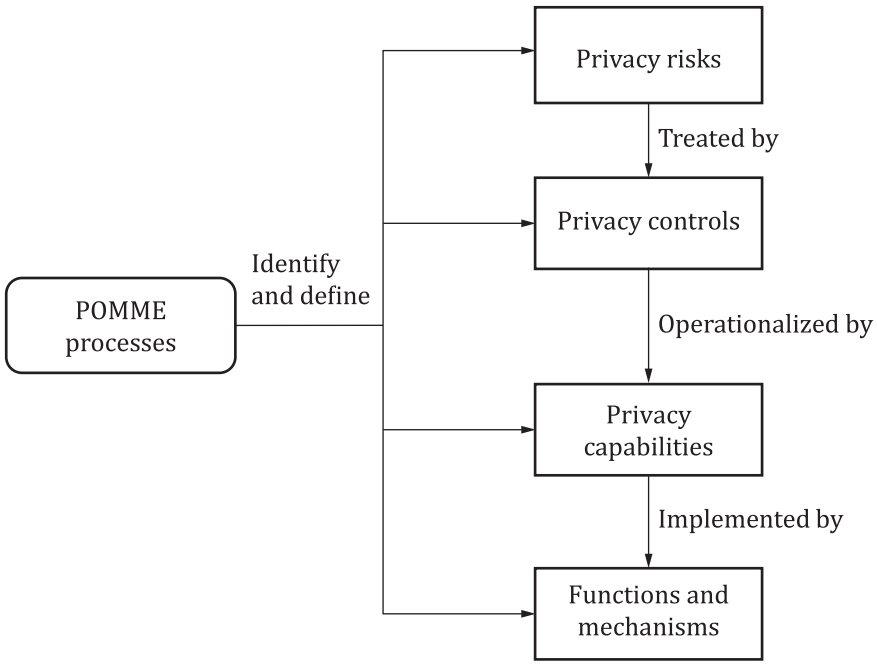


Figure 1 — POMME operationalization model

Table 1 includes an inventory process which consists of eight activities and an operationalization process which consists of five activities.

Table 1 — POMME method

POMME process	Clause	Activity
Initial information inventory process	6.3	Define and describe the TOA
	6.4	Participant and information source identification
	6.5	Systems and processes identification
	6.6	Domains and domain owners identification
	6.7	Intra-domain roles and responsibilities identification
	6.8	Touch points identification
	6.9	Data flows identification
	6.10	PII identification
Privacy controls, privacy control requirements, capabilities, risk assessment and iteration	7.3	Privacy control specification
	7.4	Privacy control requirement specification
	7.5	Capabilities specification
	7.6	Risk assessment
	7.7	Iteration

Information security, cybersecurity and privacy protection — Privacy operationalisation model and method for engineering (POMME)

1 Scope

This guidance document describes a model and method to operationalize the privacy principles specified in ISO/IEC 29100 into sets of controls and functional capabilities. The method is described as a process that builds upon ISO/IEC/IEEE 24774.

This document is designed for use in conjunction with relevant privacy and security standards and guidance which impact privacy operationalization. It supports networked, interdependent applications and systems. This document is intended for engineers and other practitioners developing systems controlling or processing personally identifiable information.

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
access capability
functionality enabling *personally identifiable information (PII) principals* (3.27) to access their *PII* (3.25) and propose changes, correction, or deletion

3.2
activity
set of cohesive tasks of a *process* (3.38)

[SOURCE: ISO/IEC/IEEE 15288:2023, 3.3]

3.3
actor
individual, or a digital proxy for an individual, who interacts with a *system* (3.41) that is processing *personally identifiable information* (3.25)

3.4
agreement capability
functionality that defines and documents the rules and options for the handling of *personally identifiable information* (3.25), consent documentation, as well as modifications to, and withdrawal of, consent

3.5
assurance capability
functionality that ensures that any *actor* (3.3), *domain* (3.10), *system* (3.41), or system component has the functionality necessary to carry out their assigned roles in processing *personally identifiable information* (3.25)

3.6
audit control
process (3.38) designed to provide reasonable assurance regarding the effectiveness and efficiency of operations and compliance with applicable policies, laws, and regulations

3.7
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.8
capability
ability of a *system* (3.41) to deliver a *function* (3.14), feature, or service

EXAMPLE "Provide confidential communication of PII in transit" is an example of a capability, whereas "encrypt data communicated to the server using TLS" is an example of a function.

[SOURCE: ISO/TR 4804:2020, 3.4, modified — substituted "product" with "system"; Note 1 to entry has been replaced by an example.]

3.9
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or *processes* (3.38)

[SOURCE: ISO/IEC 27000:2018, 3.10]

3.10
domain
set of assets and resources subject to a common privacy and security policy

[SOURCE: ISO/IEC 27033-1:2015, 3.35, modified — deleted "security" from "security domain"; added "privacy and" before "security policy".]

3.11
domain owner
stakeholder (3.40) responsible for ensuring that *privacy controls* (3.30) are implemented and managed in a *system* (3.41)

Note 1 to entry: A domain owner can be a *personally identifiable information (PII) controller* (3.26), *PII processor* (3.28), or *PII principal* (3.27) depending on the system(s) being analysed.

3.12
enforcement capability
functionality that achieves compliance with accountability requirements

Note 1 to entry: This *capability* (3.8) can initiate response actions, policy execution, recourse when audit controls and monitoring indicate operational faults and failures, record and report evidence of compliance to stakeholders, and provide evidence necessary for accountability.

3.13
exported privacy control
privacy control (3.30) that is transmitted to a *personally identifiable information (PII) controller* (3.26) or *PII processor* (3.28) in another *domain* (3.10) or *system* (3.41)

Note 1 to entry: An exported privacy control can be included in a data sharing agreement.

3.14
function
<capability> technical or manual process component of a *capability* (3.8)

EXAMPLE "Encrypt data communicated to the server using TLS" is an example of a function whereas "provide confidential communication of PII in transit" is an example of a capability.

Note 1 to entry: A function, feature or service is expressed at a more granular level than a capability.

3.15
incoming PII
personally identifiable information (PII) (3.25) flowing into a *domain* (3.10), or a *system* (3.41) or *process* (3.38) within a domain

3.16
inherited privacy control
privacy control (3.30) that is received by a *personally identifiable information (PII) controller* (3.26) or *PII processor* (3.28) from another *domain* (3.10) or *system* (3.41)

Note 1 to entry: An inherited control can be found in a data sharing agreement.

3.17
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.18
interaction capability
functionality that provides interfaces for presentation, communication, and interaction of *personally identifiable information (PII)* (3.25) and relevant information associated with the PII

Note 1 to entry: This can include user interfaces, system-to-system information exchanges, and agents.

3.19
internally generated PII
personally identifiable information (PII) (3.25) created within the *domain* (3.10) or *system* (3.41)

3.20
internal privacy control
privacy control (3.30) that is required within a *domain* (3.10) or *system* (3.41)

3.21
mechanism
<capability> specific implementation method of a *function* (3.14) in a *system* (3.41)

EXAMPLE Software, software configurations, firmware, technical products and solutions, technical settings, or detailed manual procedures.

Note 1 to entry: A mechanism is expressed at a more granular level than a function.

3.22
operationalization
knowledge compilation by conversion from a declarative form into a procedural, that is, operational form

[SOURCE: ISO/IEC 2382:2015, 2123014, modified — notes to entry have been deleted.]

3.23
outgoing PII
personally identifiable information (PII) (3.25) flowing out of a *domain* (3.10), or out of a *system* (3.41) within a domain to another system within the domain

3.24
participant
stakeholder (3.40) responsible for operational privacy management

3.25
personally identifiable information
PII
personal information
personal data
information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the PII principal. To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

[SOURCE: ISO/IEC 29100:2024, 3.7, modified — admitted terms have been added; removed "any"; substituted "can" for "might".]

3.26
PII controller
personal information controller
data controller
privacy *stakeholder* (3.40) (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.25) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others (e.g. PII processors) to process PII on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100:2024, 3.8, modified — admitted terms have been added]

3.27
PII principal
natural person to whom the *personally identifiable information (PII)* (3.25) relates

Note 1 to entry: Depending on the legal jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2024, 3.9, modified — Note 1 to entry has been added.]

3.28
PII processor
personal information processor
data processor
privacy *stakeholder* (3.40) that processes *personally identifiable information (PII)* (3.25) on behalf of and in accordance with the instructions of a *PII controller* (3.26)

[SOURCE: ISO/IEC 29100:2024, 3.10, modified — admitted terms have been added.]

3.29
privacy by design
approach in which privacy is considered at the initial design stage and throughout the complete lifecycle of products, *processes* (3.38) or services that involve processing *personally identifiable information* (3.25)

[SOURCE: ISO/IEC TS 27570:2021, 3.21, modified — removed hyphens from the term]

3.30
privacy control
measure that treats privacy risks by reducing their likelihood or their consequences

Note 1 to entry: Privacy controls include organizational, physical, and technical measures, e.g. policies, procedures, guidelines, legal contracts, management practices or organizational structures.

Note 2 to entry: Control is also used as a synonym for safeguard or countermeasure.

[SOURCE: ISO/IEC 29100:2024, 3.12]

3.31
privacy control requirement
specification for a *system* (3.41), product or service functionality to implement a *privacy control* (3.30) and operationalize the *stakeholders'* (3.40) desired privacy outcomes

Note 1 to entry: A privacy control requirement can be based on legal, regulatory, operational, or business/contractual requirements.

3.32
privacy engineer
individual with specialized knowledge of *privacy engineering* (3.33) concepts and practices and the ability to integrate privacy concerns into engineering practices for *systems* (3.41) and software engineering lifecycle *processes* (3.38)

3.33
privacy engineering
integration of privacy concerns into engineering practices for *systems* (3.41) and software engineering lifecycle *processes* (3.38)

[SOURCE: ISO/IEC TR 27550:2019, 3.14]

3.34
privacy impact assessment
PIA
overall *process* (3.38) of identifying, analysing, evaluating, consulting, communicating, and planning the treatment of potential privacy impacts with regard to the processing of *personally identifiable information (PII)* (3.25), framed within an organization's broader risk management framework

[SOURCE: ISO/IEC 29134:2023, 3.7]

3.35
privacy management
collection of policies, *processes* (3.38) and methods used to protect and manage *personally identifiable information (PII)* (3.25)

3.36
privacy policy
overall intention and direction, rules and commitment, as formally expressed by the *personally identifiable information (PII) controller* (3.26) related to the processing of *PII* (3.25) in a particular setting

[SOURCE: ISO/IEC 29100:2024, 3.14, modified – changed term to singular]

3.37
privacy principle
set of shared values governing the protection of *personally identifiable* information *(PII)* (3.25) when processed in information and communication technology systems

[SOURCE: ISO/IEC 29100:2024, 3.16]

3.38
process
interrelated or interacting activities that use inputs to deliver an intended result

[SOURCE: ISO 9000:2015, 3.4.1, modified — deleted "set of", notes to entry have been deleted]

3.39
security capability
functionality that provides the procedural and technical *mechanisms* (3.21) necessary to ensure the *confidentiality* (3.9), *integrity* (3.17), and *availability* (3.7) of *personally identifiable information (PII)* (3.25), and that safeguards privacy operations

3.40
stakeholder
person or organization that can affect, be affected by, or perceive itself to be affected by a decision or *activity* (3.2)

[SOURCE: ISO 9000:2015, 3.2.3, modified — note 1 to entry and example have been deleted.]

3.41
system
set of interrelated or interacting elements

[SOURCE: ISO 9000:2015, 3.5.1]

3.42
system-of-interest
system (3.41) whose lifecycle is under consideration

[SOURCE: ISO/IEC/IEEE 15288:2023 3.48]

3.43
target of analysis
defined and bounded *system-of-interest* (3.42) or *process* (3.38) that includes *personally identifiable information (PII)* (3.25) or in which privacy concerns are identified

Note 1 to entry: Security is integral to the analysis.

3.44
touch point
intersection of data flows with *actors* (3.3) or *systems* (3.41) or *processes* (3.38) within and across *domains* (3.10)

3.45
usage capability
functionality that ensures that the processing of *personally identifiable information (PII)* (3.25) complies with *privacy control requirements* (3.31)

Note 1 to entry: This capability primarily addresses controls associated with information minimization, linking, integration, inference, transfer, derivation, aggregation, pseudonymization, anonymization and disposal over the lifecycle of the PII.

3.46
use case
description of a sequence of interactions used to help identify, clarify, and organize requirements to support a specific business goal

[SOURCE: ISO/TR 31700-2:2023, 3.2, modified — removed “of a consumer and a consumer product”; notes to entry have been deleted]

3.47
validation capability
functionality that evaluates and ensures the information quality of *personally identifiable information (PII)* (3.25) in terms of accuracy, completeness, relevance, timeliness, provenance, appropriateness for use and other relevant qualitative factors

4 Symbols and abbreviated terms

PIA privacy impact assessment

PII personally identifiable information

POMME privacy operationalization model and method for engineering

PMRM privacy management reference model and methodology

TOA target of analysis

5 Context of privacy operationalization

5.1 General

POMME is a method for operationalizing the privacy principles specified in ISO/IEC 29100:2024, 6.1, in accordance with the terms and concepts expressed in ISO/IEC/IEEE 24774. POMME is based on the OASIS Privacy Reference Model and Methodology.[1]

ISO/IEC 29100 includes a set of 11 privacy principles, derived from widely-accepted principles developed by a number of states, countries, and international organizations. These principles guide the design, development, and implementation of privacy policies and privacy controls. These principles also serve as a baseline in the monitoring and measurement of performance, benchmarking, and auditing aspects of privacy management programmes in an organization.

POMME is also intended to be used in conjunction with privacy and system engineering standards such as ISO 31700, ISO/IEC/IEEE 15288, and ISO/IEC/IEEE 29148. It is also intended to enable privacy engineers to identify, analyse, and address issues that arise when operationalization requires the integration of different standards and policies.

NOTE 1 Annex A illustrates how POMME capabilities directly support the principles specified in ISO/IEC 29100.

NOTE 2 Information security is one of the 11 principles addressed in ISO/IEC 29100.

5.2 Privacy engineering viewpoint

Privacy engineering is applied to a system-of-interest, which can be a system, an application, a product, a service, or their associated capabilities. A system-of-interest is, in general, under the responsibility of one organization. There are cases where the system-of-interest is a system of systems, that is, a complex grouping of multiple systems, or a result of the integration of various systems under the responsibility of several organisations.

EXAMPLE A connected vehicle system can involve multiple automotive manufacturers, service providers, applications and networks.

Stakeholders having an interest in privacy engineering are:

— PII principals who are concerned for their privacy, and their ability to intervene in the processing and control of PII;

— policy makers who are concerned with enforcing privacy regulations and policies;

— business owners who are concerned with ensuring that the system they own is compliant;

— system developers who are concerned with the application of privacy engineering in the development lifecycle;

— solution providers who are concerned with the expectations of their customer related to privacy; and

— privacy advocates and experts who are concerned with ensuring that privacy and its implementations in products and services are correctly understood.

Privacy engineering includes three lifecycle process viewpoints:

— a goal-oriented viewpoint for privacy engineering, i.e. ensuring that business or functional objectives are met;

— a risk-oriented viewpoint for privacy engineering, i.e. ensuring that a risk assessment analysis has been carried out and that the corresponding controls for risk treatment are supported; and

— a collaboration-oriented viewpoint for privacy engineering, i.e. ensuring that agreement has been reached between relevant stakeholders when PII is transferred, shared, or derived.

5.3 Privacy engineering operationalization model

Privacy engineering operationalization refers to activities that take as input the privacy principles from ISO/IEC 29100, the privacy-by-design principles, all relevant data and information available from stakeholders and other sources, including supplementary policies and regulations. These activities ultimately contribute to the selection of functional capabilities that are used throughout the system's lifecycle processes.

Using this operationalization model, a system is structured into domains, including interfaces between domains called touch points. Additional operationalization activities involve the transformation of privacy management objectives into privacy engineering concepts, including the identification of privacy controls and privacy control requirements; the transformation of privacy control requirements into functional capabilities; and the iterative identification of privacy risks associated with the functional capabilities.

When operationalization activities involve multiple organisations, the operational interaction takes place through touch points. Capabilities that have been identified at the global level are transformed into capabilities at the organizational level. Additionally, when the deployment of a privacy control requires participation of an external vendor, the privacy engineer should document this information in their analysis and associated documentation to help ensure it is incorporated in the vendor's contractual obligations.

5.4 Privacy engineering operationalization method

The method for privacy engineering operationalization has the following characteristics:

— iterative with exit criteria to terminate the analysis;

— integrated into the system lifecycle processes;

— able to be mapped to existing approaches such as those specified in ISO/IEC/IEEE 15288, ISO/IEC TR 27550, ISO 31700, and frameworks, e.g. NIST privacy framework;[19]

— includes supplementary activities when multiple organisations are involved; and

— includes process steps that may be followed in any order and combination, as appropriate for an engineering analysis.

NOTE Software development lifecycle processes are fully addressed in the POMME. Annex B provides an example of a privacy engineering interaction involving a PII controller and a solution provider.

5.5 POMME processes overview

POMME incorporates two processes (see Clauses 6 and 7) and associated activities and tasks that enable privacy engineers to achieve successful operationalization. In summary, these processes:

a) define the use case, system, or entity of interest that is the TOA,

b) identify stakeholders and participants,

c) research and document all information and data relevant to the TOA using stakeholder and other relevant sources,

d) document, organize, integrate, and analyse this information and data, following a structured, repeatable method,

e) determine and document the privacy controls that are relevant to the TOA,

f) define and document the privacy control requirements necessary for the operationalization of the privacy controls,

g) select or provide advice on the functionality and the technical and procedural mechanisms necessary in the TOA in order to:

   1) implement privacy control requirements,

   2) integrate interdependent privacy control requirements, including those relevant to external systems,

   3) submit reusable assets (e.g. engineering components, privacy enhancing features) to the organization's reusable repository, whenever possible,

h) assess and address risks associated with operationalization,

i) perform iterative TOA research and analysis, as illustrated in Figure 2.

Figure 2 illustrates the interaction of POMME processes, which are described in Clauses 6 and 7.

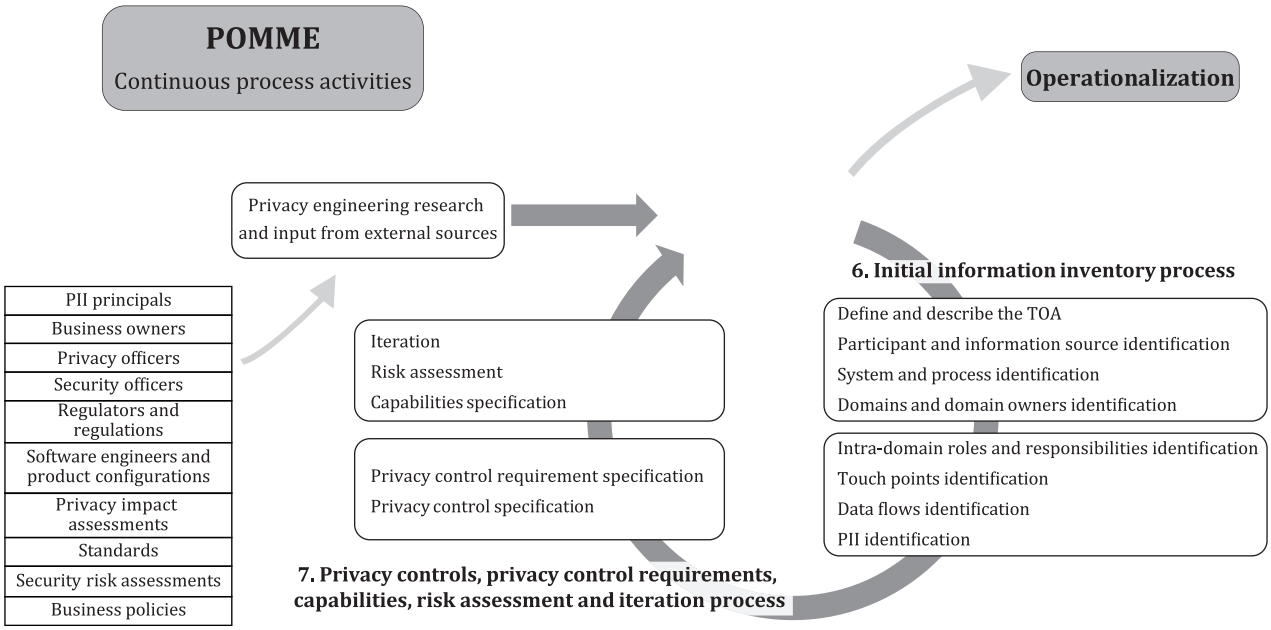


Figure 2 — POMME processes

5.6 Privacy and security

POMME treats security controls as integral to the TOA and not as an adjunct. Privacy controls and security controls should be completely integrated to provide privacy assurance. As explained in ISO/IEC 29100, adhering to the information security principle requires:

— protecting PII with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the PII;

— protecting PII against risks such as unauthorized access, destruction, use, modification, disclosure, or loss throughout the whole of its lifecycle; and

— protecting PII through appropriate controls in proportion to the likelihood and severity of the potential consequences, the sensitivity of the PII, the number of PII principals that can be affected, the PII processor involved, and the context in which it is held.

Beyond these determinants, POMME addresses the scope and importance of security controls in managing security risks associated with the operation of privacy control functionality in system processes, including processes having multiple interdependencies. For example, security failures affecting the availability of privacy functionality (e.g. a PII principal is denied access to their current consent agreements because of a compromised subsystem or cloud provider) extend beyond confidentiality protections.

6 Initial information inventory process

6.1 Purpose

The purpose of the initial information inventory process is to enable the privacy engineer to research and develop the essential baseline information that is required to define the privacy controls, privacy control requirements and capabilities that are appropriate for a TOA. This research may be undertaken by the privacy engineer or provided by external sources. This process includes the information collection and research necessary to define the requisite security controls and method of integration with the privacy controls. Since POMME addresses security as fully integrated with privacy (as defined in ISO/IEC 29100), including security controls, security control requirements, and capabilities, it is essential to identify and document this relationship in all activities.

This process involves discovering, creating, and documenting the inventory of participants, systems, business processes, domains, roles and responsibilities, touch points, data flows, PII, and privacy and security policies, thereby enabling a privacy engineer to define the necessary functions to instantiate control requirements in the TOA. This process includes information obtained by the privacy engineer through direct research or from external stakeholders and other sources.

NOTE The activities in this process are not necessarily intended to be followed sequentially. As additional information becomes available, the engineer contacts additional information sources related to the TOA.

6.2 Outcomes

Successful completion of the initial information inventory process leads to:

— identification of the TOA and its boundaries;

— identification of participants, systems, business processes, domains, roles and responsibilities, touch points, data flows and PII within the TOA;

— identification of the privacy and security policies applicable to the TOA;

— documentation of these elements for use by the privacy engineer and for further analysis and processes; and

— identification of information gaps or the need for additional research.

6.3 Define and describe the TOA

This activity defines, describes, and names the TOA and establishes the boundaries within which the process activities and tasks are undertaken.

The tasks of this activity are to:

a) determine the boundaries of the TOA and the scope of analysis,

b) provide a narrative description of the TOA,

c) provide a label or identifier for the TOA.

NOTE The label or identifier for the TOA provides an anchor usable for processes throughout lifecycle analysis, as well as for extensions to associated interdependent TOAs and ecosystem components.

6.4 Participant and information source identification

This activity identifies all individuals, entities, and roles (including PII principals, if applicable) that have a responsibility for operational privacy management in the TOA, as well as the source information used in the TOA.

The tasks of this activity are to:

a) identify and document the sources of information relevant to the TOA,

b) identify and document the privacy policies relevant to the TOA,

c) identify and document data controllers, data processors, sub processors, and other stakeholders such as privacy officers and security officers with privacy responsibilities relevant to the TOA, and document why they have been identified,

d) in organizations where naming an individual stakeholder is not possible or appropriate, identify the specific organizational entity or role with operational privacy responsibility,

e) obtain contact information for each stakeholder individual or role, as appropriate.

6.5 Systems and processes identification

This activity identifies the end-to-end spectrum of systems and processes through which PII is collected, stored, used, shared, transmitted, transferred across borders, retained, or disposed across the domains defined in the TOA.

The tasks of this activity are:

a) identify and document the systems and processes and the types or categories of PII that is processed within a domain,

b) prepare and document an architectural representation of the systems and processes, if this task is appropriate to the TOA.

6.6 Domains and domain owners identification

This activity identifies all domains and their respective owners that are associated with the systems and processes documented in the previous activity.

The tasks of this activity are:

a) identify and document the domains with each respective named owner, or optionally, the specific organizational role or owner,

b) document each system and related processes associated with their respective owners,

c) identify any additional information involving the identified owner or organizational role that can be relevant to the TOA,

d) include, as appropriate, details enabling contact with the domain owner.

NOTE 1 Domains can be under the control of PII principals or participants with a specific responsibility for privacy management within a domain, such as PII controllers, PII processors, PII sub processors, and other distinct entities having defined operational privacy management responsibilities.

NOTE 2 Individual domains can be “nested” within wider, hierarchically structured domains, which can have their own defined ownership, roles, and responsibilities. Domain owner identification is important to obtain accurate information and to establish accountability.

NOTE 3 A data processing agreement can serve to document domains and their owners. PII principals can have domain owner characteristics and obligations depending on the specific application design.

NOTE 4 Further guidance on PII handling based on user preferences and privacy preference administration can be found in ISO/IEC 27556.

6.7 Intra-domain roles and responsibilities identification

This activity identifies the different roles and responsibilities associated with PII within domains.

The tasks of this activity are to:

a) identify and document the roles and responsibilities assigned to specific participants, processes, and systems within a specific domain,

b) identify and document the specific areas of responsibility for participants who carry multiple roles.

6.8 Touch points identification

This activity delivers an end-to-end mapping of the intersection of data flows with actors or systems or processes within and across each domain in the TOA. This mapping illustrates the intersections of the data flows, which ensures a complete picture of all domains and systems and processes in which PII is processed, and establishes both physical and logical locations for processing and other actions.

The tasks of this activity are to:

a) identify the touch points at which the data flows intersect with actors or systems or processes within and across domains within the TOA,

b) document the location of PII input and output points for each PII-relevant system node,

c) create a mapping or architectural view of the touch points.

6.9 Data flows identification

This activity delivers a comprehensive detailing of the flow of both PII and privacy control requirements across touch points.

The tasks of this activity are to:

a) identify and document the data flows carrying PII, or privacy control requirements associated with the PII, among domains associated with the TOA,

b) map the identified data flows,

c) identify and document the PII input and output methods associated with the data flows.

NOTE 1 Data flows can be multidirectional or unidirectional.

NOTE 2 Security control requirements can be associated with data flows with respect to access control and authentication.

NOTE 3 Privacy control requirements, such as data minimization, have an impact on data flows.

6.10 PII identification

This activity delivers a comprehensive identification of the PII.

The tasks of this activity are to:

a) identify and document the PII collected, stored, used, shared, transmitted, transferred across borders, retained or disposed within domains or systems or processes in the following three categories:

   1) incoming PII (received from an external domain, system, or process),

   2) internally generated PII (created within a domain, system, or process),

   3) outgoing PII (sent to an external domain, system, or process),

b) identify and document PII characterized by special designation relevant to the TOA (e.g. sensitive or other designations) for each of the three categories.

NOTE 1 Incoming PII flows into a domain, or a system or process within a domain.

NOTE 2 Internally generated PII is created within the domain or system. Examples include device information, timestamps, location information, and other system-generated data that can be associated within a device or application and linked to an identity.

NOTE 3 Outgoing PII flows out of a domain, or out of a system within a domain to another system within the domain.

NOTE 4 PII can be defined at the degree of granularity appropriate for the scope of analysis and relevant privacy policies and privacy control requirements.

7 Privacy controls, privacy control requirements, capabilities, risk assessment and iteration process

7.1 Purpose

This process identifies and documents the operational components necessary to enforce the privacy policies and risk management objectives associated with the TOA. These include:

— the functions and/or mechanisms necessary to implement privacy control requirements in the TOA;

— the integration and sequencing of privacy delivery mechanisms (products, technologies, processes); and

— the privacy service delivery architecture appropriate for interdependent, complex networked systems.

The objectives and remit of the privacy engineer determine if the identification and documentation of capabilities extend to the mechanism level.

NOTE 1 The activities in this process are not necessarily intended to be followed sequentially. They become iterative. That is, as information becomes available, the engineer contacts additional information sources related to the TOA. For example, if additional PII processors or sub processors are identified, this can impact interdependent control requirements or functions. It is likely that the iteration of certain activities is necessary, resulting in modification to the documentation and decisions or recommendations of the privacy engineer.

NOTE 2 The remit given to the privacy engineer conducting a POMME analysis will also determine the limits of iteration cycles for the TOA.

NOTE 3 The identification of security controls, security control requirements, and security capabilities is essential to this process. They are documented in concert with the privacy controls, control requirements, and privacy capabilities.

7.2 Outcomes

Successful completion of the privacy controls, privacy control requirements, capabilities, iteration and risk assessment process results in:

— identification, categorization and documentation of all privacy controls, privacy control requirements, and capabilities identified within the TOA;

— identification, categorization and documentation of the relationships and interdependencies among privacy controls, privacy control requirements, and privacy capabilities;

— structured mapping of the relationships and interdependencies; and

— documentation resulting from iteration and risk assessment activity.

NOTE This mapping enables analysis and modifications over the lifecycle of the systems included in the TOA or extensions to the TOA.

7.3 Privacy control specification

This activity identifies and documents the privacy controls required in the TOA.

The tasks of this activity are to identify and document:

a) inherited privacy controls,

NOTE 1 The inherited privacy controls are required by an external source and received by a PII controller or PII processor. They can be required by a data sharing agreement.

b) internal privacy controls,

NOTE 2 The internal privacy controls are required within a domain or system within the domain.

c) exported privacy controls.

NOTE 3 The exported privacy controls are those that the exporting entity requires a PII controller or PII processor to implement in an external domain or in an external system within a domain. They can be required by a data sharing agreement.

7.4 Privacy control requirement specification

This activity focuses on operational implementation, in contrast to general and abstract privacy control policy expressions.

The tasks of this activity are to:

a) identify and document privacy control requirements associated with the identified privacy controls,

b) identify and document privacy control requirement interdependencies,

c) map the privacy control requirements to the inherited, internal, and exported privacy controls.

NOTE 1 In instances where privacy control statements address functionality, the privacy control and privacy control requirement are equivalent.

NOTE 2 Privacy control requirements can be based on legal, regulatory, operational, or business requirements.

7.5 Capabilities specification

This activity defines the capability functions and capability mechanisms necessary to operationalize privacy control requirements. Capability functions and capability mechanisms represent the two levels of functionality applicable to an operational implementation.

The tasks of this activity are to identify and document:

a) the capability functions required in the TOA,

b) the capability mechanisms required in the TOA,

c) the interdependencies among capability functions or capability mechanisms,

d) the risks associated with the operation of the interdependent capabilities.

NOTE The scope of a TOA and the privacy engineer's remit define the level of granularity (that is, the identification at the function or mechanism level) of the capabilities identified in the TOA.

7.6 Risk assessment

This activity addresses the need to comprehensively evaluate the privacy and security risks inherent in the TOA, including those related to operational interdependencies among capabilities.

The tasks of this activity are to:

a) examine all information identified and defined in the TOA from a risk management perspective,

b) identify and document privacy and security risks that can result from operationalization,

c) address any identified risks in the selection of controls, control requirements, or capabilities applicable to the TOA.

NOTE 1 This activity supports the method of privacy engineering operationalization, which is iterative and includes exit criteria (e.g. constraints on the ability of the privacy engineer to carry out additional iterative cycles of research and analysis, or constraints placed by the remit given to the privacy engineer for the analysis).

NOTE 2 POMME addresses technical and operational risks in a TOA (e.g. impact of a control failure in a process, information system, program, software module, or device) as well as risks associated with the processing of PII in conformance or in violation of privacy safeguarding as identified in a PIA. ISO/IEC 29134 provides guidelines for privacy impact assessments. Additionally, ISO/IEC 27557 addresses organizational privacy risk management.

NOTE 3 Iteration and risk assessment are interrelated and are especially important in operational systems because systems and their associated privacy controls are interconnected and interdependent.

7.7 Iteration

This activity addresses the need for privacy engineers to discover and analyse additional information impacting the TOA. As more information becomes available to the engineer while developing the TOA knowledge base, additional research can be needed. The additional information and analysis can require the iteration of processes and activities associated with the TOA.

The tasks of this activity are to:

a) iterate information gathering and stakeholder contact as necessary to ensure a complete and accurate knowledge base in order to operationalize privacy and security in the TOA,

b) undertake review of, and revisions to, processes, activities and tasks, as needed,

c) document the additional information for use in the TOA processes, activities, and tasks.

NOTE 1 This activity supports the method of privacy engineering operationalization, which is iterative and includes exit criteria (e.g. constraints on the ability of the privacy engineer to carry out additional iterative cycles of research and analysis, or constraints placed by the remit, given to the privacy engineer for the analysis)

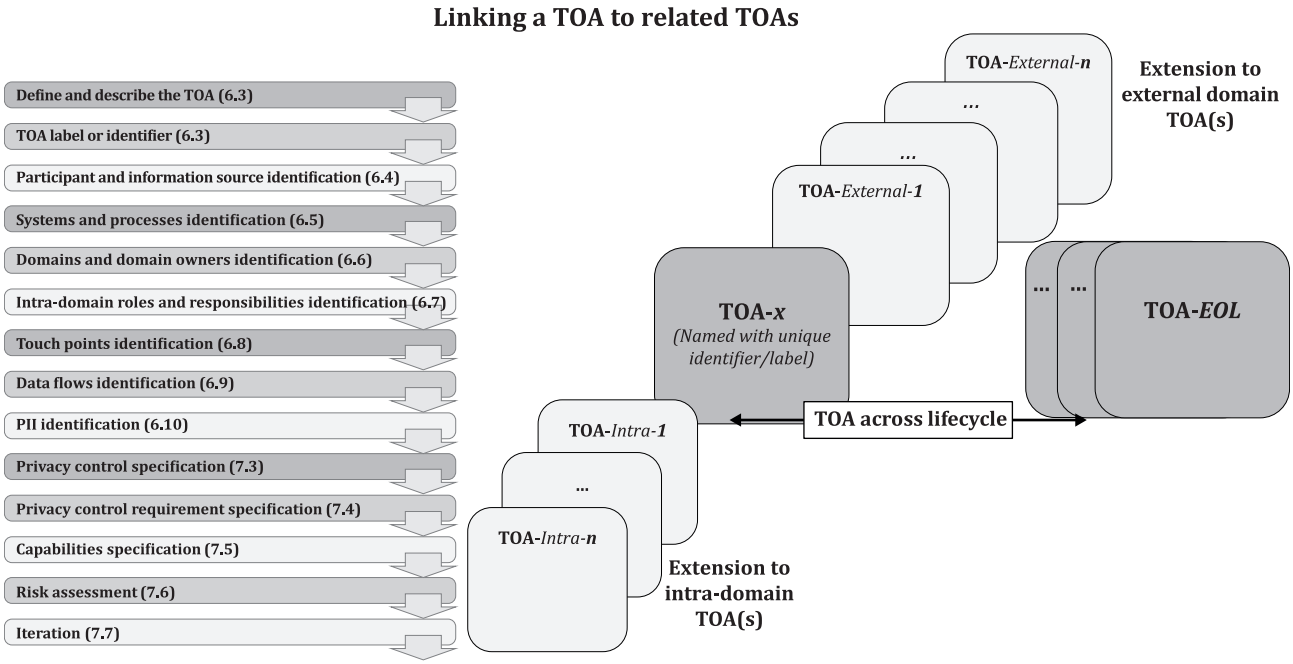
NOTE 2 This activity requires contact with additional stakeholders and repeated contact as necessary throughout both the information gathering and analysis processes.

NOTE 3 Iteration and risk assessment are interrelated and especially important in operational systems because systems and their associated privacy controls and capabilities can be interconnected and interdependent.

NOTE 4 In addition to iteration of TOA activities, any modifications contemplated, or recommendations made, during the lifecycle of the TOA can necessitate the update of the analysis and operational risk assessment. This includes the iterative and updated identification of both privacy and related security controls, control requirements, and capabilities.

NOTE 5 Iteration is also necessary, for example, when a TOA is impacted by the addition of, or changes to, interdependent systems or when the boundaries of the TOA are expanded to incorporate additional domains or systems.

An illustration of iteration across interdependent and linked TOAs and lifecycle is shown in Figure 3.



NOTE The numbers in parentheses on the left-hand side of this figure refer to the subclause numbers within this document.

Figure 3 — Iteration of POMME

8 Privacy capabilities

8.1 Capabilities overview

Capabilities and their associated functions serve as an analytic construct which enable privacy engineers to associate related privacy controls within a defined application. They do not replace privacy control requirements, but rather reflect general privacy functionality. They can provide support for privacy engineers in the analysis and documentation of applications by providing an organizing construct, particularly in complex systems.

The eight privacy capabilities are agreement, usage, validation, assurance, enforcement, security, interaction, and access. They are derived from the OASIS Privacy Reference Model and Methodology. [1]

Operational capabilities and associated functions also comprise an ontological construct that is useful for establishing the linkage between the required privacy controls and the functionality (both manual and automated) that is necessary for implementation.

The privacy capabilities represent groupings of privacy controls at a functional level. They serve as a tool and checklist for the design and selection of specific functions and mechanisms. The eight capabilities are grouped into three categories:

— core policy capabilities: agreement, usage;

— privacy assurance capabilities: validation, assurance, enforcement, security; and

— presentation and lifecycle capabilities: interaction, access.

These groupings, illustrated in Table 2, enable privacy engineers to compose the “architectural” relationship of the capabilities in an operational design. Annex C provides an expanded discussion and illustration of the

relationship and interaction of capabilities and their associated functions and mechanisms in the context of a consumer-focused use case.

NOTE The functions within each category are available for mutual interaction without restriction.

Table 2 — POMME capabilities

Core policy capabilities	Privacy assurance capabilities		Presentation and lifecycle capabilities
Agreement	Validation	Assurance	Interaction
Usage	Enforcement	Security	Access

Using these groupings of capabilities as a tool, a privacy engineer, system architect or technical manager can organize associated capabilities identified in a TOA. This capability tool can also stimulate design and analysis of the specific mechanisms that are required to implement privacy policies and controls, and to ensure their interoperability.

The capabilities encompass system and process functionality not typically described in privacy principles or not specifically addressed in typical privacy control statements. For example, functionality enabling the management and delivery of privacy controls across integrated systems is typically not addressed in privacy principles and privacy control statements.

Understanding such inferred functionality is necessary if systems and associated processes are intended to be made "privacy-configurable and compliant" and to ensure accountability. Without this understanding, enforcing privacy policies in a distributed, fully automated environment is not possible. This is a challenge for privacy engineers.

To address this challenge, the capability groupings provide an organizing structure that addresses the relationship among capabilities and their associated functions, and provides visibility into the operation of privacy management systems in applications and networks for participants and stakeholders. The use of capabilities can also help achieve a more complete understanding of the interaction of privacy controls and their operation.

The capabilities support a detailed privacy engineering analysis, interact with one another, and, in many applications, are co-dependent. Operationally, they encompass an interrelated set of privacy control requirements identified by the privacy engineer.

A capability and its associated functions can interact with one or more other capabilities and their functions. In other words, functions under one capability category can be interdependent with functions under another capability category (e.g. "pass information to a new function for subsequent action"). The capabilities can interact in an arbitrary, interconnected sequence to operationalize a privacy management task or a set of privacy lifecycle policy and control requirements. A detailed privacy engineering analysis should illustrate such interactions and their sequencing.

8.2 Capability details and associated functions

8.2.1 Core policy capabilities

8.2.1.1 Agreement capability

The agreement capability constitutes a functionality that:

a) defines and documents permissions and rules for the handling of PII, based on applicable policies, individual preference and consent, and other relevant factors,

b) provides relevant actors with a mechanism to negotiate, modify or establish new permissions and rules,

c) expresses the agreements for use by other capabilities.

8.2.1.2 Usage capability

The usage capability ensures that the use of PII complies with the terms of any applicable consent agreement, policy, law or regulation, as well as privacy control requirements related to information minimization, linking, integration, inference, transfer, derivation, aggregation, pseudonymization, and anonymization, storage and destruction over the lifecycle of the PII.

8.2.2 Privacy assurance capabilities

8.2.2.1 Validation capability

The validation capability ensures the information quality of PII in terms of accuracy, completeness, relevance, timeliness, and other relevant qualitative factors.

8.2.2.2 Assurance capability

The assurance capability ensures that any actor, domain, system, or system component has the functionality necessary to carry out its assigned roles in processing PII.

8.2.2.3 Enforcement capability

The enforcement capability constitutes a functionality that:

a) initiates continuous monitoring capabilities to ensure the effective operation of all capabilities,

b) initiates response actions, policy execution, and recourse actions when audit controls and monitoring indicate operational faults and failures,

c) records and report evidence of compliance to stakeholders or regulators,

d) provides data needed to demonstrate accountability.

8.2.2.4 Security capability

The security capability constitutes a functionality that:

a) enables the trustworthy processing, communication, storage, and disposition of privacy operations,

b) provides the procedural and technical mechanisms necessary to ensure the confidentiality, integrity, and availability of PII.

8.2.3 Presentation and lifecycle capabilities

8.2.3.1 Interaction capability

The interaction capability constitutes a functionality that:

a) provides generalized interfaces necessary for presentation, communication, and interaction of PII and relevant information associated with PII,

b) encompasses functionality such as user interfaces, system-to-system information exchanges, and agents.

8.2.3.2 Access capability

The access capability enables PII principals to review their PII and to propose changes, corrections, or deletions, as required or allowed by permission, consent, policy, or regulation.

Annex A
(informative)

Mapping of the privacy principles from ISO/IEC 29100 to POMME capabilities

Table A.1 shows the mapping of POMME capabilities to ISO/IEC 29100 privacy principles.

Table A.1 — Mapping POMME to ISO/IEC 29100

Privacy principles specified in ISO/IEC 29100	POMME capabilities
Consent and choice	Interaction, agreement, access, security, usage
Purpose legitimacy and specification	Interaction, agreement, usage, security
Collection limitation	Usage, assurance, interaction, agreement, security
Data minimization	Agreement, usage, security
Use, retention, and disclosure limitation	Agreement, usage, security
Accuracy and quality	Validation, assurance, enforcement, security
Openness, transparency, and notice	Interaction, agreement, access, security
Individual participation and access	Access, validation, usage, enforcement, security
Accountability	Assurance, usage, enforcement, interaction, access, security
Information security	Security, usage, assurance
Privacy compliance	Enforcement, assurance, security

As stated in 7.5, the privacy engineer identifies the specific capability functions and capability mechanisms as appropriate for the engineering analysis of the TOA under consideration (see 8.1 for further information). As an example of this association, Table A.2 displays the consent and choice principle and its associated five capabilities, illustrating the linkage of functions and mechanisms with each capability.

Table A.2 — Example of functions and mechanisms associated with capabilities

Capability	Functions and mechanisms
Interaction	function 1…n mechanism 1…n
Agreement	function 1…n mechanism 1…n
Access	function 1…n mechanism 1…n
Security	function 1…n mechanism 1…n
Usage	function 1…n mechanism 1…n

NOTE 1 ISO/IEC 29100 lists privacy principles as well as sets of practices that demonstrate adherence to each of these principles. For the purposes of this document, the practices that are primarily operationally focused are of greatest relevance to the privacy engineer. Practitioners can consult ISO/IEC 29100 and the adherence practices when evaluating the privacy engineering aspects of a TOA.

NOTE 2 The security capability is included in Table A.1 for all privacy principles to reinforce the association of security and privacy, as discussed in 5.6.

Annex B
(informative)

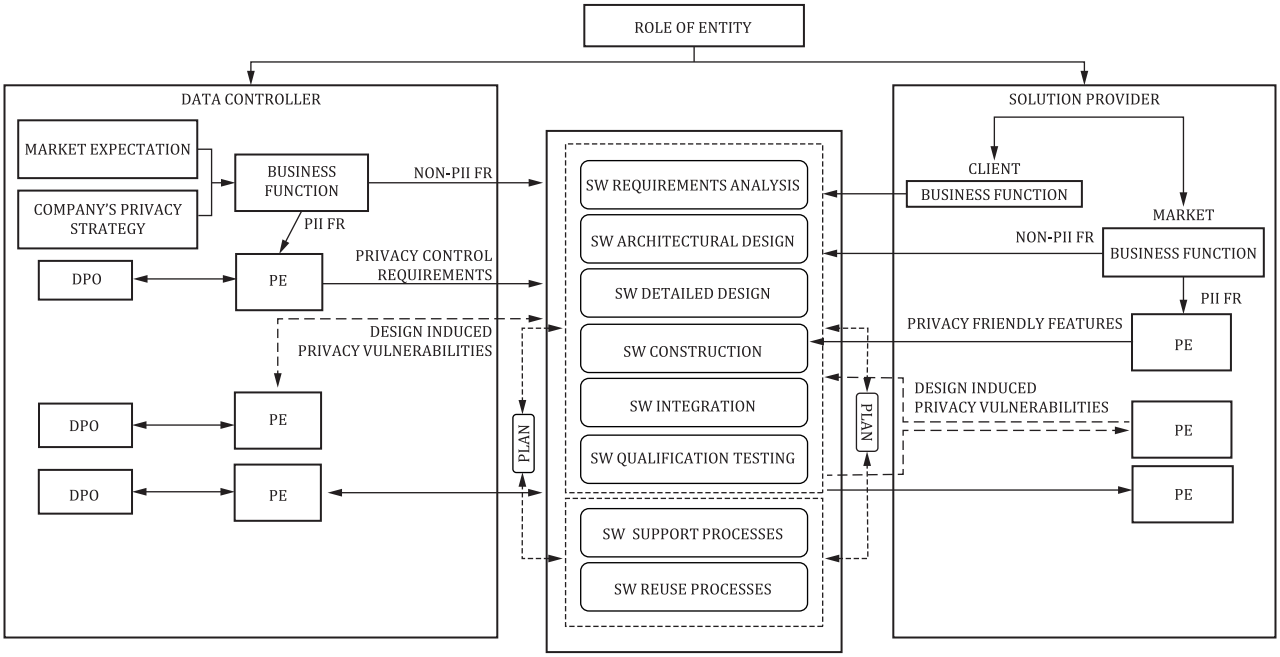
Lifecycle process example involving a PII controller and a solution provider

When following POMME processes, it is fundamental to establish the roles played by organizations and individuals contributing to the privacy engineering objectives within the scope of an entity of interest (e.g. a company going to market with a new application that includes privacy concerns). The roles played by the organizations (see ISO/IEC TR 27550:2019, Table 2) can help to establish a common understanding of the taxonomy used in this annex.

ISO/IEC TR 27550:2019, Figure B.3 illustrates the important difference between conventional programming and Agile programming and their potential treatment when using POMME. Lifecycle processes in conventional programming are carried out in sequence (e.g. A followed by B followed by C), while in Agile programming, each sprint process can contribute to an incremental outcome of A, B and C. In any methodology where outcomes are incremental in nature, the lifecycle can repeat in an iterative or recursive fashion. This implies that the privacy engineering considerations should be modularized to meet the needs of the sprint or the individual iterations driving the specific outcome for a given iteration.

In addition, focus should remain on the overall goal of the privacy engineering program with respect to the final outcome expected by the entity of interest, which can include an overall analysis of multiple TOAs impacting the lifecycle. This can be achieved by analysing the iterations and the overall goal, not only from a functional privacy perspective, but also from a privacy risk perspective (see 7.6 for details). This can also enable the stakeholders to establish a cost-benefit map of the privacy controls and measures that, when implemented in the right stage of the lifecycle, can produce the optimal functional outcome for privacy operationalization of a product or service, while also providing maximum benefit from a privacy engineering goal perspective.

An example of a privacy engineering interaction scenario using the POMME in a PII controller and solution provider lifecycle scenario is depicted in Figure B.1.



Key

DPO data privacy officer
FR functional requirement
PE privacy engineer
SW software

Figure B.1 — Privacy engineering interaction in a data controller/solution provider scenario

In this lifecycle scenario, while non-PII related functional requirements (non-PII FR) can be directly taken as input for requirements engineering, the PII related functional requirements (FR) – referred to as privacy compliant functional requirements - are assessed by the privacy engineer (PE) and the data privacy officer (DPO) before they are taken forward. This is because privacy control requirements emerging from data privacy regulations can impact the non-PII functional requirements of the solution.

Examples of this impact include:

— the type of processing that can be undertaken;

— the stage when PII can be collected;

— the particular types of processing that are permitted based on the legal basis for the collection of PII;

— geographic location of the cloud storage server; and

— whether biometric authentication is permissible.

The outputs of this analysis by the PE and DPO are new privacy control requirements that become input for identifying enabling capabilities, functions, and mechanisms, as provided in POMME.

Figure B.1 depicts two distinct but interdependent elements:

a) Where the role of the privacy engineer in a software development lifecycle is performed as part of the privacy engineering activity that is within the data controller organization.

This element is illustrated on the left-hand side of Figure B.1, labelled “data controller.” The privacy control requirements in this case are driven primarily by market expectations as well as the controller organization’s privacy strategy. While non-PII related functional requirements are directly decided upon by the associated business functions, PII-related functional requirements are assessed by the privacy engineer. In this example, with oversight from the data controller organization’s DPO, the privacy engineer can define

the privacy control requirements to be addressed during the development lifecycle, by using the methods and definitions of POMME.

b) Where the role of the privacy engineer is performed within the solution provider organization.

This is illustrated in the right-hand side of Figure B.1, labelled “solution provider.” In this case, the privacy requirements are considered throughout the software development lifecycle and are primarily driven by the requirements from clients and market expectations. In the context of the solution provider, the privacy friendly features introduced by privacy engineers of the solution provider organization can also be driven directly by interaction with a customer seeking specific privacy controls and capabilities from the solution provider. Such interaction is depicted in Figure B.1.

The key distinction between the data controller and solution provider contexts, as shown in Figure B.1, is the absence of a specific role for a DPO for the solution provider. Here, the privacy engineer is part of the application development team, and the solution provider’s DPO does not have advisory and inspection role. Although Figure B.1 depicts both data controller and solution provider together, they can exist independently. In the case of a solution provider, the DPO would be part of the data controller organization (which is not shown in Figure B.1), for which the solution is intended to be built by the solution provider.

In both scenarios described above, during the various stages of an iterative development approach, it is possible that privacy vulnerabilities are introduced by virtue of changing other design parameters or considerations during the software development process. These possibilities are collectively indicated as “design induced privacy vulnerabilities” in Figure B.1.

Such vulnerabilities can be accounted for and remediated in tandem with the rest of the development process by continuously engaging the privacy engineer to assess, evaluate and treat the impact of changes in design considerations during the various software development stages. POMME processes support continuously focusing on outcomes that meet the privacy engineering operationalization objectives of the TOA(s) (see 7.7 for details) in various, real-world lifecycle scenarios, such as the example illustrated in Figure B.1.

Annex C
(informative)

POMME capability functions and mechanisms in a consumer application use case

C.1 General

This annex provides simplified examples of capability functions and mechanisms for a new consumer fitness data application being considered for development by a global fitness company. A use case template modelled from ISO/TR 31700-2 describes the overall consumer application. Table C.1 describes this use case.

The privacy engineer in this example is a fitness company employee and is directed to focus on one specific element – a wearable "Fitness Tracker" device that a consumer will use while exercising - and to conduct a POMME analysis. The engineer provides preliminary recommendations regarding necessary privacy and security control requirements and operationalization capabilities.

The capability functions and mechanisms in Table C.2 are presented as simplified, representative examples only, and are not as detailed or comprehensive as would result from an actual POMME analysis.

Table C.1 — Use case description from a consumer-business perspective

Use case name	**Fitness company exercise fitness data application**
Description of product, service, or process	This networked service application enables customers of a global fitness centre company to track and review aggregated fitness and exercise-related information captured during the use of the fitness centre in any the company's global facilities with specialized equipment. During each exercise session, registered customers wear a portable device supplied by the fitness centre. The device is initialised by the customer at a dedicated kiosk, enabling the device to receive exercise data from each of the exercise machines used by the customer during their workout. The data include the exercise machines used and time duration using each machine, weights or other machine settings, duration of exercise sets, and estimated calories expended. The date, total duration of the workout and the fitness centre location are also recorded. At the end of a complete exercise session, the customer transfers the exercise data from the portable device to a fitness centre kiosk, where the integrated data are transmitted to an external processor, associated with the customer's data record, and integrated with data collected at prior exercise sessions. The historical exercise data are accessed by the customer via a separate application available on the customer's personal smart phone or via a Web interface.
Privacy protection goal	Ensure security and privacy of fitness and physical activity-related PII and other PII associated with the customer.
Ecosystem and systems of interest	Fitness centre local area network; external data processor hosting the backend exercise data processing and storage systems; fitness centre supplied device; fitness centre exercise machines; fitness centre kiosks; exercise and a tracking application accessed by the customer on a smart phone or at the fitness centre Web portal.
Users	Fitness company customers who have registered to use the fitness data application.
Stakeholders	PII principal/customer; fitness company as data controller; fitness company executive responsible for launch of the application; external data processor; application developer team leader; fitness company Chief Privacy Officer (CPO) and Chief Information Security Officer (CISO).

Table C.1 *(continued)*

Use case name	Fitness company exercise fitness data application
PII	Customer's name, address, and other registration information; exercise data including exercises machines used, levels of exertion, duration of exercises, intensity of exercise at each workout station, calories burned at each station, date, time, and location of workout; data stored and processed by the external data processor for access by the customer's smart phone and Web fitness application.
Product use purpose	Tracks and provides information related to customer's exercise regimen, useful for evaluating workouts, times, location, intensity, distances, and health parameters (e.g. calories consumed, strength), aggregated to support the fitness and workout objectives of the customer.
Main narrative and figures	A customer who has previously registered to use the fitness data application offered by the global fitness company goes to a fitness centre location where this program is available. The customer is provided a specially designed, wearable fitness tracker device and initialises the device at a kiosk. The device communicates with the exercise equipment in the facility during its use by the customer. Following a complete workout, the customer offloads data from the smart device at the kiosk. The data are communicated from the kiosk to the external data processor. Using a downloadable app or Web access, the customer can, at any time, access all historical exercise-related information and PII.

C.2 POMME Initial information inventory process scenario

NOTE This refers to the activities specified in 6.3 to 6.10.

In this simplified scenario, the privacy engineer is an employee of the fitness company. The engineer is tasked with conducting a preliminary analysis of the fitness tracker device and reporting findings and initial recommendations regarding privacy and security to the company executive. The initial information inventory process is defined in one TOA, including the fitness tracker and its interaction with the kiosk and exercise machines. The engineer consults with the CPO, the CISO, the company development team manager, the executive leading the project, and other relevant sources. The information received is documented and updated as the inventory process continues.

Given that the engineer confirms that the fitness tracker development will be completed internally, the primary list of participants and information sources are all within the company domain. The privacy engineer uses a label and information management schema and tool (such as a Graph Database) to record all TOA data developed throughout the POMME analysis.

The engineer confirms the data flows and touch points in and out of the device including PII and associated privacy and security controls. The engineer documents associated contact information.

C.3 Privacy controls, privacy control requirements, capabilities, risk assessment and iteration process

NOTE This refers to the activities specified in 7.3 to 7.7.

The privacy engineer further identifies and documents the specific privacy controls, privacy control requirements and capability functions and mechanisms associated with all domain systems and processes within the scope of the TOA.

Since application operationalization environments and ecosystems are unique, the engineer identifies interdependent privacy and security functions and mechanisms to assess their implementation and to manage the risks associated with operationalization of the TOA including failures of interdependent operations. Throughout all POMME process activities, the engineer regularly carries out iterative information gathering and analysis, revisiting information sources and making modifications, additions, and deletions of the TOA knowledge base revising initial findings within the TOA, as needed.

C.4 Capability functions and capability mechanisms mapped to privacy capabilities

For the purposes of this fictional, simplified illustration, it is assumed that the engineer has completed all POMME process activities relevant for a preliminary application analysis and a TOA report to the application executive (these are not presented in this annex.) The engineer understands that the TOA is part of a much larger application ecosystem, with both internal and external domains, systems, and processes. The privacy and security controls, control requirements, and capability functions and mechanisms associated with these interdependent externalities will also impact the management decisions made by the application executive and the other stakeholders associated with building, operationalizing, funding, and marketing this new application. To comprehensively address all privacy and security objectives to bring this application to market, the engineer's initial recommendations are only a beginning stage for analysing the larger ecosystem issues in the use case.

Figure C.1 is a representation of the overall application ecosystem, including domains, data flows and touch points within the TOA. An actual analysis would include details regarding the data flowing across the touch points. Data flows from TOA domains to external domains are not illustrated in this example.

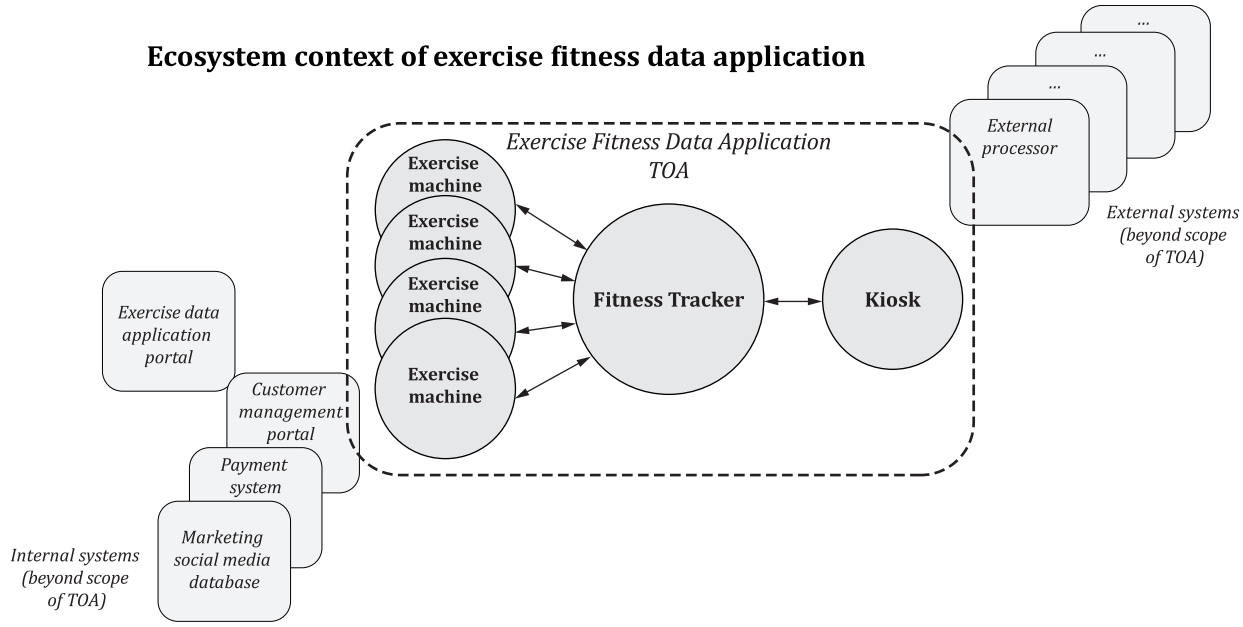


Figure C.1 — Ecosystem context of exercise fitness data application

Table C.2 represents a very limited illustration of the capability functions and mechanisms that would be identified in an actual POMME analysis of even this simplified scenario. Its purpose is to show examples of privacy capabilities only, not a comprehensive list.

Table C.2 — Example TOA: Fitness tracker and kiosk capability functions and mechanisms

Capabilities		Examples of capability functions	Examples of capability mechanisms
Core policy capability	Agreement	Obtaining and retaining evidence that the user clicked on the consent option on the touchpad.	— Implementing a system within the kiosk that records the customer's and fitness tracker's interactions with the kiosk, including the touchpad. — Retaining consent data in a secure file in the kiosk until it has been transmitted to the backend-server.
	Usage	Ensuring the customer account identifier is pseudonymized on the fitness tracker, consistent with corporate privacy policy.	— Implementing code in the kiosk to create and transmit a randomly generated string to use as the pseudonymous identifier in the fitness tracker. — In the kiosk, linking the pseudonymous identifier to customer's account information to enable exercise data transmission to the customer's exercise data record.
Privacy assurance capability	Validation	Ensuring data received by the kiosk from the fitness tracker at the end of the exercise session has been checked for quality and completeness, and anomalies are detected and stored in the kiosk.	— Writing data validation code for kiosk that checks all data recorded on the fitness tracker to ensure completeness and to record anomalies.
	Assurance	Ensuring that the interdependent mechanisms of the kiosk and fitness tracker are implemented effectively to meet privacy and security control requirements.	— Developing test code to verify that the privacy controls between the kiosk and fitness tracker are properly configured and are operational. — Initiating verification testing and document results.
	Enforcement	Detecting and recording operational faults and failures in the processing of exercise data contained in the fitness tracker and kiosk.	— Developing code in the kiosk that will identify and record operational faults or failures. — Developing code for the fitness tracker that will identify and record operational faults or failures. — Implementing visual indicators for the fitness tracker device so user is aware that the device is operating properly during exercise sessions.
	Security	Developing cryptographic functionality to ensure that data on the fitness tracker are not accessible by unauthorized third parties.	— Using PKI solution to ensure that all data on the Fitness Tracker is encrypted and may only be decrypted when connected to the kiosk. — After successful transmission and decryption of the fitness tracker's data at the kiosk, the kiosk triggers the erasure of all data on Fitness Tracker.

Table C.2 *(continued)*

Capabilities		Examples of capability functions	Examples of capability mechanisms
Presentation and lifecycle capability	Interaction	Displaying a consent option for the customer on the kiosk.	— Present consent screen on kiosk which includes the options to consent or not consent to the collection of personal data by the fitness tracker and an option to read the consent agreement. — Setting the system so that it requires users to confirm consent on the touchpad to initialize the fitness tracker.
	Access	Enabling PII principals to review their PII collected by this application during exercise sessions and propose changes, corrections, or deletions.	Outside of the scope of this fitness tracker TOA analysis

Bibliography

[1] OASIS Privacy Management Reference Model and Methodology (PMRM), Version 1.0. 17 May 2016. Edited by Michele Drgon, Gail Magnuson and John Sabo. Committee Specification 02. available at http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html

[2] ISO/IEC/IEEE 24774, *Systems and software engineering — Life cycle management — Specification for process description*

[3] ISO/IEC TR 27550:2019, *Information technology — Security techniques — Privacy engineering for system life cycle processes*

[4] ISO/IEC 27556, *Information security, cybersecurity and privacy protection — User-centric privacy preferences management framework*

[5] ISO/IEC 29184:2020, *Information technology — Online privacy notices and consent*

[6] ISO/IEC TS 27560, *Privacy technologies — Consent record information structure*

[7] ISO/IEC 29134:2023, *Information technology — Security techniques — Guidelines for privacy impact assessment*

[8] ISO/IEC 29151:2017, *Information technology — Security techniques — Code of practice for personally identifiable information protection*

[9] ISO/IEC 27018:2019, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[10] ISO/IEC 29100:2024, *Information technology — Security techniques — Privacy framework*

[11] ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[12] ISO/IEC/IEEE 15288:2023, *Systems and software engineering — System life cycle processes*

[13] ISO/IEC/IEEE 12207, *Systems and software engineering — Software life cycle processes*

[14] ISO/IEC/IEEE 29148:2018, *Systems and software engineering — Life cycle processes — Requirements engineering*

[15] ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

[16] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[17] ISO/IEC 27034-1, *Information technology — Security techniques — Application security — Part 1: Overview and concepts*

[18] ISO/IEC 27557:2022, *Information security, cybersecurity and privacy protection — Application of ISO 31000:2018 for organizational privacy risk management*

[19] Privacy Framework Version N.I.S.T., 1.0, available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

[20] ISO/TR 31700-2:2023, *Consumer protection — Privacy by design for consumer goods and services — Part 2: Use cases*

[21] ISO/TR 4804:2020, *Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation*

[22] ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[23] ISO/IEC 27033-1:2015, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[24] ISO/IEC 2382:2015, *Information technology — Vocabulary*

[25] ISO/IEC TS 27570:2021, *Privacy protection — Privacy guidelines for smart cities*

[26] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[27] NIST SP 800-53 Rev.5, *Security and Privacy Controls for Information Systems and Organizations*, available at https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final?trk=public_post_comment-text

[28] Regulation (eu) 2016/679 of the European Parliament and of the Council of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

ICS 35.030
Price based on 29 pages

iso.org