奥邦检验认证集团有限公司企业标准

CTS_ABG 69151-2024

个人身份信息保护管理体系 要求

Personally identifiable information protection management system - 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

本标准按照 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。

本标准规定了组织建立、实施、维护和持续改进个人身份信息保护管理体系的要求，旨在帮助组织确保个人身份信息（PII）在整个生命周期内的保密性、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，降低数据泄露风险，提升组织信誉。

本标准的制定参考了 GB/T 35273-2020《信息安全技术 个人信息安全规范》、ISO/IEC 29151:2017《信息技术 安全技术 个人身份信息保护实践指南》等国内外相关标准，并结合了我国个人信息保护的实际情况和行业最佳实践。

本标准基于风险管理的理念，要求组织识别、评估和应对与 PII 相关的风险，通过制定和执行一系列控制措施，实现对 PII 全生命周期的有效管理，确保组织在处理 PII 时遵循合法、正当、必要的原则。

随着数字化进程的加速，个人身份信息在各类业务活动中的应用日益广泛，其安全保护面临着严峻挑战。个人身份信息不仅关乎个人隐私和权益，还对社会稳定和经济发展具有重要影响。建立健全的个人身份信息保护管理体系，是组织履行社会责任、提升竞争力的必然要求。

本标准主要起草人：袁海、邵优良。

本标准由奥邦检验认证集团有限公司 2024 年 06 月 28 日批准发布。

本标准自 2024 年 06 月 28 日发布之日起起实施。

本标准由奥邦检验认证集团有限公司解释。

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业务活动中处理个人身份信息的组织，无论其规模大小、行业类型和所有制形式。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，旨在为组织提供一套系统化、规范化的 PII 保护管理方法。

组织可根据自身业务特点、PII 处理规模和风险状况，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，以确保满足法律法规和相关方对 PII 保护的基本期望。

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。

GB/T 29246-2023《信息安全技术 信息安全管理体系 概述和词汇》

GB/T 35273-2020《信息安全技术 个人信息安全规范》

ISO/IEC 29151:2017《信息技术 安全技术 个人身份信息保护实施指南》

3.术语和定义

本标准采用 GB/T 29246-2023、GB/T 35273-2020、ISO/IEC 29100 和 ISO/IEC 29151:2017 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，如姓名、身份证号码、联系方式、生物识别信息等。

3.2PII 控制者：决定 PII 处理目的和方式的组织或个人。

3.3PII 处理：对 PII 进行的任何操作或一组操作，如收集、存储、使用、共享、转让、公开披露、删除等。

3.4 风险评估：对 PII 处理过程中面临的威胁、脆弱性以及可能造成的影响进行分析，确定风险等级的过程。

3.5 控制措施：用于降低风险、保护 PII 安全的技术、管理和操作方法。

4.组织环境

4.1 理解组织及其环境

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。