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.bzrz.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

仅用于公示

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/3

编　　制：

审　　核：

批　　准：

控制状态：受控

2026-05-20 发布　　2026-05-20 实施

仅用于公示

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 ISOIEC 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	
3	2026-05-20	2026-05-20	**1、补充：**隐私信息管理体系认证活动备案领域为：A05 信息安全管理体系认证。	A/3	

仅用于公示

2、补充：9.2 申请评审

f) 认证委托人已明确知晓并同意，认证费用应由其直接向认证机构（杭州邦证认证有限公司）支付，并已签署包含费用条款的认证合同。

3、补充： 9.8.1.1 明确第一阶段审核与第二阶段审核间隔不少于 5 个工作日、不超过 6 个月。

4、补充： 9.4.4 审核组专职审核员要求

为保证认证活动的质量可控性和公正性，本机构指派的审核组中，至少应有 1 名本机构的专职审核员全程参与审核过程（包括第一阶段审核、第二阶段审核及必要的补充审核）。

专职审核员是指与本机构建立劳动关系、由本机构直接支付薪酬并接受本机构统一管理的审核人员。外部审核员或技术专家可作为审核组成员参与审核，但不能替代上述专职审核员的要求。

因特殊情况无法满足本条要求时，本机构应书面说明理由，并经机构技术负责人批准后方可实施审核，相关记录应予以保存。

5、补充：9.4.5 实习审核员的使用限制

实习审核员不得独立组成审核组或独立实施审核活动。实习审核员应在具备相应资格的审核员或审核组长的指导和监督下参与审核活动，其审核发现和结论须经指导人员复核确认。

审核组中全部成员均为实习审核员的情况，不予认可。审核组组长及审核组中负责作出审核结论的关

仅用于公示

			键岗位人员，应具备有效的审核员资格。 6、**补充：**9.5.0 明确认证审核应在委托人现场且生产/服务处于正常运行状态下进行。 7、**补充：**9.8.1 明确第一阶段非现场审核的适用情形及控制要求。 8、**补充： 0 前言** 明确认证规则公开网址应为认证机构官方网站，并规范证书查询网址格式。 **9、补充：**9.5.2.4 明确现场审核应对最高管理者发挥领导作用情况进行面对面审核，并规定审核内容及例外处理。 10、**补充：** 9.11 系统化明确授予、更新、扩大、缩小认证范围及不予认证的具体条件。 11、**补充：** 5.1.3 明确审核员应具备 CCAA 或等效的管理体系认证审核员注册资格。		

仅用于公示

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（网址：www.bozrz.com）首页“文件下载”→“公开文件”栏目下载，或通过认证咨询电话（0571-86821236）、电子邮箱（bang_zheng@yeah.net）获取。

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。按照国家认监委现行分类管理要求，本认证活动备案于“A05 信息安全管理体系认证”领域。

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；公共管理与社会组织；互联网平台等，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》

仅用于公示

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)

© ISO/IEC 2025

仅用于公示

Contents

Page

© ISO/IEC 2025 – All rights reserved

仅用于公示

© ISO/IEC 2025 – All rights reserved

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

© ISO/IEC 2025 – All rights reserved