ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 45574—2025

数据安全技术
敏感个人信息处理安全要求

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

2025-04-25 发布　　2025-11-01 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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国电子技术标准化研究院、中国科学院信息工程研究所、国家信息技术安全研究中心、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、公安部第三研究所、公安部第一研究所、国家计算机网络应急技术处理协调中心、中国网络空间研究院、中国软件评测中心、北京百度网讯科技有限公司、北京大学肿瘤医院、中信银行股份有限公司、贝壳找房(北京)科技有限公司、阿里巴巴(北京)软件服务有限公司、北京华品博睿网络技术有限公司、上海识装信息科技有限公司、中国银联股份有限公司、顺丰速运有限公司、奥林巴斯(北京)销售服务有限公司、医渡云(北京)技术有限公司、飞利浦(中国)投资有限公司、厦门美柚股份有限公司、岚图汽车科技有限公司、中关村科学城城市大脑股份有限公司、西安交通大学、北京小桔科技有限公司、联想(北京)有限公司、华为技术有限公司、广西电网有限责任公司。

本文件主要起草人：姚相振、胡影、陈舒、高超、上官晓丽、牛犇、陈琳、郝春亮、白晓媛、李昳婧、王昕、朱雪峰、苏丹、于东升、陈彦如、王晖、姜伟、杨婷、孙硕、衡反修、封莎、张朝、黄天宁、王彬、徐燕、刘磊、黎琳、轷则喁、梁文韬、张灵子、黄鹏华、汪洋、徐起、王伟、程文静、刘俊、李实、张玲翠、李凤华、杨韬、石玉珍、刘笑岑、高震、落红卫、王普、顾伟、卞乐、韦宗慧、刘朝苹。

数据安全技术
敏感个人信息处理安全要求

1 范围

本文件确立了敏感个人信息识别和界定，规定了敏感个人信息处理通用安全要求和敏感个人信息处理特殊安全要求。

本文件适用于个人信息处理者开展敏感个人信息处理活动，也适用于监管部门和第三方评估机构对敏感个人信息处理活动进行监督、管理和评估。

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 35273 信息安全技术 个人信息安全规范

GB/T 40660 信息安全技术 生物特征识别信息保护基本要求

GB/T 41391 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

3 术语和定义

下列术语和定义适用于本文件。

3.1

个人信息 personal information

以电子或其他方式记录的与已识别或可识别的自然人有关的各种信息。

3.2

敏感个人信息 sensitive personal information

一旦泄露或非法使用，容易导致自然人的人格尊严受到侵害或人身财产安全受到危害的个人信息。

注：敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户和行踪轨迹等信息和不满十四周岁未成年人的个人信息。

3.3

个人信息处理者 personal information processor

在个人信息处理活动中自主决定处理目的和处理方式的组织和个人。

3.4

个人信息主体 personal information subject

个人信息所标识或关联的自然人。

[来源：GB/T 35273—2020，3.3]

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、公开和删除等活动。

3.6

单独同意　separate consent

个人针对其个人信息进行特定处理而专门作出具体、明确的同意。

[来源:GB/T 42574—2023，3.7，有修改]

4　敏感个人信息识别和界定

4.1　敏感个人信息识别

个人信息处理者应按以下规则，识别敏感个人信息。

a)　符合以下任一条件的个人信息，应识别为敏感个人信息：

1)　一旦遭到泄露或非法使用，容易导致自然人的人格尊严受到侵害；

注 1：容易导致自然人人格尊严受到侵害的情形可能包括“人肉搜索”、非法侵入网络账户、电信诈骗、损害个人名誉和歧视性差别待遇等。歧视性差别待遇可能因个人信息主体的特定身份、宗教信仰、性取向、特定疾病和健康状态等信息泄露导致。

2)　一旦遭到泄露或非法使用，容易导致自然人的人身安全受到危害；

注 2：例如泄露或非法使用个人的行踪轨迹信息，可能会导致个人信息主体的人身安全受到损害。

3)　一旦遭到泄露或非法使用，容易导致自然人的财产安全受到危害。

注 3：例如泄露或非法使用金融账户信息，可能会造成个人信息主体的财产损失。

b)　按 4.2 识别收集和产生的敏感个人信息，敏感个人信息类别应符合附录 A。

注 4：如有充分理由和证据表明处理的个人信息达不到 a)中条件的，不识别为敏感个人信息。

c)　既要考虑单项敏感个人信息识别，也要考虑多项一般个人信息汇聚后的整体属性，分析其一旦泄露或非法使用可能对个人权益造成的影响，如符合 a)所述条件，应将汇聚后的个人信息整体参照敏感个人信息进行识别与保护。

d)　法律法规规定为敏感个人信息的，从其规定。

4.2　敏感个人信息界定

敏感个人信息包括以下类别。

a)　生物识别信息：也称生物特征识别信息，是指对自然人的物理、生物或行为特征进行技术处理得到的、能单独或与其他信息结合识别该自然人身份的个人信息。

注 1：生物识别信息参考 GB/T 40660、GB/T 41819、GB/T 41807、GB/T 41773 和 GB/T 41806 等。

b)　宗教信仰信息：与个人信仰的宗教、宗教组织和宗教活动相关的个人信息。

c)　特定身份信息：对个人人格尊严和社会评价有重大影响或有其他不适宜公开的身份信息，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：与个人的医疗就诊、身体和心理健康状况相关的个人信息。

e)　金融账户信息：与个人的银行和证券等账户和账户资金交易相关的个人信息。

f)　行踪轨迹信息：个人在一定期间内因为所处具体地理位置、活动地点和活动轨迹的移动变化而形成的连续轨迹信息。

注 2：特定职业(外卖员和快递员等)用于实现服务履约场景下除外。

g)　不满十四周岁未成年人的个人信息。

h)　其他敏感个人信息：除以上信息外，其他一旦泄露或非法使用，容易导致自然人的人格尊严受到侵害或人身财产安全受到危害的个人信息。

5 敏感个人信息处理通用安全要求

5.1 基本要求

敏感个人信息处理，符合以下基本要求：

a) 敏感个人信息处理应符合 GB/T 35273 中个人信息相关要求；

b) 只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息；

c) 基于个人同意处理敏感个人信息的，应取得个人信息主体的单独同意。

5.2 收集合法性

个人信息处理者在收集敏感个人信息前，符合以下要求：

a) 不应隐瞒产品或服务所具有的收集敏感个人信息的功能，应通过隐私政策等方式明确收集敏感个人信息的类型、范围、目的、收集敏感个人信息的必要性和对个人权益的影响；

b) 不应自行或借助他人帮助，通过欺诈、诱骗、误导和胁迫等方式收集敏感个人信息，或通过非法渠道购买敏感个人信息；

c) 不应通过技术手段自动收集互联网网站页面和移动互联网应用程序传输、存储和显示的敏感个人信息；

注 1：自动收集是指通过自动下载程序和脚本等技术手段自动获取特定网页信息或数据并按指定规则提取相应内容的活动。

d) 不应基于任何违反法律法规规定的目的收集敏感个人信息，不应利用所收集的敏感个人信息从事任何违反法律法规的行为；

注 2：违反法律法规规定的目的包括但不限于非法买卖、提供或公开他人个人信息，从事危害国家安全和公共利益的个人信息处理活动，侵犯他人的知识产权或人格权等行为。

e) 不应为网络暴力、侮辱诽谤、电信网络诈骗、敲诈勒索和侵犯公民个人信息等犯罪活动收集敏感个人信息，或将所收集的敏感个人信息用于上述犯罪活动。

5.3 收集要求

个人信息处理者在收集敏感个人信息前，符合以下要求：

a) 收集非敏感个人信息可实现处理目的的，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) 应按业务功能或服务场景，分项收集敏感个人信息；

d) 利用移动互联网应用程序收集应符合 GB/T 41391 的要求。

5.4 告知同意

5.4.1 告知

个人信息处理者在收集敏感个人信息前，符合以下要求：

a) 在收集敏感个人信息前，应采用单独弹窗、短信、填写框、动画、转至单独提示界面和语音播报等方式向个人进行告知；

b) 应向个人信息主体告知个人信息处理者的名称或姓名、联系方式等基本情况，敏感个人信息的处理目的、处理方式和必要性，敏感个人信息的种类、保存期限和对个人权益的影响，个人信息主体行使个人信息主体权利的方式和途径；

c) 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信息主体告知的，个人信息处理者应在紧急情况消除后及时告知；

d) 持续收集敏感个人信息的，宜提供持续提示或间隔提示机制。

注 1：持续收集指在用户使用服务期间不间断地连续收集用户信息，如录音、录像和连续的位置信息等。

注 2：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、振动和状态栏图标等形式提醒个人信息主体当前地理位置正在被收集。

5.4.2 同意

个人信息处理者在收集敏感个人信息前，符合以下要求：

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。

注 2：单独同意的方式，可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、电话和短信等向个人信息主体进行告知并通过个人点击或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，处理敏感个人信息取得个人书面同意模板见附录 B；

注 3：书面同意的方式，可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、签章和电子签名等形式取得个人同意。

注 4：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和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，应按处理目的和业务功能为个人信息主体提供单独同意机制；

d) 单项敏感个人信息被用于多个处理目的或业务功能的，不应捆绑取得同意；

e) 在公共场所安装图像采集或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外，所收集的个人图像和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信息主体提供便捷的撤回同意的方式，同时宜向个人信息主体说明撤回同意可能对个人产生的影响。

5.5 安全保护要求

个人信息处理者处理敏感个人信息，符合以下安全保护要求：

a) 应在个人信息处理前按 4.1 识别敏感个人信息，按 4.2 对敏感个人信息进行分类管理，建立敏感个人信息目录并及时更新；

b) 敏感个人信息去标识化后应作为一般个人信息进行保护，匿名化处理后的个人信息除外；

c) 如按国家和行业数据分类分级保护有关规定，达到一定规模的敏感个人信息被认定为重要数据，应按重要数据进行保护；

注 1：重要数据识别方法参考 GB/T 43697。

d) 应针对敏感个人信息制定专门管理制度和操作规程，明确敏感个人信息处理相关方安全职责和全流程数据处理安全要求；

e) 应建立敏感个人信息处理授权审批流程，对敏感个人信息的内部共享、对外提供、公开、批量查询、明文显示、下载和输出等重要操作进行审批；

f) 应将具有敏感个人信息操作权限的人员作为关键岗位人员进行安全管理；

g) 应在涉及敏感个人信息处理的新应用使用前进行个人信息保护影响评估，评估报告应保存

三年；

注 2：个人信息保护影响评估参考 GB/T 39335 开展。

h） 应对敏感个人信息处理和操作情况进行记录，日志记录应保存三年；

i） 敏感个人信息与可识别个人身份的信息分开存储，去标识化的敏感个人信息与可用于恢复识别个人的信息分开存储；

j） 敏感个人信息应加密存储和加密传输，采用的密码算法和密码技术应符合相关密码国家标准和行业标准，或密码管理部门有关规定；

k） 使用加密技术处理敏感个人信息，解密操作与加密操作应分别授权，用于加密和解密的密钥存放在符合相关密码国家标准和行业标准的密码产品中；

l） 敏感个人信息在产品和内部系统显示时，应默认进行去标识化处理；

m） 应按最少够用原则，严格限制敏感个人信息访问权限和有效期，敏感个人信息权限申请和使用应基于业务需要，且仅授予访问其业务所必需的最少敏感个人信息类型和数量；

n） 应采取措施保障敏感个人信息字段级访问控制，原则上结构化数据权限申请应能细化到表的字段，非结构化数据权限申请应能细化到文件；

o） 应至少每月对敏感个人信息处理日志和用户权限进行安全审计，及时处理不合理的授权和操作；

p） 应按国家有关主管部门规定开展个人信息保护合规审计，针对敏感个人信息处理活动遵守法律和行政法规的情况继续进行审核和评价；

q） 应建立敏感个人信息安全风险监测预警和响应机制，对超出业务正常需求的异常操作（如频繁或大量敏感个人信息浏览查询、下载和打印，非工作时间操作等）及时响应；

r） 敏感个人信息显示界面应添加包括访问主体标识和访问时间等内容的水印，涉及集中显示的，应默认禁用复制、打印和截屏等功能；

s） 宜对敏感个人信息删除或匿名化处理效果进行评估，已删除或匿名化处理的敏感个人信息不应被还原；

t） 应定期梳理可访问敏感个人信息的应用和数据接口，应采用身份鉴别、访问控制、最小授权、安全通道、加密传输和时间戳等安全措施；

u） 应建立敏感个人信息删除机制并提供个人信息主体删除其敏感个人信息的便利机制，法律和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或匿名化处理；

注 3：到期包括处理目的已实现、无法实现，或为实现处理目的不再必要；个人信息处理者停止提供产品或服务，或保存期限已届满；个人撤回同意；个人信息处理者违反法律和行政法规，或违反约定处理个人信息；法律和行政法规规定的保存期限届满等情形。

v） 敏感个人信息处理者的数据安全能力，宜符合 GB/T 37988 三级及以上能力要求；

w） 规划建设涉及敏感个人信息的产品服务时，宜按 GB/T 41817 开展个人信息安全工程实践，同步规划、同步建设、同步部署和同步使用个人信息安全措施；

x） 敏感个人信息出境应符合国家有关部门数据出境有关规定；

y） 处理 10 万人以上敏感个人信息的，符合以下要求：

1） 应指定个人信息保护负责人和管理机构，负责对个人信息处理活动及采取的保护措施等进行监督；

2） 个人信息保护负责人应当具备个人信息保护专业知识和相关管理工作经历，由处理者管理层成员担任；

3） 应对个人信息保护负责人和关键岗位的人员进行安全背景审查；

4） 因合并、分立、解散和破产等可能影响敏感个人信息安全的，应制定敏感个人信息处置方案，采取措施保障敏感个人信息安全。

6 敏感个人信息处理特殊安全要求

6.1 生物识别信息

个人信息处理者处理生物识别信息，在符合第5章和GB/T 40660要求的基础上，还符合以下要求：

a) 基于生物识别信息进行身份识别时，应同时提供不基于生物识别信息的其他替代可选身份识别方式，并不应将基于生物识别信息的方式作为默认选项；
b) 除非个人信息主体主动要求或书面同意，不应公开生物识别信息；
c) 通过无需个人信息主体配合的方式收集生物识别信息用于身份识别前，应取得个人书面同意；
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和摘要信息提取；
e) 实现处理目的后，应删除所收集的原始生物识别信息，如原始图像、图片和视频等；
f) 将生物识别信息用于科学研究，应取得个人信息主体的书面同意。

6.2 宗教信仰信息

个人信息处理者处理宗教信仰信息，在符合第5章要求的基础上，还符合以下要求：

a) 收集个人宗教信仰信息时，应按宗教组织的有关规定，不应收集未经个人信息主体单独同意的个人宗教信仰信息；
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并取得个人信息主体单独同意的个人信息处理活动除外；
c) 未经个人单独同意，不应提供和公开个人宗教信仰和特殊宗教习俗；
d) 不应使用个人宗教信仰和特殊宗教习俗等宗教信仰信息构建用户画像。

6.3 特定身份信息

个人信息处理者处理特定身份信息，在符合第5章要求的基础上，还符合以下要求：

a) 在可采用收集非特定身份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，应在验证特定身份和实现处理目的后及时删除，法律和行政法规有留存要求的，从其规定；
c) 应去标识化显示特定身份信息，确需完整显示的，应进行个人信息主体或授权人员身份验证；
d) 未经个人信息主体单独同意，不应提供和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和用于个性化推荐。

6.4 医疗健康信息

个人信息处理者处理医疗健康信息，在符合第5章要求的基础上，还符合以下要求：

a) 应依据医疗健康行业法律和行政法规等的要求，根据医疗健康信息的敏感程度和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) 对个人医疗健康信息的收集、存储、使用和加工等环节，应建立相应的访问控制权限审批机制，例如艾滋病和性病仅限于主治医护人员访问等；
c) 应去标识化显示医疗健康信息，确需完整显示的，应进行个人信息主体或授权人员身份验证；
d) 用于临床研究、医药和医疗研发时，医疗健康信息宜按GB/T 37964去标识化后使用。

6.5 金融账户信息

个人信息处理者处理金融账户信息，在符合第5章要求的基础上，还符合以下要求：

a) 应依据法律和行政法规等的要求，根据金融账户信息的敏感程度和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、客户端应用软件和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；
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) 受理终端和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、银行卡密码和网络支付口令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) 金融账户信息应去标识化显示，确需完整显示的，应进行个人信息主体身份验证；
f) 去标识化场景应覆盖客户交易页面显示、业务管理页面显示和日志打印显示等，应在前端和服务器端均实现。

6.6 行踪轨迹信息

个人信息处理者处理行踪轨迹信息，在符合第5章要求的基础上，还符合以下要求：

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国家有关部门规定的敏感位置区域；
c) 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；
d) 如业务功能仅收集地理位置信息，但加工后产生的信息包含经纬度、时间范围和地点空间等，则应与行踪轨迹信息同等保护要求；

示例：

多次收集个人信息主体的地理位置信息，辅以收集时间戳和其他信息加工处理，能构成个人信息主体的行踪轨迹。

e) 通过界面显示行踪轨迹信息的，宜对显示的行踪轨迹信息采取去标识化处理等措施。

6.7 不满十四周岁未成年人的个人信息

个人信息处理者处理不满十四周岁未成年人的个人信息，在符合第5章要求的基础上，还符合以下要求。

a) 仅在未成年人相关法律法规有明确要求时，方可收集不满十四周岁未成年人身份信息。

注1：收集未成年人身份信息的服务如信息发布、即时通讯、网络直播和网络游戏等。

b) 对未成年人身份信息进行验证时符合以下要求：
   1) 应采取合理措施验证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；

   注2：在网络直播场景下，可采取开播前验证真实身份、人工审核和对举报投诉进行及时处置等方式建立针对网络直播发布者真实身份信息动态验证机制。

   2) 当验证个人信息主体的身份为不满十四周岁未成年人时，宜采取合理措施验证监护人的身份；
   3) 验证的方式宜充分考虑不同的产品或服务在受众群体上的差异，对于不同的产品或服务宜采取不同强度的验证方式；
   4) 验证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、电子邮箱验证、书面确认和绑定实名账户等合理措施进行。
c) 采取以下措施保障未成年人或其监护人对不满十四周岁未成年人个人信息的查阅、复制、更正、补充和删除的权利，不应对未成年人或其监护人的合理请求进行限制：
   1) 应提供便捷的不满十四周岁未成年人个人信息查阅方法和途径，并提供不满十四周岁未

成年人或其监护人查阅不满十四周岁未成年人个人信息种类和数量的方法和途径等；

2） 应提供便捷的不满十四周岁未成年人或其监护人复制、更正、补充和删除不满十四周岁未成年人个人信息的功能；

3） 应在15个工作日内或法律法规规定的期限内受理并处理未成年人或其监护人查阅、复制、更正、补充和删除未成年人个人信息的申请，拒绝未成年人或其监护人行使权利的请求的，应当书面告知申请人并说明理由。

d） 应制定专门的未成年人个人信息处理规则并公开显示。

e） 应明示收集未成年人个人信息的功能和未成年人模式与成年人模式在敏感个人信息处理方面的不同。

6.8 其他敏感个人信息

个人信息处理者处理其他敏感个人信息，在符合第5章要求的基础上，应依据其他敏感个人信息的特点，采取相应的技术和管理措施，同时充分保护个人信息权益。

附 录 A
（规范性）
敏感个人信息类别

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	描述
生物识别信息	个人基因[a]、人脸[b]、声纹[c]、步态[d]、指纹、掌纹、眼纹、耳廓和虹膜等生物识别信息
宗教信仰信息	个人信仰的宗教、加入的宗教组织、宗教组织中的职位、参加的宗教活动和特殊宗教习俗等个人信息
特定身份信息	残障人士身份信息、不适宜公开的职业身份信息等个人信息
医疗健康信息	——与个人的身体或心理的伤害、疾病、残疾和疾病风险或隐私有关的健康状况信息[e]，如病症、既往病史、家族病史、传染病史、体检报告和生育信息等； ——在疾病预防、诊断、治疗、护理和康复等医疗服务过程中收集和产生的个人信息，如医疗就诊记录（如医疗意见、住院志、医嘱单、手术及麻醉记录、护理记录和用药记录）、检验检查数据（如检验报告和检查报告）等
金融账户信息	个人的银行、证券、基金、保险和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）和基于账户信息产生的支付标记信息和个人收入明细等个人信息
行踪轨迹信息	连续精准定位轨迹信息、车辆行驶轨迹信息和人员连续的活动轨迹信息等个人信息
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
其他敏感个人信息	精准定位信息[f]、居民身份证照片、性取向、性生活、征信信息、犯罪记录信息[g]和显示个人身体私密部位的照片或视频信息等个人信息

[a] 具体可参考 GB/T 41806。
[b] 具体可参考 GB/T 41819。
[c] 具体可参考 GB/T 41807。
[d] 具体可参考 GB/T 41773。
[e] 个人的体重、身高、血型、血压和肺活量等基本体质信息，如与个人的疾病和医疗就诊无关，则可认为不属于敏感个人信息范畴。
[f] 通过调用个人移动通信终端精准位置权限采集的位置信息是精准定位信息，通过网络地址等测算的粗略位置信息不是精准定位信息，连续采集的精准定位信息可用于生成行踪轨迹。
[g] 犯罪记录，是指我国国家专门机关对犯罪人员的客观记载，如罪名和刑罚等记录。

附　录　B
（资料性）
处理敏感个人信息取得个人书面同意模板

处理敏感个人信息取得个人书面同意模板见图 B.1。

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，仔细阅读本授权书所有内容，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，我们将按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、过期自动删除机制和……】

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、复制和转移：【权利实现路径说明】

2. 更正和补充：【权利实现路径说明】

3. 撤回同意和删除：【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、去标识化和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和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：

图 B.1　处理敏感个人信息取得个人书面同意模板

参 考 文 献

[1] GB/T 37964 信息安全技术 个人信息去标识化指南
[2] GB/T 37988 信息安全技术 数据安全能力成熟度模型
[3] GB/T 39335 信息安全技术 个人信息安全影响评估指南
[4] GB/T 41773 信息安全技术 步态识别数据安全要求
[5] GB/T 41806 信息安全技术 基因识别数据安全要求
[6] GB/T 41807 信息安全技术 声纹识别数据安全要求
[7] GB/T 41817 信息安全技术 个人信息安全工程指南
[8] GB/T 41819 信息安全技术 人脸识别数据安全要求
[9] 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
[10] GB/T 43697 数据安全技术 数据分类分级规则