**企业个人信息保护合规管理体系 指南**

**编制说明**

（征求意见稿）

中国信息通信研究院

2024年2月

**一、标准“范围”的内容**

本文件规定了企业建立、实施、评估、维护及改进个人信息保护合规管理体系的总体指南。

本文件适用于开展个人信息保护合规管理相关工作的企业。

**二、工作简况，主要包括:任务来源、主要工作过程、各起草单位和起草人及其在起草标准过程中所承担的工作等情况、对标准草案进行会议讨论范围、征求意见的范围、审查的范围**

本文件由中国信息通信研究院作为牵头单位起草。

参加单位为南京苏宁易付宝网络科技有限公司、南京领行科技股份有限公司、广东小天才科技有限公司、新汽有限公司、北京小米移动软件有限公司、重庆首讯科技股份有限公司、中国联合网络通信集团有限公司、国家市场监督管理总局竞争政策与评估中心、金杜律师事务所、北京世辉律师事务所、北京雷腾律师事务所。

本文件主要起草人：李文宇、张夕夜、林中天、程晓蕾、陈慧、卢启祯、谷中宝、金诚、张强、罗浏虎、汪浩、胡尚文、方禹、王新锐、王军义、李辉 。

本文件于2023年11月9日在中国互联网协会通过立项；随后，起草组成员对多家企业个人信息保护合规管理体系进行了调研，针对标准拟制定条款进行了深入的讨论形成了征求意见稿并上传至协会网站。

**三、标准编制原则和确定标准主要内容(如技术指标、参数、公式、性能要求、试验方法、检验规则等)的依据(包括试验、统计数据)**

本文件遵循规范性、先进性与可操作性相结合的原则。一是标准编制严格遵循GB/T1.1-2009《标准化工作导则 第1部分:标准的结构和编写》及相关法律法规的要求进行；二是标准反映个人信息保护合规管理体系建设的先进技术水平，标准研制过程中持续关注国内外行业动态，及时捕捉个人信息保护技术、合规管理技术和工具的发展趋势；三是在标准的研制过程中，充分考虑标准的实施难度和操作便利性，确保标准能够在各种场景下得到有效应用。

本文件参考GB/T 35273-2020《信息安全技术 个人信息安全规范》及GB/T 35770-2022《合规管理体系 要求及使用指南》的一般规则，提供了关于企业个人信息保护合规管理体系所处环境、机构职责、运行机制、保障机制识别与建设的基本指南，增加了企业个人信息保护合规义务清单、企业个人信息保护合规义务履行等方面的指导和建议。

**四、主要试验(或验证)的分析、综述报告**

《个人信息保护法》首次从法律层面明确提出加强互联网平台个人信息保护义务的要求，其中第五十八条规定提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应按照国家规定建立健全个人信息保护合规制度体系。对于个人信息处理者而言，尤其是提供重要互联网平台服务的企业，健全的个人信息保护合规管理体系建设既是企业管理的重要内容，也是确保个人信息保护合规工作得以有效执行的基础。本文件起草过程中，对多家企业个人信息保护合规管理情况进行调研，并进行多轮专家论证，证实建立个人信息保护专项合规管理体系，有助于企业健全个人信息保护合规风险管理框架，实现对专项合规风险有效识别和管理，促进全面的风险管理体系建设，并确保组织个人信息保护工作依法合规进行。

本文件旨在从企业合规管理的角度细化并落实个人信息保护的义务和要求，助力企业开展个人信息保护合规管理工作。企业建立个人信息保护合规管理体系宜设立专门的个人信息保护机构，明确各级别的责任和职能，以及制定相应的政策和程序。通过构建组织体系，确保有明确的责任主体和执行主体，使得个人信息保护工作能够自上而下得到贯彻实施。同时，通过建立完全的运行机制，明确各项操作的具体步骤、操作规范和监督机制，以确保个人信息的处理活动符合法律法规的要求，并在整个处理过程中对个人信息的安全性进行严格控制。最后，保障机制为个人信息保护提供必要的人力、物力、财力等资源支持，包括对员工的个人信息保护培训和教育、个人信息保护合规咨询机制、信息化系统建设等。

**五、标准在起草过程中遇到的问题及解决办法；重大分歧意见的处理经过和依据；有无重要技术问题需要说明**

在本文件的修订过程中，无重大分歧意见和技术问题。

**六、与国外标准的关系：包括：采用国际标准和国外先进标准的程度，与国外标准主要技术内容的差异**

该项目没有完全对应的国际标准或国外先进标准。

**七、修订标准时，说明与标准前一版本的重大技术变化，并列出所涉及的新、旧版本的有关章条(可引用标准前言的内容)；废止/代替现行有关标准的建议**

本文件为制定标准，非修订标准。

1. **八、说明标准与其他标准或文件的关系(可引用标准前言的内容)，特别是与有关的现行法律、法规和强制性国家标准的关系**

国际：国际标准化组织（ISO）于2012年10月，成立项目委员会ISO/PC 271，制定了ISO 19600《合规管理体系——指南》国际标准。2018年11月，ISO启动了修订工作，并于2020年11月完成修订工作，发布ISO 37301：2020《合规管理体系 要求及使用指南》。

国内：我国于2020年启动ISO 37301：2020《合规管理体系 要求及使用指南》国际标准同等转化的工作，并于2022年发布GB/T 35770-2022《合规管理体系要求及使用指南》。整体而言，GB/T 35770-2022标准仅对企业合规管理体系的实施、评估、维护和改善提供了指导，而对企业个人信息保护专项合规管理体系建设，未提供特别说明或指导。而GB/T 35273-2020《信息安全技术—个人信息安全规范》规定了开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动应遵循的原则和安全要求，未涉及个人信息保护合规管理体系建设的相关内容或要求。

目前国内尚无企业个人信息保护合规管理体系的相关标准。

**九、标准作为强制性标准或推荐性标准的建议**

建议本文件作为推荐性行业标准。

**十、贯彻国家标准的要求和措施建议(包括组织措施、技术措施、过渡办法等内容)；标准发布后，对国内外业界可能产生的影响**

建议本文件作为推荐性团体标准发布实施，指导相关企业建立、实施、评估、维护及改进个人信息保护合规管理体系，同时为行业内企业提供统一的规范和参考，引导企业向着更加规范、健康的方向发展。

**十一、标准是否涉及知识产权的情况说明；如标准中含有自主知识产权，说明产品研发程度、产业化基础及进程**

本文件未涉及。

**十二、其他应予说明的事项**

本文件未涉及。