国际标准

ISO/IEC 27701

第二版 **2025-10**

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

参考编号 ISO/IEC 27701:2025(en)

版权保护文件

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：+41 22 749 01 11
电子邮箱：copyright@iso.org 网站：www.iso.org
瑞士出版

目录

页码

前言

国际标准化组织（ISO）与国际电工委员会（IEC）共同构成全球标准化专业体系。作为ISO或IEC成员的国家机构，通过各组织为特定技术领域设立的技术委员会参与国际标准制定工作。ISO与IEC技术委员会在共同关注领域开展协作。其他与ISO和IEC保持联络的国际组织（包括政府组织和非政府组织）也参与相关工作。

本文件的编制程序及其后续维护程序详见ISO/IEC指令第1部分。特别需要注意的是，不同类型的文件需满足不同的批准标准。本文件的起草遵循了ISO/IEC指令第2部分的编辑规则（详见www.iso.org/directives或www.iec.ch/members_experts/refdocs ）。

ISO和IEC提醒注意，实施本文件可能涉及使用一项或多项专利。ISO和IEC对任何相关专利权主张的证据、有效性或适用性不持任何立场。截至本文件发布之日，ISO和IEC尚未收到实施本文件可能涉及的专利通知。但需提醒实施者注意，此信息可能并非最新状态，最新专利信息可通过www.iso.org/patents 和https://patents.iec.ch查询。ISO和IEC不承担识别任何或所有此类专利权利的责任。

本文件中使用的任何商标名称仅为方便用户而提供，并不构成推荐。

关于标准自愿性的说明、ISO特定术语及符合性评估相关表述的含义，以及ISO在《技术性贸易壁垒协定》(TBT)中遵循世界贸易组织(WTO)原则的信息，请参阅www.iso.org/iso/foreword.html 。在IEC中，请参阅www.iec.ch/understanding-standards 。

本文件由国际标准化组织/国际电工委员会联合技术委员会1（JTC 1）下属信息技术分技术委员会27（SC 27）——*信息安全、网络安全与隐私保护*分技术委员会，与欧洲标准化委员会（CEN）技术委员会CEN/CLC/JTC *13*——*网络安全与数据保护*技术委员会共同编制，依据ISO与CEN技术合作协议（维也纳协议）完成。

本第二版取代并废止了经技术修订的第一版（ISO/IEC 27701:2019）。

主要变更如下：

— 本文件已重新编写为独立的管理体系标准。

关于本文件的任何反馈或疑问，请联系用户所在国家的国家标准机构。这些机构的完整列表可查阅www.iso.org/members.html 和www.iec.ch/national-committees 。

引言

0.1 概述

几乎所有组织都会处理个人身份信息（PII）。随着组织间协作处理PII的情形日益增多，所处理PII的数量与类型也在持续增长。在处理PII过程中保障隐私既是社会需求，也是全球专项法律要求的核心议题。

本文档包含以下映射关系：

— ISO/IEC 29100 中定义的隐私框架和原则；

— ISO/IEC 27018；

— ISO/IEC 29151；

— 欧盟《通用数据保护条例》。

注 这些映射可根据当地法律要求进行解释。

本文件适用于个人身份信息（PII）控制者（包括共同控制者）及处理者（包括使用分包处理者的控制者，以及作为处理者分包商的处理者）。

通过遵守本文件的要求，组织可生成其处理个人身份信息（PII）方式的证据。此类证据可用于促进与业务伙伴的协议达成，尤其在双方均涉及PII处理时。这亦有助于维护与其他相关方的关系。采用本文件可为该证据提供独立验证。

0.2 与其他管理体系标准的兼容性

本文件采用ISO制定的框架，旨在提升其管理体系标准间的协调性。

本文件使组织能够将其隐私信息管理体系（PIMS）与其他管理体系标准的要求进行协调或整合，特别是与ISO/IEC 27001中规定的信息安全管理体系相协调。

信息安全、网络安全与隐私保护——隐私信息管理体系——要求与指南

0 范围

本文件规定了建立、实施、维护和持续改进隐私信息管理体系（PIMS）的要求。

同时提供实施指南以协助落实本文件要求。

本文件适用于对个人身份信息（PII）处理负有责任和问责的PII控制者和PII处理者。

本文件适用于所有类型和规模的组织，包括公共和私营公司、政府实体和非营利组织。

1 规范性引用

以下文件在本文中被引用，其部分或全部内容构成本文件的要求。对于带日期的引用，仅适用所引用的版本。对于不带日期的引用，适用被引文件的最新版本（包括任何修订）。

ISO/IEC 29100，*信息技术——安全技术——隐私框架*

2 术语、定义和缩写

为本文件之目的，除另有规定外，采用ISO/IEC 29100所载术语及定义。ISO与IEC在下列网址维护标准化用术语数据库：

— ISO在线浏览平台：可访问 https://www.iso.org/obp

— IEC Electropedia：访问地址 https://www.electropedia.org/

3.1
组织
具有自身职能、责任、权限及关系以实现其*目标*（3.6）的个人或群体

注1：组织的概念包括但不限于个体经营者、公司、企业、机构、企业、当局、合伙企业、慈善机构或机构，或其部分或组合，无论是否注册成立，无论公营还是私营。

注释 2：若该组织隶属于更大实体，则"组织"仅指该实体中属于*隐私信息管理体系*（3.23）范围的部分。

3.2
相关方
能够影响、受影响或认为自己受某项决定或活动影响的个人或*组织*（3.1）。

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

Reference number
ISO/IEC 27701:2025(en)

COPYRIGHT PROTECTED DOCUMENT

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

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.

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.

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

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：17312273399@163.com

2）也可通过客服电话咨询 025-85307007。