BSI Standards Publication

Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

National foreword

This British Standard is the UK implementation of EN ISO/IEC 27701:2025. It is identical to ISO/IEC 27701:2025. It supersedes BS EN ISO/IEC 27701:2021, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/5, Identity Management and Privacy Technologies.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2025

ISBN 978 0 539 24576 9

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2025.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPÄISCHE NORM

October 2025

ICS 35.030

Supersedes EN ISO/IEC 27701:2021

English version

Information security, cybersecurity and privacy protection - Privacy information management systems - Requirements and guidance (ISO/IEC 27701:2025)

Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la protection de la vie privée - Exigences et recommandations (ISO/IEC 27701:2025)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Datenschutz-Informationsmanagementsysteme - Anforderungen und Leitlinien (ISO/IEC 27701:2025)

This European Standard was approved by CEN on 4 August 2025.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

European foreword

This document (EN ISO/IEC 27701:2025) has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" in collaboration with Technical Committee CEN-CENELEC/ JTC 13 “Cybersecurity and Data Protection” the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by April 2026, and conflicting national standards shall be withdrawn at the latest by April 2026.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO/IEC 27701:2021.

Any feedback and questions on this document should be directed to the users’ national standards body/national committee. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27701:2025 has been approved by CEN-CENELEC as EN ISO/IEC 27701:2025 without any modification.

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms, definitions and abbreviations **1**
4 Context of the organization **4**
4.1 Understanding the organization and its context 4
4.2 Understanding the needs and expectations of interested parties 5
4.3 Determining the scope of the privacy information management system 5
4.4 Privacy information management system 6
5 Leadership **6**
5.1 Leadership and commitment 6
5.2 Privacy policy 6
5.3 Roles, responsibilities and authorities 7
6 Planning **7**
6.1 Actions to address risks and opportunities 7
6.1.1 General 7
6.1.2 Privacy risk assessment 7
6.1.3 Privacy risk treatment 8
6.2 Privacy objectives and planning to achieve them 9
6.3 Planning of changes 10
7 Support **10**
7.1 Resources 10
7.2 Competence 10
7.3 Awareness 10
7.4 Communication 10
7.5 Documented information 11
7.5.1 General 11
7.5.2 Creating and updating documented information 11
7.5.3 Control of documented information 11
8 Operation **12**
8.1 Operational planning and control 12
8.2 Privacy risk assessment 12
8.3 Privacy risk treatment 12
9 Performance evaluation **12**
9.1 Monitoring, measurement, analysis and evaluation 12
9.2 Internal audit 13
9.2.1 General 13
9.2.2 Internal audit programme 13
9.3 Management review 13
9.3.1 General 13
9.3.2 Management review inputs 13
9.3.3 Management review results 14
10 Improvement **14**
10.1 Continual improvement 14
10.2 Nonconformity and corrective action 14
11 Further information on annexes **14**
Annex A (normative) **PIMS reference control objectives and controls for PII controllers and PII processors** **15**

Annex C (informative) **Mapping to ISO/IEC 29100** **51**
Annex D (informative) **Mapping to the General Data Protection Regulation** **53**
Annex E (informative) **Mapping to ISO/IEC 27018 and ISO/IEC 29151** **56**
Annex F (informative) **Correspondence with ISO/IEC 27701:2019** **58**
Bibliography **64**

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

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

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13, *Cybersecurity and data protection*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO/IEC 27701:2019), which has been technically revised.

The main changes are as follows:

— the document has been redrafted as a stand-alone management system standard.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

0.1 General

Almost every organization processes personally identifiable information (PII). Further, the quantity and types of PII processed are increasing, as are the number of situations where an organization needs to cooperate with other organizations regarding the processing of PII. Protection of privacy in the context of the processing of PII is a societal need, as well as the topic of dedicated legal requirements worldwide.

This document includes mapping to:

— the privacy framework and principles defined in ISO/IEC 29100;

— ISO/IEC 27018;

— ISO/IEC 29151;

— the EU General Data Protection Regulation.

NOTE These mappings can be interpreted to take into account local legal requirements.

This document can be used by PII controllers (including those that are joint PII controllers) and PII processors (including those using subcontracted PII processors and those processing PII as subcontractors to PII processors).

By complying with the requirements in this document, an organization can generate evidence of how it handles the processing of PII. Such evidence can be used to facilitate agreements with business partners where the processing of PII is mutually relevant. This can also assist in relationships with other interested parties. The use of this document can provide independent verification of this evidence.

0.2 Compatibility with other management system standards

This document applies the framework developed by ISO to improve alignment among its management system standards.

This document enables an organization to align or integrate its privacy information management system (PIMS) with the requirements of other management system standards, and in particular with the information security management system specified in ISO/IEC 27001.

Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

1 Scope

This document specifies requirements for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS).

Guidance is also provided to assist in the implementation of the requirements in this document.

This document is intended for personally identifiable information (PII) controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to all types and sizes of organizations, 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, *Information technology — Security techniques — Privacy framework*

3 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions given in ISO/IEC 29100 and the following apply.

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.6)

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: If the organization is part of a larger entity, the term “organization” refers only to the part of the larger entity that is within the scope of the *privacy informationmanagement system* (3.23).

3.2
interested party
person or *organization* (3.1) that can affect, be affected by, or perceive itself to be affected by a decision or activity