IEEE SA
STANDARDS ASSOCIATION

IEEE Standard for Transparent Employer Data Governance

STANDARDS

IEEE Computer Society

Developed by the
Software & Systems Engineering Standards Committee

IEEE Std 7005™-2021

IEEE

IEEE Standard for Transparent Employer Data Governance

Developed by the

Software & Systems Engineering Standards Committee
of the
IEEE Computer Society

Approved 23 September 2021

IEEE SA Standards Board

Abstract: Specific methodologies to help employers in accessing, collecting, storing, utilizing, sharing, and destroying employee data are described in this standard. Specific metrics and conformance criteria regarding these types of uses from trusted global partners and how third parties and employers can meet them are provided in this standard. Certification processes, success criteria, and execution procedures are not within the scope of this standard.

Keywords: employer governance, IEEE 7005™, personal data protection

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-1-5044-8011-6 STD24972
Print: ISBN 978-1-5044-8012-3 STDPD24972

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the IEEE SA myProject system. An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; https://www.copyright.com/. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website. Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the IEEE SA Patent Policy.

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this IEEE standard was completed, the Employer Data Governance Working Group had the following membership:

Ulf Bengtsson, *Chair*

Vincent Bryce	Dennis Holstein	Bryan Reese
Diego Chiozzi	Daniel Huegli	Jesus Salgado
Christina Colclough	Zvikomborero Murahwi	Matthew Silveira
Vicky Hailey	Matthew Newman	Alexander White

The following members of the individual/entity Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Robert Aiello	Mark Henley	Maximilian Riegel
Johann Amsenga	Werner Hoelzl	Pablo Rivas Perea
Ulf Bengtsson	Dennis Holstein	Subrato Sensharma
Juris Borzovs	Piotr Karocki	John Sheppard
Pieter Botman	Edmund Kienast	Carl Singer
Diego Chiozzi	Ansgar Koene	Robert Soper
C. Clifton	Sean Laroque-Doherty	Walter Struppler
Ronald Dean	Javier Luiso	Abd-Elhamid Taha
Luis Andrey Fajardo	Lingzhong Meng	Thomas Tullia
Rodolfo Fiorini	Rajesh Murthy	Eleanor Watson
David Fuschi	Laura Musikanski	Alexander White
Paulo Goncalves	Brian Page	Forrest Wright
Didem Gurdur Broo	R.K. Rannow	Naritoshi Yoshinaga
Tamas Haidegger	Bryan Reese	Oren Yuen
	Annette Reilly	

When the IEEE SA Standards Board approved this standard on 23 September 2021, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy	Howard Li	Mehmet Ulema
Doug Edwards	Daozhuang Lin	Lei Wang
Ramy Ahmed Fathy	Kevin Lu	F.Keith Waters
J.Travis Griffith	Daleep C. Mohla	Karl Weber
Thomas Koshy	Chenhui Niu	Sha Wei
Joseph L. Koepfinger*	Damir Novosel	Howard Wolfman
David J. Law	Annette Reilly	Daidi Zhong
	Dorothy Stanley	

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 7005-2021, IEEE Standard for Transparent Employer Data Governance.

Today, employees have little influence on how their personal data is stored, tracked, and utilized while on the job. In many situations, biometric or other employee data is collected and used. Organizations may lack the adequate knowledge or tools to implement these efforts in a safe and trusted manner for long-term care of the worker's digital information. Furthermore, as digital technologies develop, the necessity of transparent, ethical, and responsible handling and utilization of all forms of sensitive personal data that can be used to distinguish one person from another and can that be used for de-anonymizing anonymous data will rise.

In addition, as an increasing number of organizations monitor employee activities during working hours to optimize workflows and processes, employees should have insight into how this data is stored, used, and applied. This also applies to data and other information derived from activities outside of work (e.g., wellness programs). Ideally, to improve transparency and workplace trust, employees and their representatives should have access to the data and influence over what data can be collected.

The stakeholders for this standard include all organizations within the value chain of an enterprise, including but not limited to corporate-level management, line managers, human resources, trade unions, shop stewards, and representatives. Transparency can be enabled by adequately resourced education, training, and support for employees, whether full time or part time, to provide the tools and knowledge to protect and utilize their data to their own best advantage while also a trusted information exchange with their employers.

Contents

List of Figures

List of Tables

IEEE Standard for Transparent Employer Data Governance

1. Overview

1.1 Scope

This standard defines specific methodologies to help employers in accessing, collecting, storing, utilizing, sharing, and destroying employee data. The standard provides specific metrics and conformance criteria regarding these types of uses from trusted global partners and how third parties and employers can meet them. Certification processes, success criteria, and execution procedures are not within the scope of this standard.

1.2 Purpose

This standard is designed to provide organizations with a set of clear requirements and guidelines for storing, protecting, and utilizing employee data, where, once deployed, will support ethical and transparent behavior. One important objective addressed in this standard is the need for well-defined processes and documents that can be explained in non-technical terms understood by a data subject. The data subject needs to understand the underlying issues of personal data collection, the processing of personal data, storage of personal data, and how the personal data is shared and used. Each issue is addressed in terms of the means used to protect the data subject's personal data and the data subject's options if the personal data is compromised. Inspired by the European Union (EU) General Data Protection Regulation (GDPR) legislation, the standard is designed so that workers facing widespread automation issues potentially displacing their jobs will have control and influence over the personal information that directly represents a core asset of their identity and lives whether derived from work-flow monitoring or personal data storage.

1.3 Objectives

This standard is concerned with the transparent and responsible use of potential, former, and current employee data. It describes a set of principles and activities to be undertaken by an organization in their quest to implement a transparent, co-created, and rights-based employee data policy. The key objectives are:

a) Establish a consistent and transparent framework for handling all employee data across all organizational units

b) Establish organizational procedures for assessing the impact of projects that affect access to and use of employee data

c) Establish oversight and governance of the data policy

1.4 Verification methods

This standard includes the following methods to verify that an employer's implementation conforms to the requirements:

a) Approved documentation describing the processes, organizational responsibility, and accountability for adverse consequences to conform to the corporate policy procedures and organizational directives

b) Documented analysis of actionable efforts to improve all employer data governance processes and transparency

c) Demonstration and supporting documentation of algorithmic processes used by the organization's information system to protect sensitive employee data during its lifecycle

d) Routine testing and supporting documentation of algorithmic processes used by the organization's information system to improve proper maintenance of data storage and communication constraints needed to protect sensitive employee data at rest or in transit

1.5 Limitation of scope

This standard is a process-based standard that specifies requirements, i.e., what is required. It does not specify how to implement the requirements. This standard applies to any organization that has personal identifiable information related to potential, current, and former employees.

1.6 Document organization

Informative annexes are included to provide supporting data, rationale, and examples for the requirements specified in this standard.

1.7 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals is *required to*).[1,2]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals is *recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals is *permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals is *able to*).

[1]The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.
[2]The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

ISO 26000:2010, Social responsibility.[3]

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause. [4]

application program interface (API) management platform: A proxy for client request to protect the backend of an online serve from being disable from too many queries.

NOTE—An API management platform can limit the number of queries for each employer entity per second or per day. Generally, API management platforms include analytics and usage reporting, API key and authorization management, and live updated documentation.[5]

awareness requirement: Reference to other requirements or domain assumptions and their success or failure.

NOTE—Awareness requirements are mapped to other requirements.

chain of custody: Process of maintaining and documenting the handling of evidence.

NOTE—Involves keeping a detailed log showing who collected, handled, transferred, or analyzed evidence [e.g., personal identifiable information) PII breach data] during an investigation.

CMP administrator: Role assigned to an individual.

NOTE—Role assignment is managed by the responsible organization unit (ROU).

compliance: Adherence to laws and regulations.

NOTE—Local laws and regulations are subject to adjudication by the courts.

conformance: Adherence to specified requirements.

consent: Voluntary agreement with an action proposed by another. *See also:* **informed consent**.

NOTE 1—Consent is an act of reason; the person giving consent is of enough mental capacity and in possession of all essential information to give valid consent that includes personal identifiable information.

NOTE 2—The data subject is also free from pressure administered by the employer representative to provide consent.

[3]ISO publications are available from the ISO Central Secretariat (https://www.iso.org/). ISO publications are also available in the United States from the American National Standards Institute (https://www.ansi.org/).
[4]*IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.
[5]Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

content management platform (CMP): a managed system that builds a unified, persistent database that is accessible to other systems.

NOTE 1—CMP acts as a fusion center and repository for all sorts of data from various internal and external systems.

NOTE 2—CMP provides the ability to accommodate different data types and formats that might have varying structures and naming conventions.

data governance: Execution and enforcement of authority over the definition, production, and usage of data and data related assets.

data management: A disciplined process that plans for, acquires, and provides stewardship for business and technical data, consistent with data requirements throughout the life cycle.

data subject: Identifiable natural person.

NOTE 1—GDPR Article 4.1 [B8][6] defines data subject.

NOTE 2—This standard uses the term data subject when it applies to employees and to persons that are not directly employed by the employer.

data user: Role assigned to an individual.

NOTE—Role assignment is managed by the responsible organizational unit (ROU).

employee: A person who works in a subordinate arrangement within or beyond the physical boundaries of an organization.

NOTE—This standard uses the term employee when it applies to a person that is directly employed by the employer. *See:* **data subject**.

employer data management policy: The basis for the requirements for employer data lifecycle projects.

NOTE—Data management is a disciplined process that plans for, acquires, and provides stewardship for business and technical data, consistent with data requirements throughout the life cycle.

epistemic logic: Relating to knowledge or to the degree of its validation.

ethics: Principles of conduct governing an individual or group.

governing authority: Entity responsible for establishing the rules for specifying types and uses of sensitive data.

immunity provision: Exemption granted by statute or government authorities from a legal duty, penalty, or prosecution.

NOTE—As a rule, only personally identifiable information is afforded special protection by local data privacy laws.

information system: A system that is designated to collect, organize, store, communicate, and process data.

NOTE—Because transparency and privacy are two primary attributes (core values) of an information system (Hosseini,Shahri, Phalp,and Ali [B6]).

[6]The numbers in brackets correspond to those of the bibliography in Annex F.

informed consent: Permission granted in the knowledge of the possible consequences.

NOTE—Informed consent is a process for getting permission before performing an action involving personal identifiable information.

local matter: Not specified in this document, but subject to other reference documents.

measure of effectiveness: Criterion used to assess change in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective or creation of an effect.

metric: Measure or unit of measure that is designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant data.

norm: Something that is usual, typical, or standard.

personal data: Any information relating to an identified or identifiable natural person (data subject).

NOTE—By reference to an identifier, e.g., name, an identification number, location data. Or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

policies, procedures, and organizational directives: Compilation of employer governance documents.

NOTE—Includes employee data policy, data project document, and supporting documents describing implementation procedures, audits, action plans, etc.

positive control: State of affirmative physical or non-physical control.

NOTE 1—Human action (with automated assist) taken in response to direct observations.

NOTE 2—Passive control is monitoring only.

program effectiveness report: Document detailing the exposure of personal identifiable information (PII), the corrective action taken to mitigate the exposure of PII, and the impact on consent agreements.

responsibility: Ability to give account to somebody or some organization for one's actions.

NOTE—Refers to the actions and their consequences that a person executes out of free will, knowing what they are doing.

secure: Combination of people process, and technology to protect data from authorized access and use.

NOTE—See IS0 27000 for security guidance [B10].

solution: Combination of people, processes, and technologies to implement a desired capability.

transparency: Property describing the transfer of information relevant to evaluating solutions defined by context.

NOTE 1—Local laws and regulations may require employer governance to regard information transparency as a verifiable requirement.

NOTE 2—An organization's information system is transparent when it discloses to its users the information it deals with and its internal functioning processes.

NOTE 3—In requirements engineering transparency is generally viewed as a non-functional requirement. See MBSE notation for non-functional requirements (Aleksandraviciene and Morkevicius [B1]).

without prejudice: Without any loss or waiver of the data subject's rights, privileges, or conditions of employment.

NOTE 1—Refusal of consent cannot be used to terminate or demote a data subject, but it may result in the need to reassign the data subject.

NOTE 2—Acceptance of informed consent can be used as a condition for extending an offer of employment.

3.2 Acronyms and abbreviations

ABAC	attribute-based access control
AP	alignment processor
API	application program interface
CMP	content management platform
DMS	data management system
DPIA	data protection impact assessment
EU	European Union
FEP	front-end processor
FF	file formatter
GDPR	General Data Protection Regulation
GSiU	grievance system in use
ibd	internal block diagram (according to OMG's specification for SysML)
KPI	key performance indicator
MBSE	model-based systems engineering
MoE	measure of effectiveness
MTTD	mean-time-to-detect
MTTR	mean-time-to-respond
NSBGM	non-state-based grievance mechanism
OLGM	operational level grievance mechanism
OMG	Open Management Group
PbD	privacy by design
PER	program effectiveness report
PII	personal identifiable information
PP&OD	policies, procedures, and organizational directives
RBAC	role-based access control
RFID	radio-frequency identification
ROU	responsible organizational unit
SAF	sensor availability flag
SBO	select-before-operate

SiU	system in use
SME	subject matter expert
SoI	system of interest
SysML	system modeling language

4. Policy requirements

4.1 Governance requirements

Transparency requires the representation of stakeholders, what stakeholders shall provide as input, and the results of this dialog in the form of proper documentation and communication to the organization and its suppliers.

a) Transparency of all employment records (e.g., references and performance) that may be disclosed to third parties shall be made explicit.

NOTE—Some of the requirements included in this standard may overlap with local data protection legislation, since it is not homogeneous worldwide. Employer would need to follow whichever is more stringent.

b) Transparency of any record that excludes or includes a person or organization shall be made explicit.

4.2 Management requirements

Management requirements are as follows:

a) An organization-wide dialog with approved documentation shall be created to include management, as the accountable party, and data subject representatives to establish the baseline for the requirements for employer data lifecycle projects, to be known as the employer's data management policy.

b) Data management shall be assessed for its process capability and organizational maturity level. A data management process capability assessment and maturity model may be derived from ISO/IEC 33004:2015 [B12].

NOTE—Also consider ISO/IEC 38500 [B13], ISO 38505-1 [B14], ISO/IEC FDIS 38503 [B15], and ISO/IEC 27701 [B10].

c) The appropriate organizational capabilities and resources to translate the results of the dialog, including the employer data management policy into business activities, technical controls, and risk management shall be allocated.

d) Subject to items b) and c), if a data governance council is established it shall be tasked to:

1) Audit executive management actions to assess compliance with agreed policy and risk control.

2) Review suspected breaches of employee data policy complaints and questions including but not limited to "whistleblowing" submittals.

3) Conduct audits across the organization to determine the degree of compliance with the employee data policy and to determine that issues are correctly addressed in a timely manner.

NOTE—Timeliness is a local matter.

4) Maintain ongoing transparency of the data governance council decision processes, findings, and actions.

NOTE—Transparency is a contextual matter, with factors unique to the circumstances of the data subject, and include local matters, such as compliance with applicable laws and regulations.

5) Prevent data from being sold, shared, or given away without prior employee consent, unless other legal requirements control, such as national security requirements.

6) An employee data policy shall be established to document an explicit position on the limitation that address the following concerns:

   i) Human-in-the-loop (human-in-command) to improve the presence of competent, accountable, able humans exercising control within processes performed in autonomous and semi-autonomous information systems.

   ii) Fairness to minimize biases in data, in processing performed, and in the application of recommendations to individuals or groups.

   iii) A data subject retains the rights of their data, which implies the right to edit, withdraw, port, or withhold consent.

   iv) Direction toward the protection of data an individual considers private, triangulation to reidentify anonymized data, or data relating to the individual's private life, regardless of whether it is published, including concerns on restricting access to the data, requirements for data security, and actions following unauthorized access to data (data breaches).

   v) Accountability to identify persons and organizations responsible for the lack of due diligence resulting in harm or negative impact of data breaches (auditability), and the employees right to challenge any result or conclusions.

      NOTE—See ISO 26000:2010[7] for a comprehensive discussion of this point.

   vi) Transparency to provide the traceability of any conclusions drawn as a result of data processing to the collected data, the explicability of the conclusions, active communication about intent of data projects, impact on the data subjects, and their rights concerning these issues.

   vii) Data minimization so that only agreed-to data is collected for the agreed-to purpose and used by the agreed-to people and organizations for the agreed-to period of time.

   viii) Beneficial side-effects that reflect the employee's agreement and decisions where the addition of minor incremental cost can bring benefit to more parties.

e) A data policy shall include:

   1) Respect of human rights and fundamental rights, such as defined by ISO 26000:2010.

   2) Compliance with local norms, regulations, conventions, and laws.

   3) Provide secure collection, processing, storage, use, and disposal of sensitive personal identifiable information (PII) data, including potentially sensitive aggregated data.

   4) In situations where artificial intelligent or autonomous systems are used, human agency shall govern the final decision.

   5) Beneficence and non-maleficence as described in ISO 26000:2010.

f) A system shall be established to provide ongoing technical control of collecting, processing, storing, communicating, using, and disposing of employee's personal data.

g) Technical controls shall be aligned with the maturity of the organization's data management system.

[7]Information on references can be found in Clause 2.

4.3 Data project requirements

Data project requirements include the following:

a) For all new data projects and repurposing, including those involving external data subjects in the recruitment process,[8] the organization shall create a data project document including but not limited to the following:

   1) Purpose of the data project including its relationship to the business goal and addressing the possible benefits to the stakeholders.

   2) Identification of communication plans and channels for transparency and informing the data subjects before seeking consent.

   3) Description of the process to be used to gain data subject consent while ensuring employee's rights over PII and process used to exercise those rights.

   4) Description of how fairness is addressed.

   5) Description of considerations and mitigation strategy regarding the intended and unintended consequences of the data project on the data subjects.

   6) Description of the data management system including protecting confidentiality and integrity of data at rest and in transit.

   7) Description of persons and organization that have access to the data, the period of access, and the purpose of access and its use.

   8) Description of data sources used to collect data and the means to conform to the principle of data minimization.

   9) Description of data processing algorithms including consideration of data triangulation.

   10) Description of procedures and mechanisms to notify the data subject s informed of all actions in a timely manner.

       NOTE—Timeliness is a local matter.

   11) Identification of changes related to data policy revisions.

b) Approval of the data project document by executive management, or designated authority, shall be required prior to commencing the project.

   NOTE—Document approval indicates that the data project has been reviewed and warrants that project complies with the data policy.

c) Commensurate with the employee data policy, the responsible organizational unit (ROU) shall review in detail with the data subject all aspects of the approved data project document and provide the opportunity to resolve any issues raised by the data subject. This review includes but is not limited to the following:

   1) Output from automated processing, including data sets used, as defined by the approved data management system document.

   2) Human-in-control procedures to maintain positive control and protection of the data subject's data.

   3) Automated and manual measures to counteract discrimination and unwanted bias.

d) Commensurate with the employee data policy, the ROU, without prejudice, shall solicit consent of the data subject with regards to the collection of data for purposed detailed in the data project document.

[8]Data subjects with no contractual relationship to the organization responsible for the data project are governed by local laws and regulations, e.g., GDPR.

e) Commensurate with employee data policy, the ROU shall review the procedures needed to protect the data subject's data so it cannot be shared, sold, or given away to a third party without prior consent of the data subjects involved.

f) Where applicable in accordance with employee data policy, the ROU shall honor the data subject's request for specific data deletions or request for data porting in a timely manner.

NOTE—Timeliness is a local matter.

5. Data management system technical control requirements

5.1 Data classification requirements

Data classification requirements address what is sensitive data and how best to establish a classification or catalog to logically group the sensitive data. Annex A helps explain the answer to this issue. Data classification requirements are as follows:

a) Classification shall be grouped by sector, domain, and governing authority.

b) Data sensitivity and the need to protect sensitive data shall be determined by context, i.e., relationship to mission critical functions.

c) Pursuant to local norms, laws, and regulations, role-based access control (RBAC) and attribute-based access control (ABAC) shall be used to identify who has authority to access sensitive data.

5.2 Informed consent requirements

Informed consent requirements address processes required for the data subject to clearly understand the employer's implementation of the employee data policy. Annex B helps explain the key capabilities for implementation. Following are the informed consent requirements.

5.2.1 Policies, procedures, and organizational directives

Informed consent policies, procedures, and organizational directives include the following:

a) The ROU shall select their representative to conduct the interview with the data subject to solicit informed consent who is free of bias (for or against) the data subject and has no conflict of interest in representing the employer.

NOTE 1—For example, the candidate representative conducting the interview is disqualified because they are a family relative of the data subject. The relationship has the appearance of bias.

NOTE 2—For example, the candidate representative conducting the interview is disqualified because they have a vested interest in the external staffing organization submitting the data subject for employment. The relationship has the appearance of bias.

b) In terms understandable by the data subject, the employer's policies, procedures, and organizational directives (PP&OD) shall restrict the informed consent process so that the data subject is not pressured or coerced to accept the obligations and risk associated with the ROU's action plan.

c) In terms understandable by the data subject, the employer's PP&OD shall restrict the informed consent process so that the decision to accept or refuse consent to participate in the ROU's action plan is made only when the data subject is satisfied that all obligations and risks are understood.

d) In terms understandable by the data subject, the employer's PP&ODs shall restrict the informed consent process so that potentially sensitive PII data is *securely* collected, processed, stored, used, and disposed.

e) In terms understandable by the data subject, the employer's PP&ODs shall restrict the informed consent process so that all potential PII data is properly qualified by supporting data.

NOTE—Identification of supporting data is a local matter determined by the ROU.

f) In terms understandable by the data subject, the employer's PP&ODs shall restrict the informed consent process so that potential PII data is categorized by the risks entailed by its exposure including but not limited to data of techno-security value, unidentifiable data, and protected data.

NOTE 1—PII data of techno-security value are indicators of a hostile cyber-physical event.

NOTE 2—Unidentifiable PII data is data that cannot reasonably allow for the identification of a data subject.

NOTE 3—Protected PII data is determined by local norms, laws, and regulations.

g) In terms understandable by the data subject, the employer's PP&ODs shall restrict the informed consent process so that potential PII data is supported with metadata including but not limited to data type, unique source identifier, and source location.

NOTE—Data type includes status data, analog data, video data, etc.

h) The employer's PP&ODs shall include an informed consent form that acknowledges the data subject is volunteering without prejudice to accept or decline the obligations and risks associated with the potential exposure of PII.

NOTE 1—A proper informed consent form includes all notifications that can be used to support its use as a legal contract between parties.

NOTE 2—Selection of the informed consent form is a local matter.

i) The employer's PP&ODs shall instruct ROUs to report to the governing authority, the results of soliciting consent agreements with recommendations to improve the program in a timely manner.

NOTE 1—Recommendations are supported by measure of effectiveness (MoE) and key performance indicator (KPI) based assessments.

NOTE 2—Timeliness is a local matter determined by the ROU.

j) The employer's PP&OD shall instruct ROUs to update their action plan and update their employees (data subjects) at least annually.

5.2.2 Action plan requirements

In terms understandable by the data subject, the ROU's action plan shall include the following:

a) That potential PII data collected is securely stored in repositories that comply with applicable norms, laws, and regulations.

NOTE—Independent of storage format and schema, data repositories include device memory storage, server storage, etc.

b) That secured storage provides adequate protection against unauthorized access to and use of the stored data.

NOTE—Adequate protection is defined by local norms, laws, and regulations as adjudicated by the courts.

c) That data is securely destroyed when it is no longer needed.

d) That data is securely destroyed when requested by the data subject.

e) That breaches exposing potential PII data are reported via specified interfaces to the data subject in a timely manner.

NOTE—Time stamping accuracy is a local matter determined by the ROU.

f) That the data user, with acknowledgment from the data subject (data owner), maintains throughout the life cycle of the data, positive control of the processes that contain potential PII data.

NOTE 1—The mechanism used to notify the data subject is a local matter.

NOTE 2—The data user that is responsible for managing the process is not responsible for the use of data disseminated to other users.

g) That the data user, with acknowledgment from the data subject (data owner), maintains positive control over access to and use of the data that contains potential PII data.

The employer's PP&OD shall restrict the action plan process so that the data user, with acknowledgment from the data subject (data owner), maintains positive control of the data that contains potential PII data while in transit or at rest.

5.2.3 System-in-use (SiU) requirements

Informed consent SiU requirements include the following:

a) In terms understandable by the data subjects, The ROU shall notify the data subject in a timely manner that their PII data has been exposed, and the corrective action taken to mitigate the damage.

NOTE 1—The mechanism used to notify the data subject and receive acknowledgment is a local matter.

NOTE 2—Subject to local norms, laws, and regulations, timely response is a local matter.

b) In accordance with the employer's PP&OD, the ROU shall provide the option for the data subject to withdraw agreement of consent.

c) In accordance with local laws and regulations, all data collected, transmitted, analyzed, and stored for forensic analysis shall be preserved with supporting chain of custody documentation.

NOTE—Duration of preserving the chain of custody is a local matter.

d) In a timely manner, the ROU shall file a program effectiveness report (PER) with the governing authority detailing the beach of PII, the corrective action taken to mitigate the exposure of PII, and the impact on consent agreements.

NOTE—Subject to local norms, laws, and regulations, timely response is a local matter.

e) Periodically, the ROU shall file a summary PER, including breach metrics describing mean time to detect (MTTD), mean time to respond (MTTR), and trends in effectiveness, with the governing authority describing the performance of their SiU.

NOTE—Subject to local norms, laws, and regulations, the frequency of filing a summary PER is a local matter.

5.3 Content management requirements

The data management system is responsible for managing data in transit and at rest. A key component of the data management system is the content management platform (CMP). Understanding the complexity of CMP requirements is the issue. Annex C helps explain CMP complexity. Following are the content management requirements.

5.3.1 Secure collection requirements

The employer's PP&OD shall provide for the following collection capabilities:

a) The capability to securely collect potentially sensitive data from all applicable sources.

NOTE 1—Determining level of sensitivity is a local matter determined by the ROU.

NOTE 2—Identification and authentication of applicable sources is a local matter determined by the ROU.

b) The capability to allow collection of data of different types and formats that have varying structures and naming conventions.

NOTE—Admissible types and formats are a local matter.

c) The capability to properly qualify with supporting data that all data is collected in the prescribed manner agreed-to in the approved consent document.

NOTE 1—Identification of supporting data is a local matter determined by the ROU.

NOTE 2—Supporting data includes, but is not limited to, environmental conditions (usually the sensor has limits of temperature and humidity), range specifying the measurement limit of the sensor, calibration (essential for most measuring devices as the reading change with time), resolution (smallest increment detected by the sensor), and repeatability.

5.3.2 Secure processing requirements

The employer's PP&OD shall provide for the following processing capabilities:

a) The capability to collect data that is reformatted so other authorized systems can access and act upon possible sensitive data.

b) The capability to collect meta data including but not limited to data type, unique sensor identifier, and sensor location.

NOTE 1—Data type includes status data, analog data, video data, etc.

NOTE 2—Sensor identifier includes type of sensor, e.g., wearable sensor, tracking sensor, video sensor, etc.

NOTE 3—Sensor location includes static location or mobile device to associate with other data (groups).

c) The capability to qualify in terms of the risks entailed by exposing sensitive data, including but not limited to data of a techno-security value, unidentifiable data, and protected data.

NOTE 1—Data of techno-security value are indicators of hostile cyber-physical event.

NOTE 2—Unidentifiable data is data that cannot reasonably allow for the identification of an individual or organization.

NOTE 3—Protected data is determined by local norms, laws, and regulations.

d) The capability to publish collected data a consistent format so it can be correlated with other data.

NOTE—Methods used to correlate data are a local matter determined by the ROU.

e) The capability to align data collected to support analytical determination of sensitivity level.

NOTE—Methods used to align data is a local matter determined by the ROU.

f) The capability to publish collected data with sufficient information to determine sensitivity and to determine what action to take in response to receiving the data.

NOTE 1—The criteria for enough information is a local matter determined by the ROU.

NOTE 2—Action in response to receiving data is a local matter determined by the ROU.

5.3.3 Secure storage requirements

The employer's PP&OD shall provide for the following secure storage capabilities:

a) The capability to securely store data collected in any repository in accordance with applicable norms, laws, and regulations.

NOTE—Data storage includes device memory storage, server storage, etc.

b) The capability to restrict data storage to provide adequate protection against unauthorized access to and use of the data.

NOTE—Adequate protection is defined by local norms, laws, and regulations as adjudicated by the courts.

5.3.4 Secure disposal requirements

The employer's PP&OD shall provide for the following secure disposal capabilities:

a) The capability to securely destroy collected data when it is no longer needed.

b) The capability to securely destroy collected data when requested by the data subject.

5.3.5 CMP user requirements

The employer's PP&OD shall provide for the following CMP administrator user[9] and other data user[10] capabilitie:

a) The capability to securely administer the configuration and settings for all functions used to collect, process, reformat, prioritize, publish, and destroy data are correctly enabled and maintained.

b) The capability to report in a timely manner to specified interfaces measures of effectiveness (MoEs) and key performance indicators (KPIs) of end-to-end processes.

NOTE 1—MoEs established by the ROU include, but are not limited to, number of errors that occur during each step of the collection, processing, storage, and disposal stages.

NOTE 2—MoEs established by the ROU include, but are not limited to, number of retries that occur during each step of the collection, processing, storage, and disposal stages.

NOTE 3—MoEs established by the ROU include, but are not limited to, measurement of operating loads as a percentage of design capacity during each step of the collection, processing, storage, and disposal stages.

NOTE 4—MoEs established by the ROU include, but are not limited to, measurement of throughput based on the time from receipt of an input file to the time of publication to a specified interface. Time stamping accuracy is a local matter determined by the ROU.

c) The capability to maintain positive control of access to and use of sensitive data in transit or at rest throughout the life cycle of the data in use.

d) The capability to notify in a timely manner the data user, with acknowledgment from the data subject (data owner) all actions performed by automated and positive control processes.

NOTE 1—The mechanism used to notify the data subject and receive acknowledgment is a local matter.

NOTE 2—The data user that is responsible for managing the collection, processing, storage, and disposal processes is not responsible for the use of data disseminated to other users.

NOTE 3—This requirement is independent of and is indifferent to the communication network configuration and topology in use.

[9]The CMP administrator user is a role assigned to an individual.
[10]The data user is a role assigned to an individual.

5.4 Data management system derived requirements

Within the data management system (DMS), a critical component is the data controller. Understanding the complexity of DMS's data controller requirements is the issue. Annex D helps explain the data control complexity, the technical challenges, and solutions. Following are the DMS requirements:

a) In accordance with local norms, laws, and regulations, the employer shall conduct a data protection impact assessment (DPIA) to assess privacy issues that might arise when the employer deploys new products and services that involve the processing of personal data.

NOTE—The DPIA assists the employer selecting the best DMS commercial solution for their mission requirements.

b) Privacy, by design, shall be included in employer's procurement specifications solutions offered to provide the needed protection capabilities.

c) The data governance council shall hold all levels of management accountable and auditable in relation to PII transparency, inclusion, fairness, use, storage, offboarding, etc.

d) All processes performed by the data controller shall be subject to the council's audit.

e) The data controller shall implement protections for the data subject's geolocation and biometric data.

f) At each stage of the lifecycle the data controller shall have the capability to securely handle the sensitive data.

g) The data controller status reports shall document that a specific action has been successfully completed.

5.5 Information sharing requirements

This standard identifies the need for secure and automated information sharing. Annex B.5 helps explain the complexity, the technical challenges, and solutions to share personal data is protected. Acceptable use PP&ODs assist the employer in setting ground rules concerning fundamental questions on the use of personal data including sensitive personal data; e.g., who needs access to these data, which regulations a company follows, where are the vulnerabilities in the company's use of these data, and the rules and permissions the user of these data follow.

The derived requirements to protect sensitive personal data that is shared are as follows. Additional legal restrictions may apply to the categories of sensitive personal data, PII, and other special data categories.

a) In accordance with local norms, laws and regulations, the employer shall conduct a DPIA to assess the privacy issues that might arise when sensitive personal data, PII, and any other personal data is shared.

NOTE—Special attention to immunity provisions is advised.

b) During the exchange of personal data, the employer shall securely protect these data against unauthorized use, retention, or disclosure.

c) During the exchange of sensitive personal data, the employer shall maintain positive control under human management of the overall automated exchange activities.

d) The employer shall authorize mechanisms (including but not limited to computing devices, storage devices, and communication systems) to be used to facilitate the exchange of sensitive personal data.

5.6 Grievance redress requirements

This standard identifies the need for secure grievance redress options available to the data subject. Annex E helps explain the complexity, the technical challenges and solution for a fair process to provide the data subject the capability to file a grievance and seek proper redress. This standard provides for grievance redress by a data subject, or a body of employee representation, or a third-party retained by the data subject.

The requirements for grievance redress are as follows:

a) It is imperative that the employer's PP&OD shall identify all parties in a properly filed grievance process.

b) The employer's PP&OD shall restrict the process to file so a grievance process is fairly performed in a timely manner.

NOTE—An administrative oversight function shall be implemented to review the grievance filing process and initiate appropriate action if there is a lack of fairness or unacceptable delays. How this oversight function is implemented is a local matter.

c) The employer's PP&OD shall include properly filed grievance provisions for the following:

1) Assignment of grievance review by an internal or external panel of subject matter experts (SMEs) that are agreeable to all parties of the grievance (including the rules for selecting the panel of experts

2) A framework describing the options and criteria for rendering judgement on the facts of the grievance

3) An authority to initiate enforcement action based on the finding of facts

4) A procedure for appeal of the judgement rendered by the panel of SMEs

d) The employer's PP&OD shall include a grievance remedy arrangement process that has provisions for the following:

1) Imposing appropriate sanctions, including the option to pursue public prosecutions, if applicable (an example is the abuse that is the subject of local laws)

2) Providing a range of appropriate reparations, such as compensation, restitution, rehabilitation, and changes in PP&OD requirements, assignment of responsibility and accountability

e) The employer's PP&OD shall include assignment of responsibility for assessing the effectiveness of all matters related to grievance redress.

Annex A

(informative)

Data classification

A.1 Introduction

Most employers recognize the necessity to protect their valuable and sensitive information to mitigate attempts to steal the information and use it to harm the reputation, or to interfere with, disrupt, or disable mission critical functions. Given the volatile threat landscape and rapidly evolving protective solutions, risk assessment teams are challenged to balance the risk against solution cost.

This informative annex addresses the basic question "what data is sensitive?" To a large degree, the answer lies in the how the employer classifies the data. Sometimes local norms, laws and regulations[11] provide the guidelines for data classification (Leichter and Berman [B18]), but in most cases the risk assessment teams, and responsible organizational units decide what data is to be classified and what level of classification is appropriate.

To address the basic question, Object Management Group's (OMG) system modeling language (SysML) is the modeling approach of choice [B20].[12] SysML is a well-defined specification that facilitates model-based system engineering (MBSE). Commercial tools are available that provide different views of the common system elements, better definitions of the relationships between components, an integrated glossary of the terms used in the model, and a seamless transition between business processes and technical control processes. The following notes describe the notation used in the SysML models.

NOTE 1—A pool is used to define either a group of participants such as an area within an organization or an external entity that collaborates within a process.

NOTE 2—A process model is normally created from the perspective of a single participant—the white box pool and contains the detail of that process. Black box pools are considered external to the scope of the process (although not necessarily outside of the organization), and do not show flow and activities. Black box pools may be collapsed and rotated, but do not have to be.

NOTE 3—A lane is used to define a specific participant or role within a process.

NOTE 4—A task is something that a lane (role) does during the process. A task is a granular (atomic) activity that cannot or does not need to be broken down any further.

NOTE 5—A sub-process summarizes a group of activities and can be expanded out into further detail. Sub-processes can be shown as collapsed (with the [+] symbol) or expanded.

NOTE 6—Data objects are inputs to and outputs from activities. Data objects could be used to represent documents, data or other objects that are passed between the activities in a process.

NOTE 7—Annotations allow additional information relevant in documenting the process to be shown on the diagram.

NOTE 8—A multi-instance loop indicator [↻] shows that a desired number of Activity instances can be created. The instances can be executed in parallel or sequentially. Either expression is used to specify the desired number of instances or a data driven setup that can be used.

[11]Examples include EU's data protection regulations and EU privacy laws.
[12]IEEE Std 7007™-2021 [B9] offers an excellent example of using MBSE to define the ontology for ethically driven robotics and automation systems that address may of the issues described in this standard.

A.2 An overview of the business processing model

Before diving into the details related to the protection of sensitive data, it is helpful to understand the common processes organizations use to understand the local norms, laws, and regulations. To facilitate this understanding, a business processing model (BPM) is helpful. Figure A.1 shows an SysML/BPM describing the common processes undertaken by stakeholders performing bottom-up risk assessment and by stakeholders performing top-down decision analysis. Both processes start with a specification of local personal data laws and regulations[13] that are under consideration (P2.1). An important input for risk assessment is the relevant operating histories (P2D3).

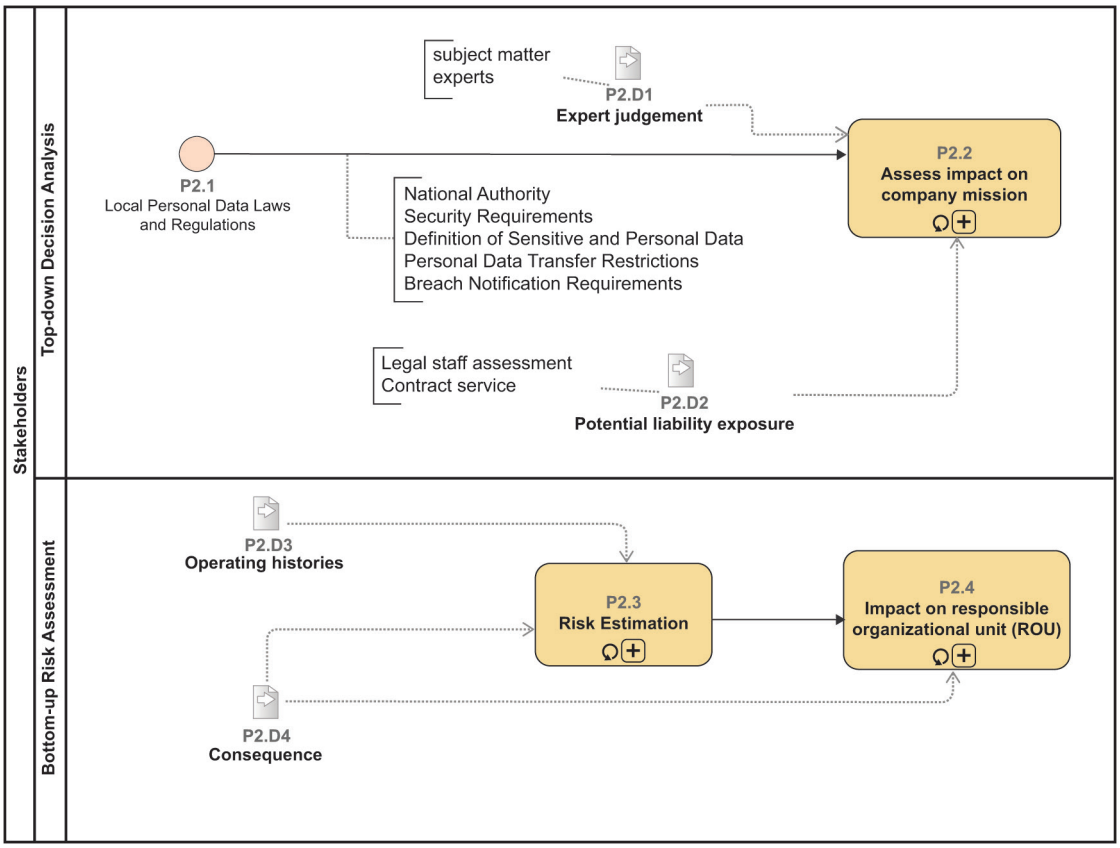

Figure A.1—Assessment of the impact on company mission and staffing

Independently, the two stakeholder groups commonly perform several sub-processes before working together to develop common criteria with waiting factors (P3.4) shown in Figure A.2. Sub-processes are staffing activities initiated by the risk assessment team to solicit input from organizations that have primary responsibility for managing the assets that could be impacted by the local laws and regulations. These organizations have the detailed knowledge and historical data needed for the risk assessment

[13]Local norms, laws, and regulations include views offered by the applicable national authority, security requirements to protect the personal data, local definition of sensitive and personal data, local restrictions on personal data transfer and storage location, and local breach notification requirements.

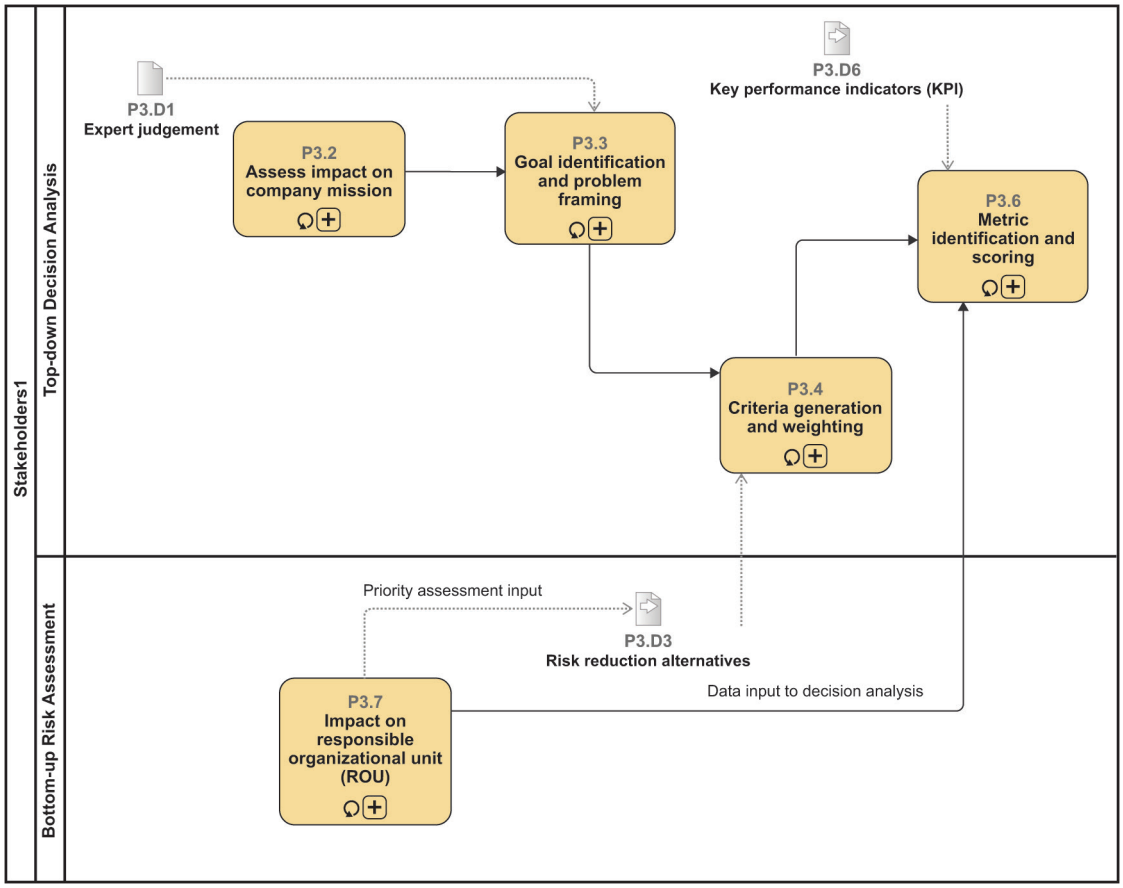

Figure A.2—Establishment of metrics and scoring criteria

It is important to understand that the objective of the top-down decision analysis is to produce a viable action plan (P4.D7) shown in Figure A.3. To be effective the action plan is properly resourced.

A.2.1 Bottom-up risk assessment

A collection of data is needed for the complex task[14] of estimating risk (P2.3). A critical input to estimate risk is a clear understanding of the consequence that could result from exploiting personal data (P2.D4). This process assumes that SMEs participating as stakeholders can clearly articulate the potential consequences.

Next, the output from risk estimation along with the output from data collection, and the potential consequences are the input to examining the potential impact on ROUs as shown a complex task (P2.4 and P3.7). Assessing the impact on ROUs is needed so that any forthcoming organizational directives can be seamlessly integrated into their normal operational responsibilities. Seamless integration is the criteria used by the ROUs to establish priorities on alternative solutions and risk reduction alternatives (P3.D3).

A.2.2 Top-down decision analysis

A.2.2.1 The legal assessment

Top-down decision analysis begins with a legal assessment of the application of relevant local norms, laws, and regulations (P2.1). This assessment includes adjudicated case opinions that could influence the

[14]The BPM notation for complex tasks or complex sub-processes is the symbol "+".

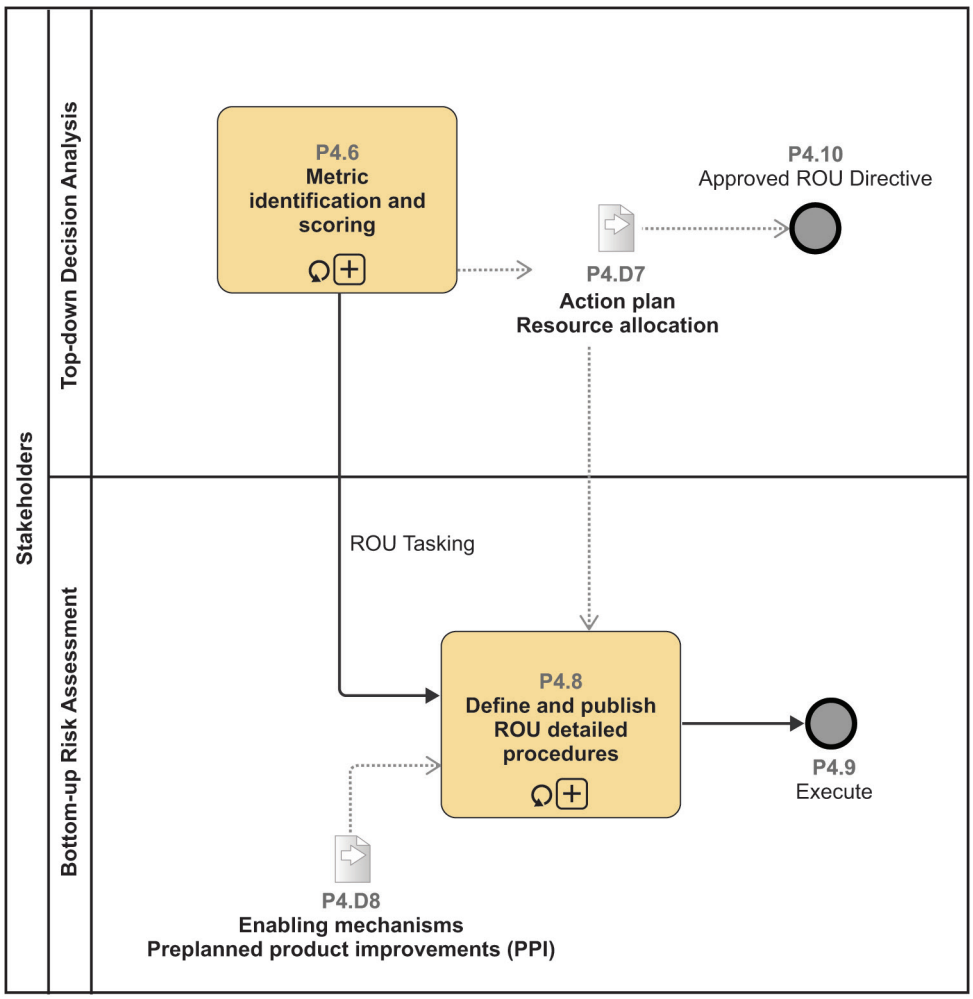

Figure A.3—Finalization and execution of the action plan

determination of liability exposure (P2.D2). This may require a contracted service that specializes in privacy laws and regulations.

There are multiple sources of information describing the legal assessment process; two of particular interest are (Raul, Manoranjan, and Mohan [B21], Committee of Ministers [B3]). As Raul noted in the editor's preface (pg. vi), "the EU's constraints on international data transfers have substantially inhibited the ability of multinational companies to move personal data around the world efficiently for business purposes." Exacerbated by the Snowden leaks regarding US government surveillance, conflicts in the US abound. More importantly, Raul goes on to conclude "The fact that the US does not have an omnibus data protection law, and thus does not have a top-level regulator or coordinator, means that it has been difficult for the US to explain and advocate for it approach to protecting person information. This has allowed the EU to fill a perceived policy void by denying mutual recognition to US practices, and to impose significant extraterritorial regulatory constraints on American and other non-European businesses."

Raul, Manoranajan, and Mohan note in the overview ([B21], pg. 268) "With certain exceptions, the US system does not apply a 'precautionary principle' to protect privacy, but rather, allows injured parties (and government agencies) to bring legal action to recover damages for, or enjoin in, 'unfair or deceptive' business practices." It is these adjudicated case options that are reviewed to determine the applicability to the local norms, law, and regulation under consideration.

A.2.2.2 Process leading to an action plan

It is important to understand that the objective of the top-down decision analysis is to produce a viable action plan (P4.D7). To be effective the action plan is properly resourced.

Given the potential liability exposure and relying on the stakeholder's expert judgement (P2.D1), the task is to assess the potential impact on the company's mission (P2.2 and P3.2). With this impact assessment and again relying on the stakeholder's expert judgement, the decision-makers can establish a broad framework that sets forth their goals to address the constraints imposed by the local norms, laws, and regulations to minimize their liability exposure (P2.D2).

The next step, albeit one of the more complex sub-processes, is to develop the criteria and parameter weighting needed to develop realizable metrics that to manage the execution of the action plan. Developing the criteria and parameter weighting (P3.4) needs the goals and framework from P3.3 and the risk reduction alternatives from the bottom-up risk assessment (P3.D3).

Equally challenging is the complex sub-process to establish the metric needed to manage the action plan. In addition to the criteria and parameter weighting factors (P3.4) and the ROU's impact assessment (P3.7), well understood KPIs are needed (P3.D6. The last output of the top-down decision analysis is the resourced action plan (P4.D7) that is properly documented in ROU directives (P4.10).

A.2.2.3 Closure to execute the resourced action plan

Given the metric and scoring (P4.6) from top-down decision analysis, the resourced action plan (P4.D7), each ROU has a well-defined tasking directive. With the enabling mechanisms and pre-planned product improvement (PPI) scheme (P4.D8), the ROU can develop, publish, and execute detailed procedures, including procurement initiatives, (P4.8), that are needed to protect personal data in their domain of responsibility (P4.9).

A.3 Reference model

A reference model is needed to understand the interaction of system components related to personal data protection. The goal is to discover what data is sensitive and what mechanism are needed to access and use the sensitive data. Assessment of these mechanisms is needed for proper protection of the sensitive data.

Figure A.4 is a SysML model used to capture the need to identify data classification. Data classification commonly depends on the governing authority as enumerated in the model. Generic types of classification are needed when the classification is not specified by the governing authority; the employee data policy should cite the proper governing document if one exists.

NOTE—The cardinality assignment specified between the sensitive data and data classification blocks. To explain further, an instance of sensitive data may have no part association with any instance of data classification, or it may have many instances of data classification as its parts. The reverse is also true. This cardinality is important because employee data policy can establish the recommended classifications based on the governing authority, and for some classifications state it is a "local matter" if it applies to a specific instance of sensitive data.

As data are compiled, the compilation should include the data source, data controls, and data characteristics. The list of data characteristics should be mappable to the enumerations described in the reference model. Some enumerations are complex, for example, device settings for protection, restoration, and sensors maybe a function of time of day. Unless these enumerations are relatable to sensitive personal data, they are not within the scope of this standard. However, if a person is assigned to manage the settings, the operating logs provide a strong coupling between the identity of the person and the persons access and use privileges. Such data is exploitable by unauthorized entities. Furthermore, these logs expose information that can be used to determine the most likely attack points to gain access to sensitive areas and opportunity to migrate the attack vector to gain access to other sensitive areas.

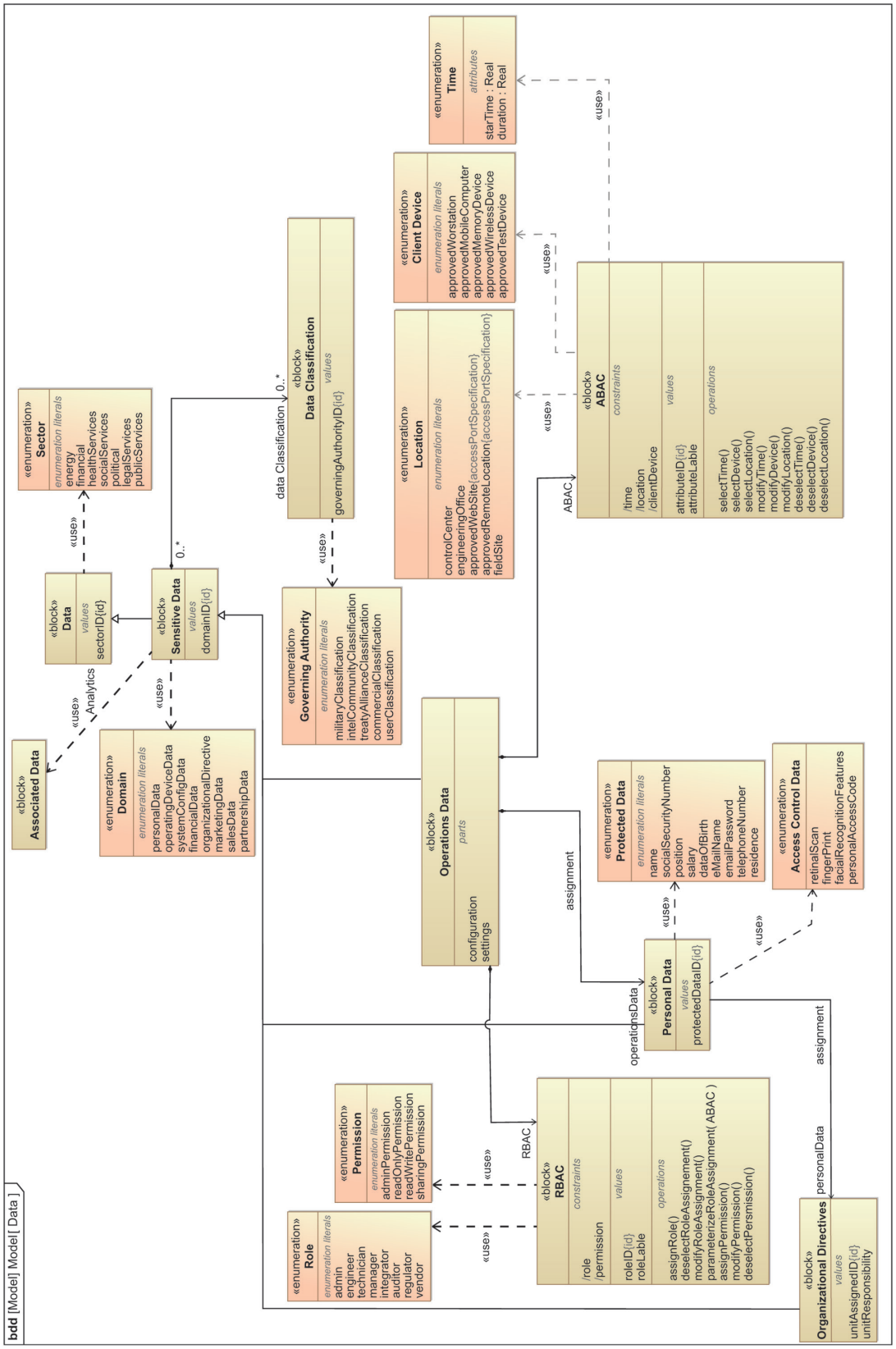

Figure A.4—Interaction of components related to personal data protection

A.3.1 Data enumerations

Figure A.5 highlights the sector, domain, and governing authority enumerations addressed in this employee data policy. An instance of data uses at least one of the sector enumerations to catalog the application under consideration.

NOTE—At this point, data is simply a compilation of all data owned by the system under consideration (SuC). No distinction is made to determine the sensitivity of each data object. Such a determination requires a risk assessment and consequence analysis.

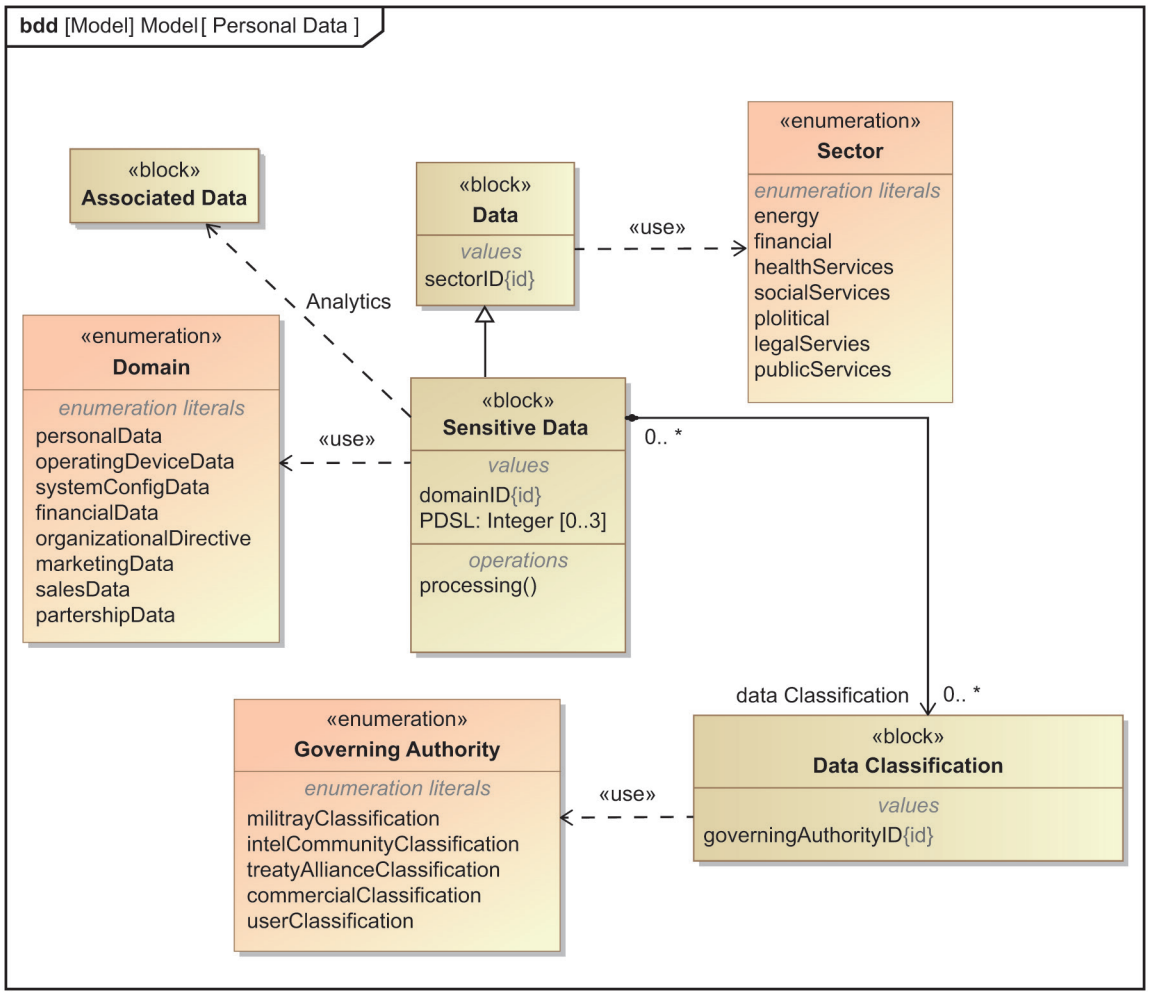

Figure A.5—Sector, domain, and governing authority enumerations

A specialization of data is sensitive data. Sensitive data references a domainID that needs to be explained in the employee data policy. An instance of sensitive data uses at least one of the domain enumerations to specialize the catalog of application under consideration.

One of the more difficult problems is to determine what data is sensitive. Figure A.5 identifies the need to address the analytics needed to determine sensitivity by associating data from different sources. The approach to do this is described in Annex C and the requirements for content management are summarized in 5.3.

Part of sensitive data is the directed association with data classification. Again, data classification references a governingAuthorityID that needs to be explained in the employee data policy. An instance of data classification uses at least one of the governing authority enumerations to further specialize the catalog of application under consideration. It should be noted by the cardinality 0..* that there may be no instance of data classification included as part of an instance sensitive data, or there may be many instances included as part of an instance of sensitive data. The reverse is also true as shown by 0..* label on the attachment to the sensitive data block.

A.3.2 Personal data enumerations

Two documents were used as the primary source of information to develop these enumerations: the GDPR[15] and the steering committee on media an information society's explanatory memorandum [B7]. In addition to the GDPR and explanatory memorandum, legal opinions and open commentaries were reviewed to better understand the interpretation of the applicable norms, laws, and regulations (Raul, Manoranjan, and Mohan [B21]).

Figure A.6 focuses attention the personal data enumerations. It should be noted that an instance of personal data is defined by two directed assignments. The assignment is based on an instance of the organizational directives applicable to the assignment of the person's assigned responsibility. Furthermore, the assignment is based on an instance of operational data that is applicable to the person's assigned responsibility.

Personal Data references a protectedDataID that needs to be explained in employee data policy. An instance of personal data uses the protected data enumerations to further specialize the catalog of the application under consideration. The protected data enumerations are the minimum set to be specified in employee data policy. In Figure A.6, the enumeration of protected data is not exhaustive.

A.3.3 Role-based access control enumerations

As shown in Figure A.7, an instance of RBAC is part of a directed association of an instance of operational data. The cardinality of this association will be explained in the employee data policy. RBAC treats roles and permissions as constraints. Furthermore, RBAC includes specific operations required for the management of the roles and permissions.

RBAC references a roleID and roleLabel that needs to be explained in the employee data policy. An instance of RBAC uses the role enumerations and permission enumerations to further specialize the catalog of the application under consideration. The role and permission enumerations are the minimum set that should be specified in the employee data policy.[16]

A.3.4 Attribute-based access control enumerations

As shown in Figure A.8, an instance of access-based access control (ABAC) is part of a directed association of an instance of operational data. The cardinality of this association will be explained in the employee data policy. ABAC treats location, client device, and time as constraints. Furthermore, ABAC includes specific operations required for the management of the location, client device, and time.

ABAC references an attributeID and an attributeLabel that needs to be explained in employee data policy. An instance of ABAC uses the location, client device, and time enumerations to further specialize the catalog of

[15]The General Data Protection Regulation (GDPR) replaces the EU's 1995 Data Protection Directive 95/46/EC. The GDPR has been developed to strengthen and unify online privacy rights and data protection for individuals within the European Union (EU) while streamlining the data protection obligations of businesses serving EU citizens through a single regulation instead of 28 different national laws. On April 9, 2016, the Council adopted the GDPR and an associated Directive. And on April 14, 2016 the Regulation and the Directive were adopted by the European Parliament. On May 4, 2016, the official texts of the Regulation and the Directive were published in the Official Journal of the European Union. The Regulation applies from May 25, 2018.

[16]The enumerated roles and permissions are common to the use cases reviewed for this annex. However, most use cases included other roles and permissions that reflected operational needs unique to a specific use case.

the application under consideration. The location and client device enumerations are the minimum set that should be specified in the employee data policy.[17]

Time is a special attribute used to constrain the period of authorization for access and use control. If duration is set to "0" the authorization is persistent with no end time.

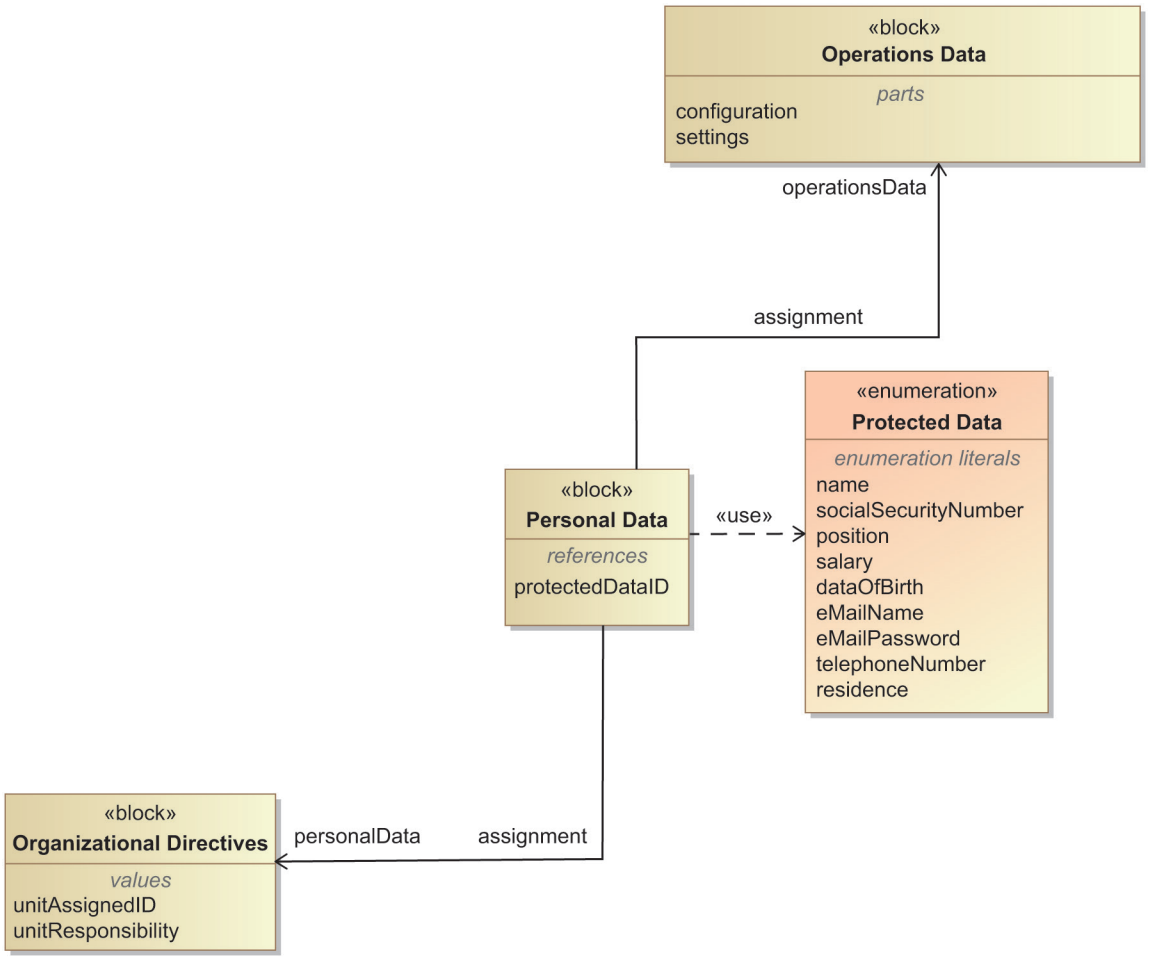

Figure A.6—Personal data enumerations

[17]The enumerated location, client device, and time are common to the use cases reviewed for this technical note. However, most use cases included other parameters that reflected operational needs unique to a specific use case.

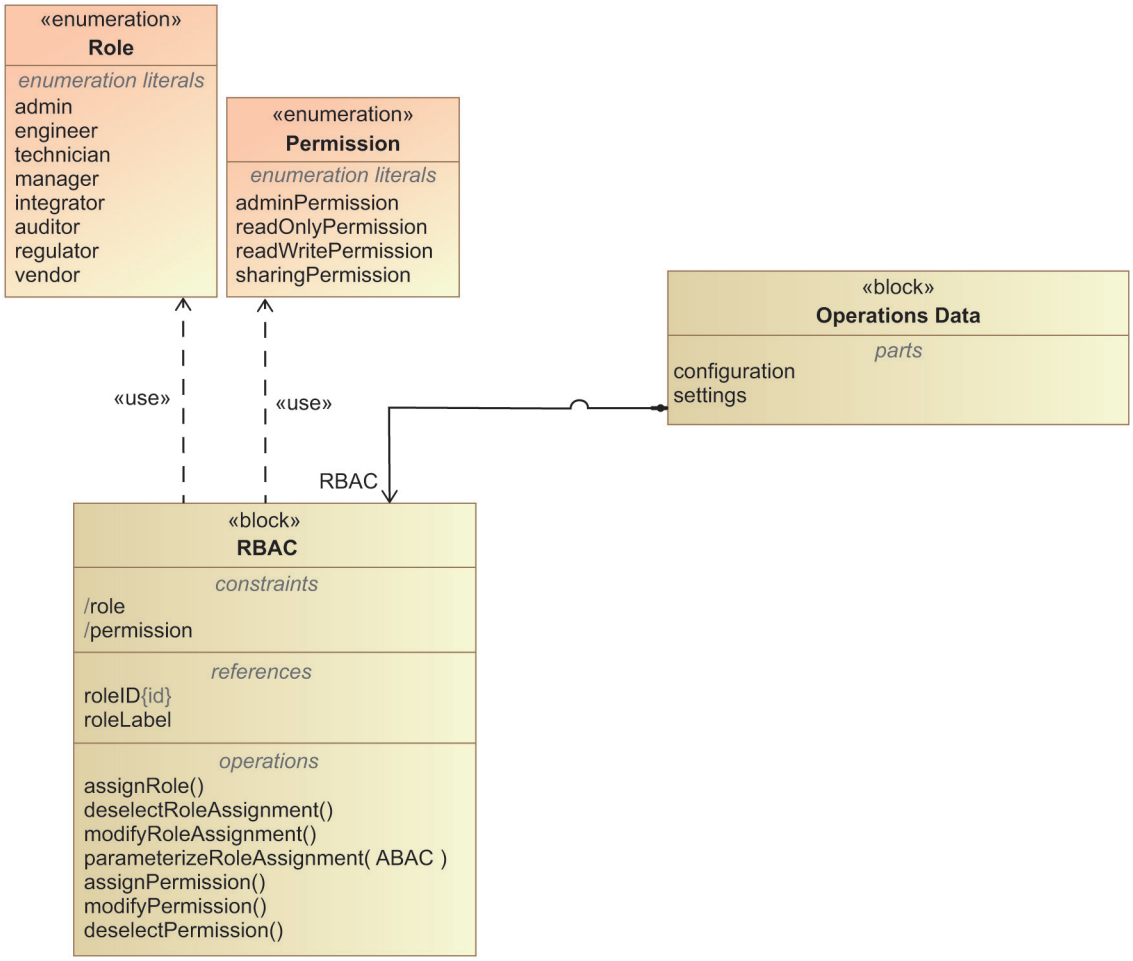

Figure A.7—RBAC role and permission enumerations

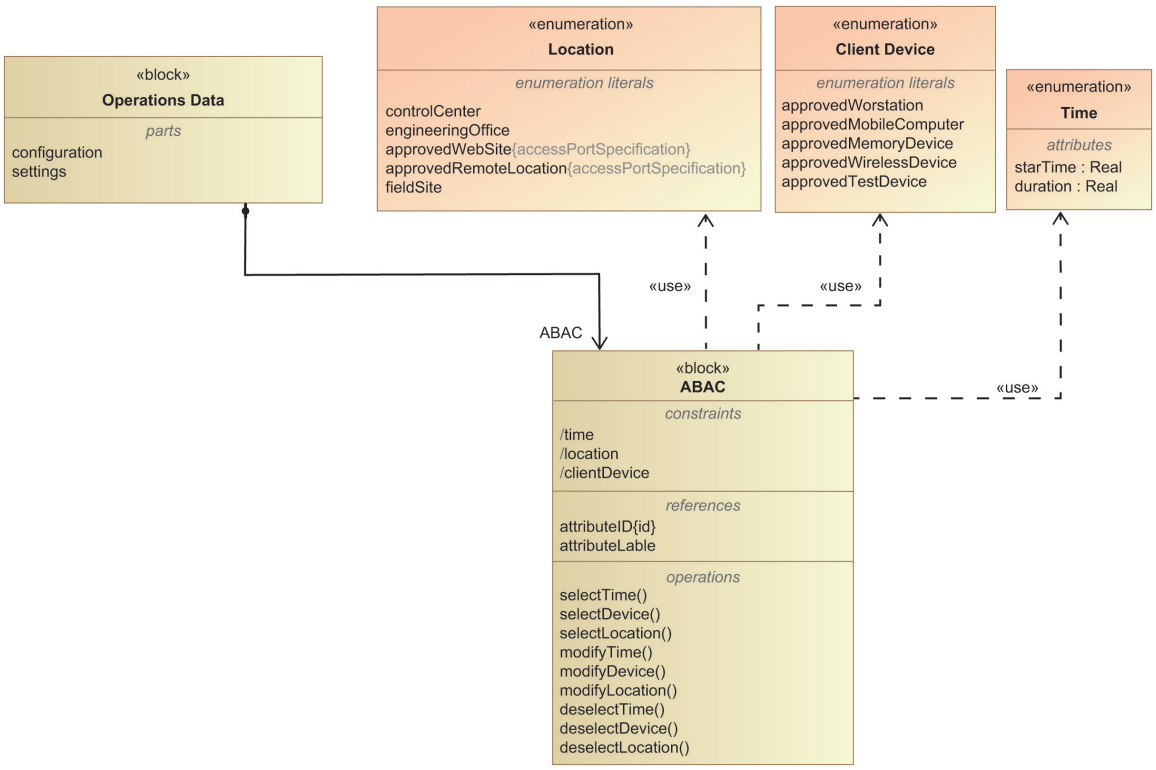

Figure A.8—ABAC location, client device, and time enumerations

Annex B

(informative)

Informed consent

B.1 Introduction

This annex describes the due diligence governance for informed consent from a data subject to securely collect, process, disseminate, use, and dispose of PII.

The purpose of this annex is to define a reference model to establish a basis for a coherent set of informed consent governance requirements that can be a legal basis for declaration of a clear affirmative act. This standard recognizes the on-going debate regarding "informed consent." For this reason, it is imperative that the consent form used by the employer and signed by both parties include all necessary statements to support the use of the agreement as a legal contract between employer and a data subject.

A legal contract is a local matter, to be determined in compliance with applicable laws and regulations, which may define requirements to obtain informed consent in relevant circumstances and set out legal criteria and requirements for such consent to be valid. Users of IEEE standards documents evaluate the standards for considerations of data privacy and data ownership in compliance with the applicable laws and regulations.

Many local laws and regulations include "exceptional circumstances" clauses that need to be included in the employer's policies, procedures, and organizational directives. Interpretation of these clauses such as when they are invoked and when they are revoked, how the exceptional circumstances process is managed, and who is the authority for managing the process are important clarifications to understand the limits of informed consent. In view of the GDPR consent [B7], the following seven minimum criteria need to be met in order to obtain informed consent:

a) Competence to understand and to decide[18]

b) Voluntary (freely given without implied coercion) decision making

c) Disclosure of material information including the risks entailed or alternatives

d) Recommendation of a plan

e) Comprehension of terms described in items c) and d)

f) Decision in favor of a plan

g) Authorization of the plan

A data subject gives informed consent only if all these criteria are met. If all criteria are met except that the data subject rejects the plan, that data subject makes an informed refusal.

Effective data governance is articulated in the employer's PP&OD. Clarity of intent is a prerequisite for each ROU to understand their responsibility and how they will be held accountable. PP&ODs usually state their mission objectives and general principles, but enforcement of each directive is adequately resourced with skilled personnel and funding. Accountability requires well-defined metrics to manage continuous process improvement and maturity.

[18]Some legal regimes may stipulate that consent for the use of personal data is always subject to the data subject's right to withdraw at any time. It may not always be possible to obtain valid consent from an employee without creating an inference of undue pressure, which can legally invalidate the consent."

Steiner postulates that data modeling is a form of data governance (Steiner [B23]). Given Steiner's approach, this annex uses MBSE to establish a coherent reference model. Zachman's life-cycle model is used to define black-box and white-box representations of the problem domain (Aleksandraviciene and Morkeviciius [B1], Earley [B4]). Given this standard's wide range of target audiences and applications, the reference model and governance requirements will represent a framework that can be tailored by the employer to comply with local norms, laws, and regulations and to address their unique operating constraints.

B.2 Informed consent model

B.2.1 Stakeholder needs

There are two principal players that focus attention on defining the stakeholder needs: the employer and the data subject. The responsibility of the employer is to provide skilled practitioners that can clearly articulate the applicable PP&OD requirements in terms that can be understood by the data subject. This includes disclosing all material information including risks entailed in the collection, processing, dissemination, use and disposal of PII. Lastly, the employer recommends a detailed plan of action so the data subject understands that every step of the process is under positive control and the data subject has a voice in this process.

In turn the data subject needs to acknowledge that consent or refusal is volunteered without prejudice. The consent process provides a reasonable exchange of questions and answers so that the data subject understands the obligations of consenting to the plan. When this exchange reaches a reasonable conclusion, the data subject formal signs a document that indicated acceptance or refusal of the plan of action.

Table B.1 is an MBSE description of these stakeholder needs to be addressed in the reference model and normative governance requirements specified in the employer's PP&OD. These needs represent a compositive view expressed by employers.[19]

Table B.1—Employer and data subject needs

SN-1: Employer needs	SN-1.1: Skilled practitioners	It is imperative that the employer resource skilled practitioners to facilitate the discussion of informed consent with the data subjects.
	SN-1.2: Disclosure	It is imperative that the employer disclose all material information, including risks entailed and alternatives.
	SN-1.3: Plan of action	It is imperative that the employer recommend a plan of action.
SN-2: Data subject needs	SN-2.1: Volunteer consent	It is imperative that the data subject acknowledge that consent or refusal is volunteered without prejudice.
	SN-2.2: Understand the obligations of consent	It is imperative that the data subject acknowledge that the material information, including obligations and risk, are understood.
	SN-2.3: Authorization of consent	It is imperative that the data subject formally authorize or refuse the plan of action.

B.2.2 System context to solicit consent

Figure B.1 is an internal block diagram (ibd) of the PP&OD in use. These are the principal actors and supporting documents needed to define the system of interest (SoI) process to solicit consent from the data subject. The two human actors are the employer's representative and the data subject. The consent form is the outcome under discussion. Supporting references to this process are comprehensive descriptions of the applicable PP&OD requirements for the role of the data subject, the obligations assumed by the data subject if consent is granted, the risks associated with the use of the data subjects PII, and the plan of action needed for positive control during every step of the process.

[19]The view was not solicited by a formal survey. They are the result of limited interviews by members of the working group for this standard.

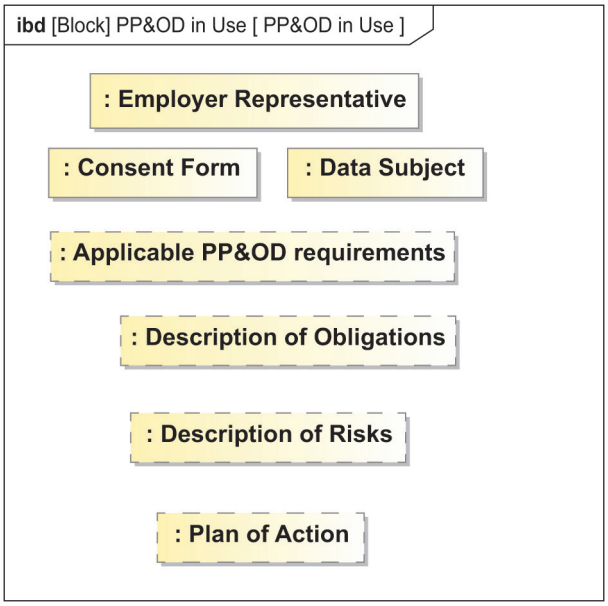

Figure B.1—System context to solicit consent

B.3 Use case reference models

B.3.1 Informed consent use case

Figure B.2 represents the MBSE use case for informed consent. The rake symbol identifies the need to create a detailed activity diagram of the process the employer determines if the data subject agrees to the action plan thereby gaining formal consent or if the data subject refuses consent.

To define this process, we use MBSE's activity diagrams to addresses the stakeholder needs (Table B.1) and the system context (Figure A.7).

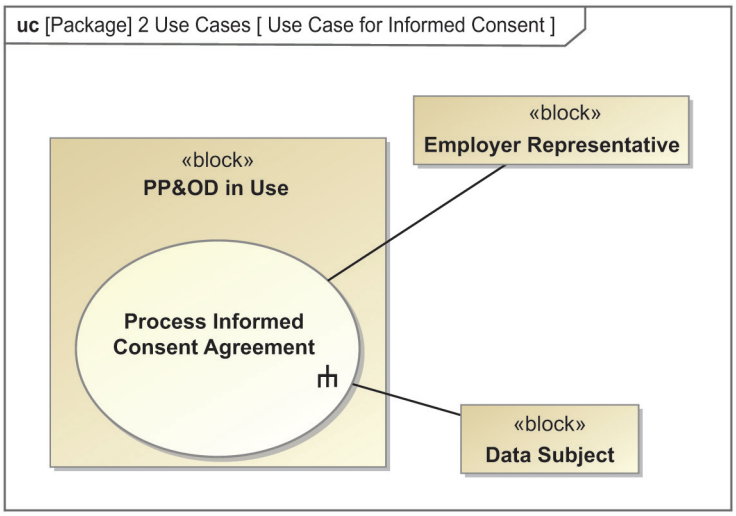

Figure B.2—Use case to solicit informed consent

B.3.2 Understanding the consent form

An informed consent form is a document that both parties (employer representative and data subject) should sign before participating in the action plan. This document gives specific information about the action plan, including but not limited to title of the activity, data subject name, the purpose of the action plan, the reason the data subject is offered to participate, and the duration of the action plan.

A proper informed consent form acknowledges that the data subject is volunteering without prejudice to accept the obligations and risks associated with the potential exposure of PII. Alternatively, the data subject can sign the form showing refusal to participate in the action plan without prejudice.

B.3.3 Understanding the applicable PP&OD requirements

A prerequisite for this task is the need for the ROU SMEs to tailor the PP&OD to identify the applicable requirements and provide additional specificity. Such tailoring requires approval from the governing authority.

The next task is for the employer representative to explain to the data subject the applicable PP&OD requirements that will influence the decision to participate in the action plan. Figure B.3 shows the iterative nature of this exchange. This part of the discussion ends when the data subject expresses an affirmative assent that they understand the applicable PP&OD requirements.

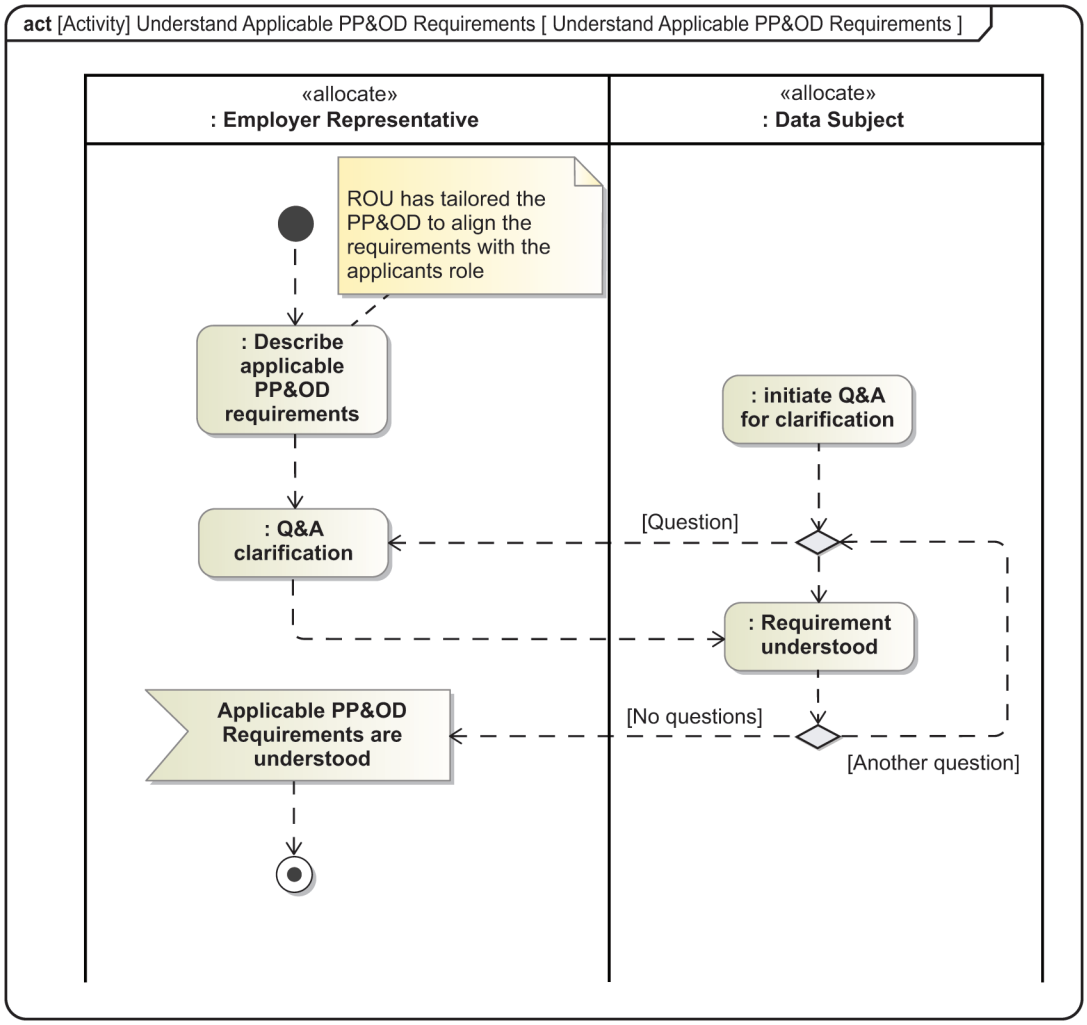

Figure B.3—Review and acceptance of the applicable PP&OD requirements

B.3.4 Understanding the obligations and risks

A prerequisite for this task is the need for the ROU SMEs to list the obligations and potential risk of PII exposure and provide additional specificity. Such descriptions require approval from the governing authority.

Figure B.4 shows a sequence similar to Figure A.1. Again, the data subject is offered every opportunity to request clarification of the obligations and potential risk of PII exposure that will influence the decision to participate in the action plan. This part of the discussion ends when the data subject expresses an affirmative assent that they understand the obligations and potential risks.

An important element of this discussion is to understand what happens if PII is exposed. This will be explained in more detail in B.5 and B.6, including the following:

— What security safeguards are used to minimize the risk of exposure?

— What is the notification procedure?

— What are data subject's options if PII is exposed?

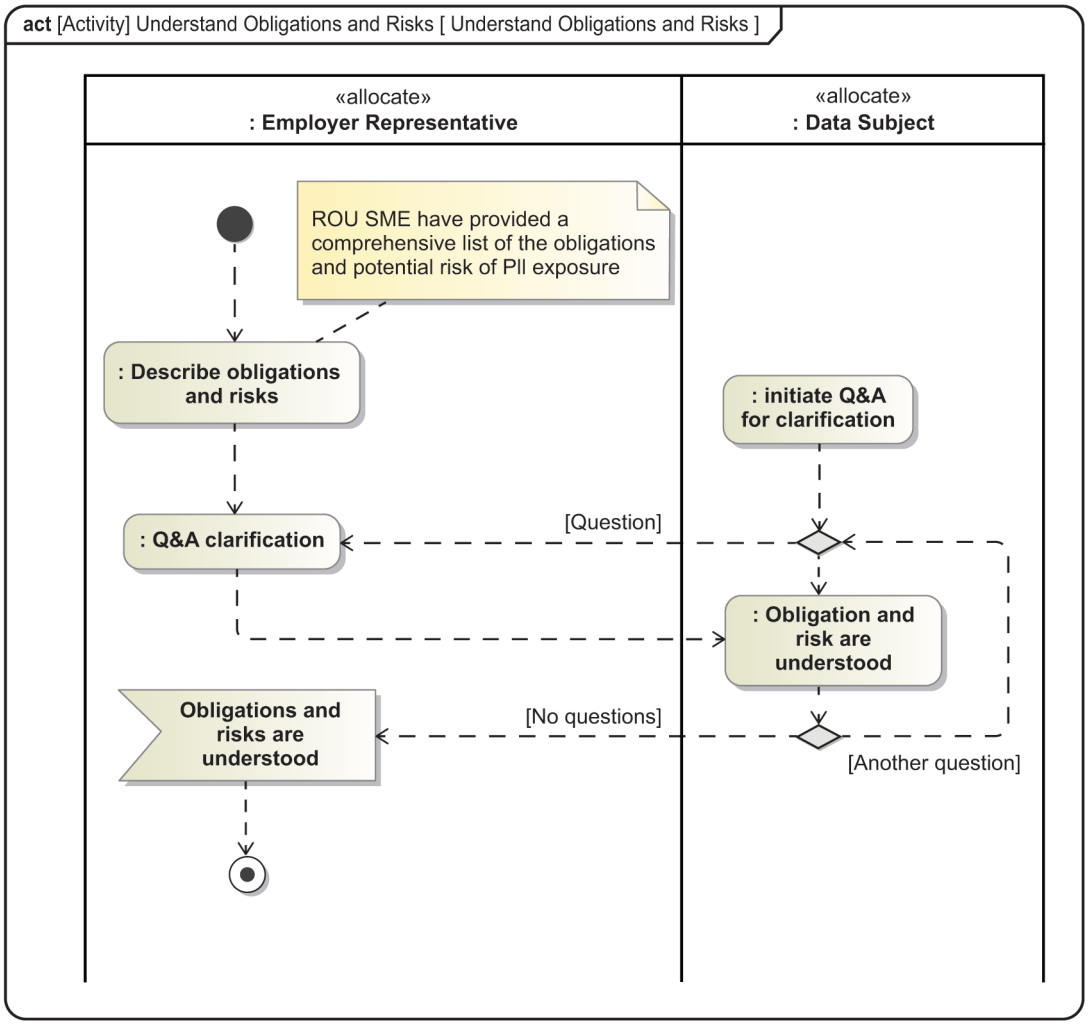

Figure B.4—Review and acceptance of data subject's obligations and risks

B.3.5 Understanding the plan of action

A prerequisite for this task is the need for the ROU SMEs to describe a comprehensive action plan and provide additional specificity. Such descriptions require approval from the governing authority.

The same procedure discussed in Figure B.3 and Figure B.4 applies here; only the topic is the action plan. This part of the discussion ends when the data subject expresses an affirmative assent that they understand all elements of the action plan.

B.4 Measures of effectiveness

Figure B.5 captures the KPIs and MoEs. These metrics are important to effectively manage the employer's informed consent program. The governing authority is responsible for reviewing the results of executing the program and determining the corrective action needed to improve the program. For example, if the acceptance level is less than what is expected, some corrective action is in order. For this reason, the PER includes the reasons for rejection and recommendations to improve the program.

As described in B.3.5, informed consent requires the data subject to understand the plan of action implementing the consent agreement. This implementation is described as the SiU. Commonly, MTTD, and MTTR are the metrics used to evaluate the effectiveness of the SiU implementation. SiU references shown in Figure B.4 are discussed in more detail in B.6.

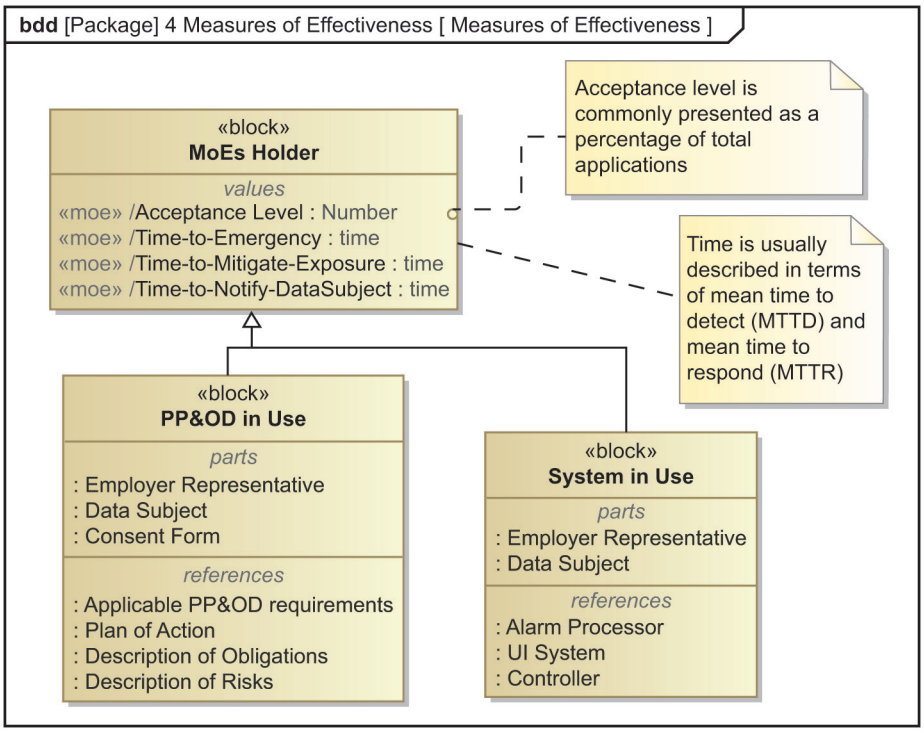

Figure B.5—Acceptance level MoE and SiU performance

In the context of a data breach, the exposure of the data subject's PII, MTTD and MTTR is described in terms of three MoEs:

a) *Time-to-emergency:* This is the time from the onset of the attack sequence to collect PII to the first instance when a PII breach is confirmed. Time of onset is difficult to establish; therefore, this metric needs to be qualified with properly stated assumptions.

b) *Time-to-mitigate-exposure:* This is the time from when a PII breach is confirmed to the deployment of corrective action to mitigate the potential damage resulting from the exposure of the data subject's PII.

c) *Time-to-notify-data subject:* This is the time from when a PII breach is confirmed to the time when the data subject has been notified that PII has been exposed.

When notified of the PII breach, the data subject is fully briefed on the corrective action taken to mitigate the potential damage resulting from the exposure of PII. With this information, the data subject has the option to withdraw (opt-out) agreement of consent.

B.5 Functional analysis

B.5.1 White-box technical approach

In Zachman's model [B24], functional analysis, using a white-box representation of the problem domain, is the first step to describe the behavior of the SoI. From a governance perspective, the issue is addressed is to establish a framework for ROUs to respond to the exposure of the data subject's PII. The approach used in this annex is to address this issue in terms of the risk of exposure introduced by the need for transparency.

B.5.2 Use case for the SoI

Without going step-by-step through the development of a transparency model, consider the use case for a generic SoI shown in Figure B.6. We assume that the SoI in use is exchanging data between sources and receivers, and in accordance with the action plan summarized in 5.2.2, these data include the data subject's PII.

Also, the model includes an observer in this scenario. Figure B.7 shows that an observer is legitimate in the sense of authentication where the role is an administrator or a supervisor. However, one should keep in mind that an authenticated observer is possibly an insider threat—a most difficult issue to address. Also, an observer is possibly an unauthorized observer sponsored by a nation state, a criminal activity, or a simple hacker.

For either case the data exchange scenario is described in Figure B.8. In this example, the focus is on the exposed communication port used by the observer to monitor the communication traffic. The data packets shown in Figure B.8 contain the data subject's PII, and the scenario assumes the observer has developed the capability to process the data packet and expose the PII. Thus, there is the potential for a breach to be addressed in the PP&OD and reflected in the ROU's action plan.

B.6 Logical architecture

Lastly, the generic solution needs a model of the logical architecture representing the data exchange in Figure B.8 to identify other components and issues that need to be addressed in the PP&OD and ROU's action plan.

Figure B.9 describes a logical architecture of a typical SoI addressed by ROU's action plan. One important feature illustrated in Figure B.9 is the need for alarm notification to warn the data user of anomalous activity introduced by an observer. For this annex, the intent is not to design the system operation but to identify issues that need to be addressed in the ROU's action plan. This is needed so that enough information is exposed to satisfy the questions raised by the data subject.

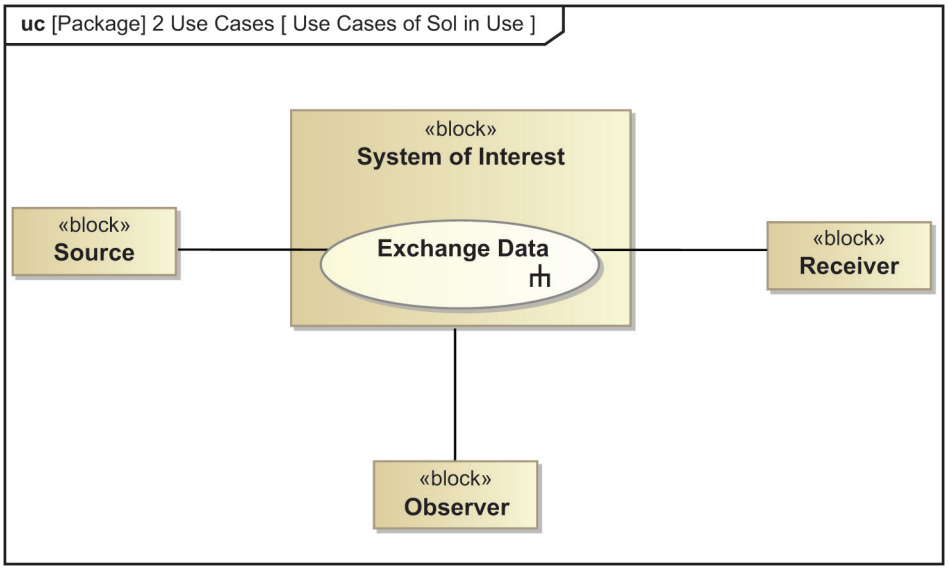

Figure B.6—Use case of a generic system of interest

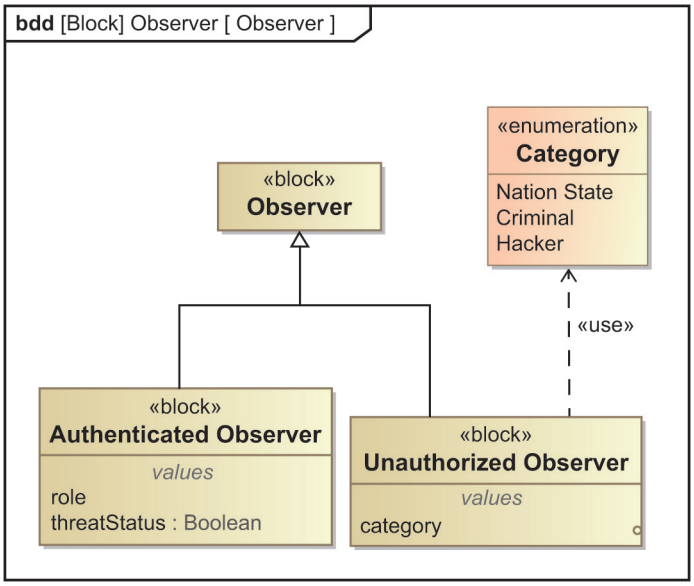

Figure B.7—Focus on the observer during the data exchange

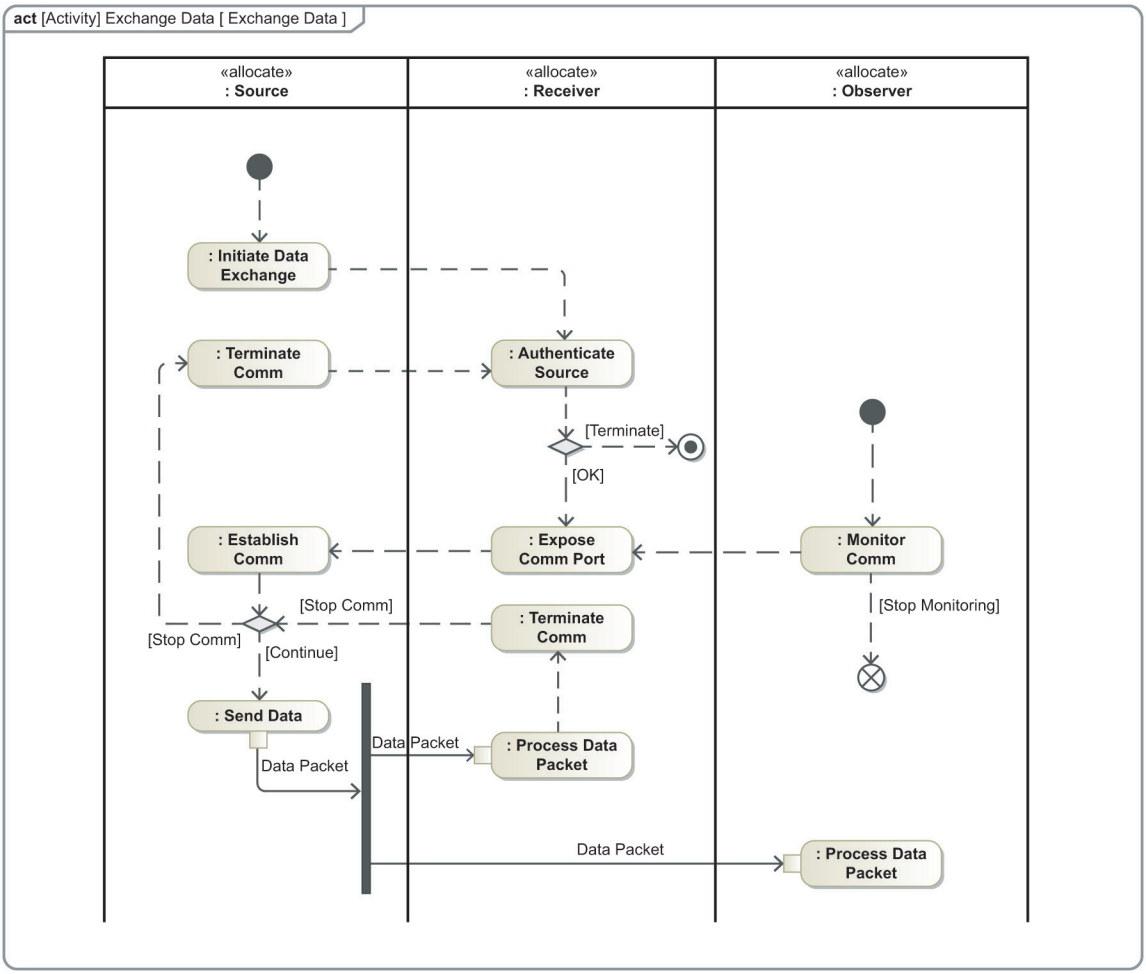

Figure B.8—Data exchange scenario

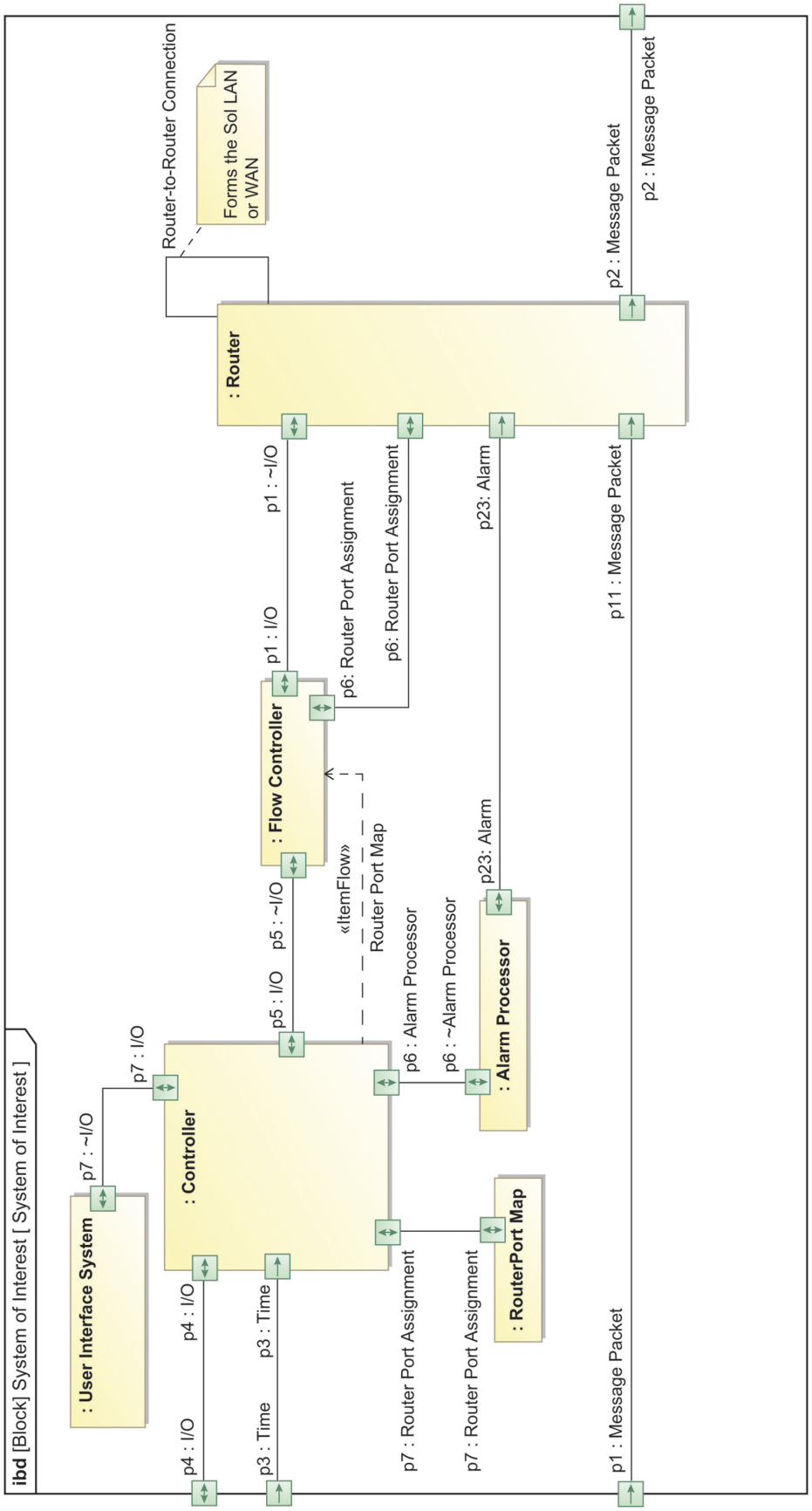

Figure B.9—Logical architecture for a typical SoI

Annex C

(informative)

Content management platform

C.1 Introduction

This annex describes a coherent approach to determining the sensitivity of PII derived from data obtained from disparate sources. Understanding the technical challenges for a content management platform (CMP) established the basis for the requirements summarized in 5.3. The technical challenge is addressed in terms of the data collection complexity and data fusion complexity. McCallister, Grance, and Scarfone [B19] address some of the technical challenges to protect the confidentiality of personal identifiable data.

C.1.1 Data collection complexity

As noted by Earley [B4], in addition to receiving data of different types and in different formats that have varying structures and naming conventions, data might come into the CMP through a live feed via an application program interface (API) or web service layer or might be input on batch basis through a file transfer[20]. Thus, one task of the CMP is put the data into a consistent format so that it can be correlated with other data. Rules for cleansing, enriching, appending, and correction data is needed to reduce the cost and complexity of data hygiene by automating remediation. How this is accomplished is not addressed in this standard.

Metadata probably comes from many sources. Some are based on explicit attributes such as demographics, content preferences, and account information. Furthermore, sensitive PII probably comes from subjective or behavioral attributes, such as social media patters. From Kremer, Mé, Rémy, and Roca [B17], some examples, modified to focus on the data subject's PII of explicit, objective, or applied metadata are:

— Employer type (consumer, business, non-profit, public)
— Data subject's demographics (age, gender, language, location, income level)
— Data subject's data (account, names, address, contact phone, email address)
— Data subject's account details (products, service plans, billing, rate plans, credit information)
— Data subject's relationship details (trouble tickets, call history, account access details)
— Data subject's content preferences (product updates, technical, communities, topics, offerings)
— Data subject's equipment (devices, configurations)

Also, from Kremer, Mé, Rémy, and Roca [B17], some examples of implicit, subjective, or derived PII metadata are:

— Data subject's social groups (LinkedIn profile, Facebook information, Twitter, Instagram)
— Data subject's marketing activity (website store, email open, campaign history)
— Data subject's strategic segmentation (high value, high growth)
— Data subject's social media (forum discussions, participatory marketing, social conversations)
— Data subject's loyalty attributes (predicted lifetime values, likelihood to recommend value, length of relationship)
— Data subject's behavioral segmentation (purchase behavior, motivational behavior)

[20]As applicable to PII sensitive data, this annex maps the consumer data platform to the content management platform.

A major function of the CMP is to act as a centralized location so other systems can access and act upon possible sensitive data. For example, in a cloud service environment, CMP becomes a broker or orchestration layer that can take the output from one application, process it, convert the format, and export it or make it available via an API for fusion with other data.

C.1.2 Data fusion complexity

A PII CMP-centric model identifies the factors that can predict a person's behavior. Without a model, there is no way to systematically test the effectiveness of different exploitation strategies. A well-defined CMP model captures a variety of data like name, address, and demographic details that can be derived or inferred.

Despite variations in the data, CMP contains enough detail and the correct attributes to support advanced functionality such as predicting patterns. CMP stores sensitive data that is leveraged by various downstream systems to predict and influence employer governance needed to protect the data subject's PII.

CMP needs to have the capability to align specific pieces of information to understand the level of sensitivity. The challenge lies in identifying what data is important, understanding how it contributes to determining sensitivity, and determining what to do with it.

C.2 Content management platform

C.2.1 User needs

Zachman's lifecycle framework is used in this annex [B24]. MBSE is used to develop the specification at each stage in Zachman's framework. OMG's SysML provides a formal structure for the CMP model.

Table C.1 establishes the user needs, where "F" designates a functional requirement, and "I" designates an interface requirement. User control is a functional requirement that is addressed in final specification for the solution. This is a minimum set of needs; it is not exhaustive. R, F, and I are SysML notations, they should not be interpreted as normative requirements.

Table C.1—CMP user needs

SN-5: User Needs	
SN-5.1: Collection	It is imperative that the CMP have the capability to receive data of different types and formats that have varying structures and naming conventions.
SN-5.2: Formatting	It is imperative that the CMP have the capability to put the data into a consistent format, so that it can be correlated with other data.
SN-5.3: Visibility	CMP must make the reformatted data visible so other systems can access and act upon possible sensitive data.
SN-5.4: Alignment	CMP needs to have the capability to align specified pieces of information to understand the level of sensitivity.
SN-5.5: Prioritization	CMP needs to identify what data is important, understanding how it contributes to determining sensitivity, and determining what to do with it.
SN-5: User control	The user needs to maintain control of the protection of data in transit and at rest in a manner independent and indifferent to network configuration and topography.

C.2.2 System context

Figure C.1 identifies the CMP system components needed to perform all actions. The front-end processor (FEP) receives the data from each authorized source and call the file formatter (FF) to convert the data to the common format used by the CMP. When successfully reformatted, the FF calls the alignment processor (AP) to align

specified pieces of information according to prespecified rules. When alignment is successfully completed, the AP calls the prioritization processor to prioritize the information in accordance with prespecified rules. When successfully completed, the prioritization processor calls the interface controller to publish the file to a specified interface.

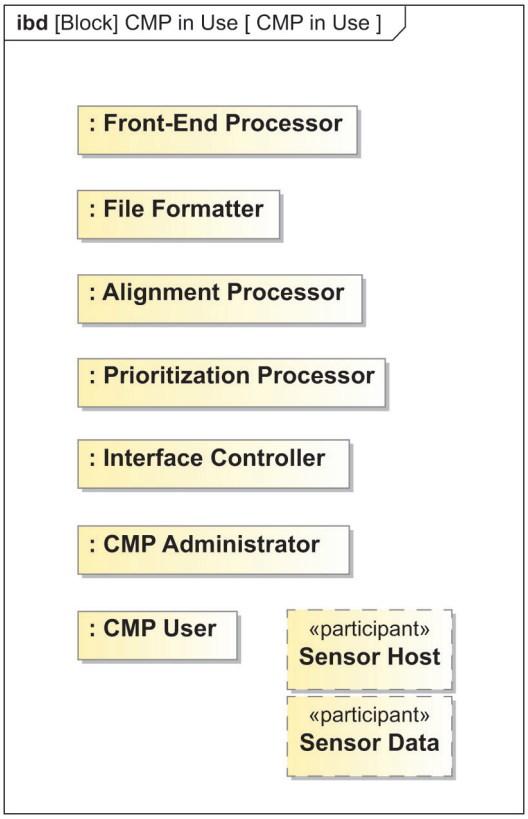

Figure C.1—CMP system components

All actions are under the positive control of the CMP administrator. Once the CMP is configured, the CMP user maintains positive control of access to and use of data in transit and at rest, in a manner that is independent and indifferent to the communication network configuration and topography. The CMP user protects and controls the data, not the communication network.

Figure C.2 identifies the CMP use case under positive control of the CMP administrator. The rake icon symbol indicates that an activity diagram (process flow) establishes the basis for specify the normative requirements summarized in 5.3. Figure C.2 also identifies the CMP use case under positive control of the CMP data user.

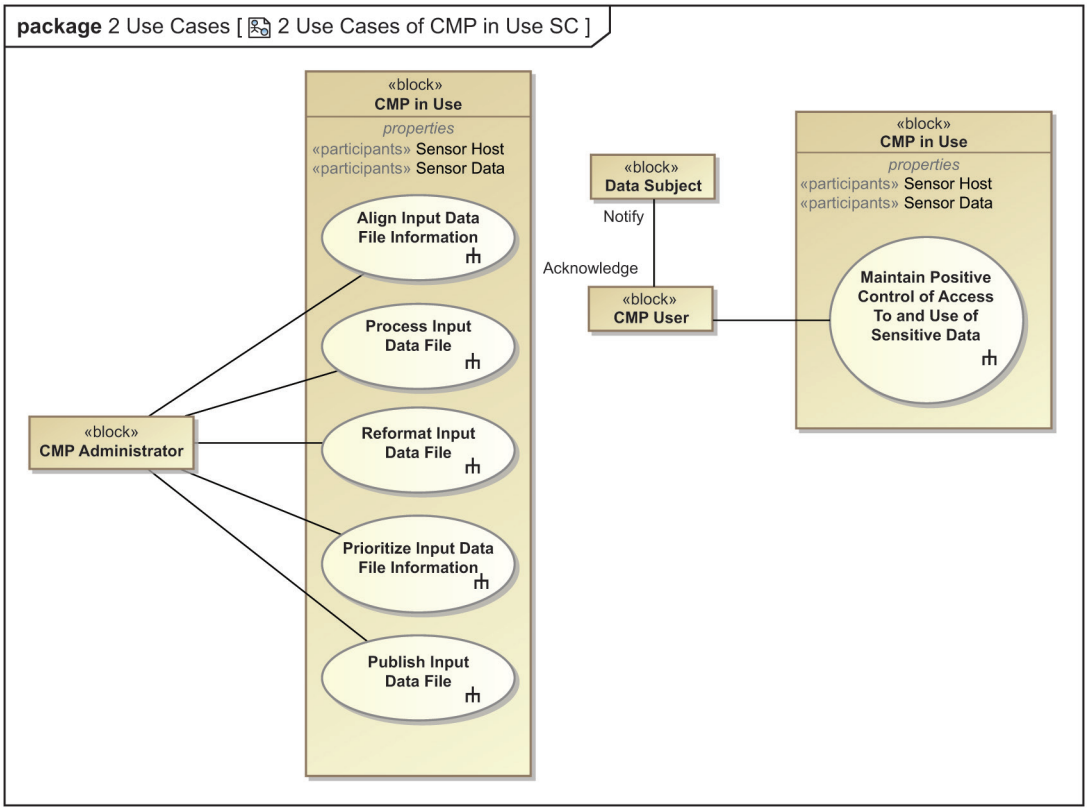

Figure C.2—Use cases of CMP in use

C.2.3 Measures of effectiveness

Figure C.3 identifies the MoEs used to evaluate CMP end-to-end performance, including the following:

a) Number of errors that occur during each step of CMP's process

b) Number of retries that occur during each step of CMP's process

c) Operation load as a percentage of CMP's design capacity

d) Throughput measures as the time from receipt of an input file to the time of its publication to a specified interface. Throughput time requires accurate time stamping.

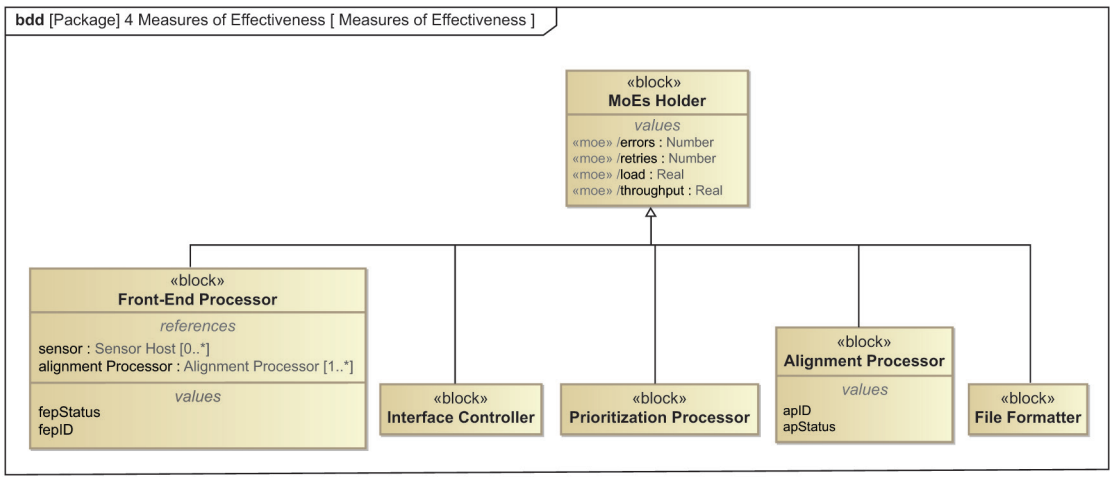

Figure C.3—CMP measures of effectiveness

C.3 Functional analysis

C.3.1 Process input data

This annex assumes that sensor[21] data is collected by a sensor host as shown in Figure C.4. The sensor host also uses environmental data to qualify the sensor data. An instance of the sensor host may be associated[22] with no sensor or multiple sensors (0..*). However, and instance of a sensor is associated with at least on instance of sensor host (1..*).

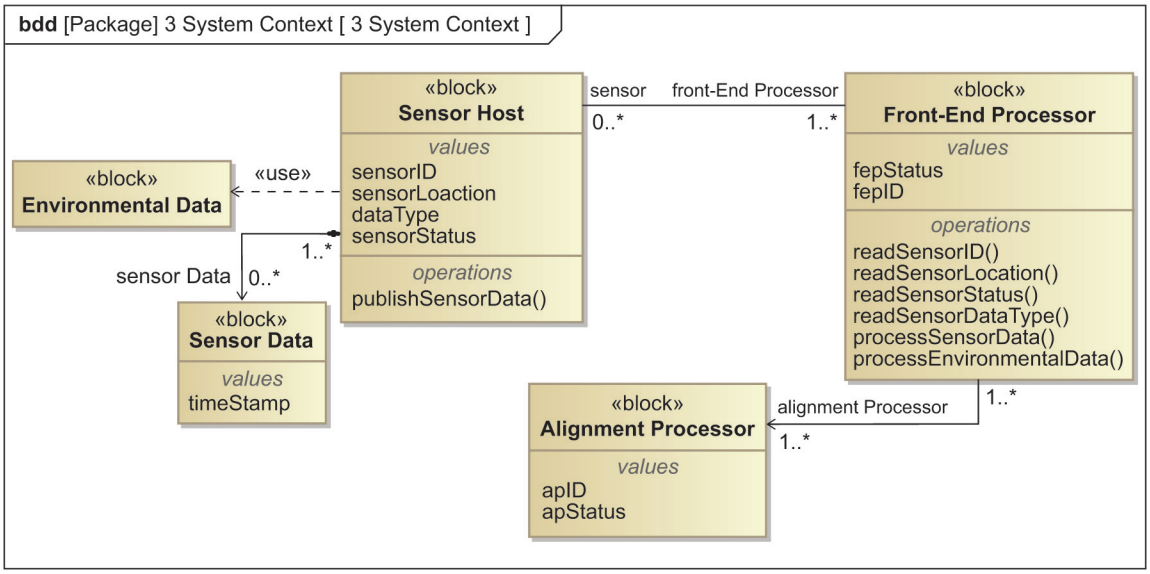

Figure C.4—Interaction between sensor host and front-end processor

[21]The term "sensor" is used with the recognition that data can be collected from other devices that are not sensors.
[22]The term "associate" or "association" does not imply a physical connection. It simply associates or describes the relationship and cardinality between to object of interest.

Given the sensorID, the appropriate sensor data FEP is selected. The FEP is associated with no sensor host or multiple sensor hosts (0..*). However, an instance of a sensor host is associated with at least on instance of FEP (1..*).

C.3.2 Initialize sensor host

Figure C.5 shows the activity needed for the CMP to initialize the sensor host that manages sensors under its control. The process begins with the CMP administrator establishing the conditions and constraints to initialize the sensor host and sensor selection. The message containing these data is broadcast to all sensor hosts on the network. Sensor hosts receiving this message check their availability and the availability of the sensors under their control for the conditions and constraints requested in the message.

If a sensor host is not available, it is removed from the inventory associated with the request. The same is true for and sensor under control of the sensor host for the conditions and constraints requested in the message.

If the sensor host and selected sensors are available, it returns an affirmative acknowledgment to the CMP administrator. This initiates the sensor selection by the CMP administrator in a manner that provides positive control of the selection process.

Based on the CMP administrator's selection of the applications required by an authorized data user, acceptable sensor locations and networks that are verified are selected and the sensor availability flag (SAF) is set to enable. If the candidate is not verified, the SAF is set to disable. The CMP generates a SAF broadcast message to sensor host with SAF set to enable or SAF set to disable.

For SAF set to enable, the sensor host updates the availability of the selected sensor's status and maintains availability for the conditions and constraints established. For SAF set to disable, the sensor host deletes those sensors from the selected application inventory.

C.3.3 Initialize front-end processor

Initializing the FEP under positive control of the CMP administrator is similar to the process described in C.3.2 except that the candidates are FEPS not sensor hosts.

C.3.4 Generate a composite data file

Figure C.6 shows the activity needed for the sensor host to collect the data and for the FEP to process these data. As shown by the rake symbols there is an initial activity to initialize the sensor host (see C.3.2) and to initialize the FEP (see C.3.3). these processes establish the communication sessions between sensor host and each sensor that provides the data to that instance of the sensor host. Similarly, the communication sessions are established between each instance of the sensor host and each instance of the FEP.

For each instance of the sensor host and its associated instances of sensors, the sensor host reads the configuration data for the sensor. Each sensor host then collection the environmental data that could influence the relevance of the sensor data to the process of determining if the data is classified as PII. In addition, each instance of the senor host collects the sensor data from each sensor associated with that host.

The sensor configuration data, environmental data, and sensor data are then merged into a file formatted for the instance of the FEP that requested the sensor file. The FEP receives the sensor file and proceeds to process the file. This process is another activity designated by the rake symbol. Once processed, the data is formatted for alignment processing (see C.3.5).

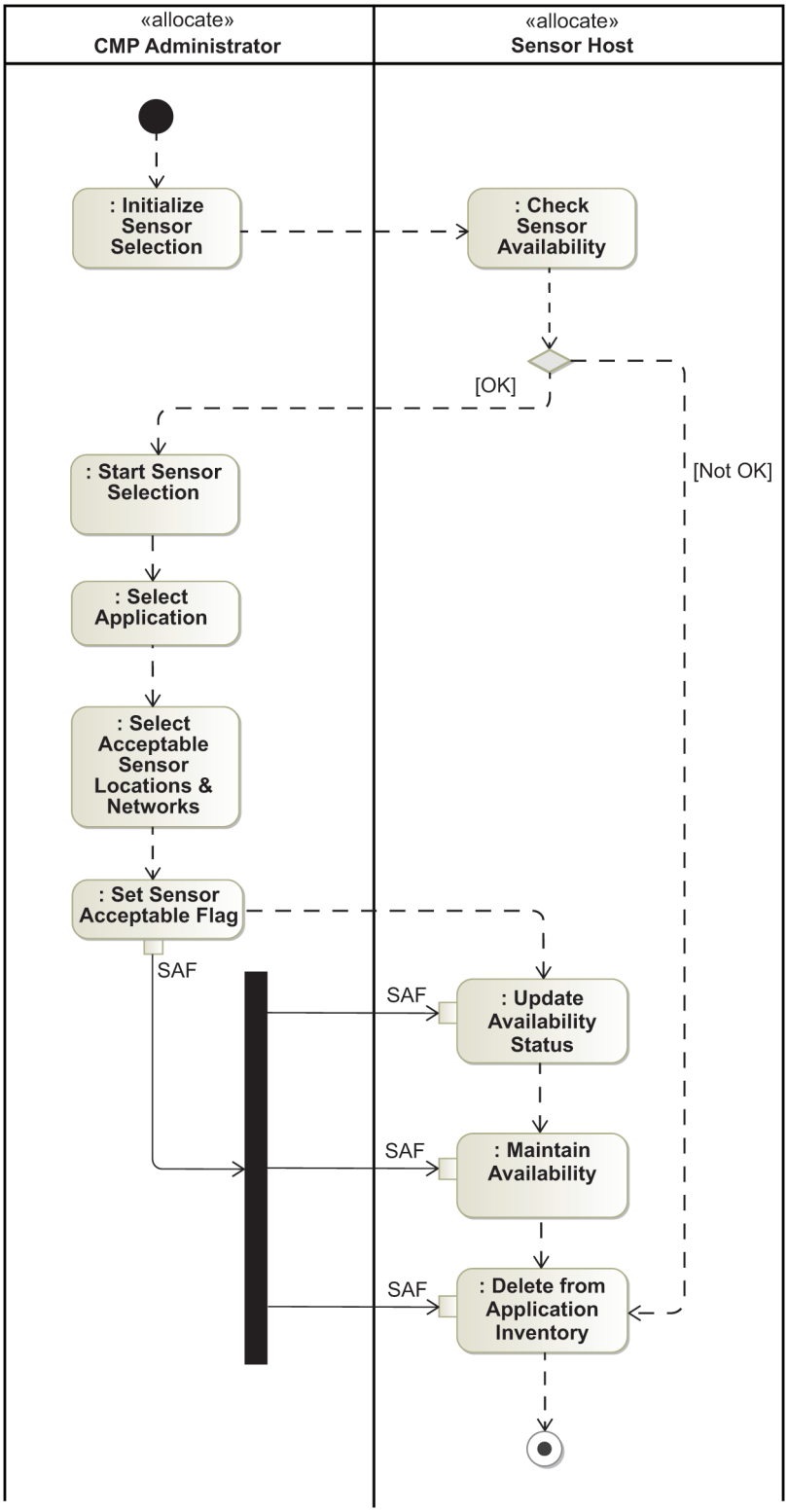

Figure C.5—Process to initialize sensor host

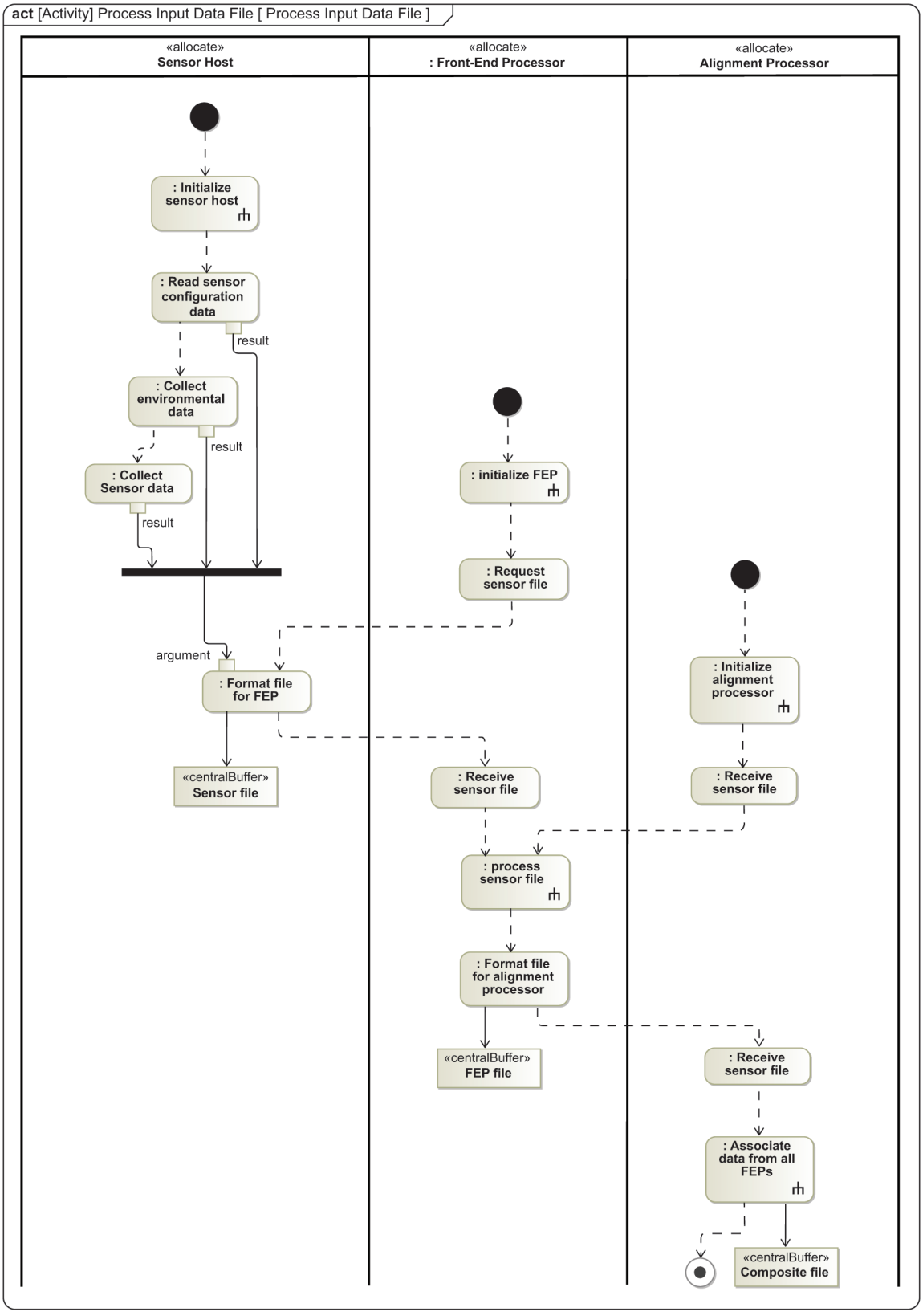

Figure C.6—Process to generate a composite data file

C.3.5 Align input data

Figure C.4 shows that an instance of the FEP has a direct association (->) with at least one instance of an alignment processor (1..*). Furthermore, an instance of the alignment processor has at least one association with an instance of the FEP (1..*). These combinations provide the capability to process the sensor data and associated information collected by the FEP from the sensor host. For example, the alignment processor qualifies the use or alignment of the sensor data based on the following:

- Accuracy
- Environmental condition, which usually has limits for temperature and humidity
- Range describing a measurement limit of the sensor
- Calibration, which is essential for most measuring devices as the readings change with time
- Resolution, which describes the smallest increment detected by the sensor
- Repeatability, which describes variations measured under the same environment

Output from the alignment processor is timestamped and sequentially ordered with the following information to be used by the file formatter.

- dataType: sensor data, analog data, video data, etc.
- sensorID: type of sensor; e.g., wearable sensor, tracking sensor, video sensor, etc.
- sensorLocation: static location or mobile device to associate with other data (groups)

Like the sensor host and FEP, each instance of an alignment processor is initialized to establish its communications sessions with each instance of the FEP. Each alignment process receives FEP files from the relevant FEPs and performs the complex task (shown by the rake symbol) to associate these data. The result is an ordered composite file that can be used by a prioritization processor discussed in C.3.4.

The last step in the process is to securely publish the composite data to a user-defined interface. Most probably there are multiple users of the composite data file: e.g., security SMEs to improve the organization's security posture, legal SMEs that use the data as forensic evidence and legal action, and operations SMEs that use the data to improve the functional capabilities of their system. Each receiving organization adds information to the data file to support their work.[23] Preserving the chain of evidence is governed by the local laws and regulations. Post processing the composite data by these users is not CMP's responsibility.

C.4 CMP user's positive control over access to and use of sensitive data

As stated earlier, the data subject retains ownership of their data, which requires all data users to use the data in accordance with the permissions agreed to by the data subject. The subject of informed consent is addressed in Annex B. Figure C.7 shows the interaction between the data subject (data owner), the ROU's CMP user and the CMP control unit. The CMP control unit is either the sensor host discussed earlier, or a separate controller.

Upon receipt of a legal order,[24] the ROU initiates the process to collect the data. If the output from the configuration file has classified this data as sensitive PII, the data subject is notified of the collection before collection is initiated. Collection is only started when the [Acknowledge] guard shown in Figure C.7 is received from the data subject. When collection is complete the process is terminated, and the data subject is notified as shown by the [Notify] guard.

[23]For example, a legal action may require indexing the composite file to the catalogs recognized by the court of jurisdiction.
[24]A legal order may be an order from an accredited regulatory agency, or its agent, a court order, or an order based on the approve PP&OD.

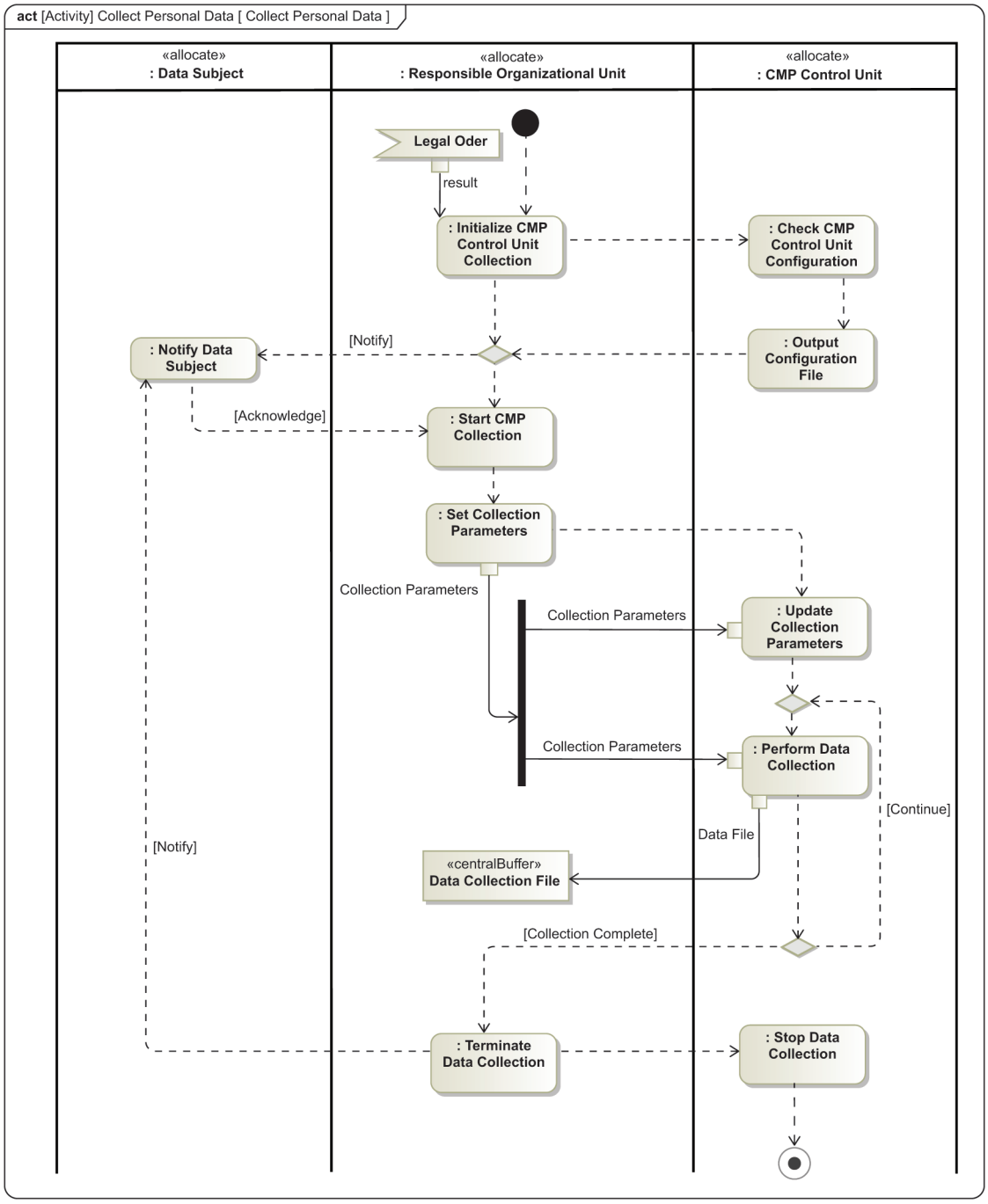

Figure C.7—Interaction with the data subject

Annex D

(informative)

Data management system

D.1 Introduction

This annex describes a coherent approach to understand the challenges imposed by the data project requirements specified in 4.2 on the derived technical requirements for a data management system (DMS). Emerging regulations such as EU's GDPR has shifted the emphasis put on the responsibility of the DMS regardless of whether it is implemented and managed by the employer or by a managed service provider contracted by the employer. From a governance point of view, Figure D.1 frames the problem addressed in this annex. The implementation package describes four capabilities that need to be addressed by the DMS: data subject control, privacy-by-design, privacy risk analysis, and verifiable accountability and transparency.

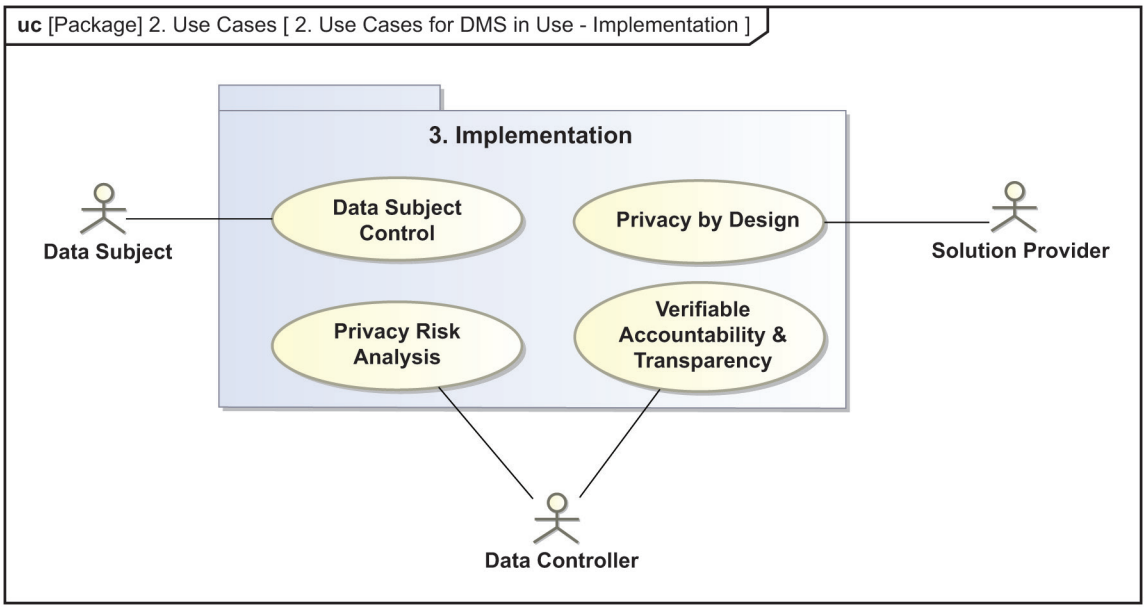

Figure D.1—Data management system use case

Privacy-by-design (PbD) is first addressed by the solution provider who is responsible for the SoI to be implemented. The SoI is developed by the solution provider[25] to leverage market share and it may be tailored to provide options in response to a procurement specification issued by the employer organization. Privacy risk analysis and managing the verification of accountability and transparency are the responsibility of the employer's data controller.[26] No matter how it is implemented, configured, and managed, the data subject always maintains positive control over how their sensitive PII is collected, processed, stored, used, and destroyed.

[25]Solution provider is a role assigned to an organization internal to the employer's enterprise or under contract to the employer's enterprise.
[26]Data controller is a role assigned to a person or to an organization.

D.2 Technical challenges

D.2.1 Data protection impact assessment

As noted in Leichter and Berman [B18], data protection impact assessment (DPIA) is required by multiple local norms, laws, and regulations to assess privacy issues that might arise when the employer deploys new products and services that involve the processing of a data subject's personal data.[27] Findings that result from the employer's DPIA will guide the selection of the DMS solution offered by vendors.

DPIA addresses the commonalities between privacy and risk assessment. However, from a legal point-of-view (privacy harm) the DPIA focuses attention on the protection of people as individuals, in groups, and society rather than the resources or organizations. The lack of metrics to effectively manage the data controller configuration and to generate timely reports and alarms is a topic addressed in this annex.

D.2.2 Privacy by design

Requirements for PbD are included in user employer's procurement specifications so that solutions offered provide the needed protection capabilities. Kramer suggested that a formal framework based on epistemic logic can be used to express data minimization requirements as properties defining for each stakeholder the information that the stakeholder is allowed to know (Andrés, Bordenabe, Chatzikokolakis, and Palamidessi [B2]).

A major technical challenge is the need to anonymize the data controller's database. It should be noted that no commercial anonymization algorithm has proven 100% effective. Therefore, this annex simply identifies the subject of an appropriate trade-off study.

In this annex a formal framework is offered for a given logical architecture that meets the expected privacy and integrity requirements. For example, systems that embed a radio-frequency identification (RFID) token, like electronic passports,[28] includes the capability to prohibit linking the personal data to an unauthorized application or interface. Another example is fingerprinting which is a direct threat to linking personal data to an application or interface.

D.2.3 Accountability and transparency

This standard focuses on the need of an employer to establish and verify the use of well-formed PP&ODs for the accountability and transparency framework. As noted in the data project requirements (see 4.2) enforcement needs real evidence in the form of auditable data to translate PP&OD governance into practical measures of effectiveness throughout the PII lifecycle.[29] One approach is to establish a data governance council consisting of representatives of employees and management. There are probably other approaches that are equally effective. Continuing with the idea for a data governance council, the council holds all levels of management accountable and auditable in relation to PII transparency, inclusion, fairness, use, storage, offboarding, etc. All processes performed by the data controller are the subject of the council's audit.

[27]Commercial tools are available to assist DPIA processing; e.g., https://www.cnil.fr/fr/pia-privacy-impact-assessment.
[28]A case in point is when a person checks into a hotel, the receptionist requests their passport, and scans the information into the hotel's database.
[29]Lifecycle includes the data controller's responsibility for collection, processing, storage, dissemination, and destruction of PII.

The technical challenge is to align accountability requirements imposed on the data controller with an authorized data user's expectation. Organizational directives assign responsibility and accountability for enforcement of this alignment. Basically, this approach relies on empowerment through data user control As noted by Kremer, Mé, Rémy, and Roca [B17], study of control as used by lawyers and computer scientists has led to identify three dimensions corresponding to the capacities for a person, as follows:

— To perform action on the data subject's personal data

— To prevent others from performing actions on the data subject's personal data

— To be informed of actions performed by others on the data subject's personal data

Two main conditions make it possible for data subjects to exercise control over their personal data:

— The data subject is properly informed about the collection of their data, its purpose, the entity collecting the data, and the period of retention.

— The data subject is able to express their choice to have their data collected or not for a given purpose and be assured that choice is followed.[30]

D.3 Special topics of interest

Geolocation is a type of PII that is commonly shared with either tacit or informed consent by the data subject. For example, work crew location information is commonly collected when the crew is dispatched to perform an authorized work order. Collection, processing, and regaining geolocation of a data subject over time can be used inappropriately (Zagelmeyer, Bianchi, and Shemberg [B25]). Protecting the data subject's geolocation data is the responsibility of the data controller.

D.4 Governance responsibility for the data controller

Administrative control over all data controller functions are addressed in employer's specification for the data management system (DMS). Table D.1 specifies the governance requirements (GR); where "F" designates a functional requirement, and "I" designates and interface requirement.

Table D.1—Data controller governance

GR-1: Governance	
GR-1.1: Collection	Subject to the employer's approved PP&OD restrictions and the data subject's informed consent, it is imperative that the data controller be able to securely collect and verify the subject's sensitive personal data.
GR-1.2: Processing	Subject to the employer's approved PP&OD restrictions and the data subject's informed consent, it is imperative that the data controller be able to securely process and verify the use of the data subject's sensitive personal data.
GR-1.3: Storage	Subject to the employer's approved PP&OD restrictions and the data subject's informed consent, it is imperative that the data controller be able to securely store and verify the location and duration settings for storing the data subject's sensitive personal data.
GR-1.4: Dissemination	Subject to the employer's approved PP&OD restrictions and the data subject's informed consent, it is imperative that the data controller be able to securely disseminate and verify the use of approved interfaces transmitting the data subject's sensitive personal data.
GR-1.5: Disposal	Subject to the employer's approved PP&OD restrictions and the data subject's informed consent, it is imperative that the data controller be able to securely destroy and verify the destruction of the data subject's sensitive personal data.

[30]In many work situations the right to object is difficult because objection may be negatively viewed and not a team player.

During the time the data controller has operational control of the data subject's personal data, it is the data controller responsibility to check for restrictions and consent at each stage in the lifecycle of the PII. Operation control over these data begins with the receipt of data at specified interfaces and ends with the delivery of the data to a specified interface for dissemination or disposal. At each stage of the lifecycle the data controller has the capability to securely handle the data. Furthermore, data controller status reports[31] include verification that a specific action has been successfully completed.

D.5 Data management system context

D.5.1 Data management SiU

Figure D.2 describes the six major subsystems of the data management SiU. These control units are directly aligned with the governance requirements in Table D.1. Positive control over each control unit activity is provided by an instance of an authorized data controller logged on to an authorized workstation. As will be discussed later, if confidentiality and integrity are required,[32] there are multiple implementations of a cryptographic platform; i.e., cardinality [0..*]. There is at least one instance of each control unit; i.e., cardinality [1..*].

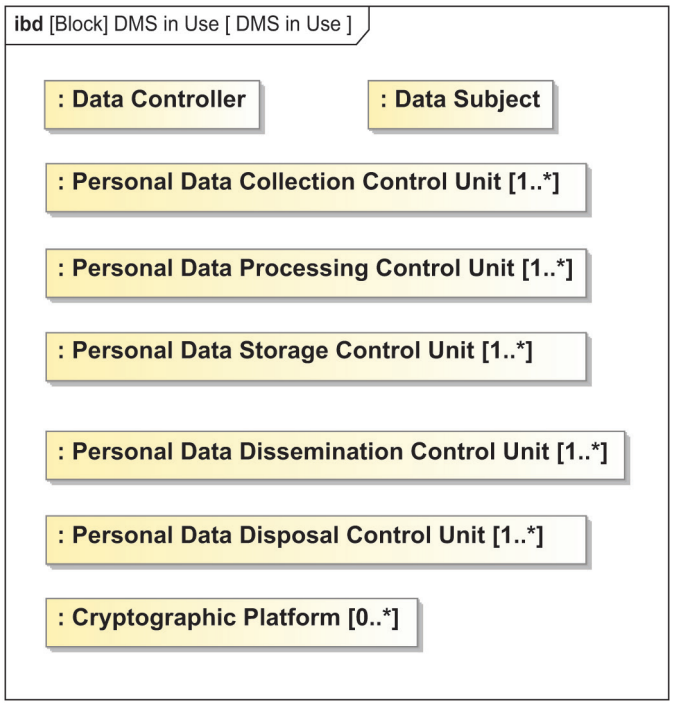

Figure D.2—Data management SiU

Data controller and data subject are roles assigned to a person with the requisite skills. Examples of various roles are discussed in the context of the control unit in use.

Following are the use case and activity diagrams for each control unit. A rake icon is shown in each diagram to indicate a detailed process to perform the task.

[31]Status reports are output to a specified interface.
[32]Multiple local laws and regulations require strong confidentiality and integrity to protect PII. This is particularly true for government agencies.

D.5.2 Personal data collection control unit

Figure D.3 describes the use case to securely collect and verify the source of the data subject's sensitive personal data collected. Initially, the data controller selects and configures the personal data collection control unit to identify the approved collection interfaces and communication protocol used for that interface. Figure D.3 exposes the possible existence of multiple instances of DMS in use and multiple instances of data collection control units used. It's also possible that the data collection control unit be an orphan and cannot be associated with any DMS in use, or there may be more than one for the data controller to select; i.e., cardinality 0..*. However, the DMS in use knows of at least one data collection unit, but more than one is also a possibility for the data controller to select; i.e., cardinality 1..*.

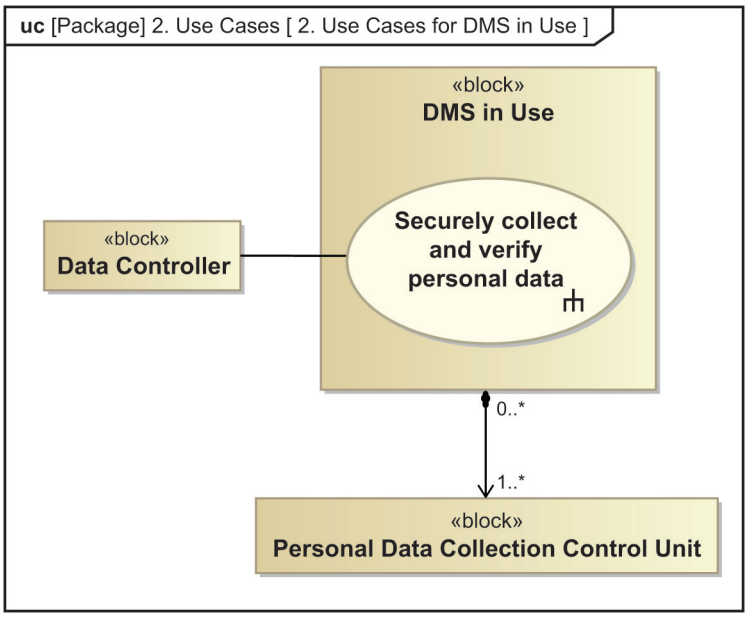

Figure D.3—Use case to securely collect and verify personal data

To help ensure data integrity, data entering each approved interface is verified by an approved source. If confidentiality is required, the data will probably be encrypted. However, the data collection control unit is not responsible for decryption, that is the responsibility of the processing control unit described in D.5.3. Lastly, the data controller sets the thresholds that are triggered when integrity is violated. If an alarm is triggered, the event and supporting data is output from the personal data control unit to a specified interface.

Figure D.4 describes the interaction between the data controller and the personal data collection unit. Several important features are exposed in this diagram, and all actions shown are logged in the system historian for future audits.

a) Throughout the collection process the data controller maintains positive control over all activity. One instance of the data controller is someone responsible for selection and configuration settings, and another instance is possibly an on-shift operator. This is simply the difference in role assignment.

b) The state of readiness is determined by the personal data collection unit. If it is not ready, guard [not OK], the process is stopped and reported to a specified interface including the information about the data controller and workstation used to select and configure the system.

c) If the system is ready to configure, guard [OK], the data controller initiates a select-before-operate (SBO) procedure. The set point is selected and confirmed by the personal data collection unit. The data controller then sets the value of the set point, which is confirmed by the personal data collection unit. Data collection is now ready to receive data on selected ports.

d) The clear text header in each data packet received is checked by the personal data collection unit to verify that the data is received from a legitimate source. If so, guard [OK], it continues to receive data packets. If not, guard [not OK], the personal data collection unit stops the collection and reports the event to a specified interface.

e) Throughout the data collection activity, a data controller monitors the progress. At any time, a data controller issues a controlled stop message to the personal data collection unit.

f) Another setting that is not shown is the time-out setting to control the duration of data collection.

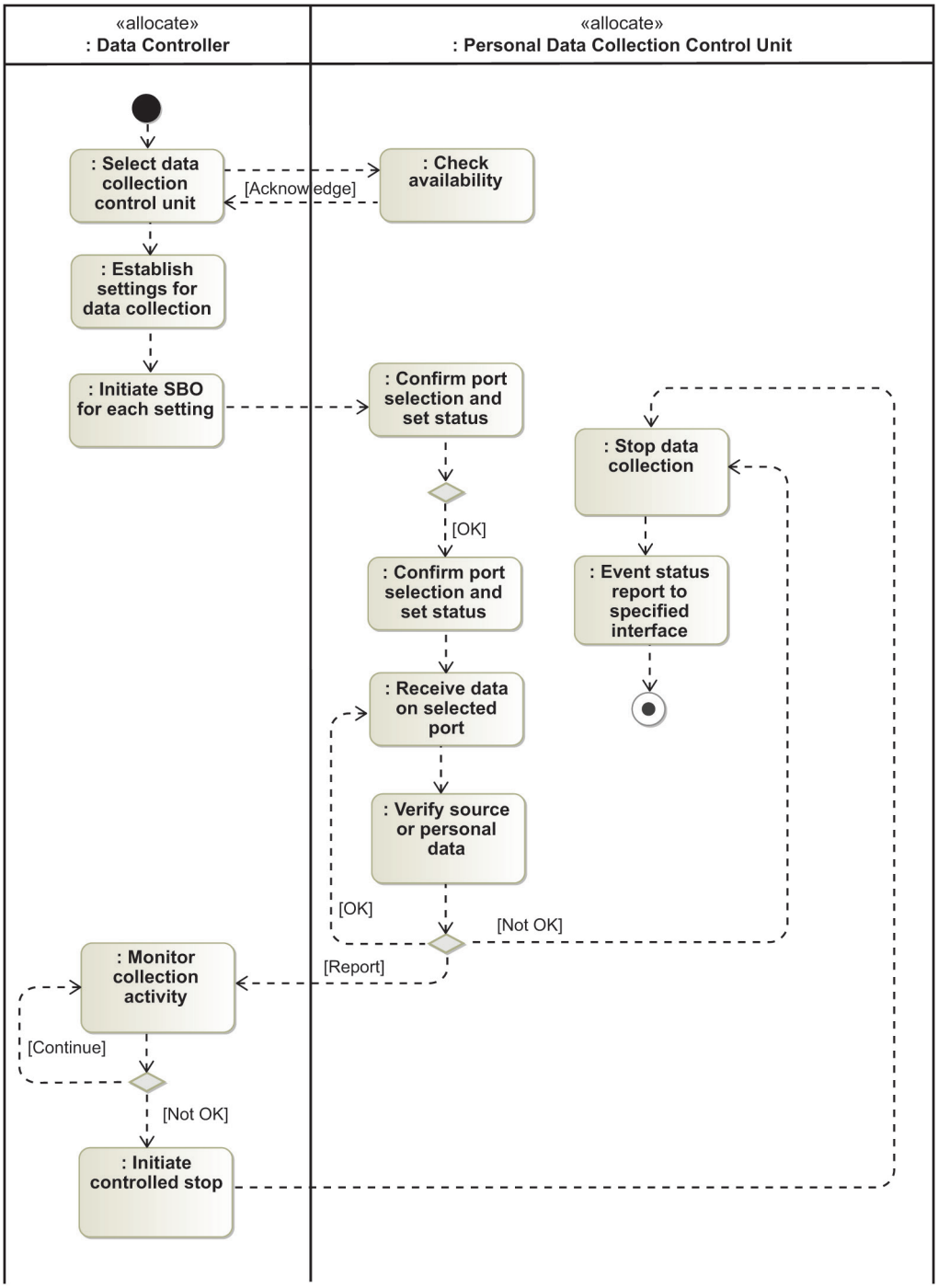

Figure D.4—Personal data collection control unit activity

D.5.3 Personal data processing control unit

Figure D.5 describes the use case to securely process and verify intended use of personal data. Initially the data controller configures the personal data process control unit with the algorithms approved for each combination of data subjects and intended use. Again, the data controller sets the alarm thresholds.

If confidentiality is required, the data is probably encrypted, and a cryptographic platform is needed to perform encryption/decryption and to manage the exchange of cryptographic keys or key fragments.[33] The cryptographic platform encrypts the data output from the data processing control unit to protect the data—both at rest (D.5.4) or in transit (D.5.5).

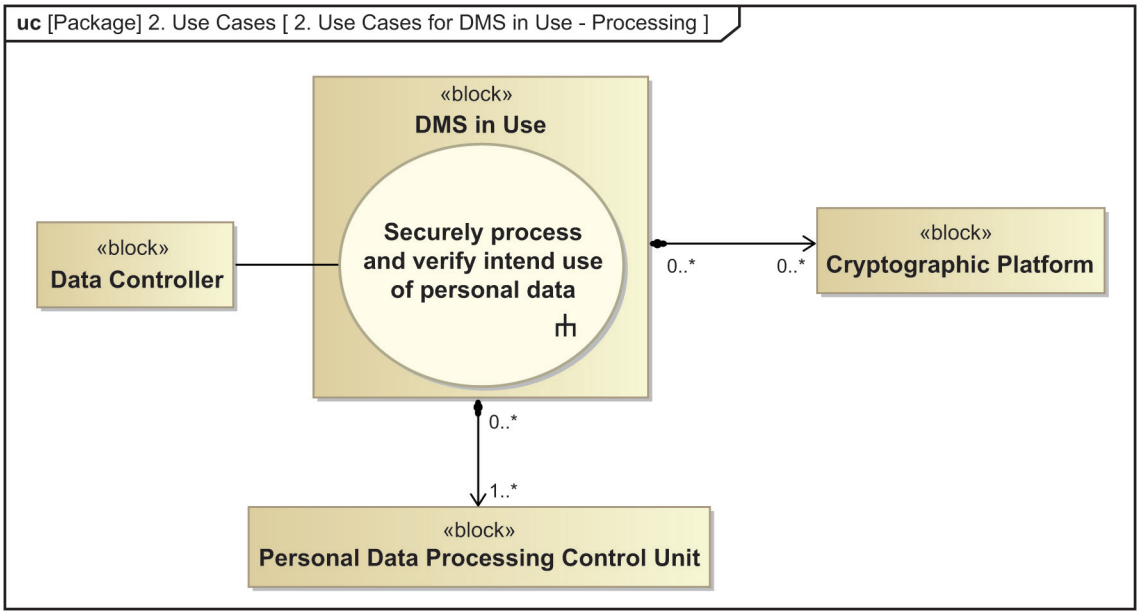

Figure D.5—Use case to securely process and verify intended use of personal data

Figure D.5 exposes the possible existence of multiple instances of DMS in use and multiple instances of data processing control units and cryptographic platforms that are possible. It's also possible that the data processing control unit or cryptographic platform are an orphan and cannot be associated with any DMS in use, or it is also possible that more than one data controller is available to be selected; i.e., cardinality 0..*. However, the DMS in use knows of at least one data processing control unit, but there is possibly more than one data controller available to be selected; i.e., cardinality 1..*. If the data is not encrypted, the DMS in use does not associate with any cryptographic platform; i.e., cardinality is 0.

Figure D.6 describes the interaction between the data controller and the personal data processing control unit, including the cryptographic platform.

[33] Encryption/decryption processes and key management are not addressed in the standard.

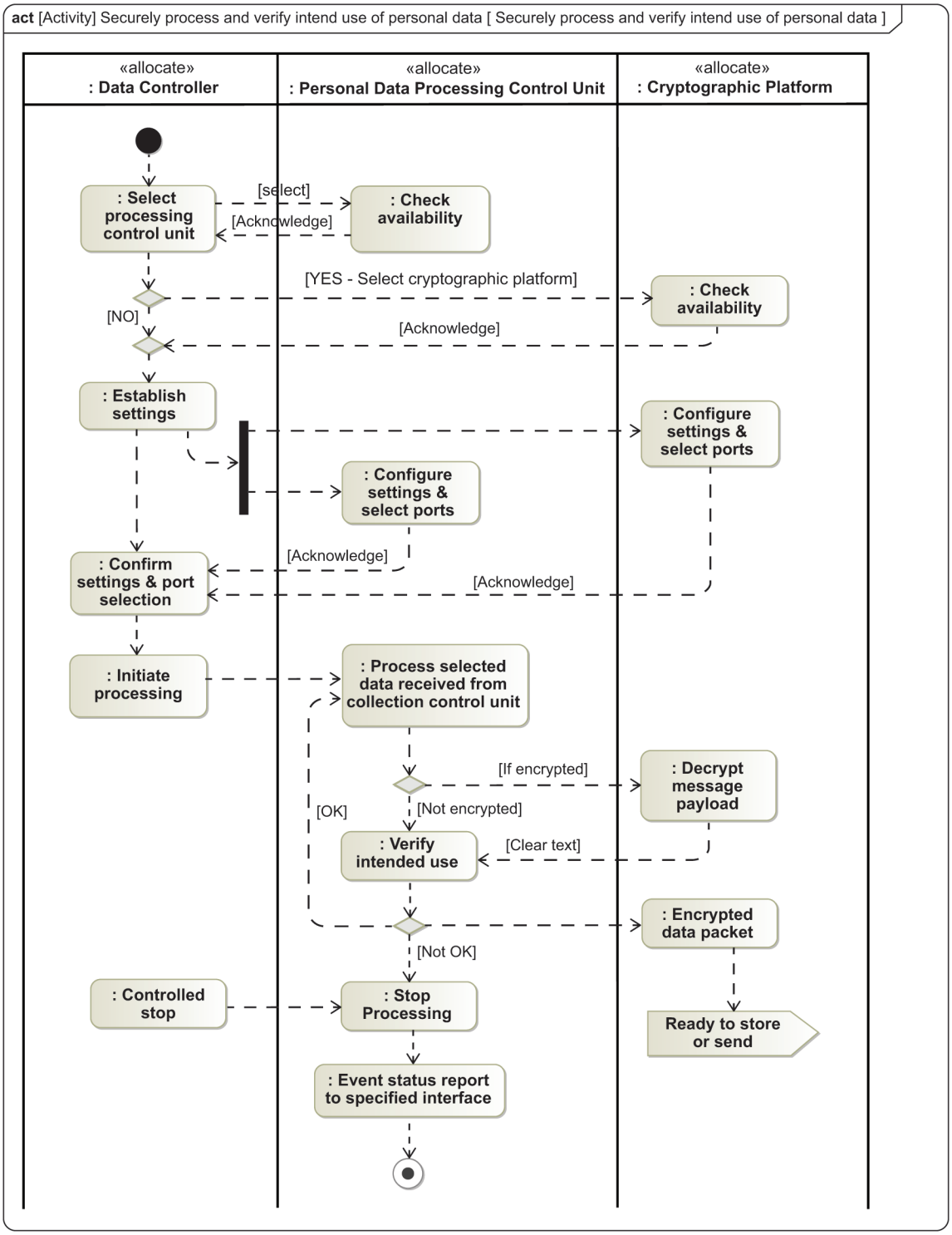

Figure D.6—Personal data processing control unit activity

Several important features are exposed in this diagram and all action are logged in the system historian for future audits.

a) Positive control and the state of readiness are similar to the activities shown in Figure D.4.

b) As in Figure D.4, SBO is the recommended procedure to select and approve interface ports. This is shown by the select and acknowledge guards.

c) Once the DMS is ready to process it receives a message containing the data from the collection control unit.

d) If confidentiality is required, the message payload is decrypted to provide clear text to validate intended use.

e) Once the system is ready to process, it proceeds to verify intended use based on the appropriate settings.

f) If confidentiality is required, processed personal data is re-encrypted and made ready to transmit or store.

g) Throughout the process, the data controller monitors all activity. At any time, the data controller has the capability to issue a controlled stop message to the personal data processing control unit.

h) All event status reports are output to a specified interface for future audit.

D.5.4 Personal data storage control unit

Figure D.7 describes the use case to securely store personal data and verify the approved location and duration of storage. Initially the data controller selects and verifies the availability of personal data storage control units and communication ports that have been approved. The data controller configures the settings and ports for the storage control unit selected. Several important features are exposed in this diagram and all action are logged in the system historian for future audits.

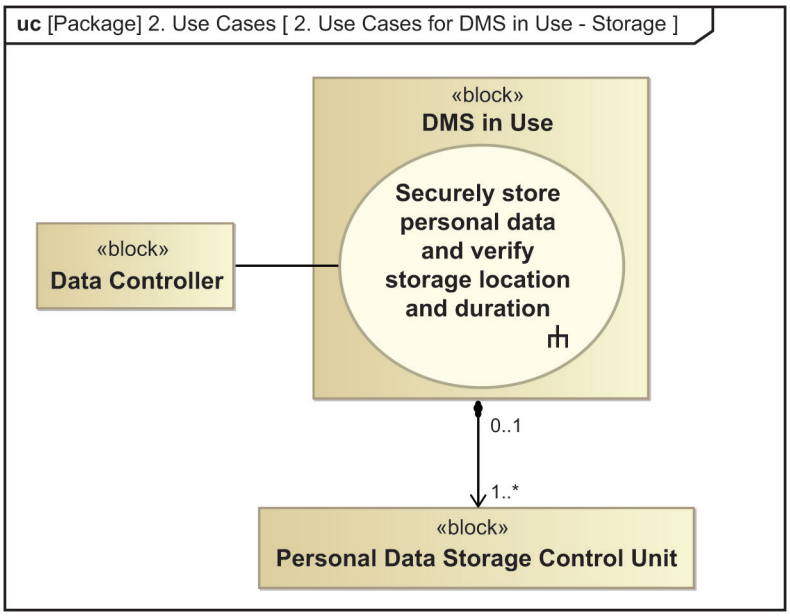

Figure D.7—Use case to securely store personal data and verify location and duration

Figure D.8 describes the use case to securely store personal data and verify the approved location and duration of storage. Initially the data controller selects and verifies the availability of personal data storage control units and communication ports that have been approved. The data controller configures the settings and ports for the storage control unit selected.

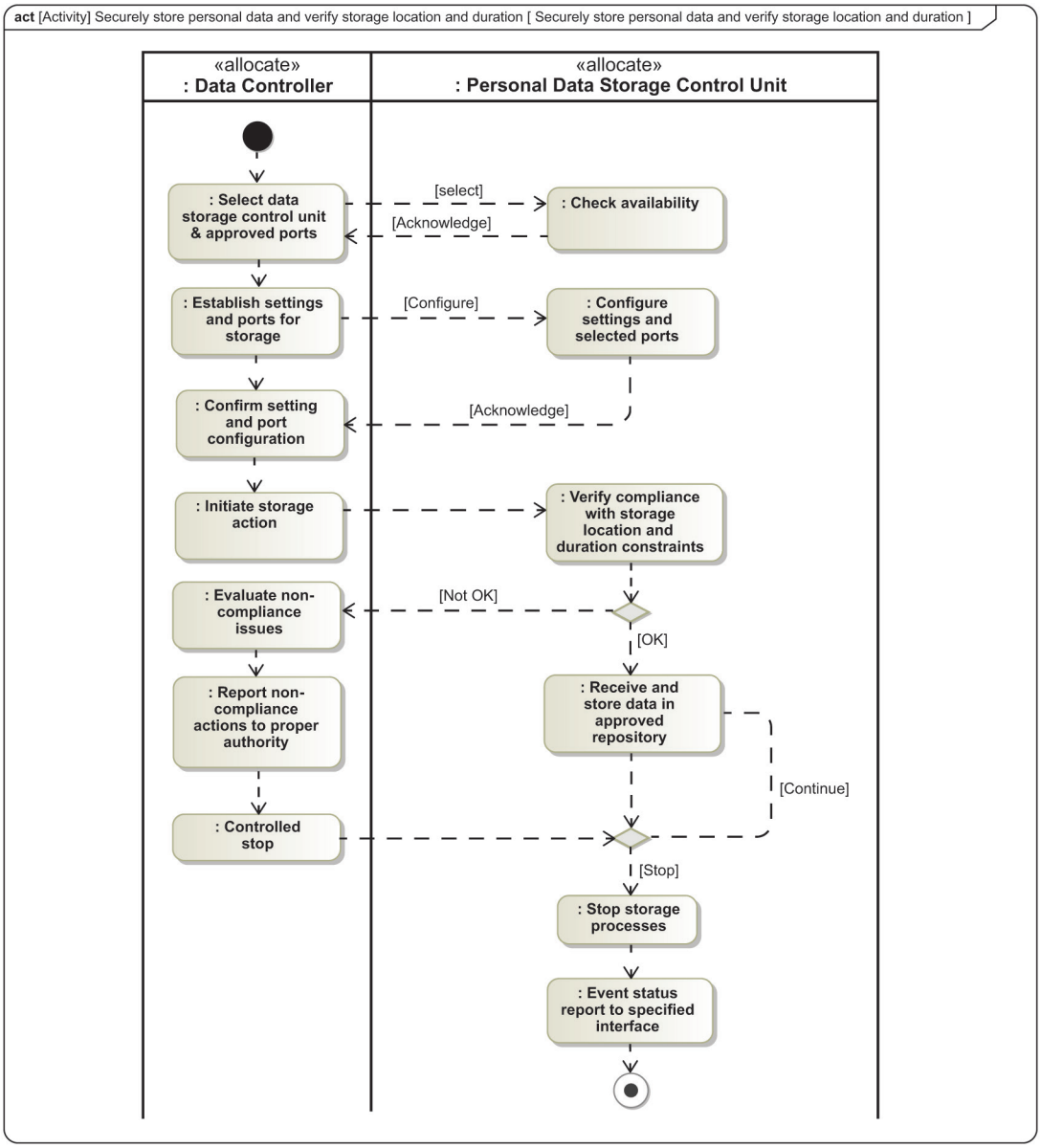

Figure D.8—Personal data storage control unit activity

Several important features are exposed in this diagram and all action are logged in the system historian for future audits.

a) Positive control and the state of readiness are similar to the activities shown in Figure D.2.

b) As in Figure D.2, SBO is the procedure to select and approve interface ports. This is shown by the select and acknowledge guards.

c) Once the system is ready to process, it proceeds to verify compliance with the approved location and duration constraints based on the appropriate settings.

d) If approved, the DMS is ready to process to receives a message containing the data from the processing control unit and store the data in the approved repository.

e) Throughout the process, the data controller monitors all activity. At any time, the data controller has the capability to issue a controlled stop message to the personal data storage control unit.

f) All event status reports are output to a specified interface for future audit.

g) Although not shown, if the data is stored in an encrypted format, retrieval for audit will require the approved keying material to decrypt the data. Cryptographic processes and key management are not addressed in this standard.

D.5.5 Personal data dissemination control unit

Figure D.9 describes the use case to securely disseminate personal data and verify the approved interface. Initially the data controller configures the personal data dissemination control unit with settings to aligned approved interfaces with applicable PP&ODs and constraints imposed by the data subjects informed consent agreement. Again, the data controller sets the alarm thresholds.

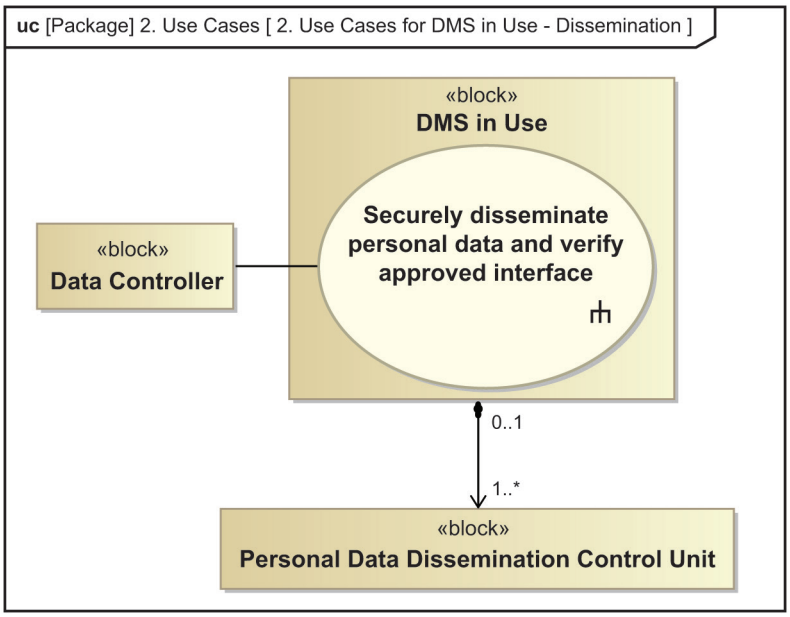

Figure D.9—Use case to securely disseminate personal data and verify approved interface

Figure D.10 describes the use case to securely fetch and transmit personal data and via approved interfaces. Initially the data controller selects and verifies the availability of applicable dissemination control units and communication ports that have been approved. The data controller configures the settings and selected ports for the dissemination control unit selected.

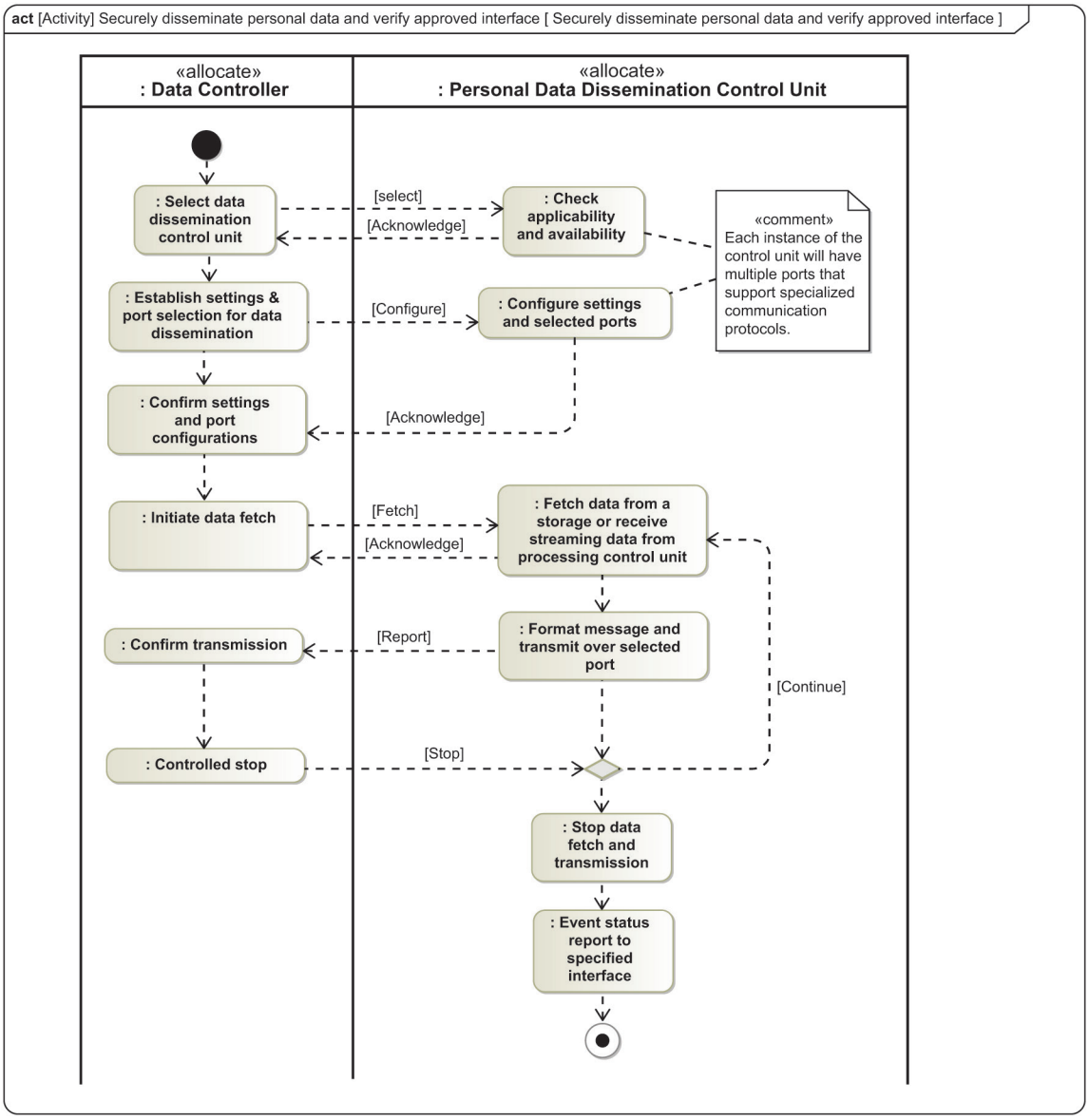

Figure D.10—Personal data dissemination control unit activity

Several important features are exposed in this diagram and all action are logged in the system historian for future audits.

a) Positive control and the state of readiness are similar to the activities shown in Figure D.2.

b) As in Figure D.2, SBO is the procedure to select and approve interface ports. This is shown by the select and acknowledge guards.

c) Once the system is ready to fetch and transmit, it proceeds to verify compliance with the approved interface constraints based on the appropriate settings.

d) If approved, the DMS is ready to fetch data from an approved data repository or receive streaming data from an approved processing control unit.

e) For transmission via an approved interface, the dissemination control unit formats the data into a message that conforms to the protocol for the selected port.

f) Throughout the process, the data controller monitors all activity. At any time, the data controller has the capability to issue a controlled stop message to the personal data storage control unit.

g) All event status reports are output to a specified interface for future audit.

D.5.6 Personal data disposal control unit

Figure D.11 describes the use case to securely destroy and verify destruction of personal data. Initially the data controller[34] configures the personal data disposal control unit with settings to align approved disposal algorithms and processes with applicable PP&ODs and constraints imposed by the data subjects informed consent agreement. Again, the data controller sets the alarm thresholds.

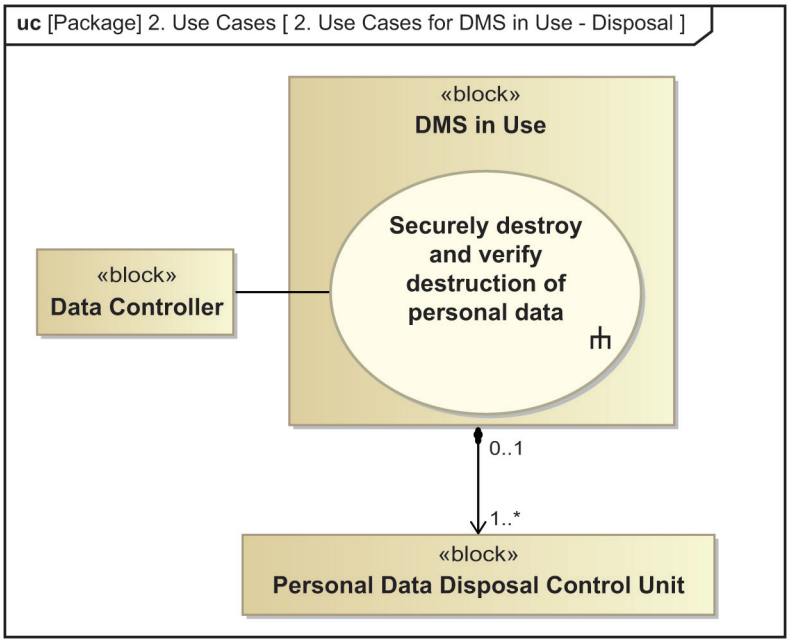

Figure D.11—Use case to securely destroy and verify destruction of personal data

Figure D.12 describes the activity to securely destroy and verify destruction of personal data. The important entities in this process are the data controller (authorized controller for disposal of personal data), data subject, and selected data disposal control unit. The data controller configures the settings and selected ports for the selected data disposal control unit. Several important features are exposed in this diagram and all action are logged in the system historian for future audits.

a) The process begins by notifying the data subject that specific pieces of personal data are to be securely destroyed. The process will only begin when the data subject responds with a positive acknowledgment.

b) After initializing the data disposal unit, including its repository containing the data files to be destroyed, the command is issued to execute the disposal procedure. To help ensure positive control, explicit commands are issued to erase personal data files and to test for remnants.

c) Techniques used to perform secure destruction of data files and testing for remnants are not addressed in this standard.

[34] An authorized disposal controller is a role assigned to an individual with the requisite skills to manage the destruction of sensitive data.

d) If remnants are found, the action is repeated until the destruction is complete.

e) All actions are reported to the data controller.

f) When completed the data controller notifies the data subject that secure destruction of personal data has been successfully completed.

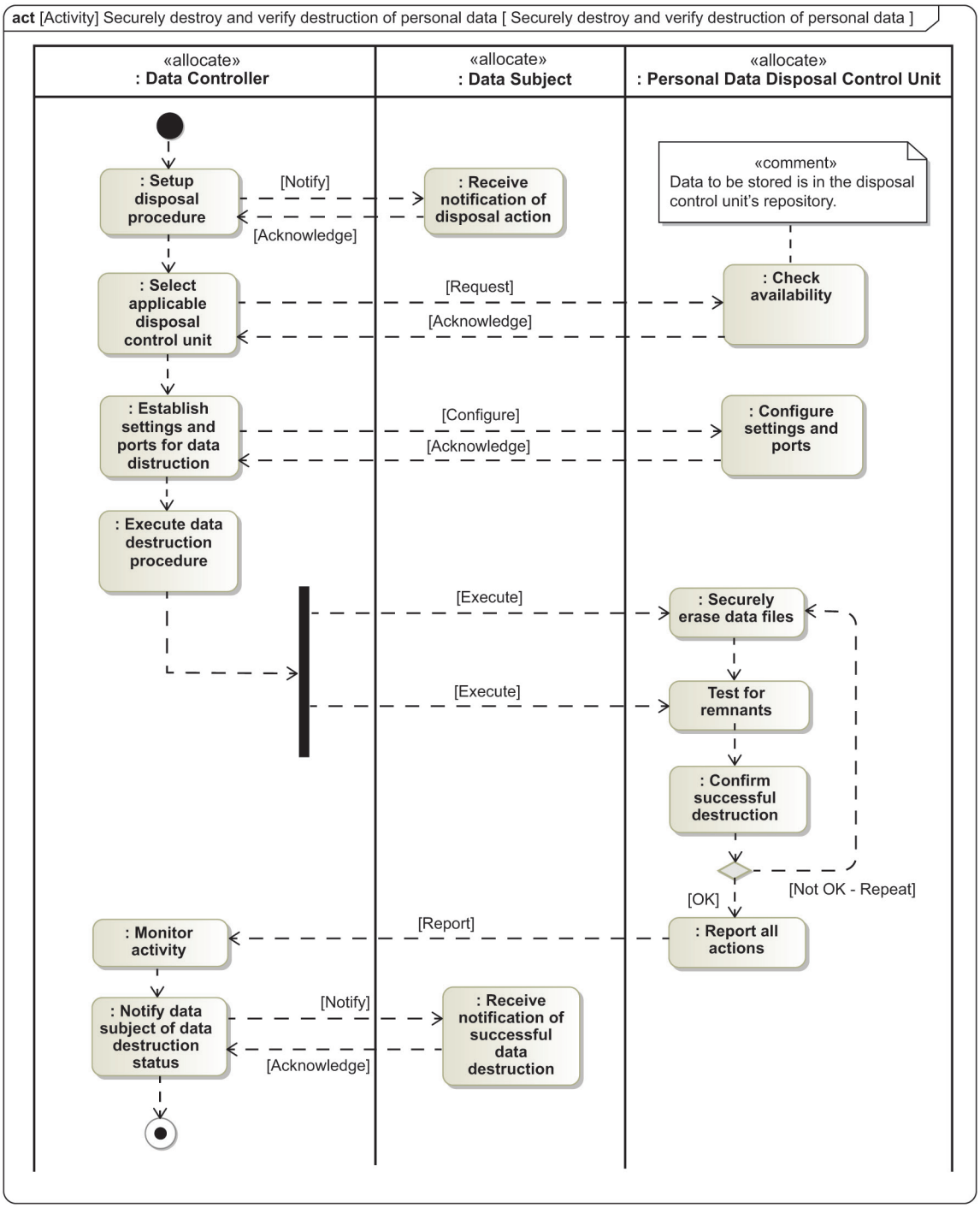

Figure D.12—Personal data disposal unit activity

Annex E

(informative)

Grievance redress mechanisms available to the data subject

E.1 Stakeholder needs for effective grievance redress mechanisms

Table E.1 shows a high-level view of the stakeholder needs for effective grievance redress mechanisms. The four requirements that are the focus of this annex are as follows:

a) Grievance redress policies procedures and organizational directives

b) Eligibility to file a grievance

c) Disposition of a proper grievance

d) Enforcement of the remedy arrangement resulting from the outcome of the grievance review

Table E.1—Stakeholder needs for effective grievance redress mechanisms

1: Grievance redress PP&OD	The employer needs to establish and enforce grievance redress options available to the data subject as they relate to the exposure of personal identifiable information. Union membership, membership in any collective bargaining unit, is not a prerequisite for a data subject, which includes employees and non-employees.
1.1: State-based judicial grievance mechanism	Commensurate with state-based judicial grievance mechanisms, the employer needs to establish and enforce grievance redress options available to the data subject as they relate to the exposure of personal identifiable information.
1.2: State-based non-judicial grievance mechanisms	Commensurate with state-based grievance mechanisms that do not provide for judicial action, the employer needs to establish and enforce grievance redress options available to the data subject as they relate to the exposure of personal identifiable information.
1.3: Non-state based non-judicial grievance mechanism	Given the situation when no state-based grievance mechanism (NSBGM) is available, the employer needs to establish and enforce grievance options available to the data subject as they relate to the exposure of personal identifiable information.
2: Eligibility to file a grievance	The employer needs to establish the rules for who can file a grievance, the supporting data to support the grievance, and the authority responsible for receiving the grievance.
3: Disposition of a proper grievance	The employer needs to establish and enforce the disposition of a proper grievance in a timely and transparent manner. Disposition stages include all rulings for or against the plaintiff, appeal of a ruling, and final decision.
4. Enforcement of remedy arrangement	Given the disposition of a proper grievance, the employer needs to establish and enforce the remedy arrangement decided in the outcome of the grievance review.

Commonly, grievance redress is addressed by examining the external requirements imposed by state-based norms, laws, and regulation (Table E.1 item 1.1 and item 1.2). However, the third extended requirement (Table E.1 item 1.3) is the focus of this annex.

E.2 Focus on non-state-based mechanisms

Non-state-based mechanisms (NSBGM) provide the means by which data subjects or their legitimate representatives, can seek remedy with respect to the adverse impact of exposing their sensitive personal identifiable information. This annex builds on Zagelmeyer, Bianchi, and Shemberg paper that scopes the issue of accountability and remedy, as related to NSBGM[35] (*Guiding Principles on Business and Human Rights* Framework [B5]).

a) The distinguishing characteristic of the NSBGM with respect to other mechanisms is, that the state is neither involved in establishing or setting the framework for nor is actively intervening into the operations of the grievance mechanisms (as in the example of statutory arbitration and conciliation services), nor is the grievance mechanism in any way directly linked to the legal and judicial system of a particular country (as for example general domestic courts).

b) NSBGM, as elements of private governance seem to be far less well documented, and civil society pressure for additional transparency from companies does not seem to have created an increase in disclosure related to NSBGM.

c) As companies possibly benefit from NSBGM through flexibility with respect to grievance management, by avoiding the escalation of conflicts over human rights issues, and by avoiding public shaming, they should be interested in learning about good practices.

d) There is a myriad of grievance mechanisms and a high degree of institutional diversity within and across the suggested groups of NSBGM.

e) All of the grievance mechanisms have in common that they affect the business and human rights sphere, but many of the mechanisms may not necessarily have been established specifically and exclusively to cover business and human rights related grievances.

f) The intention is to set up specific types of mechanisms may vary, as may the role and function from the perspectives of the actors. This also includes the potential of role conflicts.

g) NSBGM at company and corporate levels, in the literature frequently labeled operational level grievance mechanisms (OLGMs), exist in various shapes and sizes.[36]

h) Understanding the effectiveness of OLGMs also means looking to company and corporate level grievance mechanisms. For example, an OLGM within a global value chain is possibly linked to a mechanism of the brand at the top of the chain that helps to ensure the effectiveness of the OLGM, for example, in terms of ensuring timely resolution and communication with affected individuals. For this reason, the assurance role is probably factored into judgements of effectiveness.

Figure E.1 describes the use case for the grievance system in use (GSiU) that is used to derive the requirements specified in 5.6. Each stage of the use case identifies the objective, and the primary players that must interact to satisfy the objective.

Stage 1: Either the data subject or the data subject representative files a properly formed grievance.

Stage 2: Under the supervision of the grievance enforcement authority, a grievance panel is empowered to judge the merits of the grievance, and render a finding based on the facts of the grievance.

Stage 3: Either the data subject or the data subject representative is informed of the remedy arrangement, which is enforced by the grievance enforcement authority.

In the objective of each stage is a rake icon used to indicate that a complex activity is executed to perform the task. This standard is silent on how the task is executed (noted as a local matter).

[35]NSBGM processes are continuously reviewed to identify improvements to satisfy the effectiveness criteria set out the UN Guiding Principles on Business and Human Rights on access to remedy; see guiding principle 31.
[36]The diversity of the phenomenon is matched by a similar diversity of available information in terms of sources of information, research methods, presentation style, and purpose/function of the information.

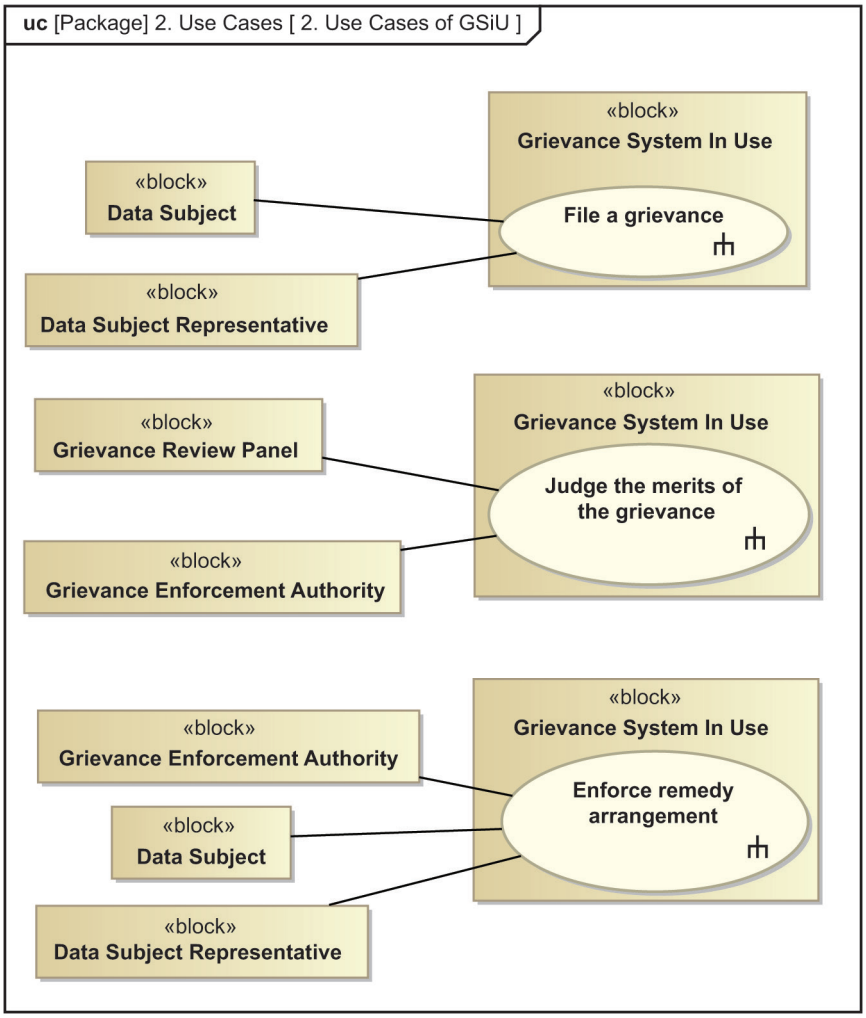

Figure E.1—Use case for GSiU

E.3 Eligibility to file a grievance

This standard assumes that either the data subject, or a body of employee representation, or a third-party retained by the data subject who would be eligible to file a grievance. In accordance with the PP&OD requirements specified in this standard, there are three levels of accessibility toward multi-actor mechanisms:

a) Only data subjects from a specific site are eligible to file grievances.

b) Members or participants to a particular initiative are eligible to lodge grievance against another member/participant.

c) Any person or organization, including third parties, are eligible to file grievance. However, the grievance refers to a specific breach of standards included in codes or principles of reference.

In all situations, the employer's PP&OD provide the guidance so that all parties are to be treated fairly and the process to file a grievance is performed in a timely manner. For this reason, an administrative oversight function is needed to review the grievance filing process and initiate the appropriate action if there is a lack of fairness or unacceptable delays. How this oversight function is implemented is a local matter.

E.4 Disposal of a proper grievance

In the employer's PP&OD, NSBGM disposition of a proper grievance has provisions for:

a) Assignment of grievance review by an internal or external panel of SMEs that are agreeable to all parties of the grievance (including the rules for selecting the panel of SMEs)

b) Framework of options and criteria for rendering judgement on the facts of the grievance

c) Authority to initiate enforcement action based on the finding of facts

d) A procedure for appeal of the judgement rendered by the panel of SMEs

E.5 Enforcement of remedy arrangement

In the employer's PP&OD, NSBGM enforcement of remedy arrangement has provisions for:

a) Imposing appropriate sanctions, including criminalizing conduct and pursuing prosecutions where abuses amount to local crimes

b) Providing a range of appropriate reparations, such as compensation, restitution, rehabilitation, and changes in PP&OD requirements, assignment of responsibility and accountability

E.6 Assessing the effectiveness of remedy outcomes

The UN's guiding principle 31 under their third pillar of access to remedy, address the question of what makes a NSBGM effective in practice. The *Guiding Principles on Business and Human Rights* Framework [B5] states:

a) *Legitimate:* enabling trust from the stakeholder groups for whose use they are intended and being accountable for the fair conduct of grievance processes.

b) *Accessible:* Being known to all stakeholder groups for whose use they are intended and providing adequate assistance for those who may face barriers to access.

c) *Predictable:* Providing a clear and known procedure with and indicative time frame for each stage, and clarity on the types of process and outcomes available and means of monitoring implementation.

d) *Equitable:* Seeking confidence that the aggrieved parties have reasonable access to sources of information, advice and expertise needed to engage in a grievance process on fair, informed and respectful terms.

e) *Transparent:* Keeping parties to grievance informed about its progress, and providing sufficient information about the mechanism's performance to build confidence in its effectiveness and meet any public interest at stake.

f) *Rights-compatible:* Ensuring that outcomes and remedies accord with internationally recognized human rights.

g) *A source of continuous learning:* Drawing on relevant measures to identify lessons for improving the mechanism and preventing future grievances and harms.

h) *Based on engagement and dialog:* Consulting the stakeholder groups for whose use they are intended on their design and performance and focusing on dialog as the means to address and resolve grievances.

Scheltema's commentary on this principle elucidates that grievance mechanism can only serve its purpose if the people it is intended to serve know about it, trust it and are able to use it (King and Raja [B16]).

Annex F

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] Aleksandraviciene, A. and A. Morkevicius, *MagicGrid Book of Knowledge*. Kaunas, Lithuania: Vitae Litera, UAB, 2018.

[B2] Andrés, M.E., N.E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-Indistinguishability: Differential Privacy for Location-Based Systems," February 2014.[37]

[B3] Committee_of_Ministers, "Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment."[38]

[B4] Earley, S., "The Role of a Customer Data Platform," IT Professional, vol. 20, no. 1, pp. 69–76, January/February 2018.[39]

[B5] "Guiding Principles on Business and Human Rights: Implementing the UN "Protect, Respect and Remedy" Framework," *Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises,* 2011.[40]

[B6] Hosseini, M., A. Shahri, K. Phalp, and R. Ali, "Four reference models for transparency requirements in information systems," Requirements Engineering, vol. 23, pp. 251–275, 2018.[41]

[B7] Intersoft_Consulting, *General Data Protection Regulation: Consent*.[42]

[B8] Intersoft_Consulting, *General Data Protection Regulation: Article 4: GDPR Definitions.*[43]

[B9] IEEE Std 7007™-2021, IEEE Ontologicial Standard for Ethically Driven Robotics and Automation Systems.

[B10] ISO/IEC 27001, Information Security Management.

[B11] ISO/IEC 33001:2015 Information technology—Process assessment—Concepts and terminology.[44]

[B12] ISO/IEC 33004:2015 Information technology—Process assessment—Requirements for process reference, process assessment and maturity models, p. 9.

[B13] ISO/IEC 38500, Information technology—Governance of IT for the organization.

[37]Available at: https://arxiv.org/abs/1212.1984
[38]Available at: https://www.apda.ad/sites/default/files/2018-10/cm-rec-2015-5-en.pdf
[39]Available at: 10.1109/MITP.2018.011301803
[40]Available at: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf
[41]Available at https://link.springer.com/content/pdf/10.1007/s00766-017-0265-y.pdf.
[42]Available at: https://gdpr-info.eu/issues/consent/
[43]Available at: https://gdpr-info.eu/art-4-gdpr/
[44]ISO/IEC publications are available from the ISO Central Secretariat (https://www.iso.org/). ISO/IEC publications are available in the United States from the American National Standards Institute (https://www.ansi.org/).

[B14] ISO/IEC 38505-1, Information technology—Governance of IT—Part 1: Application of ISO/IEC 38500 to the governance of data.

[B15] ISO/IEC FDIS 38503, Information technology—Governance of IT—Assessment of governance IT.

[B16] King, N. J. and V. T. Raja, "Protecting the privacy and security of sensitive customer data in the cloud," Computer Law & Security Review, vol. 28, no. 3, pp. 308–319, June 2012.[45]

[B17] Kremer, S., L. Mé, D. Rémy, and V. Roca, "Cybersecurity: Current challenges and Inria's research directions," 2019.

[B18] Leichter, W. and D. Berman, Global Guide to Data Protection Laws: Understanding Privacy & Compliance Requirements in More than 80 Countries. CreateSpace Independent Publishing Platform, 2017.

[B19] McCallister, E., T. Grance, T. and K.A. Scarfone, SP 800-122. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).[46]

[B20] OMG Systems Modeling Language (OMG SysML™) Specification.[47]

[B21] Raul, A. C., T. D. Manoranjan, and V. Mohan, "United States," Privacy, Data Protection and Cybersecurity Law Review, November, pp. 268–294, 2014.

[B22] Scheltema, M., Assessing the effectiveness of remedy outcomes of non-judicial grievance mechanisms. Dovenschmidt Quarterly, 2014, pp. 190–197.[48]

[B23] Steiner, R. S., "Data modeling is a form of data governance [Whitepaper].[49]

[B24] Zachman, J. A., "A framework for information systems architecture," IBM Systems Journal, vol. 26, no. 3, pp. 276–292, 1987.[50]

[B25] Zagelmeyer, S., L. Bianchi, and A.R. Shemberg, "Non-state based non-judicial grievance mechanisms (NSBGM): An exploratory analysis," July 2019.[51]

[45]Available at: http://dx.doi.org/10.1016/j.clsr.2012.03.003.
[46]Available at: https://csrc.nist.gov/publications/detail/sp/800-122/final
[47]Available at: https://sysml.org/.res/docs/specs/OMGSysML-v1.4-15-06-03.pdf
[48]Available at https://core.ac.uk/reader/19915800
[49]Available at: https://www.idera.com/resourcecentral/whitepapers/data-modeling-form-of-data-governance/
[50]Available at: 10.1147/sj.263.0276
[51]Available at: https://www.ohchr.org/Documents/Issues/Business/ARP/ManchesterStudy.pdf

IEEE SA
STANDARDS ASSOCIATION

RAISING THE WORLD'S STANDARDS

Connect with us on:

Twitter: twitter.com/ieeesa
Facebook: facebook.com/ieeesa
LinkedIn: linkedin.com/groups/1791118
Beyond Standards blog: beyondstandards.ieee.org
YouTube: youtube.com/ieeesa

standards.ieee.org
Phone: +1 732 981 0060

IEEE