

个人信息保护国家标准体系（2025 版）

全国网络安全标准化技术委员会秘书处

2025 年 9 月

前 言

根据中央网信办、原国家质检总局、国家标准委联合印发的《关于加强国家网络安全标准化工作的若干意见》（中网办发文〔2016〕5号）（简称《若干意见》）规定，经中央网络安全和信息化领导小组同意，建立统一权威的网络安全国家标准工作机制，全国信息安全标准化技术委员会（简称“信安标委”或“TC260”）在国家标准委的领导下，在中央网信办的统筹协调和有关网络安全主管部门的支持下，对网络安全国家标准进行统一技术归口，统一组织申报、送审和报批。《若干意见》同时指出，信安标委要持续完善网络安全标准体系，加快开展关键信息基础设施保护、数据安全、个人信息保护、关键信息技术产品等领域的标准研究和制定工作。2024年，为贯彻落实中央网络安全和信息化工作会议关于构建大网络安全工作格局的要求，在信安标委基础上组建全国网络安全标准化技术委员会（简称“网安标委”），网络安全国家标准化工作统筹协调机制进一步加强。

近年来，随着《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规相继出台，我国数据安全政策法规体系日趋完善，对数据安全标准化工作提出更高要求。《中华人民共和国数据安全法》明确提出“国家推进数据开发利用技术和数据安全标准体系建设”，体现了开展数据安全标准体系建设工作的重要性。

数据安全作为《若干意见》的重点任务方向，网安标委

一直高度重视数据安全标准研究和制定工作。2016 年，为支撑国家大数据发展行动纲要等国家战略需求，网安标委成立“大数据安全标准特别工作组”（SWG-BDS），开始研制数据安全和个人信息保护国家标准。2024 年，该工作组更名为“数据安全标准工作组”（WG8），并报国标委同意，新增“数据安全技术”开头的标准名称，用于标识数据安全、个人信息保护国家标准。截至 2025 年 8 月，网安标委在数据安全和个人信息保护领域已制定发布 44 项国家标准，正在制修订 2 项强制性国家标准和 16 项推荐性国家标准，同时配套研制发布 3 项委员会技术文件¹和 21 项网络安全标准实践指南²，初步构建了数据安全和个人信息保护标准体系，为支撑数据安全政策法规落地实施、护航产业数字化转型提供了安全规范。

为积极适应新形势新要求，更好发挥数据安全标准化工作的基础性、规范性、引领性作用，网安标委秘书处在梳理数据安全国家标准研制现状、分析数据安全标准需求的基础上，遵循标准体系建设客观规律，按照国家标准 GB/T 13016-2018《标准体系构建原则和要求》，组织编制了《数据安全国家标准体系（2025 版）》《个人信息保护国家标准（2025 版）》，以更好指导下一步数据安全和个人信息保护国家标准研制，为有效保障数据安全、促进数字经济高质量发展提供安全标准依据。

¹ 委员会技术文件是指围绕国家网络安全监管急需、迭代快速、创新活跃的技术应用领域，由网安标委组织编制和发布的指南类文件，旨在引导网络安全技术、产业发展。

² 网络安全标准实践指南是网安标委秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

目 录

前言	I
一、 标准体系编制原则	1
二、 标准体系思路和框架	2
三、 标准体系主要内容	5
(一) 基础共性标准	5
(二) 个人信息保护技术标准	6
(三) 个人信息保护管理与权益保障标准	7
(四) 个人信息保护测评和认证标准	8
(五) 产品和服务个人信息保护标准	9
(六) 行业与应用个人信息保护标准	11
四、 下一步标准化工作建议	13
附件 1 现有个人信息保护标准文件	14

一、标准体系编制原则

以习近平新时代中国特色社会主义思想为指导，全面贯彻落实党的二十大和二十届二中、三中全会精神，坚持网络安全为人民、网络安全靠人民，深入落实《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》《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》《国家标准化发展纲要》等法律法规和政策文件要求，建立健全个人信息保护国家标准体系，加快弥补关键基础标准短板，强化重点急需标准供给，着力推动标准实施应用和国际标准化工作，保护公民个人信息权益，规范个人信息处理活动，促进个人信息合理利用。

（一）统筹规划，全面布局。统筹高质量发展和高水平安全，全面梳理政策法规、产业发展、安全风险等方面的标准需求，以标准“快、优、强”为导向，以满足个人信息保护管理需求、提升个人信息保护合规水平、促进个人信息合理利用为目标，开展个人信息保护标准分类分级管理，建立健全支撑个人信息保护政策法规落地、规范引导产业个人信息处理活动、保障公民个人信息权益的个人信息保护国家标准体系。

（二）基础先立，急用先行。聚焦个人信息保护重点工作和技术产业发展需要，加快制修订个人信息处理安全、敏感个人信息、个人信息保护技术、个人信息保护管理和权益保障等基础通用标准；同时，重点考虑亟待解决的产业高质量发展难题和个人信息保护突出问题，结合不同行业领域和新技术新应用的标准需求，加强个人信息保护标准和实践指南供给，推进

重点急需标准研制。

(三) 注重实效，开放兼容。健全完善标准制修订、试点验证、宣贯培训、应用推广、实施评价等标准化工作机制，持续强化标准影响力、不断提升标准应用效果；坚持标准高水平开放发展，积极开展国际交流合作，加强隐私保护和消费者隐私设计领域的国际标准化工作，主动对接国际高标准经贸规则，推动具有我国先进技术成果的标准“走出去”，并促进实施效果好、应用广泛的国际标准在我国落地应用。

二、标准体系思路和框架

依据《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》等个人信息保护政策法规，综合考虑个人信息保护在监督管理、产业规范、问题风险、技术发展、国际接轨等方面的标准化需求，建立健全个人信息保护国家标准体系。该体系在数据安全国家标准体系的基础上，以个人信息权益保护为核心，涉及与个人信息紧密相关的组织、产品、服务、系统、活动、技术、管理等标准化对象，涵盖个人信息收集、存储、使用、加工、传输、提供、公开、删除等处理活动，保障个人信息的知情权、决定权、限制处理、拒绝处理等权利。

个人信息保护国家标准体系由基础共性、个人信息保护技术、个人信息保护管理与权益保障、个人信息保护测评和认证、产品和服务个人信息保护、行业与应用个人信息保护六大类标准组成，如图 1 所示。其中，基础共性标准作为个人信息保护标准体系的基础，为标准体系中其他部分提供支撑；个人信息保护技术标准用于明确个人信息保护技术的框架、规范和指南；

个人信息保护管理与权益保障标准用于明确个人信息保护管理相关内容，给出个人信息主体权益保障的要求、方法和指南；个人信息保护测评和认证标准用于规范个人信息保护的检测评估、合规审计、安全认证等工作；产品和服务个人信息保护标准在基础共性、个人信息保护技术、个人信息保护管理与权益保障标准之上，用于明确移动应用、网络平台服务等典型产品和服务的个人信息保护要求和指南；行业与应用个人信息保护标准位于个人信息保护标准体系最上层，是在其他标准的基础上，面向重点行业领域和技术应用开展个人信息保护标准研制。



图1 个人信息保护国家标准体系框架

三、标准体系主要内容

(一) 基础共性标准

基础共性标准为个人信息处理一般规则、敏感个人信息处理规则及标准体系中其他部分提供基础支撑，包括术语、个人信息处理安全、敏感个人信息保护三个子类标准，如图2所示。

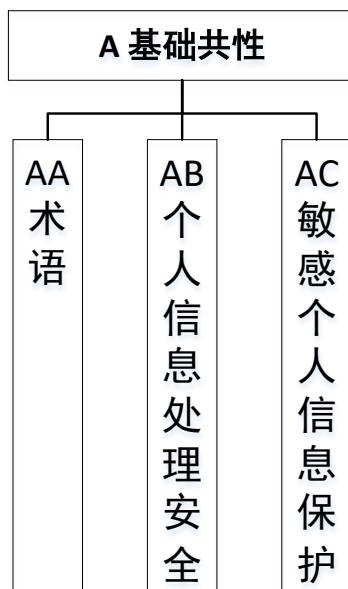


图2 基础共性标准

1. 术语

主要规范个人信息保护相关概念和术语定义，标准的术语定义应与个人信息保护法律法规政策的概念描述保持一致。

2. 个人信息处理安全

主要规定个人信息处理的原则和基本保护要求，给出个人信息的识别规则和方法等，为其他个人信息保护标准提供基础支撑。

3. 敏感个人信息保护

主要明确敏感个人信息识别和界定规则，规定敏感个人信息处理的通用安全要求、特定类型敏感个人信息的特殊处理要求等。

(二) 个人信息保护技术标准

个人信息保护技术标准主要明确个人信息保护的技术框架、规范和指南等，包括去标识化和匿名化、隐私工程与隐私设计、隐私增强技术三个子类标准，如图 3 所示。



图 3 个人信息保护技术标准

1. 去标识化和匿名化

主要围绕个人信息去标识化和匿名化，明确去标识化、匿名化的技术指南、效果评估、实施规范等。

2. 隐私工程与隐私设计

主要围绕隐私工程（Privacy Engineering，也称“个人信息安全工程”）与隐私设计（Privacy by Design），明确产品服务在需求、设计、开发、测试、发布等阶段的个人信息安

全工程化指南和评价方法，并结合典型产品服务的隐私设计需求，给出隐私设计要点和参考等。

3. 隐私增强技术

明确隐私增强技术（Privacy-Enhancing Technologies，简称 PETs）的指南、评估方法等，例如差分隐私、零知识证明等。

（三）个人信息保护管理与权益保障标准

个人信息保护管理与权益保障标准用于明确个人信息保护管理相关要求，给出个人信息主体权益保障的要求、方法和指南，包括个人信息保护管理、个人信息权益保障两个子类标准，如图 4 所示。

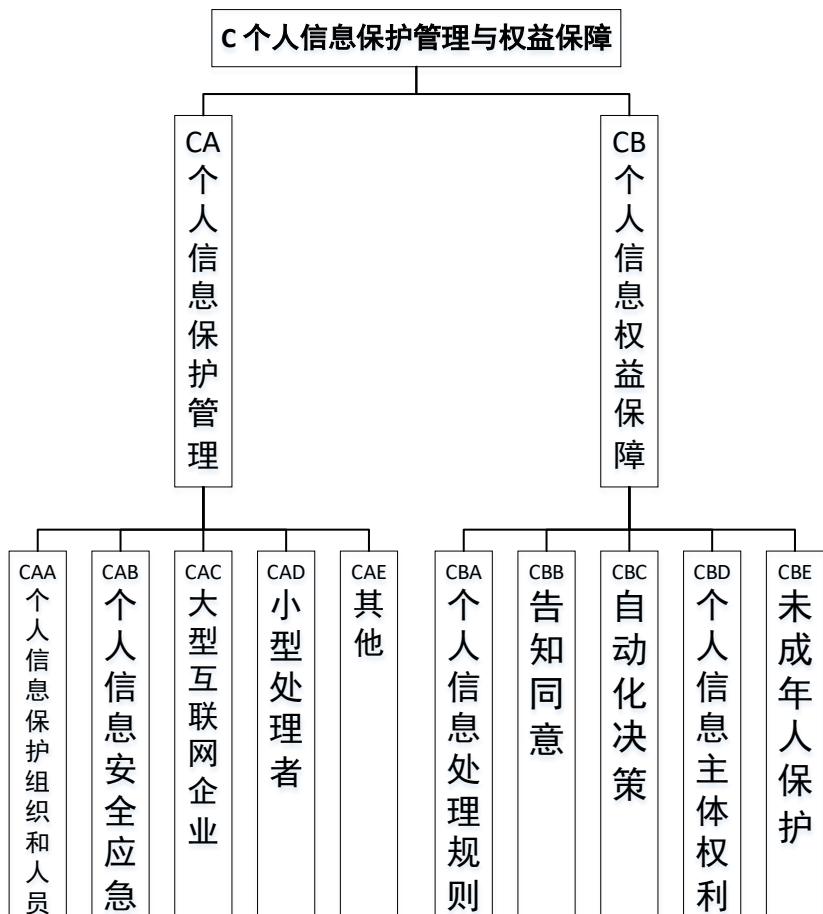


图 4 个人信息保护管理与权益保障标准

1. 个人信息保护管理

主要规定个人信息保护管理相关要求和指南，包括个人信息保护组织和人员、个人信息安全应急等管理标准，以及针对大型互联网企业、小型处理者等不同规模和类型的个人信息处理者的标准。

2. 个人信息权益保障

主要明确保障个人信息主体各项权益的要求和指南，包括个人信息处理规则（例如隐私政策）、告知同意、自动化决策、个人信息主体权利、未成年人保护等标准。

（四）个人信息保护测评和认证标准

个人信息保护测评和认证标准主要明确个人信息安全测评的相关评估方法、审计依据、认证依据等，包括影响评估、合规审计、应用检测、出境认证四个子类，如图 5 所示。

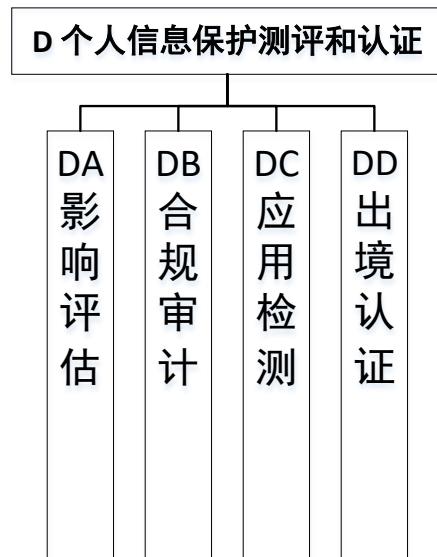


图 5 个人信息保护测评和认证标准

1. 影响评估

围绕个人信息保护影响评估，主要明确影响评估的基本原理、实施流程、评估方法等。

2. 合规审计

围绕个人信息保护合规审计，针对个人信息处理者自行开展合规审计、按照部门要求委托专业机构开展合规审计的工作需要，明确个人信息保护合规审计的基本原则、总体要求、实施流程、内容和方法、专业机构能力要求及相关配套实践指南等。

3. 应用检测

主要制定应用程序个人信息安全检测标准，明确检测流程、检测方法、判定规则等。

4. 出境认证

主要针对个人信息出境个人信息保护认证、粤港澳大湾区个人信息跨境安全互认的工作需求，明确认证的依据标准、评价指标等。

（五）产品和服务个人信息保护标准

产品和服务个人信息保护标准在基础共性、个人信息保护技术、个人信息保护管理与权益保障三类标准之上，聚焦产品和服务的个人信息保护违法违规问题，明确常见产品和服务的个人信息保护要求和指南，包括移动应用、云计算服务、网络平台服务、智能终端、线下消费场景、其他六个子类，如图 6 所示。



图 6 产品和服务个人信息保护标准

1. 移动应用

主要聚焦移动互联网应用生态的个人信息保护问题，明确移动互联网应用程序（App）、软件开发工具包（SDK）、应用商店、移动智能终端操作系统、移动智能终端预置应用等相关方的个人信息保护要求和指南。

2. 云计算服务

主要围绕公有云的个人信息保护需求，给出公有云个人信息保护指南，明确保护目标和措施等。

3. 网络平台服务

主要针对即时通信、快递物流、网上购物、网络支付、网络音视频、网络约车等典型网络平台服务，明确相关个人信息保护要求和指南。

4. 智能终端

主要针对智能穿戴、智能家居、学习终端、儿童手表等各类智能终端设备的个人信息保护需求，明确相关终端产品的个人信息处理规则、保护要求、测评方法和实践指南等。

5. 线下消费场景

主要针对收集个人信息的常见线下消费场景的个人信息保护需求，明确相关场景的个人信息处理规则、保护要求、测评方法和实践指南等，如自动售卖、扫码点餐、出行乘车、入场停车、商超支付、扫码充电、房屋租赁等场景。

6. 其他

明确上述类别之外的其他产品和服务的个人信息处理规则、保护要求和实践指南等。

（六）行业与应用个人信息保护标准

行业与应用个人信息保护标准位于个人信息保护国家标准体系最上层，是在其他个人信息保护标准的基础上，面向重点行业领域和技术应用开展个人信息保护标准研制，包括行业领域个人信息保护、技术应用个人信息保护两个子类，如图 7 所示。

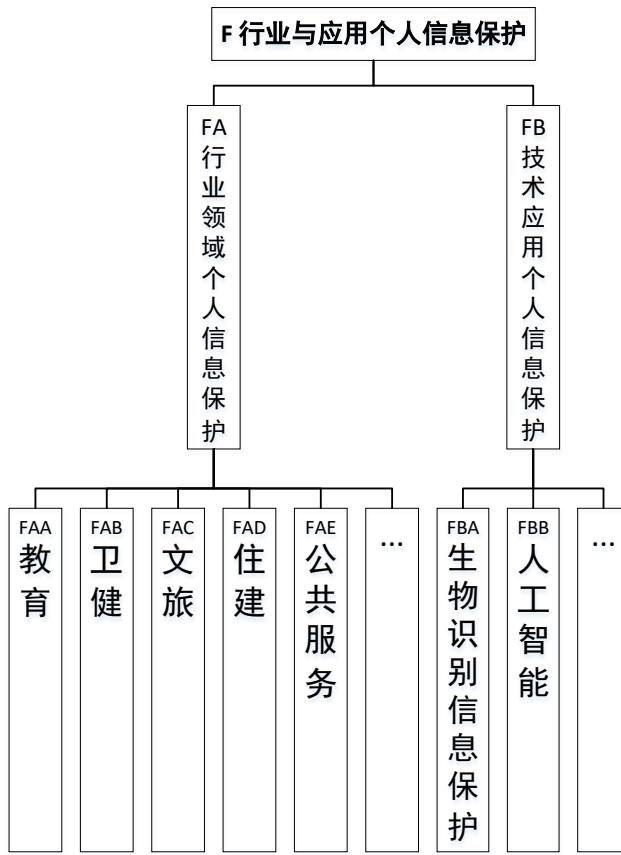


图 7 行业与应用个人信息保护标准

1. 行业领域个人信息保护

主要针对特定行业领域的个人信息保护需求，给出行业领域个人信息保护标准，如教育、卫健、文旅、住建、公共服务等。

2. 技术应用个人信息保护

主要聚焦技术应用的个人信息保护问题隐患，研制特定技术应用的个人信息保护标准，如生物识别信息（也称“生物特征识别信息”）保护、人工智能等。其中生物识别信息保护标准主要明确个人生物识别信息（包括人脸、指纹、声纹、步态、基因等）的个人信息处理规则和保护要求；人工智能标准主要针对人工智能应用中的个人信息保护需求，研制相关标准。

四、下一步标准化工作重点

一是按照法律法规政策要求、技术产业发展和个人权益保障需要，持续完善个人信息保护国家标准体系，逐步健全以国家标准为核心、技术文件和实践指南为配套、应用案例和研究报告为补充的多层体系。

二是针对个人信息保护的重点工作、突出问题和难点堵点，以标准“快、优、强”为目标，加快研制出台儿童手表安全技术要求等强制性国家标准，及个人信息保护合规审计、个人信息匿名化、未成年人个人信息保护、个人信息安全规范（修订）等标准。

三是加大个人信息保护标准供给，开展小型个人信息处理者、人工智能个人信息保护、个人信息保护公益诉讼、人脸识别数据安全等标准或实践指南制修订，同时结合行业领域和产品、服务、场景的个人信息保护标准需求，推进具有行业、产品、服务和场景特点的个人信息保护标准文件研制。

四是着力提升个人信息保护标准应用效果，持续开展网络安全标准贯标应用深度行、数安标准强“基”助“力”计划（DSEP）等活动，加强对个人信息安全规范、敏感个人信息处理、移动应用个人信息、生物识别信息保护等已发布标准的应用推广，建立配套重点标准实施的技术文件、实践指南和应用工具，构建个人信息保护国家标准应用实践案例库，深入重点行业领域和地方区域开展贯标应用。

附件1 现有个人信息保护标准文件

序号	标准/文件名称	标准号/计划号/ 文件编号	标准/文件类型	状态
A 基础共性				
AA 术语				
1	信息安全技术 术语	GB/T 25069-2022	推荐性国家标准	已发布
AB 个人信息处理安全				
2	信息安全技术 个人信息安全规范	GB/T 35273-2020	推荐性国家标准	修订中 (草案)
AC 敏感个人信息保护				
3	数据安全技术 敏感个人信息处理安全要求	GB/T 45574-2025	推荐性国家标准	已发布
4	网络安全标准实践指南—敏感个人信息识别指南	TC260-PG-20244A	网络安全标准实践指南	已发布
B 个人信息保护技术				
BA 去标识化和匿名化				
5	信息安全技术 个人信息去标识化指南	GB/T 37964-2019	推荐性国家标准	已发布
6	信息安全技术 个人信息去标识化效果评估指南	GB/T 42460-2023	推荐性国家标准	已发布
7	数据安全技术 个人信息匿名化处理指南及评价方法	20250864-T-469	推荐性国家标准	在研(征求意见稿)
BB 隐私工程与隐私设计				
8	信息安全技术 个人信息安全工程指南	GB/T 41817-2022	推荐性国家标准	已发布
BC 隐私增强技术				
C 个人信息保护管理与权益保障				
CA 个人信息保护管理				
CAA 个人信息保护组织和人员				
CAB 个人信息安全应急				
CAC 大型互联网企业				
9	数据安全技术 大型互联网企业内设个人信息保护监督机构要求	GB/T 45404-2025	推荐性国家标准	已发布
10	数据安全技术 数据安全和个人信息保护社会责任指南	GB/T 46071-2025	推荐性国家标准	已发布
CAD 小型处理器				
11	数据安全技术 小型个人信息处理器个人信息保护指南		推荐性国家标准	在研(草案)
CAE 其他				
CB 个人信息权益保障				

序号	标准/文件名称	标准号/计划号/ 文件编号	标准/文件类型	状态
CBA 个人信息处理规则				
12	数据安全技术 互联网平台及产品服务个人信息处理规则	GB/T 44588-2024	推荐性国家标准	已发布
CBB 告知同意				
13	信息安全技术 个人信息处理中告知和同意的实施指南	GB/T 42574-2023	推荐性国家标准	已发布
CBC 自动化决策				
14	数据安全技术 基于个人信息的自动化决策安全要求	GB/T 45392-2025	推荐性国家标准	已发布
CBD 个人信息主体权利				
15	数据安全技术 基于个人请求的个人信息转移要求	20242027-T-469	推荐性国家标准	在研(报 批稿)
CBE 未成年人保护				
16	数据安全技术 未成年人产品和服务个人信息保护要求	20251312-T-469	推荐性国家标准	在研(征 求意见 稿)
D 个人信息保护测评和认证				
DA 影响评估				
17	信息安全技术 个人信息安全影响评估指南	GB/T 39335-2020	推荐性国家标准	已发布
DB 合规审计				
18	数据安全技术 个人信息保护合规审计要求	20240896-T-469	推荐性国家标准	在研(报 批稿)
19	数据安全技术 个人信息保护合规审计专业机构服务能力要求		推荐性国家标准	在研(草 案)
20	网络安全标准实践指南个人信息保护合规审计 专业机构服务能力要求	TC260-PG-20254A	网络安全标准实践 指南	已发布
21	网络安全标准实践指南个人信息保护合规审计要求	TC260-PG-20255A	网络安全标准实践 指南	已发布
DC 应用检测				
22	信息安全技术 移动互联网应用程序(APP)个人信息安全测评规范	GB/T 42582-2023	推荐性国家标准	已发布
23	网络安全标准实践指南—移动互联网应用程序(App)收集使用个人信息自评估指南	TC260-PG-20202A	网络安全标准实践 指南	已发布
DD 出境认证				
24	数据安全技术 个人信息跨境处理活动安全认证要求	GB/T 46068-2025	推荐性国家标准	已发布

序号	标准/文件名称	标准号/计划号/ 文件编号	标准/文件类型	状态
25	网络安全标准实践指南—个人信息跨境处理活动安全认证规范（V2.0）	TC260-PG-20222A	网络安全标准实践指南	已发布
26	网络安全标准实践指南—粤港澳大湾区（内地、香港）个人信息跨境处理保护要求（V1.0）	TC260-PG-20245A	网络安全标准实践指南	已发布
E 产品和服务个人信息保护				
EA 移动应用				
EAA 移动互联网应用程序				
27	信息安全技术 移动互联网应用程序（App）收集个人信息基本要求	GB/T 41391-2022	推荐性国家标准	已发布
28	网络安全实践指南—移动互联网应用基本业务功能必要信息规范	TC260-PG-20191A	网络安全实践指南	已发布
29	网络安全标准实践指南—移动互联网应用程序（App）个人信息保护常见问题及处置指南	TC260-PG-20203A	网络安全实践指南	已发布
30	网络安全标准实践指南—移动互联网应用程序（App）系统权限申请使用指南	TC260-PG-20204A	网络安全实践指南	已发布
31	网络安全标准实践指南—摇一摇广告触发行为安全要求	TC260-PG-20256A	网络安全实践指南	已发布
EAB 软件开发工具包				
32	信息安全技术 移动互联网应用程序（App）软件开发工具包（SDK）安全要求	GB/T 43435-2023	推荐性国家标准	已发布
33	网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引	TC260-PG-20205A	网络安全实践指南	已发布
EAC 应用商店				
34	数据安全技术 应用商店的移动互联网应用程序（App）个人信息处理规范性审核与管理指南	GB/T 43739-2024	推荐性国家标准	已发布
EAD 移动智能终端操作系统				
35	数据安全技术 移动智能终端的移动互联网应用程序（App）个人信息处理活动管理指南	20220783-T-469	推荐性国家标准	在研（报批稿）
EAE 移动智能终端预置应用				
36	信息安全技术 移动智能终端预置应用软件基本安全要求	GB/T 43445-2023	推荐性国家标准	已发布

序号	标准/文件名称	标准号/计划号/ 文件编号	标准/文件类型	状态
37	智能手机预装应用程序分类指南	TC260-002	委员会技术文件	已发布
EB 云计算服务				
38	信息技术 安全技术 公有云中个人信息保护实践指南	GB/T 41574-2022	推荐性国家标准	已发布 (国际采标)
EC 网络平台服务				
39	信息安全技术 即时通信服务数据安全要求	GB/T 42012-2022	推荐性国家标准	已发布
40	信息安全技术 快递物流服务数据安全要求	GB/T 42013-2022	推荐性国家标准	已发布
41	信息安全技术 网上购物服务数据安全要求	GB/T 42014-2022	推荐性国家标准	已发布
42	信息安全技术 网络支付服务数据安全要求	GB/T 42015-2022	推荐性国家标准	已发布
43	信息安全技术 网络音视频服务数据安全要求	GB/T 42016-2022	推荐性国家标准	已发布
44	信息安全技术 网络预约汽车服务数据安全要求	GB/T 42017-2022	推荐性国家标准	已发布
ED 智能终端				
45	儿童手表安全技术要求	20243076-Q-339	强制性国家标准	在研(送审稿)
EE 线下消费场景				
46	网络安全标准实践指南—扫码点餐个人信息保护要求		网络安全实践指南	在研(征求意见稿)
EF 其他				
F 行业与应用个人信息保护				
FA 行业领域个人信息保护				
FAA 教育				
FAB 卫健				
FAC 文旅				
FAD 住建				
FAE 公共服务				
FB 技术应用个人信息保护				
FBA 生物识别信息保护				
47	信息安全技术 生物特征识别信息保护基本要求	GB/T 40660-2021	推荐性国家标准	已发布
48	信息安全技术 步态识别数据安全要求	GB/T 41773-2022	推荐性国家标准	已发布

序号	标准/文件名称	标准号/计划号/ 文件编号	标准/文件类型	状态
49	信息安全技术 基因识别数据安全要求	GB/T 41806-2022	推荐性国家标准	已发布
50	信息安全技术 声纹识别数据安全要求	GB/T 41807-2022	推荐性国家标准	已发布
51	信息安全技术 人脸识别数据安全要求	GB/T 41819-2022	推荐性国家标准	已发布
52	网络安全标准实践指南—人脸识别支付场景个人信息安全保护要求	TC260-PG-20251A	网络安全标准实践 指南	已发布
FBB 人工智能				