TC260-PG-20244A

网络安全标准实践指南

—敏感个人信息识别指南

(v1.0-202409)

全国网络安全标准化技术委员会秘书处

2024 年 9 月

本文档可从以下网址获得：

www.tc260.org.cn/

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“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。

声　明

技术支持单位

本《实践指南》得到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、北京理工大学、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、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、中国银联股份有限公司、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、北京小桔科技有限公司、华为技术有限公司等单位的技术支持。

摘　要

依据《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律法规，支撑敏感个人信息处理安全要求国家标准研制工作，指导各组织开展敏感个人信息识别工作，制定本实践指南。

本实践指南给出了敏感个人信息识别规则以及常见敏感个人信息类别和示例。可用于指导各组织识别敏感个人信息，也可为敏感个人信息处理和保护工作提供参考。

目　录

1 范围

本实践指南给出了敏感个人信息识别规则以及常见敏感个人信息类别和示例。

本实践指南可用于指导各组织识别敏感个人信息，也可为敏感个人信息处理和保护工作提供参考。

2 术语与定义

2.1 个人信息

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。

[来源：GB/T 35273—2020, 3.1，有修改]

2.2 敏感个人信息

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。

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、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]

2.3 个人信息主体

个人信息所标识或关联的自然人。

[来源：GB/T 35273—2020, 3.3]

2.4 个人信息处理者

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 敏感个人信息识别规则

个人信息处理者应按照以下规则，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) 一旦遭到泄露或者非法使用，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、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) 一旦遭到泄露或者非法使用，容易导致自然人的人身安全受到危害；

注 2：例如泄露、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危害。

3) 一旦遭到泄露或者非法使用，容易导致自然人财产安全受到危害。

注 3：例如泄露、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。

b) 按照本实践指南第 4 章识别收集、产生的常见敏感个人信息，常见敏感个人信息类别示例见本实践指南附录 A。

注 4：如有充分理由和证据表示处理的个人信息达不到 a）中条件的，可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或融合后的整体属性，分析其一旦泄露或非法使用可能对

个人权益造成的影响，如果符合 a）所述条件，应将汇聚或融合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 常见敏感个人信息

常见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。

注 1：生物识别信息可参考 GB/T 40660、GB/T 41819、GB/T 41807、GB/T 41773、GB/T 41806 等生物识别信息安全国家标准。

b) 宗教信仰信息：与个人信仰的宗教、宗教组织、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、身体或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、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、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常见个人信息。

附录 A　常见敏感个人信息类别示例

常见敏感个人信息见表 A.1。

表 A.1 常见敏感个人信息

类别	典型示例
生物识别信息	个人基因[注 1]、人脸[注 2]、声纹[注 3]、步态[注 4]、指纹、掌纹、眼纹、耳廓、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、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	1. 与个人的身体或心理的伤害、疾病、残疾、疾病风险或隐私有关的健康状况信息[注 5]，如病症、既往病史、家族病史、传染病史、体检报告、生育信息等 2. 在疾病预防、诊断、治疗、护理、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、用药记录）、检验检查数据（如检验报告、检查报告）等
金融账户信息	个人的银行、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、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、人员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[注 6]、身份证照片、性取向、性生活、征信信息、犯罪记录信息[注 7]、展示个人身体私密部位的照片或视频信息等个人信息

注1：基因信息即基因识别数据，具体可参考国家标准GB/T 41806-2022《信息安全技术 基因识别数据安全要求》。

注2：人脸信息即人脸识别数据，具体可参考国家标准GB/T 41819-2022《信息安全技术 人脸识别数据安全要求》。

注3：声纹信息即声纹识别数据，具体可参考国家标准GB/T 41807-2022《信息安全技术 声纹识别数据安全要求》。

注4：步态信息即步态识别数据，具体可参考国家标准GB/T 41773-2022《信息安全技术 步态识别数据安全要求》。

注5：个人的体重、身高、血型、血压、肺活量等基本体质信息，如果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。

注6：通过调用个人手机精准位置权限采集的位置信息是精准定位信息，通过IP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。

注7：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、刑罚等记录。

参考文献

[1] 《中华人民共和国个人信息保护法》

[2] 《中华人民共和国数据安全法》

[3] 《网络数据安全管理条例（征求意见稿）》

[4] GB/T 35273—2020 《信息安全技术 个人信息安全规范》

[5] GB/T 43697—2024《数据安全技术 数据分类分级规则》

[6] GB/T 40660《信息安全技术 生物特征识别信息保护基本要求》

[7] GB/T 41819《信息安全技术 人脸识别数据安全要求》

[8] GB/T 41807《信息安全技术 声纹识别数据安全要求》

[9] GB/T 41773《信息安全技术 步态识别数据安全要求》

[10] GB/T 41806《信息安全技术 基因识别数据安全要求》