ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 敏感个人信息处理安全要求

Information security technology—Security requirements for processing of sensitive personal information

（征求意见稿）

（本稿完成时间：2023 年 8 月 8 日）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—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。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：中国电子技术标准化研究院、国家信息技术安全研究中心、中国科学院信息工程研究所、蚂蚁科技集团股份有限公司、北京抖音信息服务有限公司、北京快手科技有限公司、北京百度网讯科技有限公司、公安部第三研究所、北京交通大学、公安部第一研究所、西安交通大学、中国信息安全测评中心、中国科学院软件研究所、中国网络空间研究院、医渡云（北京）技术有限公司、北京小桔科技发展有限公司、北京华品博睿网络技术有限公司、阿里巴巴（中国）有限公司、深圳市腾讯计算机系统有限公司、成都卫士通信息产业股份有限公司、联想（北京）有限公司、北京汉华飞天信安科技有限公司、顺丰速运有限公司，中关村科学城城市大脑股份有限公司等。

本文件主要起草人：姚相振、胡影、陈舒、高超、上官晓丽、杨韬、李凤华、郝春亮、白晓媛、李昳婧、王昕、邓婷、于东升、王伟、李秋香、刘烃、关泰露、程文静、王彬、杨光、张严、田申、郭建领、黄天宁、徐永太、查海平、李汝鑫、蔡旭、姜伟、黎琳、徐起等。

信息安全技术　敏感个人信息处理安全要求

1　范围

本文件给出了敏感个人信息界定方法，规定了敏感个人信息处理安全要求。

本文件适用于规范个人信息处理者的敏感个人信息处理活动，也可为监管部门、第三方评估机构对个人信息处理者开展敏感个人信息处理活动进行监督、管理、评估提供参考。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022　信息安全技术 术语

GB/T 35273—2020　信息安全技术 个人信息安全规范

GB/T 37964—2019　信息安全技术 个人信息去标识化指南

GB/T 37988—2019　信息安全技术 数据安全能力成熟度模型

GB/T 39725—2020　信息安全技术 健康医疗数据安全指南

GB/T 39335—2020　信息安全技术 个人信息安全影响评估指南

3　术语和定义

GB/T 25069-2022、GB/T 35273—2020界定的以及下列术语和定义适用于本文件。

3.1

个人信息　personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

[来源：GB/T 35273—2020, 3.1，有修改]

3.2

敏感个人信息　sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

[来源：GB/T 35273—2020, 3.2，有修改]

3.3

个人信息处理者　personal information processor

自主决定处理目的、处理方式的组织、个人。

[来源：GB/T 35273—2020, 3.4，有修改]

3.4

个人信息主体 personal information subject

个人信息已识别或者可识别的自然人。

[来源：GB/T 35273—2020, 3.3，有修改]

3.5

个人信息处理活动 personal information processing activities

个人信息的收集、存储、使用、加工、传输、提供、公开、删除等活动。

3.6

特定身份信息 personal information of specific identities

对个人人格尊严和社会评价有重大影响的身份信息。

注：主要包括民族、种族、犯罪记录、残障人士身份信息、身份证件号码等。

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

5 敏感个人信息界定

5.1 敏感个人信息识别

a) 个人信息处理者在进行个人信息处理前，应按照以下方法识别敏感个人信息。

b) 符合以下任一属性的，应识别为敏感个人信息：

1) 个人信息遭到泄露或者非法使用，容易导致自然人的人格尊严受到侵害；

示例 1：个人信息主体可能会因特定身份、犯罪记录、宗教信仰、性取向、特定疾病和健康状态等信息泄露遭到歧视性待遇。

2) 个人信息遭到泄露或者非法使用，容易导致自然人的人身安全受到危害；

3) 个人信息遭到泄露或者非法使用，容易导致自然人的财产安全受到危害；

示例 2：泄露、非法使用金融账户信息及其相关的鉴别信息（如支付口令），可能会造成个人信息主体的财产损失。

c) 总体考虑个人信息汇聚融合后的整体属性，如汇聚融合的个人信息遭到泄露或者非法使用容易对个人权益造成较大影响的，应判断个人信息整体具有敏感个人信息属性。

5.2 常见敏感个人信息类别

常见敏感个人信息包括以下类别见附录 A。

a) 生物识别信息：对自然人的物理、生物或行为特征进行技术处理得到的、能够单独或者与其他信息结合识别该自然人身份的个人信息。

b) 宗教信仰信息：与信仰的宗教、宗教组织、宗教活动相关的信息。

c) 特定身份信息：对个人人格尊严和社会评价有重大影响的身份信息，特别是那些可能导致社会歧视的特定身份信息。

d) 医疗健康信息：与自然人的健康状况以及医疗就诊相关的信息。

e) 金融账户信息：与银行、证券等账户和交易相关的信息。

f) 行踪轨迹信息：与个人所处地理位置、活动地点和活动轨迹等相关的信息。

g） 身份鉴别信息：用于验证主体是否具有访问或使用权限的信息。例如登陆密码、支付密码、动态口令、口令保护答案等。

h） 未成年人个人信息：不满十四周岁未成年人的个人信息。

i） 其他敏感个人信息：除以上信息外，应作为敏感个人信息保护的信息。

6 敏感个人信息处理通用安全要求

6.1 敏感个人信息处理基本要求

处理敏感个人信息应具有特定的目的和充分的必要性，取得个人的单独同意，应在满足GB/T 35273—2020要求的基础上，在收集、存储、使用、加工、传输、提供、公开、删除等处理的各个环节采取严格保护措施。

6.2 收集必要性

个人信息处理者在收集敏感个人信息前，应遵守以下要求：

a） 收集非敏感个人信息可以实现处理目的的，不应收集敏感个人信息；

b） 应仅在个人信息主体使用业务功能期间，收集该业务功能所需的敏感个人信息；

c） 应按照业务功能或服务场景，分项收集敏感个人信息。

6.3 告知同意

6.3.1 告知

个人信息处理者在收集敏感个人信息前，应遵守以下要求：

a） 在收集敏感个人信息前，应采用增强形式向个人进行告知；

注 1：如通过单独弹窗、短信、填写框、动画、转至单独提示界面等方式告知个人信息主体。

b） 利用App持续收集敏感个人信息的，应提供持续提示或间隔提示机制；

注 2：持续收集指在用户使用服务期间不间断的连续收集用户信息，如录音、录像、连续的位置轨迹等。

注 3：如出行导航类需持续收集个人信息主体地理位置信息的，以浮窗、弹窗、语音或振动等形式间隔一定时间提醒个人信息主体当前地理位置正在被使用。

c） 应向个人信息主体告知个人信息处理者的身份和联系方式等基本情况，敏感个人信息的处理目的、处理方式以及必要性，敏感个人信息的种类、保存期限以及对个人权益的影响，个人信息主体行使个人信息权利的方式和途径；

d） 紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应在紧急情况消除后及时告知；

e） 所提供的服务明确不再收集敏感个人信息时或不承担敏感个人信息保护责任时，应对个人信息主体进行提示。

6.3.2 同意

个人信息处理者在收集敏感个人信息前，应遵守以下要求：

a） 基于个人同意进行处理的，个人信息处理者应在处理敏感个人信息前，取得个人信息主体的单独同意；

注1：单独同意的方式，可以由个人信息主体主动完成填写提交，也可通过设置独立页面、电话、短信等向个人信息主体进行告知并支持个人通过点击、分项勾选等肯定性动作作出同意表示。

b） 在法律法规另有明确规定时取得个人信息主体的书面同意；

注2：书面同意的方式，可以由个人信息处理者以纸质或数字电文等有形地表现所载内容，并由个人信息主体通过主动签名、签章等形式取得个人同意。

注3：书面同意的情形包括但不限于采集人类遗传资源、向征信机构查询个人信息、从事信贷业务的机构向其他主体提供信贷信息、使用房地产经纪服务过程中提供房地产交易相关信息等。

c) 多项敏感个人信息处理活动，应按处理目的为个人信息主体提供单独同意机制；

注4：单独同意是指个人信息处理者处理敏感个人信息不应与一般个人信息一并取得个人同意。单独同意处理敏感个人信息的界面不应包含其他信息处理事宜。

d) 个人信息处理者基于个人同意处理不满十四周岁未成年人个人信息的，应取得未成年人的父母或者其他监护人的同意；

e) 在公共场所安装图像采集、个人身份识别设备的，应设置显著的提示标识，除取得个人信息主体单独同意以外，所收集的个人图像、身份识别信息类敏感个人信息原则上只能用于维护公共安全的目的，不应用于其他目的；

f) 个人信息处理者处理已公开的敏感个人信息，经评估对个人权益有重大影响的，应取得个人的单独同意；

g) 基于个人同意处理敏感个人信息的，个人信息处理者应为个人提供便捷的撤回同意的方式，同时宜向个人说明撤回同意可能对个人产生的影响。

6.4 安全保护要求

个人信息处理者处理敏感个人信息，应遵守以下要求：

a) 应遵循所约定的处理目的、处理方式开展敏感个人信息处理活动，并对处理情况进行记录；

b) 应在个人信息接收方的个人信息保护能力不低于个人信息处理者的条件下传输敏感个人信息；

c) 互联网传输敏感个人信息时，应至少采用通道加密方式进行传输，宜采用通道加密与内容加密两种加密方式结合进行，通道加密和内容加密算法应符合有关行业技术标准与行业主管部门有关规定要求；

d) 应定期评估或验证敏感个人信息传输方式的安全状况，网络环境发生重大变化时，应及时调整安全策略；

e) 经过加密、去标识化处理后的敏感个人信息应与解密密钥、其他个人信息等分开存储；

注：个人信息去标识化处理宜参考 GB/T 37964—2019 开展。

f) 对敏感个人信息的访问、修改、删除、导出等操作，应在对角色权限控制的基础上，按照业务流程的需求触发操作授权，定期针对敏感个人信息的访问、修改、删除、导出等操作进行日志审计；

g) 敏感个人信息存储环境应建立异常监测和分析能力，对出现的异常情况进行及时响应，动态调整安全保护措施，按照就高从严原则设定安全保护措施；

h) 对敏感个人信息的处理活动应建立异常监测预警和响应机制，对超出业务正常需求的异常操作（如频繁、大量敏感个人信息浏览查询、下载、打印，非工作时间操作等）应采取中断操作，并通过邮件、消息、弹窗等形式进行告警，开展分析调查，提前排除隐患；

i) 敏感个人信息展示界面宜添加包括访问主体标识、访问时间等内容的水印，宜默认禁用复制、打印、截屏等功能；

j) 应定期评估敏感个人信息删除或匿名化处理效果，确保已删除或匿名化处理的敏感个人信息不具备还原能力；

k) 应定期梳理应用及API资产清单，定期针对应用及API传输敏感个人信息情况进行审计；

l) 应建立敏感个人信息过期自动删除机制，法律、行政法规规定需要留存敏感个人信息的，应在到期后及时删除。

6.5 安全管理要求

对敏感个人信息处理者的要求如下：

a) 对敏感个人信息实行分类管理；

b) 如按照有关规定，达到一定量级的敏感个人信息，应参照重要数据进行保护；

c) 应建立敏感个人信息安全管理策略，对敏感个人信息的处理行为进行识别、审批、记录、审计；

d) 应进行个人信息保护影响评估，并对处理情况进行记录；

注：个人信息保护影响评估宜参考 GB/T39335—2020 开展。

e) 数据安全能力应达到GB/T 37988—2019三级及以上能力要求；

f) 规划建设涉及敏感个人信息处理产品和服务时，宜参考GB/T41817—2022开展个人信息安全工程实践，同步规划、同步建设、同步部署、同步使用个人信息安全措施。

g) 处理敏感个人信息超过1万条、涉及个人信息跨境传输的，应开展数据出境风险自评估，并通过所在地省级网信部门向国家网信部门申报数据出境安全评估。

7 敏感个人信息处理特殊安全要求

7.1 生物识别信息

个人信息处理者处理生物识别信息，应在遵守第6章要求并满足GB/T 40660—2021要求的基础上，遵守以下要求：

a) 处理指纹、人脸、声纹、基因、虹膜、步态等不同生物识别信息应符合相应的国家和行业标准；

b) 不应以生物识别信息处理为唯一的身份识别方式，法律法规另有规定的除外；

c) 应采用明确的提示方式向个人信息主体告知，确保所采集的生物识别信息不包含其他敏感个人信息；

注：如所采集的音频、图片、影像中包含身份证件号码、账户密码等。

d) 在保证实现业务功能的基础上，应对所收集的生物识别信息直接进行特征、摘要信息提取；

e) 应确保以非身份识别目的收集的生物识别信息，不用于身份识别用途；

f) 在科学研究场景，应与个人信息主体签署知情同意书，并对输出的研究成果进行去标识化处理。

7.2 宗教信仰信息

个人信息处理者处理宗教信仰信息，应在遵守第6章要求的基础上，遵守以下要求：

a) 收集个人宗教信仰信息时，应符合宗教组织的信息披露要求，不应收集未经宗教组织或个人授权同意的信息；

b) 原则上不应处理个人宗教信仰信息，宗教组织内部范围开展或取得宗教组织授权的个人信息处理活动的除外；

c) 未经个人单独同意，不应提供、公开个人宗教信仰或特殊宗教习俗；

d) 不应使用个人宗教信仰、特殊宗教习俗等宗教信仰信息构建用户画像。

7.3 特定身份信息

个人信息处理者处理特定身份信息，应在遵守第6章要求的基础上，遵守以下要求：

a) 在可采用收集个人信息实现处理目的时，不应强制收集特定身份信息；

b) 确需收集特定身份信息的，应在验证特定身份后立即删除，法律、行政法规有留存要求的，从其规定；

c) 应去标识化展示特定身份信息，确需完整展示的，应进行个人信息主体或授权人员身份验证；

注：特定身份信息去标识化展示示例见附录C.1。

d) 未经个人单独同意，不应提供、公开已识别的特定身份信息；

e) 不应使用个人特定身份信息构建用户画像、用于个性化推荐。

7.4 医疗健康信息

个人信息处理者处理医疗健康信息，应在遵守第6章要求和在满足GB/T 39725—2020要求的基础上，遵守以下要求：

a) 应依据医疗健康行业法律、行政法规等的要求，根据医疗健康信息的敏感程度以及对个人信息主体可能造成的影响进行分类分级管理和保护；

b) 对患者医疗数据的收集、查询、处理、使用等环节，应建立相应的访问控制权限审批机制，例如艾滋病、性病仅限于主治医护人员访问等；

c) 应脱敏展示医疗健康信息，确需完整展示的，应进行个人信息主体或授权人员身份验证；

注：医疗健康信息去标识化展示示例见附录C.2。

d) 用于临床研究、医药/医疗研发时，医疗健康信息宜按照GB/T 37964-2019去标识化后使用；

7.5 金融账户信息

个人信息处理者处理金融账户信息，应在遵守第6章要求的基础上，遵守以下要求：

a) 应依据金融行业法律、行政法规等的要求，根据金融账户信息的敏感程度以及对个人信息主体可能造成的影响进行分类分级管理和保护；

b) 通过受理终端、客户端应用软件、浏览器等方式收集金融账户信息时，应使用加密等技术措施保证数据的保密性；

c) 不应留存非本机构的个人金融账户相关个人信息主体鉴别信息，确有必要留存的，应取得个人信息主体及账户管理机构的授权；

d) 受理终端、个人终端及客户端应用软件均不应存储银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN 和CVN2）、银行卡密码、网络支付密码等支付敏感信息及个人生物识别信息的样本数据，仅可保存完成当前交易所必需的基本信息要素，并在完成交易后及时删除；

e) 对于银行卡号或其他识别标识信息等可以直接或组合后确定个人信息主体的信息应脱敏展示金融账户信息，确需完整展示的，应进行个人信息主体身份验证。

注：金融账户信息去标识化展示示例见附录C.3。

7.6 行踪轨迹信息

个人信息处理者处理行踪轨迹信息，应在遵守第6章要求的基础上，遵守以下要求：

a) 持续收集行踪轨迹信息的，应提供持续提示机制；

b) 不应标注行踪轨迹涉及的已知国家敏感位置区域；

c) 因业务需要处理行踪轨迹信息的，应对行踪轨迹信息的访问进行严格权限控制；

d) 应仅在使用涉及行踪轨迹相关业务功能时，以最小频率和范围调用行踪轨迹信息；

e) 如果业务功能仅收集地理位置信息，但加工信息包含经纬度、时间范围、地点空间等元数据，则应与地位置信息同等要求；

f) 通过界面展示行踪轨迹信息的，宜对展示的行踪轨迹信息采取去标识化处理等措施。

7.7 不满十四周岁未成年人信息

7.7.1 基本要求

个人信息处理者处理不满十四周岁未成年人信息，应进行单独存储管理。

7.7.2 处理规则

个人信息处理者处理不满十四周岁未成年人的个人信息，应制定专门的个人信息处理规则，应告知但不限于以下内容：

a) 未成年人个人信息处理的目的、方式、范围，处理的必要性；
b) 未成年人个人信息存储的地点、期限及到期后的处理方式；
c) 对未成年人个人信息采取的安全保障措施；
d) 未成年人的监护人投诉、举报的渠道和方式；
e) 未成年人的监护人查询、复制、更正、删除信息、撤回同意、注销账户等的途径和方法；
f) 未成年人的监护人拒绝个人信息处理规则的后果；
g) 专门的个人信息处理规则中以上告知事项发生实质性变化的，应再次征得未成年人的监护人的同意。

7.7.3 告知同意方式

个人信息处理者处理不满十四周岁未成年人的个人信息时，告知同意的要求如下：

a) 宜使用未成年人可理解的方式说明应由未成年人的监护人确认同意；
b) 通过简明、易于理解的形式，向未成年人的监护人，说明未成年人信息收集、使用的情况；
c) 在协议或交互界面中重点说明收集、使用未成年人个人信息的情况和敏感性；
d) 以适当方式向未成年人的监护人告知，并为未成年人的监护人同时提供同意和拒绝的选项，避免不满十四周岁未成年人自行确认或同意。

7.7.4 核验流程

个人信息处理者处理不满十四周岁未成年人的个人信息时，核验流程的要求如下：

a) 应采取合理技术措施核验个人信息主体的年龄，确认个人信息主体是否为不满十四周岁未成年人；
b) 当核验个人信息主体的身份为不满十四周岁未成年人时，宜继续采取合理措施核验监护人的身份；
c) 核验的方式宜充分考虑不同的产品或服务在受众群体上的本质差异，对于不同的产品或服务宜采取不同强度的核验方式；

注：低强度核验方式要求未成年人自主填写其年龄；中强度核验方式要求未成年人提供其身份证照片或姓名及身份证号码，以判断其年龄；高强度核验方式通过身份证照片及人脸识别共同判断其年龄。

d) 核验监护人身份的流程和方式宜采取短信验证、电话验证、视频验证、邮箱验证、书面确认等合理措施进行。

附 录 A
（规范性）
常见敏感个人信息类别

常见敏感个人信息类别见表A.1。

表 A.1 敏感个人信息类别

类别	典型示例
生物识别信息	个人基因、指纹、声纹、掌纹、眼纹、耳廓、虹膜、面部识别特征、步态等
宗教信仰信息	信仰的宗教、加入的宗教组织、宗教组织中的职位、参加的宗教活动、特殊宗教习俗等
特定身份信息	犯罪人员身份信息、残障人士身份信息、特定工作信息（如军人、警察）、身份证件号码等
医疗健康信息	病症、住院志、医嘱单、检验报告、检查报告、手术及麻醉记录、护理记录、用药记录、生育信息、家族病史、传染病史等
金融账户信息	银行、证券、基金、保险、公积金等账户的账号及密码，公积金联名账号、支付账号、银行卡磁道数据（或芯片等效信息）以及基于账户信息产生的支付标记信息等
行踪轨迹信息	实时精准定位信息、GPS 车辆轨迹信息、航班车票信息、特定住宿信息等
不满十四周岁未成年人个人信息	不满十四周岁未成年人的个人信息
身份鉴别信息	登陆密码、支付密码、账户查询密码、交易密码、动态口令、口令保护答案等
其他敏感个人信息	网页浏览信息、婚史、性取向、通信内容、征信信息、未公开的违法犯罪记录等

附 录 B
（资料性）
处理敏感个人信息取得个人书面同意模板

本授权书是您与【机构名称】就敏感个人信息处理事宜出具的授权书，为了维护您的权益，请在签署本授权书前，仔细阅读本授权书各条款，在确认充分了解后慎重决定是否同意本授权书。

一、目的及类型

为了【敏感个人信息收集目的】，我们需要收集您的【敏感个人信息类型】，用于【敏感个人信息收集用途】。

二、存储

1.存储地点：本次获取和处理的敏感个人信息将存储于中华人民共和国境内，如需要向境外传输的，我们将会遵循相关国家规定并经您授权同意。

2.存储期限：【敏感个人信息的存储期限说明、过期自动删除机制……】

三、您的权利

在我们处理您敏感个人信息的活动中，您享有如下权利：

1.查阅、复制、转移：【权利实现路径说明】

2.更正、补充：【权利实现路径说明】

3.撤回同意、删除：【权利实现路径说明】

……

四、风险提示

1.【敏感个人信息类型】为您的敏感个人信息。一旦泄露或者非法使用，可能导致【对个人权益的影响，如人格尊严受到侵害或者人身、财产安全受到危害等】。

2.我们承诺对您的个人信息严格保密，并按照国家法律法规规定，采用【保护个人信息安全的措施，如加密、匿名化、去标识化、访问控制等技术和管理措施】。

五、其他事项

如您对本授权书内容有任何疑问、意见或建议，可通过【联系方式】与我们联系。

本人声明：本人已知悉本授权书所有内容以及由此产生的法律效力，自愿作出上述授权，本授权书是本人真实的意思表示。

姓名：

日期：

附 录 C
（资料性）
去标识化展示示例

C.1 特定身份信息去标识化展示示例见表C.1。

表 C.1 特定身份信息去标识化展示示例

类型	脱敏要求
身份证号码	显示前 4 位，如：1101**********
中国护照	显示前一位和后一位，如：P*******3

C.2 医疗健康信息去标识化展示示例见表C.2。

表 C.2 医疗健康信息去标识化展示示例

类型	脱敏要求
姓名	宜删除或置空、随机替换
联系方式	手机号脱敏中间四位，如：138****1111 详细住址，如：住址只具体到市县区级，隐藏区级以下地区
日期	宜采用时间偏移法、转换法或泛化 如：入院日期2020-01-01+随机偏移量100=入院日期：2020-04-11
生物识别信息	宜删除或置空

C.3 金融账户信息去标识化展示示例见表C.3。

表 C.3 金融账户信息去标识化展示示例

类型	脱敏要求
基金账户	显示后四位，如：**********4309
保险账户	显示前 4 位和后 4 位，其余屏蔽，如 P231********4532
公积金账户	账号长度为 9 位，屏蔽后 5 位；账号长度为 12 位，屏蔽后 8 位，如：6375********
社保号	保留前 2 位和后 2 位（若值为身份证号，则同身份证号码脱敏方式），如 23**********46
银行卡号或账号	包括借记卡卡号/信用卡卡号/电子账户账号，保留开头 4 位和末尾 4 位，其余中间位数屏蔽，如：6217 **** **** 1234
存折号	显示前 4 位和后 4 位，屏蔽中间，如：1231*********3825
磁道信息	全部屏蔽

类型	脱敏要求
账户密码	全部屏蔽

参 考 文 献

[1] GB/T 35274-2017 信息安全技术 大数据服务安全能力要求
[2] GB/T 37973-2019 信息安全技术 大数据安全管理指南
[3] GB/T 41391-2022 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
[4] GB/T 42574-2023 信息安全技术 个人信息处理中告知和同意的实施指南