ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 41773—2022

信息安全技术　步态识别数据安全要求

Information security technology—Security requirements of gait recognition data

2022-10-12 发布　　2023-05-01 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。

本文件由全国信息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：银河水滴科技(北京)有限公司、中国电子技术标准化研究院、中国科学院自动化研究所、哈尔滨工程大学、北京邮电大学、北京奇虎科技有限公司、公安部第一研究所、中国信息通信研究院、国家工业信息安全发展研究中心、蚂蚁科技集团股份有限公司、北京警察学院、国家计算机网络应急技术处理协调中心、每日互动股份有限公司、OPPO广东移动通信有限公司、公安部物证鉴定中心、南方科技大学、北京得意音通技术有限责任公司、华为技术有限公司。

本文件主要起草人：黄永祯、刘麒赟、郝春亮、张曼、曹春水、谷晓霞、李文英、胡影、许晓耕、王亮、王科俊、卢旗、张屹、刘冬妮、黄岩、傅山、何召锋、柳彩云、孙岩、林冠辰、武鸿浩、赵芸伟、董霖、方毅、杨明慧、叶方坚、于仕琪、邬晓钧、黄小妮、严敏瑞、靳晨、王秉政、黄馨蓓。

信息安全技术　步态识别数据安全要求

1　范围

本文件规定了步态识别数据收集、存储、传输、使用、加工、提供、公开、删除等数据处理活动的安全要求。

本文件适用于步态识别数据处理者规范数据处理活动，监管部门、第三方评估机构对步态识别数据处理活动进行监督、管理、评估参照使用。

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　信息安全技术　术语

GB/T 35273　信息安全技术　个人信息安全规范

GB/T 37988　信息安全技术　数据安全能力成熟度模型

GB/T 39335　信息安全技术　个人信息安全影响评估指南

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 41479　信息安全技术　网络数据处理安全要求

3　术语和定义

GB/T 25069、GB/T 35273、GB/T 37988、GB/T 40660 和 GB/T 41479 界定的以及下列术语和定义适用于本文件。

3.1

步态识别　gait recognition

基于步态所包含的自然人生物学特性和行为特性对自然人进行辨识的技术。

注：步态识别除可用于身份识别应用场景外，也可用于非身份识别应用场景，如行为分析、姿态分析或异常分析等。

3.2

步态样本　gait sample

通过收集、预处理等方式获得的自然人的步态视频或图像序列。

注：步态样本包含自然人步态周期的原始（剪切）视频或连续图像序列，含有衣着、鞋帽、携带物等信息。

3.3

步态剪影　gait silhouettes

步态样本经过分割后得到的序列。

注：步态样本处理后可以得到步态剪影，还可能得到人体部件分割图像序列、三维人体模型序列等。步态剪影通常为黑白图，人体区域白色，背景区域黑色。

3.4

步态特征　gait feature

从步态剪影中提取的用于比对的数据。

注：常用的步态特征包括步态能量图(GEI)、步态熵图(GENI)、步态光流图(GFI)以及时间保持步态图(CGI)等。

3.5

步态识别数据　gait recognition data

步态样本及其处理得到的数据。

注：可单独或者结合其他数据识别自然人身份。

3.6

步态识别数据主体　gait recognition data subject

步态识别数据所标识或者关联的自然人。

注：简称“数据主体”。

4　概述

4.1　步态识别数据活动

步态识别数据活动涉及的数据处理角色包括数据主体、步态识别数据处理者、公共安全管理机构、第三方服务平台等。数据处理过程包括：

a) 步态识别数据的收集：
   1) 需求提出：组织或个人为完成业务活动，对数据主体提出步态识别数据及关联信息使用需求的活动；
   2) 知情同意书签订：数据主体了解步态识别数据的使用目的、方式、范围及步态识别数据处理者名称和联系方式等信息后，双方共同完成的签订知情同意书活动；
   3) 步态样本收集：收集自然人行走视频，并从中提取步态样本的活动。步态样本包括步态视频、图像序列等信息。此活动会产生相应的关联信息，如收集时间、收集地点、收集对象、收集者、收集方式、样本类型、规格、单位、样本保存期限等。
b) 步态识别数据的存储和传输：在数据主体知情同意情况下，对步态识别数据及关联信息进行存储和传输的活动。
c) 步态识别数据的使用：识别、检测、统计所获取的步态识别数据及关联信息。此活动会产生数据主体的关联数据，如步态特征、舞蹈姿态特征、体育竞技特征、行为康复特征等；此活动会产生统计分析数据，如比对日志、舞蹈评分合格统计、体育竞技违规统计等。
d) 步态识别数据的加工、提供、公开：在数据主体单独同意前提下，将步态识别数据及关联信息进行加工、提供和公开的活动。
e) 步态识别数据的删除：在账户注销、授权撤回、授权到期、申请删除等情况下不可逆地删除步态识别数据及关联信息的活动。

4.2　步态识别典型场景

步态识别数据活动典型应用场景包括身份识别应用场景、非身份识别应用场景和科学实验场景。

身份识别应用场景是指步态识别数据用于识别数据主体身份的场景。典型应用场景包括远程身份监控、步态门禁等。

非身份识别应用场景是指步态识别数据用于统计、检测或行为特征分析等活动的场景，不进行数据主体身份识别或验证。典型应用场景包括教育培训领域的舞蹈姿态分析，医疗领域的早期病症诊断、步态康复分析，社会治理领域的涉毒人员行为分析等。

科学实验场景是指步态识别数据用于开展与步态有关的科学实验活动的场景。典型应用场景包括高校或科研机构进行步态识别或步态分析算法研究、开展算法竞赛或评比等。

4.3 步态识别数据活动安全风险

步态识别数据活动中常见安全风险主要包括未经数据主体单独同意收集步态识别数据、紧耦合存储步态识别数据和关联信息、超授权范围使用步态识别数据、篡改步态识别数据、混淆识别对象或改变识别结果、数据传输或提供环节产生泄露、未删除授权过期的步态识别数据等风险，常见安全风险见附录A。

5 基本安全要求

对步态识别数据处理者的基本安全要求如下：

a) 应符合GB/T 35273、GB/T 40660、GB/T 41479规定的要求。

b) 应符合GB/T 37988中数据安全能力成熟度等级3规定的要求。

c) 应仅在步态识别的身份识别方式比其他身份识别方式更具有安全性或便捷性时，采用步态识别的身份识别方式。

d) 开展步态识别数据处理活动前，应按照GB/T 39335的规定开展个人信息安全影响评估，并形成评估报告。

e) 在公共场所安装步态身份识别的设备，应为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的步态识别数据只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

f) 开展步态识别数据处理活动，如需处理从公共场所收集的步态识别数据，应仅在公共安全管理部门有明确要求时与个人身份信息进行关联，其他情况均不应与个人身份信息进行关联。

g) 不应处理从非公共场所收集的步态识别数据，场所所有者或管理者授权的除外。处理活动由组织进行授权的，该组织应与数据处理者共同承担数据安全责任。

h) 应采取措施确保数据主体权利，包括但不限于保障知情同意、获取步态识别数据使用情况、撤回授权、投诉、获得及时响应等。

i) 对于未成年人或无民事行为能力的成年人，开始应用步态识别技术前应取得其监护人（法定代理人）的授权同意。

j) 应针对不同类型、不同阶段的步态识别数据处理活动制定数据安全保护计划，并宜向相关数据主体公开保护计划。

k) 应明确步态识别数据保护负责人，负责步态识别数据保护工作。

l) 应制定数据安全评估制度，定期（如每年）对步态识别技术应用的必要性、安全措施的有效性、数据使用目的的授权情况等进行评估，并根据评估结果完善保护计划。

m) 宜设立数据安全监控指标，在发生数据安全事件或确定存在发生数据安全事件的可能性时，及时评估损失情况，采取补救措施。

n) 在中华人民共和国境内收集或产生的步态识别数据应在境内存储。因业务需要确需出境的，应按照个人信息出境相关规定进行安全评估。

o) 凡涉及采用密码技术解决保密性、完整性、真实性、不可否认性需求的，应遵循密码相关国家标准和行业标准。

6 数据收集

对步态识别数据处理者的要求如下：

a) 收集步态识别数据时，应向数据主体告知步态识别数据的处理规则，包括但不限于使用步态识

别数据的目的、方式、范围及采集时间、采集区域、存储时间、步态识别数据处理者名称和联系方式等信息，并取得数据主体的单独同意。

b) 收集步态识别数据时，应明示数据收集区域并设置清晰标志。数据处理者应确保只收集已明示数据收集区域内的步态识别数据。

c) 在非身份识别应用场景中收集步态识别数据时，应向数据主体声明不将该数据用于身份识别，且采集的数据不宜关联数据主体的个人真实身份信息。

d) 在科学实验场景中收集步态识别数据时，应向数据主体展示科学实验场景知情同意书。科学实验场景知情同意书应清晰、准确、完整地描述步态识别数据处理者的步态识别数据处理活动，并取得数据主体的书面同意，且收集数据应仅记录与科学实验目的有关的必要的个人信息，科学实验场景知情同意书示例见附录B。

e) 采用交互式页面（如网站、移动互联网应用程序、客户端软件等）提供产品或服务的机构，在收集步态识别数据前，应取得数据主体的书面同意。

注：书面同意指通过合同书、信件、电报、传真、电子数据交换和电子邮件等方式进行同意。

f) 步态样本收集现场有人员监督时，监督人员应提供指导，确保不收集未授权人员信息。

g) 步态样本收集现场无人员监督时，应在多处醒目位置提示收集内容和风险。

h) 已授权的数据主体的步态样本失效后，再次收集步态识别数据前应重新取得数据主体的单独同意。

7 数据存储和传输

对步态识别数据处理者的要求如下：

a) 身份识别应用场景不应存储步态样本，仅可在建库时存储步态剪影和步态特征，数据主体单独同意存储的除外；

b) 身份识别应用场景应分开存储步态识别数据和个人身份信息，并采用加密、访问控制等安全措施；

c) 非身份识别应用场景存储数据主体主动上传原始视频信息时，应采用加密、访问控制等安全措施，并保证原始视频信息的完整性；

d) 存储不同类型的步态识别数据时，应按类型分开存储并使用不同密钥分别加密；

注：步态识别数据包括：步态样本、步态剪影、步态特征等。

e) 传输步态识别数据应采取加密等安全措施，保证数据保密性和完整性。

8 数据使用

对步态识别数据处理者的要求如下：

a) 从步态识别数据中提取其他生物特征识别数据，应重新取得数据主体的单独同意；

注：其他生物特征识别数据包括：声纹、人脸等。

b) 基于数据分析结果推荐商业化产品、服务时，应遵循GB/T 35273中对用户画像的使用限制条件，并取得数据主体的单独同意；

c) 采用交互式页面（如网站、移动互联网应用程序、客户端软件等）提供产品或服务的机构，应在其交互页面提供便于数据主体查阅、复制、更正、删除、限制处理、转移个人信息，以及注销账号、撤回处理个人信息同意等权利的功能；

d) 科学实验场景所处理的步态识别数据不应用于商业目的。

9 数据加工、提供与公开

对步态识别数据处理者的要求如下：

a） 应采用不可逆的数据处理过程。

注：如从视频提取步态样本的处理过程，步态样本不可恢复视频，不可逆定义见 GB/T 40660。

b） 应根据业务情况确定数据提供的类型、方式、用途和数量，定义不同级别数据提供安全要求，数据提供时应告知数据主体有关情况，并重新取得数据主体的同意。

c） 因业务需要进行委托处理的，应选择具备步态数据安全保护及处理能力的委托方，应与受委托方签署数据安全协议，内容包括但不仅限于明确委托内容、目的、双方责任义务。受委托方应开放相关系统权限使委托方可对数据处理活动进行监督。

d） 不应公开步态识别数据。

e） 在数据主体主动分享数据分析结果或动作评分前，宜告知数据主体分享内容中包含的敏感信息的类型和可能产生的影响。

10 数据删除

对步态识别数据处理者的要求如下：

a） 对超过数据授权存储期限、数据主体授权撤回等的步态识别数据，应及时删除步态识别数据；

b） 步态识别数据处理目的已实现或相关项目已结项时，应及时删除步态识别数据；

c） 应确保被删除的步态识别数据不可恢复。

附 录 A
（资料性）
步态识别数据常见安全风险

A.1 安全风险描述

步态识别数据常见安全风险包括：

a） 在步态识别数据收集活动中，数据主体未被告知步态识别数据处理目的或未表示单独同意即被收集步态数据；

b） 在步态识别数据存储过程中，步态识别数据处理者未采用有效的安全措施和管理方法，如过度存储步态识别数据、未采取加密措施等，产生敏感信息数据泄露、非法使用等风险；

示例 1：过度存储数据包含：原始信息、人脸图像或第三者步态识别数据等。

c） 在步态识别数据传输过程中，步态识别数据处理者未采用有效安全措施导致数据被泄露或被窃取；

d） 在步态识别数据使用活动中，存在非身份识别数据被应用于身份识别场景、科研数据被应用于商业场景等数据滥用的风险；

e） 在步态识别数据加工活动中，存在加工的目的、结果超出授权范围，或基于加工结果被滥用的风险；

示例 2：医疗康复场景，利用步态识别数据分析用户术后康复状况，用以推荐相应的康复项目；体育、艺术培训场景，利用步态识别数据分析用户动作准确度，用以推荐相应的培训课程。

f） 在步态特征提取过程中，步态识别数据处理者未采用相应的技术手段，导致提取过程或结果数据被逆向还原，产生数据主体敏感信息泄露的风险；

g） 在步态识别数据提供活动中，步态识别数据处理者超出授权范围提供数据，导致数据泄露、滥用风险；

h） 在步态识别数据处理者委托第三方处理步态识别数据的活动中，未采用有效监控，导致受委托方产生数据泄露、滥用等风险；

i） 在步态识别数据公开披露活动中，步态识别数据处理者非法公开披露的风险；

j） 个人身份信息和步态识别数据在应用界面、网站页面等上展示时，步态识别数据处理者未采用脱敏、去标识化等安全措施，或超出授权范围展示数据，造成数据泄露的风险；

k） 步态识别数据处理者未及时删除授权过期数据，或达到业务目的后继续存储数据，造成数据被恢复、泄露的风险，导致数据主体权益受损。

A.2 常见安全风险与条款对照表

本文件针对步态识别数据的常见安全风险给出了相应的要求，具体条款映射关系见表 A.1。

表 A.1 步态识别数据常见安全风险与条款映射表

常见安全风险	本文件章条号
风险 a）	第 6 章
风险 b）	第 7 章 a）～ d）
风险 c）	第 7 章 e）

表 A.1　步态识别数据常见安全风险与条款映射表（续）

常见安全风险	本文件章条号
风险 d）	第 8 章
风险 e）	第 9 章 a）
风险 f）	第 9 章 a）
风险 g）	第 9 章 b）
风险 h）	第 9 章 c）
风险 i）	第 9 章 d）
风险 j）	第 9 章 e）
风险 k）	第 10 章

附 录 B
（资料性）
科学实验场景知情同意书示例

科学实验场景知情同意书是科学实验场景中步态识别数据处理者遵循公开透明原则的重要体现，是保证数据主体知情权的重要手段，还是约束自身行为和配合监督管理的重要机制。科学实验场景知情同意书示例见表 B.1。

表 B.1 科学实验场景知情同意书示例

科学实验场景知情同意书示例	编写要求
研究题目（全称） 知情同意书 （版本号及版本日期）	该部分为科学实验场景知情同意书标题。包括科学实验研究的题目、版本号及版本日期
须知页 我们将要开展一项科学实验项目（全称），现在邀请您参加这项研究。这项实验的主要研究单位是_____（全称）。 请仔细阅读本知情同意书并慎重做出是否参加本项研究的决定，参加这项研究完全是您自主的选择。 在您做出参与本研究的决定之前，您应了解本研究可能的风险和获益。这份文件向您阐述了研究目的、步骤、给您带来的益处、您要承担的风险，同时您有权利在任何时候退出研究；该同意书可能包含您不理解的文字，请让研究人员为您解释您不能清楚理解的任何文字或信息。在做出决定前，您可以将一份未签字的同意书带回家考虑或与家人、朋友或任何您选择的人进行讨论。您有权拒绝参加本研究，也可随时退出研究，且不会受到处罚，也不会失去您应有的权利。 如果您认为您有兴趣参加这项研究，请认真阅读以下材料。我们首先声明：您在阅读后作出不参加这项研究的决定，不会影响您日常的生活或参与项目发起方组织的其他科研、教育活动。详细情况请阅读本《知情同意书》。 a） 研究目的是什么？ b） 研究背景是什么？ c） 研究过程情况是什么？ d） 研究有无任何费用或补偿？ e） 这项研究如何保护我的个人信息和隐私？ f） 这项研究产生的数据在研究结束后如何处理？ g） 我是否可以退出这项研究？ h） 如果我有问题或困难，或想了解研究进展，该与谁联系？ i） 是否存在数据的委托处理及具体情况（委托信息、受委托方信息及权利义务、委托期限等）？ j） 是否存在数据的共享及具体情况（共享方式、共享方信息及权利义务、共享期限等）？ 如果您有与这项研究相关的任何问题和建议，请通过电话或邮箱联系主要研究者。	该部分为数据主体须知范围。包括研究题目的名称、主要研究单位、研究目的、背景、研究过程情况以及数据委托处理及具体情况等

表 B.1　科学实验场景知情同意书示例（续）

<table>
<tr><th>科学实验场景知情同意书示例</th><th>编写要求</th></tr>
<tr><td>
签字页
知情同意声明：
我已被告知此项科学实验的目的、背景、过程、风险及获益等情况。我有足够的时间和机会进行提问，问题的答复我很满意。
我也被告知，当我有问题，想反映困难、顾虑、对研究的建议，或想进一步获得信息，或为研究提供帮助时，应与谁联系。
我已经阅读这份知情同意书，并且同意参加本研究。
我已知晓研究过程中关于步态识别数据的委托处理情况。
我已知晓研究过程中关于步态识别数据的共享情况。
我知道我可以选择不参加此项研究，或在研究期间的任何时候通过文中的联系方式书面通知研究者要求退出，退出后我的步态识别数据及其处理得到的数据、关联信息将被销毁（但已匿名化进行群体分析或匿名化发表的数据无法删除或撤回）。
我将得到这份知情同意书的副本，下面包含我的同意事项，以及我和主要研究者的签名。
<table>
<tr><th>数据处理活动</th><th>涉及的个人信息
（按照实际填写）</th><th>确认</th></tr>
<tr><td>收集</td><td>……</td><td>⊙同意 ⊙不同意</td></tr>
<tr><td>存储</td><td>……</td><td>⊙同意 ⊙不同意</td></tr>
<tr><td>使用</td><td>……</td><td>⊙同意 ⊙不同意</td></tr>
<tr><td>加工</td><td></td><td>⊙同意 ⊙不同意</td></tr>
<tr><td>传输</td><td></td><td>⊙同意 ⊙不同意</td></tr>
<tr><td>提供</td><td></td><td>⊙同意 ⊙不同意</td></tr>
<tr><td>公开</td><td></td><td>⊙同意 ⊙不同意</td></tr>
<tr><td>删除</td><td></td><td>⊙同意 ⊙不同意</td></tr>
</table>
参与者签名：_____　　日期：_____
联系电话：_____　　邮箱：_____
</td><td>该部分为数据主体签字页。包括提示数据主体关于科学实验项目的具体信息和相关人员的签字信息等</td></tr>
<tr><td>
（注：如果受试者不能阅读该知情同意书时，则需一名独立见证人证明研究者已将知情同意书的所有内容告知了参与者，独立见证人需签名和签署日期）
独立见证人签名：　　日期：
联系电话：　　邮箱：

主要研究者签名：　　日期：
联系电话：　　邮箱：
</td><td></td></tr>
</table>

参 考 文 献

[1] GB/T 5271.37—2021 信息技术 词汇 第37部分:生物特征识别

[2] GB 35114—2017 公共安全视频监控联网信息安全技术要求

[3] GB/T 37964—2019 信息安全技术 个人信息去标识化指南

[4] GA/T 1400(所有部分) 公安视频图像信息应用系统

[5] 中华人民共和国民法典(2020年5月28日第十三届全国人民代表大会第三次会议通过)

[6] 中华人民共和国个人信息保护法(2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过)