

IEEE Standard for Transparent Employer Data Governance

IEEE Computer Society

Developed by the
Software & Systems Engineering Standards Committee

IEEE Std 7005™-2021

STANDARDS

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

Copyright © 2021 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 19 November 2021. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

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

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

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
Diego Chiozzi
Christina Colclough
Vicky Hailey

Dennis Holstein
Daniel Huegli
Zvikomborero Murahwi
Matthew Newman

Bryan Reese
Jesus Salgado
Matthew Silveira
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
Johann Amsenga
Ulf Bengtsson
Juris Borzovs
Pieter Botman
Diego Chiozzi
C. Clifton
Ronald Dean
Luis Andrey Fajardo
Rodolfo Fiorini
David Fuschi
Paulo Goncalves
Didem Gurdur Broo
Tamas Haidegger

Mark Henley
Werner Hoelzl
Dennis Holstein
Piotr Karocki
Edmund Kienast
Ansgar Koene
Sean Laroque-Doherty
Javier Luiso
Lingzhong Meng
Rajesh Murthy
Laura Musikanski
Brian Page
R.K. Rannow
Bryan Reese
Annette Reilly

Maximilian Riegel
Pablo Rivas Perea
Subrato Sensharma
John Sheppard
Carl Singer
Robert Soper
Walter Struppler
Abd-Elhamid Taha
Thomas Tullia
Eleanor Watson
Alexander White
Forrest Wright
Naritoshi Yoshinaga
Oren Yuen

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
Doug Edwards
Ramy Ahmed Fathy
J. Travis Griffith
Thomas Koshy
Joseph L. Koepfinger*
David J. Law

Howard Li
Daozhuang Lin
Kevin Lu
Daleep C. Mohla
Chenhui Niu
Damir Novosel
Annette Reilly
Dorothy Stanley

Mehmet Ulema
Lei Wang
F. Keith Waters
Karl Weber
Sha Wei
Howard Wolfman
Daidi Zhong

*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

1. Overview	13
1.1 Scope	13
1.2 Purpose	13
1.3 Objectives	13
1.4 Verification methods	14
1.5 Limitation of scope	14
1.6 Document organization	14
1.7 Word usage	14
2. Normative references	15
3. Definitions, acronyms, and abbreviations	15
3.1 Definitions	15
3.2 Acronyms and abbreviations	18
4. Policy requirements	19
4.1 Governance requirements	19
4.2 Management requirements	19
4.3 Data project requirements	21
5. Data management system technical control requirements	22
5.1 Data classification requirements	22
5.2 Informed consent requirements	22
5.3 Content management requirements	24
5.4 Data management system derived requirements	27
5.5 Information sharing requirements	27
5.6 Grievance redress requirements	28
Annex A (informative) Data classification	29
Annex B (informative) Informed consent	40
Annex C (informative) Content management platform	50
Annex D (informative) Data management system	60
Annex E (informative) Grievance redress mechanisms available to the data subject	74
Annex F (informative) Bibliography	78

List of Figures

Figure A.1—Assessment of the impact on company mission and staffing	30
Figure A.2—Establishment of metrics and scoring criteria	31
Figure A.3—Finalization and execution of the action plan.....	32
Figure A.4—Interaction of components related to personal data protection.....	34
Figure A.5—Sector, domain, and governing authority enumerations.....	35
Figure A.6—Personal data enumerations	37
Figure A.7—RBAC role and permission enumerations	38
Figure A.8—ABAC location, client device, and time enumerations	39
Figure B.1—System context to solicit consent.....	42
Figure B.2—Use case to solicit informed consent.....	42
Figure B.3—Review and acceptance of the applicable PP&OD requirements.....	43
Figure B.4—Review and acceptance of data subject’s obligations and risks.....	44
Figure B.5—Acceptance level MoE and SiU performance	45
Figure B.6—Use case of a generic system of interest.....	47
Figure B.7—Focus on the observer during the data exchange.....	47
Figure B.8—Data exchange scenario	48
Figure B.9—Logical architecture for a typical SoI.....	49
Figure C.1—CMP system components	52
Figure C.2—Use cases of CMP in use	53
Figure C.3—CMP measures of effectiveness.....	54
Figure C.4—Interaction between sensor host and front-end processor	54
Figure C.5—Process to initialize sensor host	56
Figure C.6—Process to generate a composite data file.....	57
Figure C.7—Interaction with the data subject	59
Figure D.1—Data management system use case.....	60
Figure D.2—Data management SiU.....	63
Figure D.3—Use case to securely collect and verify personal data	64
Figure D.4—Personal data collection control unit activity.....	65
Figure D.5—Use case to securely process and verify intended use of personal data	66

Figure D.6—Personal data processing control unit activity	67
Figure D.7—Use case to securely store personal data and verify location and duration.....	68
Figure D.8—Personal data storage control unit activity	69
Figure D.9—Use case to securely disseminate personal data and verify approved interface.....	70
Figure D.10—Personal data dissemination control unit activity	71
Figure D.11—Use case to securely destroy and verify destruction of personal data.....	72
Figure D.12—Personal data disposal unit activity	73
Figure E.1—Use case for GSiU.....	76

List of Tables

Table B.1—Employer and data subject needs	41
Table C.1—CMP user needs.....	51
Table D.1—Data controller governance.....	62
Table E.1—Stakeholder needs for effective grievance redress mechanisms	74

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*).

¹The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.

²The 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.

³ISO 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.

⁵Notes 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 [\[B6\]](#)).

⁶The 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 ISO 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 26000:2010⁷ 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.

⁷Information 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 subjects 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 purposes detailed in the data project document.

⁸Data 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.