



DPC: 25/30469618 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 03 December 2025

Origin: International

Latest date for receipt of comments: 26 January 2026

Project No. 2023/00315

Responsible committee: IST/33/5 Identity Management and Privacy Technologies

Interested committees:

Title: Draft BS ISO/IEC 27091 Cybersecurity and Privacy — Artificial Intelligence — Privacy protection.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 26 January 2026

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 27091

Cybersecurity and Privacy — Artificial Intelligence — Privacy protection

ICS: 35.240.01; 35.030

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2025-12-03

Voting terminates on:
2026-02-25

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 27091:2025(en)

Full document details: 25/30469618 DC

© ISO/IEC 2025  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	4
5 Framework for privacy analysis of AI systems	4
5.1 General	4
5.2 AI systems	4
5.3 AI systems functional view	4
5.4 Taxonomies and catalogs for privacy analysis	5
6 Privacy of AI models	7
6.1 Introduction	7
6.1.1 Machine learning models	7
6.1.2 Legal basis for AI model training	7
6.1.3 Training data in machine learning	7
6.1.4 Transparency and information to PII principals	8
6.2 Privacy threats to AI models	8
6.2.1 Introduction	8
6.2.2 Membership inference attack	8
6.2.3 <u>Training data</u> extraction attack	9
6.2.4 Poisoning attack	9
6.2.5 Property inference attack	9
6.2.6 Model inversion attack	10
6.2.7 Embedding models attack	10
6.3 Other privacy risks to AI systems	12
6.3.1 Privacy attacks for knowledge transfer frameworks	12
6.3.2 Insider risk	12
6.4 Guidance on AI models	13
6.4.1 High-level guidance statement	13
6.4.2 Limiting model use and access	13
6.4.3 Model monitoring	13
6.4.4 Using anonymization techniques to build models	13
6.4.5 Using pseudonymization techniques to build models	15
6.4.6 Model retention	15
6.4.7 Input and output confidentiality control	16
6.4.8 Guidance on generative AI	16
7 Privacy in AI system lifecycle	17
7.1 Introduction	17
7.2 Guidance on AI system lifecycle	18
7.2.1 Privacy engineering	18
7.2.2 Privacy engineering of AI systems involving multiple organisations	19
7.2.3 Privacy engineering supported by AI capabilities	20
Annex A (informative) Additional information for privacy analysis of AI systems	22
Annex B (informative) Use Case Template	28
Bibliography	29

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is Joint Technical Committee ISO/TC JTC1, Information technology, Subcommittee SC 27, Information security, cybersecurity and privacy protection.

Introduction

Artificial Intelligence (AI) systems and Machine Learning (ML) are increasingly adopted across industries leveraging digital technologies. The rise of AI has profound privacy impacts and directly affects individuals because personal data could be used for training or as direct input to the AI system. Decisions made from the AI system may also have an impact on individuals and their privacy. Safeguards to mitigate privacy risks often depend on a variety of factors including the specific type of process, sensitivity of inputs used, and potential harm. While this document focuses on privacy risks, they are only a subset of risks involved in the building and use of AI systems.

[Table 1](#) provides a summary of the guidance provided in this document:

- the first column expresses a high-level guidance statement,
- the second column lists detailed guidance statements.

Table 1 — Summary of guidance statements

[G1] Conduct risk analysis on AI models and identify and implement controls.	[G1.1] Limit model use and access, as appropriate. [G1.2] Monitor models for privacy risk through the AI system lifecycle. [G1.3] Anonymize training data and model inputs and outputs. [G1.4] Use anonymization techniques to build models. [G1.5] Use pseudonymization techniques to build models. [G1.6] Apply measures related to model retention. [G1.7] Define and enforce model retention policies. [G1.8] Apply countermeasures to ensure confidentiality of input and output during inference phase. [G1.9] Apply data sanitization techniques in generative AI such as deduplication, pseudonymization, or anonymization. [G1.10] Test the model for privacy risk in generative AI. [G1.11] Apply controls in generative AI for inputs, prompts and generated outputs.
[G2] Apply privacy engineering to AI systems.	[G2.1] Perform privacy use case analysis. [G2.2] Specify the de-identification mechanisms used. [G2.3] Specify the terminology to describe privacy policies. [G2.4] Include privacy assessment and identify resulting controls. [G2.5] Include privacy testing capabilities. [G2.6] Include consumer demands and regulation if appropriate. [G2.7] Manage user preference. [G2.8] Reuse and share architecture patterns on privacy.
[G3] Establish a governance scheme for AI systems involving multiple organisations.	[G3.1] Establish an AI system privacy plan. [G3.2] Establish a governance process for AI system privacy management. [G3.3] Establish a data management process to ensure protection of PII. [G3.4] Establish a risk management process to assess privacy impact. [G3.5] Establish an engineering process to implement privacy-by-design. [G3.6] Establish a human oversight process that integrates privacy.
[G4] Use AI capabilities to enhance privacy.	[G4.1] Use AI to support data anonymization and pseudonymization. [G4.2] Use AI to support consent management and control. [G4.3] Use AI to support Privacy-Enhancing Technologies (PETs). [G4.4] Use AI to support AI-Powered Privacy Audits and Monitoring. [G4.5] Use AI to support data minimization. [G4.6] Use AI to support secure AI models and federated learning. [G4.7] Use AI to support access control and identity management. [G4.8] Use Natural Language Processing (NLP) for data privacy policies. [G4.9] Use AI to detect privacy violations.

Cybersecurity and Privacy — Artificial Intelligence — Privacy protection

1 Scope

This document provides guidance for organizations to address privacy risks in artificial intelligence (AI) systems, including machine learning (ML) models. This document helps organizations identify privacy risks throughout the AI system lifecycle, and establishes mechanisms to evaluate the consequences and treatment of such risks.

This document is applicable to all types and sizes of organizations that develop or use AI system, including public and private companies, government entities, and not-for-profit organizations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO/IEC 22989:2022, *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org>

3.1

parameter

model parameter

internal variable of a model that affects how it computes its outputs

Note 1 to entry: Examples of parameters include the weights in a neural network and the transition probabilities in a Markov model.

[SOURCE: ISO/IEC 22989:2022, 3.3.8]

3.2

federated learning

<machine learning> decentralized training using multiple independent devices, each using its own training dataset

EXAMPLE Using multiple independent sensors residing on devices such as smartphones, each using its own training dataset. Training parameters are uploaded and aggregated on a centralized repository.

3.3

model retention

<machine learning> period measured from the most recent training of a model without using any parameters from a previous training

3.4

structured data

data which are organized based on a pre-defined (applicable) set of rules

Note 1 to entry: The predefined set of rules governing the basis on which the data are structured needs to be clearly stated and made known.

Note 2 to entry: A pre-defined data model is often used to govern the structuring of data.

EXAMPLE 1 Date.

EXAMPLE 2 Country.

[SOURCE: ISO/IEC 20546:2019, 3.1.35, examples are added]

3.5

unstructured data

data that does not adhere to a specified format

EXAMPLE 1 Video.

EXAMPLE 2 Free form text (such as queries).

EXAMPLE 3 Photo.

3.6

artificial Intelligence

AI

<discipline> research and development of mechanisms and applications of *AI systems* ([3.7](#))

Note 1 to entry: Research and development can take place across any number of fields such as computer science, data science, humanities, mathematics and natural sciences.

[SOURCE: ISO/IEC 22989:2022, 3.1.3]

3.7

artificial Intelligence system

AI system

engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives

Note 1 to entry: The engineered system can use various techniques and approaches related to *artificial intelligence* ([3.6](#)) to develop a model to represent data, knowledge, processes, etc. which can be used to conduct tasks.

Note 2 to entry: AI systems are designed to operate with varying levels of automation.

[SOURCE: ISO/IEC 22989:2022, 3.1.4]

3.8

machine learning

ML

process of optimizing model parameters through computational techniques, such that the model's behaviour reflects the data or experience

[SOURCE: ISO/IEC 22989:2022, 3.3.5]

3.9**machine learning algorithm**

algorithm to determine parameters of a *machine learning model* (3.10) from data according to given criteria

EXAMPLE Consider solving a univariate linear function $y = \theta_0 + \theta_1 x$ where y is an output or result, x is an input, θ_0 is an intercept (the value of y where $x=0$) and θ_1 is a weight. In *machine learning* (3.8), the process of determining the intercept and weights for a linear function is known as linear regression.

[SOURCE: ISO/IEC 22989:2022, 3.3.6]

3.10**machine learning model**

mathematical construct that generates an inference or prediction based on input data or information

EXAMPLE If a univariate linear function ($y = \theta_0 + \theta_1 x$) has been trained using linear θ regression, the resulting model can be $y = 3 + 7x$.

Note 1 to entry: A machine learning model result from training based on a *machine learning algorithm* (3.9).

[SOURCE: ISO/IEC 22989:2022, 3.3.7]

3.11**differential privacy**

formal privacy measurement model (3.12) that ensures that the probability distribution of the output from a statistical analysis differs by at most a specified value

Note 1 to entry: The model is effective regardless of whether or not any particular *data principal* (3.13) is represented in the input dataset.

[SOURCE: ISO/IEC 20889:2018, 3.9, modified, note 1 replaced]

3.12**formal privacy measurement model**

approach to the application of data de-identification techniques that enables the calculation of re-identification risk

[SOURCE: ISO/IEC 20889:2018, 3.3]

3.13**data principal**

entity to which data relates

Note 1 to entry: The term “data principal” is broader than “PII principal” (or “data subject” as used elsewhere), and is able to denote any entity such as a person, an organization, a device, or a software application.

[SOURCE: ISO/IEC 20889:2018, 3.4]

3.14**re-identification**

process of associating data in a de-identified dataset with the original data principal

Note 1 to entry: A process that establishes the presence of a particular data principal in a dataset is included in this definition.

[SOURCE: ISO/IEC 20889:2018, 3.31]

4 Abbreviated terms

AI	Artificial Intelligence
GAN	Generative Adversarial Networks
ML	Machine Learning
PII	Personally Identifiable Information
SoS	Systems of Systems

5 Framework for privacy analysis of AI systems

5.1 General

This clause describes the framework for privacy analysis of AI systems that is used in this document. Some additional informative information is provided in [Annex A](#).

5.2 AI systems

This document considers privacy in the context of systems including AI functions as showed in [Figure 1](#):

- an AI system is a system (or an entity of interest^[1]) which is developed and operated in an environment, and
- an AI system is a system which includes AI functions.

It is important to identify the environment as it provides a context which can influence the AI system.

Example 1 An AI system in a social network in the context of children applications.

Example 2 An AI system in the context of a development, a test, or an operational environment^[1].

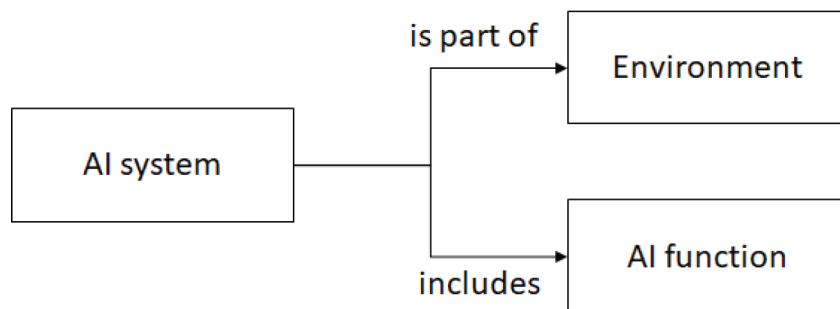


Figure 1 — AI system high-level view

5.3 AI systems functional view

[Figure 2](#) provides a functional view of an AI system.^[2] The following types of data can be involved when privacy risks are considered:

- training data, which can be based on structured data or on unstructured data,
- models (models can be shared as pointed out in the OECD report on privacy and AI^[43]),
- input data, and
- output data.