奥邦检验认证集团有限公司企业标准

CTS_ABG 67018-2024

公有云中个人身份信息保护管理体系 要求

Information Security technology -
Protection of personally identifiable information (PII) in public clouds management systems - Requirements

2024-06-28 发布　　2024-06-28 实施

奥邦检验认证集团有限公司发布

目录

前言

本文件按照 GB/T1.1—2020《标准化工作导则第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件规定了在公有云环境下建立、实施、维护和持续改进个人身份信息保护管理体系的要求。其目的在于帮助组织确保公有云中个人身份信息（PII）的保密性、完整性和可用性，满足相关法律法规及利益相关方对 PII 保护的期望。

本标准的制定参考了 ISO/IEC 27018:2019 等国际标准，并结合了国内公有云应用的实际情况和需求。

随着云计算技术的广泛应用，公有云在为组织和个人带来便捷的同时，也引发了对个人身份信息安全和隐私保护的担忧。个人身份信息包括但不限于身份证号、姓名、联系方式、医疗记录等敏感数据。建立有效的公有云个人身份信息保护管理体系，对于增强用户信任、提升组织竞争力以及满足合规要求至关重要。

本文件由奥邦检验认证集团有限公司技术部提出并起草。

本文件主要起草人：袁海、邵优良。

本文件由奥邦检验认证集团有限公司 2024 年 06 月 28 日批准发布。

本文件自 2024 年 06 月 28 日起实施。

本文件由奥邦检验认证集团有限公司负责解释。

公有云中个人身份信息保护管理体系 要求

1.范围

本标准适用于所有在公有云中处理个人身份信息的组织，无论其规模大小、行业类型。它规定了建立、实施、维护和持续改进个人身份信息保护管理体系的通用要求，包括体系规划、风险评估与处置、控制措施实施、监控与评审等方面。

组织可根据自身业务特点和风险状况，对本标准的要求进行适当剪裁，但不得排除对 PII 保护有实质性影响的核心要求。

2.规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

ISO/IEC 27001《信息安全、网络安全和隐私保护 信息安全管理体系 要求》

ISO/IEC 27018《信息技术-安全技术 个人身份信息处理者在公共云中保护 PII 的实施指南》

3.术语和定义

本标准采用 ISO/IEC 27000 中界定的以及下列术语和定义。

3.1 个人身份信息（PII）：任何可以单独或与其他信息结合，用于识别特定自然人身份的信息。

3.2 公有云：通过互联网向公众提供云计算服务的平台，多个客户共享云服务提供商的基础设施。

3.3PII 处理器：代表 PII 控制者处理 PII 的组织或个人。

4.组织环境

4.1 理解组织及其环境

组织应确定与公有云 PII 保护相关的内部和外部因素，包括但不限于：

- 适用的法律法规、行业标准和监管要求；
- 组织的业务目标、战略和文化；
- 公有云服务提供商的信誉、服务水平和安全能力；
- 技术发展趋势，特别是与云安全和 PII 保护相关的技术。

4.2 理解相关方的需求和期望

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。