隐私信息管理体系认证证书

证书编号：

统一社会信用代码：

建立的隐私信息管理体系认证符合标准：

ISO/IEC 27701:2025

注册地址：

审核地址：

认证范围：

组织[具体活动]相关的隐私信息管理活动

首次发证日期：　　本次发证日期：　　有效期至：

本证书在国家规定的行政许可、资质许可有效期内有效。获证组织应按规定执行监督审核并经审核合格的情况下方可保持认证证书的有效性。本证书可通过以下方式查询：1. 本机构网站（http:// www.bozrz.com）2. 中国国家认监委官方网站（http://www.cnca.gov.cn）

签 发：

地址：浙江省杭州市钱塘区白杨街道东部创智大厦1幢1007室
电话：0571-86821236　邮箱：bang_zheng@yeah.net

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——要求与指南

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

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 2vI0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）

3.3
最高管理层
在最高层级指导和控制*组织*的人或群体（3.1）

注 1：最高管理层有权在组织内部授权并提供资源。

注2：若*管理体系*(3.4)的范围仅覆盖组织的部分领域，则最高管理层指该部分领域的决策控制者。

3.4
管理体系
组织（3.1）中相互关联或相互作用的要素集合，用于制定*政策*（3.5）和*目标*(3.6)，以及实现这些目标*的过程*(3.8)

注 1：管理体系可涉及单一领域或多个领域。

条目注释2：管理体系要素包括组织的结构、角色与职责、规划和运作。

3.5
政策
组织（3.1）的意图和方向，由其*最高管理层*（3.3）正式表达

3.6
目标
需达成的结果

注1：目标可分为战略目标、战术目标或操作目标。

条目注释2：目标可涉及不同领域（如财务、健康与安全、环境）。例如，目标可以是全组织性的，也可以针对特定项目、产品或*过程*（3.8）。

注3：目标可通过其他形式表达，例如作为预期结果、宗旨、操作标准、隐私目标，或使用其他含义相近的词语（如宗旨、目标或指标）。

注4：*在隐私信息管理体系*（3.3）的背景下，隐私目标由组织（3.1）设定，*组织*（3.1）根据*隐私政策*（3.5）制定，以实现特定结果。

3.7
风险
不确定性的影响

注1：效应是指与预期值的偏差——可能是正向或负向偏差。

注释2：不确定性是指对某事件、其后果或发生概率的信息、理解或认知存在不足的状态，即使这种不足是部分性的。

注3：风险通常通过潜在事件及其后果，或二者的组合来表征。

注 4：风险通常通过事件后果（包括环境变化）与发生概率的组合来表述。

3.8
过程
一组相互关联或相互作用的活动，通过使用或转化投入来交付成果

注1：过程结果称作产出、产品或服务，取决于引用的语境。

3.9
能力
将知识和技能应用于实现预期结果的能力

3.10
文件化信息
组织（3.1）需要控制和维护的信息及其载体

注1：文件化信息可以采用任何格式和介质，来自任何来源。注2：文件化信息可指：

— *管理体系*（3.4），包括相关*过程*（3.8）；

— 为组织运作而创建的信息（文件）；

— 实现结果的证据（记录）。

3.11
绩效
可测量的结果

注 1：绩效可涉及定量或定性发现。

条目注释2：绩效可涉及管理活动、*流程*（3.8）、产品、服务、系统或*组织*（3.1）。

3.12
持续改进
为提升*绩效*而反复开展的活动（3.11）

3.13
有效性
计划活动实现及计划结果达成的程度

3.14
要求
明示、默示或强制性的需求或期望

注释1：“通常暗示”是指*组织*（3.1）和惯例或普遍做法*相关方*（3.2）应知悉，所考虑的需求或期望是隐含的。

注2：规定要求是指明确表述的要求，例如在*文件化信息*（3.10）中表述的要求。

3.15
符合性
满足*要求*（3.14）

3.16
不符合
未满足*要求*（3.14）

3.17
纠正措施
消除*不符合项*（3.16）原因并防止再发的措施

3.18
审计
系统化且独立*的过程*（3.8），用于获取证据并客观评估其有效性，以确定审计标准的达成程度

注1：审计可分为内部审计（第一方）或外部审计（第二方或第三方），亦可为组合审计（融合两个或多个领域）。

条目注释 2：内部审计由*组织*（3.1）自身或代表其的外部方实施。条目注释 3：“审计证据”和“审计标准”在 ISO 19011 中定义。

3.19
测量
确定数值*的过程*（3.8）

3.20
监测
确定系统、*过程*（3.8）或活动的状态

注 1：确定状态时，可能需要进行检查、监督或批判性观察。

3.21
共同个人身份信息（PII）控制者
与一个或多个其他个人身份信息（PII）控制者共同确定个人身份信息处理目的和方式的个人身份信息控制者

3.22
客户
个人或*组织*（3.1），能够或实际接收某项产品或服务，该产品或服务是为该个人或组织准备的或其所需的

示例　　消费者、客户、最终用户、零售商、*内部流程*（3.8）的产品或服务接收方、受益方及购买方。

注 1：客户可属于组织内部或外部。

注2：客户可以是与PII控制者签订合同的组织、与PII处理者签订合同的PII控制者，或是与PII处理分包商签订合同的PII处理者。

3.23
隐私信息管理系统 PIMS
管理制度（3.4），该制度旨在应对个人身份信息处理过程中可能影响隐私保护的问题

3.24
信息安全计划
旨在管理*组织风险*（3.7）的一套*政策*（3.5）、*目标*（3.6）和*流程*（3.8）
(3.1) 资产，以确保信息的机密性、完整性和可用性

注1：信息安全计划可采用信息安全管理体系形式，例如基于ISO/IEC 27001标准的体系。

3.25
适用性声明
所有必要控制措施的文件记录，以及纳入或排除此类控制措施的理由

3　组织背景

3.1　理解组织及其环境

该组织应确定与其宗旨相关且影响其实现隐私信息管理体系预期结果能力的外部和内部事项。

组织应确定气候变化是否为相关事项。

组织应确定其是否作为个人身份信息（PII）的控制者（包括作为共同控制者）或处理者。

该组织应确定与其环境相关且影响其实现计划信息管理系统的预期成果能力的外部和内部事项。

注1　　外部和内部事项可包括但不限于：

杭州邦证认证有限公司

Hangzhou Bangzheng Certification Co.， Ltd

隐私信息管理体系认证实施规则

文件编号：BZ-MC-R-067

版　　本：A/2

编　　制：

审　　核：

批　　准：

控制状态：受控

2025-11-26 发布　　2025-11-26 实施

文件修订记录表

序号	发布日期	实施日期	修订内容摘要	版次	批准
1	2024-06-06	2024-06-06	新做成	A/0	
2	2025-08-08	2025-08-08	**1 新增：**0 前言 **2 修改：**1 适用范围 **3 补充：**2 规范性引用文件 GB/T 27007 合格评定 合格评定用规范性文件的编写指南 GB/T 27060 合格评定 良好操作规范 **4 修改：**12 获证组织的信息报告 12.1 信息报送 颁证后 30 日内向国家认监委报送认证信息； 在认证证书有效期间，获证组织发生与隐私信息管理体系有关的重大变化时（如获证组织发生重大事故/行政处罚），本机构应及时做出暂停或撤销证书的措施并及时报告国家认监委。 12.2 监管配合 备案规则作为市场监管检查依据，违规行为按《认证认可条例》处罚。	A/1	
3	2025-11-26	2025-11-26	ISO/IEC 27701:2019《安全技术 针对ISOIEC 27001 和ISO/IEC 27002 在隐私信息管理的扩展 要求和指南》变更为ISO/IEC 27701-2025 《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》 **3 补充：**隐私信息管理体系的审核范围模式和示例。	A/2	

0 前言

本规则依据《中华人民共和国认证认可条例》、《认证机构管理办法》及《国家认监委关于加强认证规则管理的公告》（2025 年第 9 号）制定。

由杭州邦证认证有限公司（批准号：CNCA-R-2021-885）发布实施。认证机构对规则的合法性、合规性、科学性负责，并承担主体责任。

本规则文本可通过本机构官方网站获取（网址：www.bozi.com）。公众可通过认证咨询电话（0571-86821236）或电子邮箱（bang_zheng@yeah.net）就本规则内容进行咨询。

1 适用范围

1.1 本规则适用于本机构开展的隐私信息管理体系认证活动。

1.2 认证对象为建立并运行隐私信息管理体系的组织，包括金融行业:个人金融信息（账户、交易记录、信用信息）、身份信息、生物识别信息的安全；医疗卫生：患者健康信息、病历、诊断记录、遗传信息等高度敏感数据的机密性，医疗科研中的匿名化处理，远程医疗数据安全；科技与互联网行业：用户个人信息（身份、行为、偏好、位置等）的收集与处理，数据驱动的个性化服务，用户画像与精准广告的合规性，数据跨境传输，App 合规；电子商务与零售行业：消费者个人信息、购买历史、支付信息、联系方式，营销活动中的用户数据使用，供应链数据共享；制造业：员工个人信息、客户信息、供应商信息，智能制造过程中产生的数据，产品联网后的用户使用数据；教育行业：学生及教职工的个人信息、学业成绩、健康信息，在线教育平台的学习行为数据，科研数据；交通运输与物流行业：乘客/货主的个人信息、行程轨迹、联系方式，物流配送信息，智能网联汽车收集的各类环境与用户数据；公共服务与政府机构：公民身份信息、社保信息、税务信息、各类政务办理信息，公共数据开放与利用等，覆盖组织隐私信息管理活动的策划、运行、监控及持续改进全过程。

1.3 隐私信息管理体系认证依据标准为：ISO/IEC 27701-2025 《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》

1.4 隐私信息管理体系的审核范围模式为：组织[具体活动]相关的隐私信息管理活动。

1.5 隐私信息管理体系的审核范围模式示例：

示例 1：互联网科技公司

组织[生鲜电商移动应用程序与微信小程序的研发、运营、推广及客户服务]相关的隐私信息管理活动。

示例 2：金融机构

组织[信用卡的申请受理、额度审批、账户管理、交易授权、分期营销、风险控制及客户关系维护]相关的隐私信息管理活动。

示例 3：医疗服务与研发机构

组织[面向制药企业委托的‘针对晚期非小细胞肺癌的靶向药物’多中心临床试验项目的受试者招募、数据收集、分析与报告]相关的隐私信息管理活动。

示例 4：智能硬件制造企业

组织[‘安心看’系列智能摄像头、智能门铃等硬件产品的设计、生产、销售，以及云服务平台与移动应用的数据处理服务]相关的隐私信息管理活动。

2 规范性引用文件

下列文件对于本规则的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本规则。

CNAS-CC01　　管理体系本机构要求

GB/T 27000　　合格评定词汇和通用原则

GB/T 27021.1　合格评定 管理体系审核认证机构要求 第 1 部分：要求

GB/T 24040　　环境管理 生命周期评核 原则与框架

GB/T 27007　　合格评定 合格评定用规范性文件的编写指南

GB/T 27060　　合格评定 良好操作规范

ISO/IEC 27701-2025 《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》