

关于 ISO/IEC 27701:2019 隐私信息管理体系标准

转版至 2025 版的告知书

致获证客户：

为适配全球数据隐私合规发展新形势、应对人工智能、跨境数据传输、生物识别处理等新型隐私风险，国际标准化组织（ISO）正式发布 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—要求和指南》，全面替代旧版 ISO/IEC 27701:2019 标准。为确保各获证企业平稳完成标准转版、持续合规运营、保障证书有效性，现将标准重大变化、过渡期安排及企业转版工作要求正式告知如下：

一、标准核心改版变化说明

相较于 ISO/IEC 27701:2019 版本，2025 版标准进行了结构性、体系性全面升级，核心变革要点如下：

1. 体系定位颠覆性升级，支持独立认证

2019 版标准为 ISO/IEC 27001 信息安全管理体系的扩展标准，企业必须依托 27001 体系方可建立、认证 PIMS 隐私管理体系；2025 版正式升级为**独立的隐私信息管理体系标准**，企业无需持有 ISO/IEC 27001 认证，可直接建立并获取 PIMS 认证，大幅降低合规门槛，同时保留与 ISO/IEC 27001:2022 的高度兼容性，支持双体系融合运营。

2. 统一国际高阶架构，适配多体系集成

2025 版全面采用 ISO 通用高阶架构（HLS），第 4-10 章管理要求全部强制落地，与 ISO 9001、ISO/IEC 27001、ISO/IEC 42001 等主流管理体系框架统一，彻底解决旧版体系架构零散、多体系融合困难的问题，助力企业实现治理体系一体化、降本增效。

3. 控制措施全面重构，贴合新型业务场景

摒弃 2019 版依托 ISO27001:2013 的 14 类管控架构，全新重构为**组织、人员、物理、技术**四大类隐私控制措施，细化区分 PII 控制者、PII 处理者及通用管控要求。新增 AI 自动化决策、算法偏见防控、跨境数据流动、生物识别数据、云服务隐私保护等专项管控要求，填补了旧版对数字化、智能化业务场景的管控空白。

4. 隐私风险管理强制独立化

2019 版隐私风险管理依附于信息安全风险评估，无独立管控要求；2025 版将**隐私风险管理列为强制性核心要求**，要求企业建立独立的隐私风险评估（PIA/DPIA）机制，从数据主体权益、企业合规风险双维度开展全周期风险管控，重点覆盖 AI 模型训练、数据跨境传输、用户自动化决策等高危场景。

5. 全球法规兼容性全面升级

新版标准不再局限于欧盟 GDPR 适配，全面兼容中国《个人信息保护法》、美国 CCPA、巴西 LGPD、印度 DPDP Act 等全球主流隐私法规，配套完善的法规映射附录，支持企业“一套体系、全球合规”，适配跨境业务发展需求。

二、标准转版过渡期安排

根据 ISO 官方统一规定及国内认证行业通用规则，ISO/IEC 27701:2019 版证书过渡期至 2028 年 10 月截止。过渡期内相关规则明确如下：

1. 过渡期内，2019 版原有认证证书持续有效，企业可正常进行监督审核，也可结合监督和再认证换版；
2. 过渡期结束后，所有 ISO/IEC 27701:2019 版证书将自动失效，未完成转版的企业将失去 PIMS 合规认证资质；
3. 自本告知发布之日起，新申请认证企业统一执行 ISO/IEC 27701:2025 新版标准，不再受理 2019 版认证申请。

三、获证客户转版核心工作要求

为确保各获证客户按期完成转版，确保认证资格持续有效，请各获证企业严格落实以下工作：

1. 开展新版标准差距评估

全面对照 2025 版标准条款，梳理现有 2019 版 PIMS 体系在架构、管理制度、控制措施、风险管控、合规映射等方面的差距，形成正式差距分析报告，制定专项转版整改方案与时间规划。重点核查 AI 数据处理、跨境数据传输、敏感个人信息（生物识别、健康数据）保护等新增管控场景的落地情况。

2. 全面修订体系文件

依据 HLS 高阶架构重构隐私管理体系文件，更新隐私方针、岗位职责、全生命周期个人信息处理流程、隐私风险管理制度；重新映射新版四大类控制措施，完善 PII 清单、PIA 隐私影响评估报告、合规对照表等必备文件，编制新版适用性声明（SOA）。

3. 完善新型场景风险管控

针对新版标准新增要求，补齐 AI 隐私保护、自动化决策公平性管控、跨境数据合规、隐私增强技术应用、供应链隐私管控等专项机制；整改大数据杀熟、APP 过度索权、后台静默收集信息、算法不透明等违规问题，落实隐私设计（Privacy by Design）全生命周期保护原则。

4. 开展全员培训与内部审核

组织管理层、合规人员、技术人员、业务人员开展新版标准专项培训，明确新版管控要求及岗位职责；完成新版体系全覆盖内部审核及管理评审，验证体系有效性，闭环整改所有不符合项，确保体系稳定运行满 3 个月以上。

5. 按期完成转版审核换证

建议各企业与我公司客户服务人员保持联系，优先在 2028 年 10 月过渡期截止前完成转版审核换证，避免证书失效影响企业招投标、资质审核、业务合作及跨境合规经营。

