|  |  |
| --- | --- |
| ICS | 35.030 |
| CCS | L 80 |

中华人民共和国国家标准

GB/T XXXXX—XXXX

画着卡通人物

中度可信度描述已自动生成

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10月26日）

XXXX - XX - XX发布

XXXX - XX - XX实施

文本

中度可信度描述已自动生成文本

中度可信度描述已自动生成

目  次

[前言 III](#_Toc149860686)

[1 范围 1](#_Toc149860687)

[2 规范性引用文件 1](#_Toc149860688)

[3 术语和定义 1](#_Toc149860689)

[4 缩略语 2](#_Toc149860690)

[5 敏感个人信息界定 2](#_Toc149860691)

[5.1 敏感个人信息识别 2](#_Toc149860692)

[5.2 常见敏感个人信息类别 2](#_Toc149860693)

[6 敏感个人信息处理通用安全要求 3](#_Toc149860694)

[6.1 敏感个人信息处理基本要求 3](#_Toc149860695)

[6.2 收集必要性 3](#_Toc149860696)

[6.3 告知同意 3](#_Toc149860697)

[6.4 安全保护要求 4](#_Toc149860698)

[7 敏感个人信息处理特殊安全要求 5](#_Toc149860699)

[7.1 生物识别信息 5](#_Toc149860700)

[7.2 宗教信仰信息 5](#_Toc149860701)

[7.3 特定身份信息 6](#_Toc149860702)

[7.4 医疗健康信息 6](#_Toc149860703)

[7.5 金融账户信息 6](#_Toc149860704)

[7.6 行踪轨迹信息 6](#_Toc149860705)

[7.7 不满十四周岁未成年人的个人信息 7](#_Toc149860706)

[附录A（规范性）常见敏感个人信息类别 8](#_Toc149860707)

[附录B（资料性）处理敏感个人信息取得个人书面同意模板 9](#_Toc149860708)

[附录C（资料性）去标识化展示示例 10](#_Toc149860709)

[C.1 特定身份信息去标识化展示示例见表C.1。 10](#_Toc149860710)

[C.2 医疗健康信息去标识化展示示例见表C.2。 10](#_Toc149860711)

[C.3 金融账户信息去标识化展示示例见表C.3。 10](#_Toc149860712)

[参考文献 11](#_Toc149860713)

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。

1. 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 39335—2020　信息安全技术 个人信息安全影响评估指南

GB/T 39725—2020　信息安全技术 健康医疗数据安全指南

GB/T 40660—2021 信息安全技术 生物特征识别信息保护基本要求

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

GB/T 41817—2022 信息安全技术 个人信息安全工程指南

GB/T AAAAA—XXXX 信息安全技术 数据分类分级规则

1. 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

在个人信息处理活动中自主决定处理目的、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或有其他不适宜公开的身份信息。

注：主要包括犯罪人员身份信息、残障人士身份信息、不适宜公开的职业身份信息（如军人、警察）等。

1. 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）

1. 敏感个人信息界定
   1. 敏感个人信息识别

个人信息处理者应按照以下规则，识别敏感个人信息：

1. 符合以下任一条件的个人信息，应识别为敏感个人信息：
2. 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、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。

1. 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；
2. 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，可能会造成个人信息主体的财产损失。

1. 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，应判断汇聚融合后的个人信息整体具有敏感个人信息属性。
   1. 常见敏感个人信息类别

常见敏感个人信息包括以下类别，具体类别中的敏感个人信息示例见附录A。

1. 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。
2. 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。
3. 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。
4. 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。
5. 金融账户信息：与银行、证券等账户和交易相关的信息。
6. 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。
7. 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。
8. 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。
9. 敏感个人信息处理通用安全要求
   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，基于个人同意处理个人信息的，应取得个人信息主体的单独同意，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。

* 1. 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：

1. 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；
2. 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；
3. 应按照业务功能或服务场景，分项收集敏感个人信息；
4. 利用App收集应符合GB/T 41391-2022要求。
   1. 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：

1. 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、语音播报等方式告知个人信息主体。

1. 利用App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、振动、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。

1. 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主体权利的方式和途径；
2. 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。

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：

1. 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。

1. 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3：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、使用房地产经纪服务过程中提供房地产交易相关信息等。

1. 多项敏感个人信息处理活动，应按处理目的、业务功能为个人信息主体提供单独同意机制；
2. 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，应取得未成年人监护人的明示同意；
3. 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；
4. 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；
5. 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。
   1. 安全保护要求

个人信息处理者处理敏感个人信息，应遵守以下安全保护要求：

1. 应在个人信息处理前按照6.1识别敏感个人信息，按照6.2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；
2. 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；
3. 如按照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，应参照重要数据进行保护；

注：重要数据识别方法，可参考GB/T AAAAA—XXXX标准。

1. 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。
2. 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、导出等重要操作进行审批；
3. 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；
4. 应在处理敏感个人信息前进行个人信息保护影响评估，评估报告应保存三年；
5. 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；
6. 敏感个人信息应与其他个人信息、去标识化的敏感个人信息分开存储；
7. 敏感个人信息应进行加密存储和加密传输，并采取技术措施保障敏感个人信息存储、传输过程的完整性，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；
8. 互联网传输敏感个人信息应采取安全加密通道（如HTTPS、VPN、专线等），并对数据进行加密；
9. 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；
10. 敏感个人信息在产品和内部系统展示时，应默认进行去标识化处理；
11. 应遵循“最少够用”、“职责分离”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，且仅授予访问满足其业务所必需的最少敏感个人信息类型和数量；
12. 应采取措施保障敏感个人信息细粒度访问控制，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；
13. 应至少每月对敏感个人信息处理日志、用户权限进行安全审计，及时处理不合理的授权和操作；
14. 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、大量敏感个人信息浏览查询、下载、打印，非工作时间操作等）及时响应；
15. 敏感个人信息展示界面应添加包括访问主体标识、访问时间等内容的水印，应默认禁用复制、打印、截屏等功能；
16. 宜对敏感个人信息删除或匿名化处理效果进行评估，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；
17. 应定期梳理可访问敏感个人信息的应用和API接口，对远程访问采用双因素身份鉴别机制；
18. 应建立敏感个人信息删除机制，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；
19. 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；
20. 规划建设涉及敏感个人信息的产品服务时，宜参考GB/T 41817—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；
21. 敏感个人信息出境应符合国家网信部门数据出境有关规定。
22. 敏感个人信息处理特殊安全要求
    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：

1. 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，并不应将基于身份识别信息的方式作为默认选项；
2. 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；
3. 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。
4. 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；
5. 实现业务功能后，应删除所收集的原始生物识别信息，如原始图像、图片、视频等；
6. 将生物识别信息用于科学研究，应征得个人信息主体的书面同意。
   1. 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：

1. 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，不应收集未经个人信息主体单独同意的个人宗教信仰信息；
2. 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；
3. 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；
4. 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。
   1. 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：

1. 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；
2. 确需收集特定身份信息的，应在验证特定身份、实现业务功能后及时删除，法律、行政法规有留存要求的，从其规定；
3. 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。

1. 未经个人信息主体单独同意，不应提供、公开已识别的特定身份信息；
2. 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。
   1. 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：

1. 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；
2. 对个人医疗健康信息的收集、存储、使用、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、性病仅限于主治医护人员访问等；
3. 应去标识化展示医疗健康信息，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。

1. 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。
   1. 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：

1. 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；
2. 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机密性；
3. 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；
4. 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；
5. 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去标识化展示金融账户信息，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。

1. 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。
   1. 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：

1. 持续收集行踪轨迹信息的，应提供持续提示机制；
2. 不应标注行踪轨迹涉及的已知国家敏感位置区域；
3. 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；
4. 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；
5. 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，则应与行踪轨迹信息同等要求；

示例：多次收集个人信息主体的地理位置信息，辅以收集时间戳以及其他信息加工处理，能构成个人信息主体的活动轨迹。

1. 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。
   1. 不满十四周岁未成年人的个人信息

个人信息处理者不满十四周岁未成年人的个人信息，应在遵守第6章要求的基础上，遵守以下要求：

1. 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、网络游戏等。

1. 对未成年人身份信息进行核验时应满足以下要求：
2. 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；
3. 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；
4. 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2：在网络直播场景下，网络直播服务提供者不应向未满十四周岁的未成年人提供网络直播发布者账号注册服务，应建立针对网络直播发布者真实身份信息动态核验机制，可采取开播前核验真实身份、人工审核或对举报投诉进行及时处置等方式。

1. 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、绑定实名账户等合理措施进行。
2. 应采取以下措施保障未成年人或者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、删除的权利，不得对未成年人或者其监护人的合理请求进行限制：
3. 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，支持不满十四周岁未成年人或者其监护人查阅不满十四周岁未成年人个人信息种类、数量等；
4. 提供便捷的支持不满十四周岁未成年人或者其监护人复制、更正、补充、删除不满十四周岁未成年人个人信息的功能；
5. 应在三十天内或法律法规规定的期限内受理并处理未成年人或者其监护人查阅、复制、更正、补充、删除未成年人个人信息的申请，拒绝未成年人或者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。
6. 应制定专门的未成年人个人信息处理规则并公开展示；
7. 应提供明示收集未成年人个人信息的功能，以及未成年人模式与成年人模式在个人敏感个人信息处理方面的不同。
8. （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、不适宜公开的职业身份信息（如军人、警察） |
| 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、航班高铁出行记录、人员轨迹信息等 |
| 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 |
| 其他敏感个人信息 | 身份证件号码、精准定位信息、性取向、通信内容、征信信息、未公开的违法犯罪记录等 |

1. （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：

1. （资料性）  
   去标识化展示示例
   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** | **去标识化示例** |
| --- | --- |
| 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 |

* 1. 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** | **去标识化示例** |
| 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 |

* 1. 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** | **去标识化示例** |
| --- | --- |
| 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，则同身份证号码去标识化方式），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 |
| 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
5. GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求