International Standard

ISO/IEC 27701

Second edition
2025-10

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

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la protection de la vie privée — Exigences et recommandations

查阅全文请联系北京海德国际认证有限公司
联系电话：010-84905056，010-65817800
邮箱地址：common@hicchina.com.cn

Reference number
ISO/IEC 27701:2025(en)

© ISO/IEC 2025



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.

Published in Switzerland

Contents

Page

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**

© ISO/IEC 2025 – All rights reserved

Annex B (normative) **Implementation guidance for PII controllers and PII processors** **21**
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/IEC 2025 – All rights reserved

Foreword

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

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

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

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

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

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*, 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.

© ISO/IEC 2025 – All rights reserved

Introduction

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.

© ISO/IEC 2025 – All rights reserved