



**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



国际标准

信息安全、网络安全和隐私保护——隐私信息
管理体系
——要求与指南

信息安全、网络安全与隐私保护——隐私信息管理体系—要求与建议

ISO/IEC 27701

第二版2025-10

参考编号 ISO/IEC
27701:2025(en)

© ISO/IEC 2025



版权保护文件

CISO/IEC 2025

保留所有权利。除非另有说明，或实施过程中有特殊要求，未经事先书面许可，不得以任何形式或任何手段(包括电子或机械方式)复制或使本出版物的任何部分，包括影印、在互联网或内联网上发布。许可申请可向下述地址的ISO或申请者所在国的ISO成员机构提出。

ISO版权办公室
CP 401-布兰东内街8号CH-1214 韦尔
尼耶，日内瓦电话：+41227490111
电子邮箱：copyright@iso.org 网站：
www.iso.org

瑞士出版

目录

页码

前言	V
导言	i
1 范围	1
2 规范性引用	1
3 术语、定义和缩写	
4 组织背景	4
4.1 理解组织及其背景	4
4.2 理解相关方的需求和期望	5
4.3 确定隐私信息管理体系的范围	5
4.4 隐私信息管理体系	6
5 领导层	6
5.1 领导力与承诺	6
5.2 隐私政策	6
5.3 角色、职责与权限	7
6 规划	7
6.1 应对风险与机遇的行动方案	7
6.1.1 一般性	7
6.1.2 隐私风险评估	7
6.1.3 隐私风险处理	8
6.2 隐私目标及实现规划	9
6.3 变更规划	10
7 支持	10
7.1 资源	10
7.2 能力	10
7.3 意识	10
7.4 沟通	10
7.5 文件化信息	11
7.5.1 一般	11
7.5.2 创建和更新文件化信息	11
7.5.3 文件信息的控制	11
8 操作	12
8.1 运行计划与控制	12
8.2 隐私风险评估	12
8.3 隐私风险处理	12
9 绩效评估	12
9.1 监测、测量、分析和评估	12
9.2 内部审计	13
9.2.1 一般	13
9.2.2 内部审计计划	13
9.3 管理层评审	13
9.3.1 一般	13
9.3.2 管理评审输入	13
9.3.3 管理评审结果	14
10 改进	14
10.1 持续改进	14
10.2 不符合项与纠正措施	14
11 附件的进一步信息	14
附件A (规范性) PIMS 参考控制目标及PI 控制器与PI 处理器的控制措施	15

附件B (规范性)PII控制器和PII处理器的实施指南	21
附件C(信息性)与ISO/IEC 29100的映射关系	51
附录D (信息性)与《通用数据保护条例》的对照关系	53
附录E(说明性)与ISO/IEC27018和ISO/IEC 29151的映射关系	56
附录F (信息性)与ISO/ EC27701:2019的对应关系	58
参考文献	64



北京中交远航认证有限公司
BEIJING ZHONGJIAOYUANHANG CERTIFICATION LIMITED

如需查阅全文，可联系公司获取

联系电话:010-63260528

邮 箱:isooffer0211@sina.com