国家标准《数据安全技术 个人信息安全规范》（征求意见稿）编制说明

一、工作简况

1.1 任务来源

为支撑《个人信息保护法》《网络数据安全管理条例》《个人信息保护合规审计办法》等法律法规落地实施，提升标准在个人信息保护工作中的指导性和实用性，为个人信息安全提供更全面的保障，修订 GB/T 35273-2020《信息安全技术个人信息安全规范》，根据《个人信息保护法》等法律法规最新要求，吸纳主管监管部门开展个人信息保护工作中的相关经验，与现行法律法规配套衔接。全国网络安全标准化技术委员会于 2025 年 8 月 22 日立项《数据安全技术 个人信息安全规范》国家标准制定项目，根据国家标准化管理委员会 2026 年下达的国家标准制修订计划，《数据安全技术 个人信息安全规范》由中国电子技术标准化研究院负责承办，计划号：20260700-T-469。该标准由中国电子技术标准化研究院牵头，并联合北京理工大学、赛西（深圳）电子信息产品标准化工程中心有限公司、中央网信办（国家网信办）数据与技术保障中心、国家信息技术安全研究中心、中国网络安全审查认证和市场监管大数据中心、华为技术有限公司、荣耀终端股份有限公司、中兴通讯股份有限公司、蚂蚁科技集团股份有限公司、北京抖音信息服务有限公司、深圳市腾讯计算机系统有限公司、北京三快科技有限公司、北京快手科技有限公司、阿里巴巴（北京）软件服务有限公司、国网江苏省电力有限公司信息通信分公司、北京小桔科技集团有限公司、中国联合网络通信集团有限公司、杭州萤石软件有限公司、西安交通大学、唯品会（中国）有限公司、阿里云计算有限公司、腾讯云计算（北京）有限责任公司、北京抖音科技有限公司等单位共同编制。

标准主要起草人：姚相振、洪延青、高超、胡影、郝春亮、刘行、何延哲、国震寰、高月、杨韬、刘曦泽、魏昊、张敏、衣强、郑云文、闫金保、赵晓娜、梅傲婷、白晓媛、李海英、李昳婧、马硕、张亚男、武杨、朱玲凤、田喜清、落红卫、王昕、顾伟、刘艾婧、赵新建、张颂、李媛、黄如鑫、胡文慧、孙艺、郑鸿咚、范铭、罗丹、黄天宁、刘阳璐、杨骁涵等。

标准工作组成员中姚相振负责《数据安全技术 个人信息安全规范》国家标准文稿和项目进展整体把关；洪延青、胡影负责标准第 5 章个人信息处理合法性基础、第 11 章海外法律管辖判定与冲突处理、附录 D 合法性依据示例场景，白晓媛、李海英、李昳婧、马硕、杨骁涵、李媛、黄如鑫参与第 5 章，魏昊、张敏、梅傲婷、张亚男、武杨、刘阳璐参与第 11 章；高超负责标准第 6 章个人信息的收集、第 8 章个人信息的使用，郑鸿咚、范铭参与第 6 章，朱玲凤、田喜清、落红卫、王昕参与第 8 章；刘行负责标准第 7 章个人信息的存储、第 10 章个人信息的委托处理、提供、转移、公开，国震寰、高月参与第 7 章，杨韬、刘曦泽参与第 10 章；郝春亮负责标准第 9 章个人信息的使用、附录 A 个人信息示例、附录 B 敏感个人信息判定，衣强、郑云飞、闫金保、赵晓娜、赵新建、张颂参与第 9 章、附录 A；何延哲负责标准第 12 章个人信息安全事件处置、第 13 章组织的个人信息安全管理要求，顾伟、刘艾婧、胡文慧、孙艺参与第 12 章，罗丹、黄天宁参与第 13 章。

1.2 制定背景

近年来，随着 5G 技术的发展、人工智能和大数据等新技术的广泛应用，个人信息、个人信息处理活动面临着新的挑战和问题。本标准针对个人信息面临的安全问题，根据《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等相关法律，规范个人信息处理者在收集、存储、使用、加工、传输、提供、公开、删除等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄漏等乱象，最大程度地保障个人的合法权益和社会公共利益。

1.3 起草过程

2025 年 04 月 8 日，成立标准申报项目组，开展基本情况研究；

2025 年 05 月 31 日，在标准周汇报标准编制情况，听取大数据组成员单位专家意见，会后按照专家意见修改，形成第二版标准草案；

2025 年 08 月 19 日，召开编制组研讨会，初步确定标准范围及内容，形成第一版标准草案；

2025 年 08 月 22 日，通过安标委立项；

2025 年 09 月 23 日，公开征集标准参编单位，100 余家相关企事业单位申请

加入标准编制组；

2026 年 4 月 1 日，在安标委标准周上汇报标准工作进展，通过 WG8 工作组评审，修改完善后转为征求意见稿。

2026 年 4 月 29 日，通过安标委组织的征求意见稿专家审查会，专家组同意通过对该项标准的审查，建议编制工作组根据本次会议意见修改后，发起公开征求意见。

二、标准编制原则、主要内容及其确定依据

2.1 标准编制原则

本标准在编制过程中遵循了问题导向原则、协调性原则。

本标准旨在支撑《个人信息保护法》《网络数据安全管理条例》《个人信息保护合规审计办法》等法律法规落地实施，提升标准在个人信息保护工作中的指导性和实用性，为个人信息安全提供更全面的保障。

本标准与现行相关标准相协调，确保标准间相互协调，避免重复和不必要的差异。

2.2 主要内容及其确定依据

本标准规范了开展收集、存储、使用、加工、传输、提供、公开、删除等个人信息处理活动应遵循的原则和安全要求。适用于规范各类组织个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。主要内容包括：

（1）本标准规范了开展收集、存储、使用、加工、传输、提供、公开、删除等个人信息处理活动应遵循的原则和安全要求。

（2）本标准落实《个人信息保护法》等相关法律法规要求，按照收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动生命周期调整标准文本。

2.3 修订前后技术内容的对比[适用于国家标准修订项目]

本标准代替 GB/T 35273-2020《信息安全技术 个人信息安全规范》，与 GB/T 35273-2020 相比，主要技术变化如下：

——修改了“敏感个人信息”（见 3.2）；

——增加了“单独同意”（见 3.8）；

——增加了“保证质量原则”（见 4）；

——增加了“个人信息处理合法性基础”（见 5）；

——增加了“敏感个人信息的收集”（见 6.6）；

——增加了“人工智能类产品或服务的收集”（见 6.7）；

——增加了“终端类产品或服务的收集”（见 6.8）；

——增加了“统一账号体现的使用”（见 8.6）；

——增加了“海外法律管辖判定与冲突处理”（见 11）；

——增加了“个人信息保护负责人”（见 13.1）；

——增加了“个人信息保护工作机构与人员”（见 13.2）；

——增加了“个人信息保护合规审计”（见 13.8）。

三、试验验证的分析、综述报告，技术经济论证，预期的经济效益、社会效益和生态效益

3.1 试验验证的分析、综述报告

本标准在编制过程中充分调研了国内外相关隐私保护工作的开展情况，包括国内信息系统审计、商业银行内部审计，美国联邦信息系统控制审计，国际服务性机构控制体系鉴证（SOC），欧洲数据保护主管（EDPS）的数据保护审计，英国 ICO 数据保护审计，法国 CNIL 数据合规审计，德国 BfDI 数据保护审计等，充分吸收现有成熟的要求和方法等。标准编制组包含了开展个人信息保护工作的专业机构、专业研究审计工作的高校以及掌握大量个人信息的个人信息处理者，为标准编制提供了广泛的意见建议和工作经验。

本标准编制过程中构建了国际对标、国内实践的调研体系：国际层面系统梳理欧盟 GDPR 实施细则、美国 NIST 隐私框架、ISO/IEC 27701 隐私信息管理体系等国际规范的核心要求，吸收其在个人信息全生命周期保护中的成熟方法论。标准编制组汇聚科研院校、互联网企业及第三方检测机构等单位，确保标准要求与行业实际需求高度适配。

3.2 技术经济论证

本标准的技术经济价值主要体现在提升个人信息保护水平、提高个人信息保护工作效率、促进个人信息合法合规利用等方面。个人信息处理者可以依据该标准开展个人信息保护工作。

3.3 预期的经济效益、社会效益和生态效益

个人信息处理者可以通过检测、评估、认证对其个人信息安全措施、个人信息保护能力进行验证，为个人信息处理者、监管机构、科研院所提供了重要参考。

制定本标准有利于规范个人信息保护工作，同时为个人信息处理者开展个人信息保护能力建设提供思路和参考，及时发现个人信息处理活动的安全问题和合规风险，促进个人信息合理利用，督促个人信息处理者及时进行整改，规范个人信息处理活动。

通过该标准的实施应用，提升各行业领域个人信息处理者的个人信息保护合规水平，降低个人信息安全事件的发生，减少因个人信息泄露、违规使用等给个人和企业带来的经济损失。

四、与国际、国外同类标准技术内容的对比情况，或者与测试的国外样品、样机的有关数据对比情况

2016年4月14日，欧盟发布了通用数据保护条例（General Data Protection Regulation，GDPR），旨在保护欧盟境内所有公民的数据隐私，规范企业对于个人数据的收集、存储、处理和传输行为。

2018年6月28日，美国加利福尼亚州发布了《加州消费者隐私法案》（CCPA），该法案是一项数据隐私立法，适用于处理加州居民个人数据的大多数企业。该法案中“个人信息”指直接或间接识别、涉及、描述特定消费者或家庭或者能够合理地与特定消费者或家庭相关联的信息。

2020年11月3日，美国政府颁布《美国数据隐私和保护法案》（ADPPA）。该法案规定了公司如何处理个人数据的要求，其中包括识别个人身份或与个人合理关联的信息。

五、以国际标准为基础的起草情况，以及是否合规引用或者采用国际国外标准，并说明未采用国际标准的原因

不涉及。

六、与有关法律、行政法规及相关标准的关系

2021年11月1日，《中华人民共和国个人信息保护法》正式施行，《个人信息保护法》内容具有系统性、针对性强和可操作性特点，规范了个人信息处理活动，明确了组织的法律责任和义务，为个人信息保护提供了强有力的法律保障。

2024 年 9 月 24 日，《网络数据安全管理条例》正式发布，《条例》重点细化了《个人信息保护法》关于告知、同意、个人行使权利等方面的规定。一是明确通过制定个人信息处理规则履行告知义务的内容、形式等要求。二是明确基于个人同意处理个人信息应当遵守的基本要求。三是明确行使个人信息查阅、复制、更正、补充、删除等权利的要求，细化个人信息转移的具体条件。四是明确按照《中华人民共和国个人信息保护法》第五十三条规定在境内设立专门机构或者指定代表的要求。五是明确网络数据处理者处理 1000 万人以上个人信息还应当履行的义务。

2025 年 2 月 14 日，中央网信办发布的《个人信息保护合规审计管理办法》对个人信息保护合规审计活动的开展、合规审计机构的选择、合规审计的频次、个人信息处理者和专业机构在合规审计中的义务等作出细化规定，旨在为个人信息处理者开展个人信息保护合规审计提供系统性、针对性、可操作性的规范，提升个人信息处理活动合法合规水平，保护个人信息权益。

七、重大分歧意见的处理经过和依据

无。

八、涉及专利的有关说明

无。

九、实施国家标准的要求，以及组织措施、技术措施、过渡期和实施日期的建议等措施建议

建议个人信息处理者按照本标准开展个人信息保护工作，对本组织的个人信息保护能力进行建设，提升组织的个人信息保护能力。

十、其他应当说明的事项

我单位已按照公平竞争审查表中各项内容进行了逐项审查，从市场准入与退出、商品要素自由流动、生产经营成本、生产经营行为等方面逐项开展审查，未发现有内容存在排除、限制市场竞争的情形，符合公平竞争要求。

《数据安全技术 个人信息安全规范》标准编制组

2026 年 5 月 8 日