



**International
Standard**

ISO/IEC 27701

**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*

**Second edition
2025-10**



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	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 27701:2025(en)

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

注：本文件内容受到版权保护，未经恰当的授权禁止复制。本公司客户及相关单位，如需获取文件完整内容，请联系市场部门获取，电话：010-84720998。