



# 中华人民共和国国家标准

GB/T XXXXX—XXXX

## 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

（征求意见稿）

（本稿完成时间：2021年4月27日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

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 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 概述 .....	2
4.1 步态识别数据活动典型场景 .....	2
4.2 场景分类 .....	2
4.3 数据控制者 .....	2
5 基本安全要求 .....	3
6 步态识别数据安全处理要求 .....	3
6.1 通用安全处理要求 .....	3
6.2 身份识别应用场景 .....	4
6.3 非身份识别场景 .....	4
6.4 科研场景 .....	4
7 步态识别数据安全要求 .....	5
附录 A（资料性） 步态识别数据活动的典型场景 .....	6
A.1 身份识别应用场景 .....	6
A.2 非身份识别应用场景 .....	6
A.3 科研场景 .....	7
附录 B（资料性） 步态识别数据常见安全风险 .....	8
B.1 常见安全风险 .....	8
B.2 常见安全风险与条款对照表 .....	8
附录 C（资料性） 科学实验场景知情同意书示例 .....	10
参考文献 .....	12

# 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：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、国家计算机网络应急技术处理协调中心、浙江每日互动网络科技股份有限公司、OPPO 广东移动通信有限公司、公安部物证鉴定中心、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、郝春亮、张曼、曹春水、胡影、卢旗、王亮、王科俊、李福全、张屹、刘冬妮、傅山、孙岩、林冠辰、赵芸伟、方毅、杨明慧、叶方坚、黄小妮、严敏瑞、靳晨。

# 信息安全技术 步态识别数据安全要求

## 1 范围

本文件规定了处理步态识别数据的基本安全要求、安全处理和安全管理要求。

本文件适用于涉及步态识别数据相关业务的安全开展，第三方测评机构对涉及步态识别数据的相关业务进行安全评估亦可参照使用。

## 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 35273-2020 信息安全技术 个人信息安全规范
- GB/T AAAAA-AAAA 信息技术 词汇 第37部分：生物特征识别
- GB/T BBBB-BBBB 信息安全技术 网络数据活动安全要求
- GB/T CCCC-CCCC 信息安全技术 生物特征识别信息保护基本要求

## 3 术语和定义

GB/T 35273、GB/T AAAAA-AAAA、GB/T BBBB-BBBB和GB/T CCCC-CCCC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

基于自然人行走时的生物学特性和行为特征对其进行自动辨识。

[来源：GB/T AAAAA，3.1.3，有修改]

### 3.2

#### 步态样本 gait sample

通过采集、预处理等方式获得的自然人的步态视频或步态序列。

注：本文件中样本指包含自然人步态周期的原始视频或剪切视频片段，含有衣着、鞋帽等信息。

### 3.3

#### 人体轮廓序列 silhouettes

步态样本经过分割后得到的序列，常用的为黑白图，人体区域为白色，背景区域为黑色。

注：步态样本处理后可以得到人体轮廓序列，还可能得到人体部件分割图像序列、三维人体模型序列等。

### 3.4

#### 步态特征 gait feature

从人体轮廓序列中提取的用于比对的数据或标记。

[来源：GB/T AAAAA，3.3.11，有修改]

注1：步态特征具有不可逆性。

注2：常用的步态特征包括步态能量图（Gait Engery Image, GEI）、步态熵图（Gait Entropy Image, GEnI），步

态光流图(Gait Flow Image, GFI)以及 时间保持步态图 (Chrono Gait Image, 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，可单独或者结合其它数据识别自然人身份。

注：步态识别数据主要包含步态样本、处理过程数据和步态特征等。

### 3.6

#### 数据主体 data subject

步态识别数据标识或者关联的自然人。

[来源：GB/T 35273-2020, 3.3, 有修改]

### 3.7

#### 数据控制者 data controller

有能力决定步态识别数据处理目的、方式等的组织或个人。

[来源：GB/T 35273-2020, 3.4, 有修改]

### 3.8

#### 匿名化 anonymization

通过对个人信息的技术处理，使得数据主体无法被识别或者关联，且处理后的信息不能被复原的过程。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

[来源：GB/T 35273-2020, 3.14, 有修改]

## 4 概述

### 4.1 步态识别数据活动典型场景

步态识别数据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研场景。在各场景中步态识别数据活动所涉及的角色，以及数据控制者所控制的数据内容不同。

### 4.2 场景分类

步态识别数据应用场景主要包括：

- a) 身份识别应用场景：公共场景、企事业场景、个人应用场景等。
- b) 非身份识别应用场景：医疗康复服务、智能看护服务、体育艺术培训等。
- c) 科研场景主要：科研数据采集场景、身份识别或非身份识别算法研究场景等。

### 4.3 数据控制者

通用的步态识别数据活动及步态识别数据控制者角色和功能见附录A。根据应用场景类别，包含以下步态识别数据控制者：

- a) 身份识别应用场景中包含：涉及视频数据采集处理，个人身份信息、步态识别数据、辅助信息的传输存储，身份验证、身份识别、行动轨迹或数据展示的身份识别服务或产品提供者。
- b) 非身份识别应用场景中包含：涉及视频数据采集处理，用户信息、用户视频、步态识别数据的传输存储，社交应用、用户画像、数据展示或个性化服务的非身份识别服务或产品提供者。
- c) 科研场景中包含：涉及科研视频数据采集处理，科研数据共享、身份验证、身份识别或数据分类等算法研究者。

## 5 基本安全要求

步态识别数据控制者：

- a) 应按照 GB/T 35273-2020 和 GB/T CCCC-CCCC 的要求保护个人信息，应按照 GB/T BBBBB-BBBB 的要求保护数据安全。
- b) 应建立相关机制保障数据主体行使查询、更正、删除、撤回授权同意等权利。对于未成年人或无民事行为能力的成年人，应征得其监护人（法定代理人）的授权同意。

## 6 步态识别数据安全处理要求

### 6.1 通用安全处理要求

#### 6.1.1 数据采集

对数据控制者的要求包括：

- a) 采集步态样本前，应告知数据主体使用步态样本、步态特征等步态识别数据的目的、方式和范围，以及存储时间等信息，并征得数据主体的明示同意。
- b) 应在特定范围内采集数据，确保采集数据的摄像头拍摄区域仅覆盖已明确标识的数据采集范围。
- c) 应明示数据采集场所，设置出入口，并在入口处明确提示数据采集内容、数据采集可能对个人造成的安全风险和影响，例如采用警戒线、隔离带或墙体等方式与非采集场所隔离。
- d) 步态样本采集现场有人员监督时，监督人员应提供指导，确保不采集未授权人员信息。
- e) 步态样本采集现场无人员监督时，应在醒目地方多处提示采集内容和风险。
- f) 已授权的数据主体的步态样本失效后，再次采集数据前应重新征得数据主体的明示同意。

#### 6.1.2 数据传输和存储

步态识别数据控制者进行数据传输、存储时：

- a) 传输步态识别数据应保证通信安全，并保证数据保密性和完整性。
- b) 身份识别应用场景不应存储步态样本，有法律法规明确要求除外。

#### 6.1.3 数据使用

步态识别数据控制者进行数据使用时：

- a) 从步态识别数据中提取和应用其他生物特征识别数据应遵从相应的数据安全标准要求。  
注：其他生物特征数据包括：声纹、人脸等等。
- b) 应采用不可逆的数据处理过程。

#### 6.1.4 数据委托处理、共享、转让、公开披露

步态识别数据控制者进行数据委托处理、共享、转让、公开披露时：

- a) 不应公开披露步态识别数据。
- b) 委托第三方处理步态识别数据，以及嵌入第三方工具处理步态识别数据时，应选择具备步态数据安全保护及处理能力的第三方机构，并应具备相应的技术措施对第三方行为进行检测和记录。
- c) 不应向第三方委托步态样本。
- d) 委托第三方处理步态识别数据时，应预先向步态识别数据主体告知以下信息：
  - 1) 第三方相关信息；

- 2) 所涉步态识别数据的类型、数量和时间；
- 3) 委托处理目的。

### 6.1.5 数据删除、匿名化

步态识别数据控制者进行数据删除、匿名化时：

- a) 对超过授权存储期限、数据主体授权撤回等的步态识别数据，应进行删除或匿名化处理。
- b) 相关业务目的完成后应对步态识别数据进行删除或匿名化处理。
- c) 应定期对数据删除、数据弃用或匿名化效果进行安全评估。

### 6.2 身份识别应用场景

在满足6.1通用安全处理要求基础上，数据控制者还应满足以下要求：

- a) 应向数据主体告知采集数据的目的、使用方式、数据存储时间以及采集者联系方式等信息，并征得数据主体的明示同意。法律法规有相关明确要求的除外。
- b) 对被告知数据采集后依然进入、停留的数据主体，应删除其步态样本。
- c) 不应存储步态样本，执行法律法规等明确要求的除外。
- d) 不同类型的步态识别处理过程数据如需存储，应各类型分开存储并分别加密。  
注：步态识别处理过程数据包括：人体轮廓序列、人体部件分割图像序列等。
- e) 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。应保证处理结果与数据主体的个人信息不可链接，且存储的步态识别数据中不应包含面部图像、工牌等可关联个人身份的信息。
- f) 在本地智能设备中完成的身份识别，处理数据时应遵循最小必要原则，且不对外传输已采集的步态识别数据。

### 6.3 非身份识别场景

在满足6.1通用安全处理要求基础上，数据控制者还应满足以下要求：

- a) 应向数据主体申明不将该数据用于身份识别，且采集的数据不应关联数据主体的个人信息。
- b) 存储数据主体主动上传原始视频信息时，应采用加密等安全措施，并保证数据完整性。
- c) 使用步态识别数据的数据分析结果提供服务时，应在 GB/T 35273-2020、GB/T BBBB-BBBB 基础上遵循服务中相应的数据保护要求，且应对服务中的步态识别的传输、存储采用加密等安全措施。
- d) 基于数据分析结果推荐商业化产品、服务，应遵循 GB/T 35273-2020 7.4 对用户画像的使用限制条件，应获得数据主体同意授权。
- 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）提供产品或服务的体育、艺术培训机构，在采集步态识别数据前，提供电子方式获得数据主体的明示同意，且在其交互页面提供便于数据主体并行使其访问、更正、删除、撤回授权同意、注销账户等权利的功能或选项。
- f) 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。

### 6.4 科研场景

在满足6.1通用安全处理要求基础上，数据控制者还应满足以下要求：

- a) 不应以欺诈、诱骗、误导的方式采集步态样本。
- b) 不应从非法的渠道采集步态样本。

- c) 采集步态样本前，应向数据主体展示科学实验场景知情同意书（示例见附录 C），并获得数据主体的书面授权。
- d) 应单独向数据主体告知科学实验目的，保证不直接用于商业目的，获得数据主体书面授权后，应妥善保管授权材料以便未来追溯。
- e) 应制定科学的研究实验计划，应明确说明研究目的、意义及必要性，相关实验设计、研究过程中可能涉及到的合作及相关数据委托、共享需求，并依照最少数据需求原则，制定采集数量、步态识别数据及其关联信息的采集方法等。
- f) 不应使用概括性用语描述用途，如“用于科研目的”，应更详细说明告知具体用途。
- g) 不应采集数据主体的身份信息，应仅记录与科学实验目的有关的必要的个人信息，如年龄、性别等。
- h) 步态识别数据和关联信息应仅用于获得授权的研究开发活动。
- i) 委托第三方采集步态样本或对步态样本进行标注的，应在“科学实验场景知情同意书”中指明并获得数据主体的授权同意。
- j) 涉及委托事项的“科学实验场景知情同意书”要求如下：
  - 1) 应明确告知数据主体委托的具体信息和期限；
  - 2) 不应要求获得对步态样本委托事项以外的处理授权；
  - 3) 应明确要求被委托者完成数据交付后及时删除存储的步态样本和其他个人信息。
- k) 涉及共享的“科学实验场景知情同意书”要求如下：
  - 1) 应明确告知数据主体共享的方式、对象和期限；
  - 2) 应明确要求接受共享者完成科学实验后及时删除存储的步态识别数据和其他个人信息；
  - 3) 应明确要求接受共享者不得再次共享或转让存储的步态样本。
- l) 不应转让步态样本。
- m) 通过共享方式采集步态样本的，应规定共享使用的期限，且不应再次共享。
- n) 应对步态识别数据进行去标识化处理，科学实验目的完成后应及时删除步态识别数据。

## 7 步态识别数据安全要求

步态识别数据控制者：

- a) 在利用步态识别数据进行身份识别前，应进行安全影响评估，确保身份识别过程无安全风险。
- b) 应设立数据保护责任人负责数据保护工作。
- c) 应针对不同类型、不同处理阶段步态识别数据制定保护计划，并宜向相关步态识别数据主体公开保护计划。
- d) 应定期（如每年）对步态识别系统技术应用的必要性、数据主体授权的自愿性、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。
- e) 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，应及时评估损失情况，采取补救措施；应及时告知数据主体，并按照法律法规相关规定上报主管部门。
- f) 在我国境内采集或产生的步态识别数据，应在境内妥善存储。



附录 A  
(资料性)  
步态识别数据活动的典型场景

A.1 身份识别应用场景

身份识别类场景数据活动示例如图 A.1 所示：

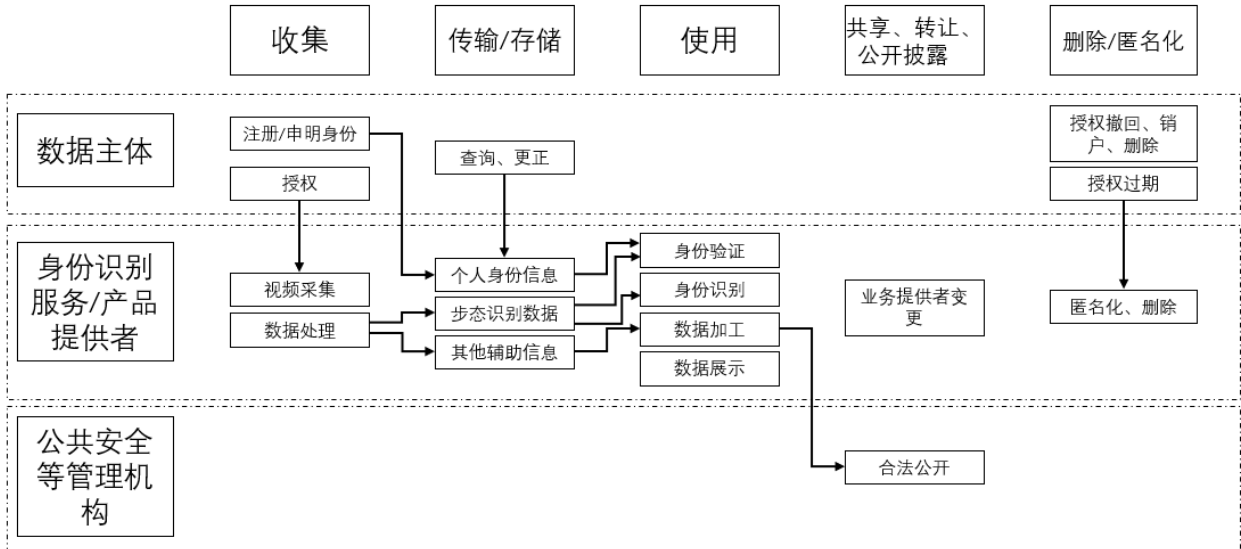


图 A.1 身份识别应用场景下的数据活动图

A.2 非身份识别应用场景

非身份识别类场景数据活动示例如图 A.2 所示：

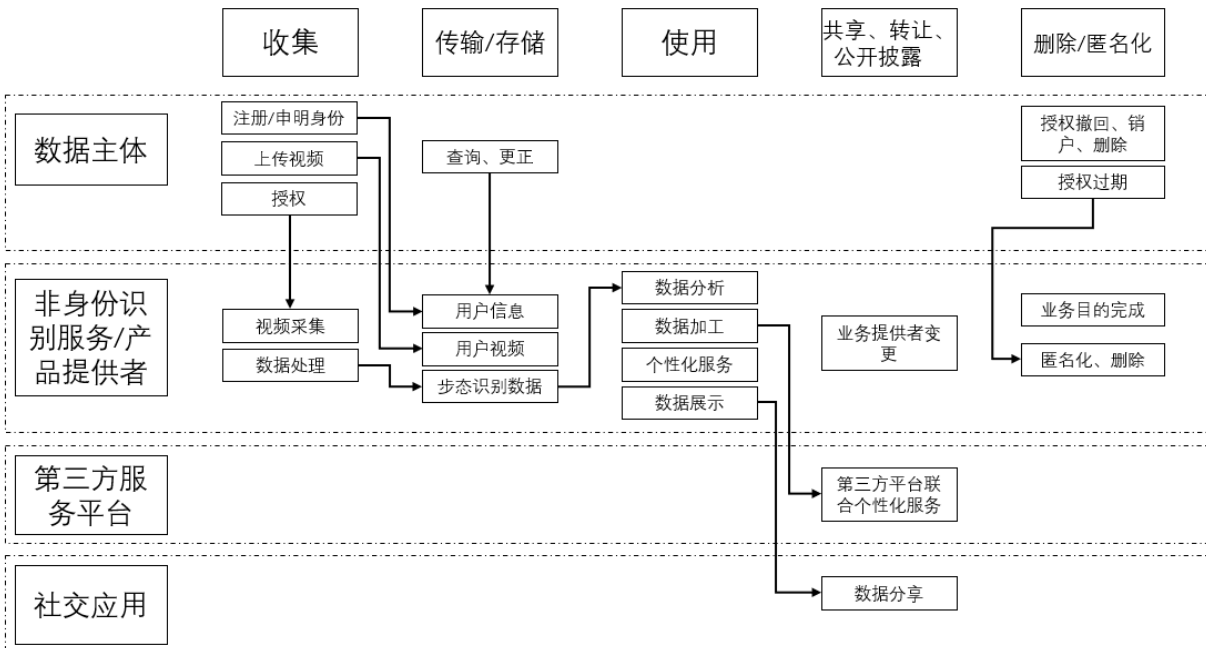


图 A.2 非身份识别类场景下的数据活动图

## A.3 科研场景

科研场景数据活动示例如图 A.3 所示：

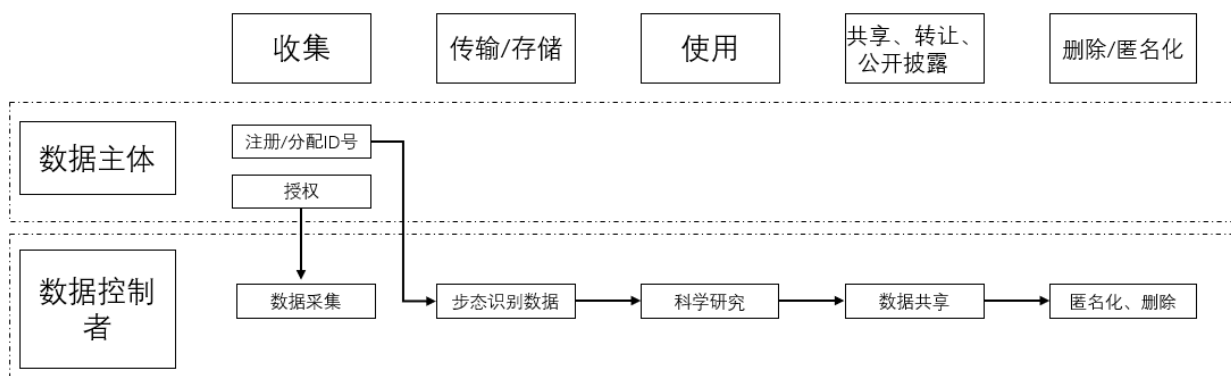


图 A.3 科研场景下的数据活动图

## 附录 B

(资料性)

## 步态识别数据常见安全风险

## B.1 常见安全风险

步态识别数据常见安全风险包括：

- a) 在步态识别数据采集活动中，数据控制者强采、滥采、过度采集步态识别数据的风险。
- b) 步态识别数据在传输过程中，数据控制者未采用有效安全措施导致数据泄露、篡改、窃取的风险。
- c) 在个人身份信息和步态识别数据存储过程中，数据控制者未采用有效的安全措施和管理方法，过度存储步态识别数据，导致数据泄露、异常访问、篡改、窃取等风险。

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。

- d) 在步态识别数据使用活动中，数据被滥用的风险。身份识别结果未采用有效的安全措施，导致数据泄露、存在异常访问等风险。
- e) 在步态特征提取过程中，数据控制者未采用相应的技术手段，导致提取过程或结果数据可结合其他数据通过技术手段逆向还原原始信息或与个人身份信息存在直接关联的风险。
- f) 在步态识别数据公开披露活动中，数据控制者非法公开披露的风险。
- g) 在步态识别数据转让活动中，数据控制者超出授权范围转让数据，导致数据泄露、滥用风险。
- h) 在数据控制者委托第三方接入处理步态识别数据的活动中，未采用有效监控、记录操作日志等措施，导致数据泄露、篡改、窃取等风险。
- i) 数据控制者未及时删除、匿名化授权过期数据，或达到业务目的后继续存储数据，造成数据主体权益受损。
- j) 数据控制者未通过第三方机构对删除、匿名化效果进行安全评估，造成数据被恢复、泄露的风险。
- k) 在步态识别数据加工活动中，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，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，推荐相应的培训课程。

- l) 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，数据控制者未采用脱敏、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。

## B.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响应的要求，具体条款映射关系见表B.1。

表 B.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	本文件条款
风险 a)	6.1.1
风险 b)	6.1.2 a)
风险 c)	6.1.2 b)
风险 d)	6.1.3 a)
风险 e)	6.1.3 b)
风险 f)	6.1.4 a)
风险 g)	6.1.4 d)

风险 h)	6.1.4
风险 i)	6.1.5 a)、 b)
风险 j)	6.1.5 c)
风险 k)	6.3 d)
风险 l)	6.3 f)

## 附录 C

(资料性)

## 科学实验场景知情同意书示例

知情同意书是科学实验场景中数据控制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应清晰、准确、完整地描述数据控制者的步态识别数据处理行为。科学实验场景知情同意书示例见表C.1。

表 C.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
<p style="text-align: center;"><b>研究题目_____（全称）</b> <b>知情同意书</b> <b>（版本号及版本日期）</b></p>	<p>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。</p>
<p style="text-align: center;"><b>须知页</b></p> <p>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）。</p> <p>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。</p> <p>在您做出参与本研究的决定之前，您应该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。</p> <p>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》。</p> <p>a) 研究目的是什么？</p> <p>b) 研究背景是什么？</p> <p>c) 研究过程情况是什么？</p> <p>d) 研究有无任何费用或补偿？</p> <p>e) 这项研究如何保护我的个人信息和隐私？</p> <p>f) 这项研究产生的数据在研究结束后如何处理？</p> <p>g) 我是否可以退出这项研究？</p> <p>h) 如果我有问题或困难，或想了解研究进展，该与谁联系？</p>	<p>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。</p>

<p>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）？</p> <p>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）？</p> <p>如果您有与这项研究相关的任何问题和建议，请联系主要研究者、电话、邮箱。</p>	
<p style="text-align: center;"><b>签字页</b></p> <p>知情同意声明：</p> <p>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。</p> <p>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，应当与谁联系。</p> <p>我已经阅读这份知情同意书，并且同意参加本研究。</p> <p>我已知晓研究过程中关于步态识别数据的委托处理情况。</p> <p>我已知晓研究过程中关于步态识别数据的共享情况。</p> <p>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）。</p> <p>我将得到这份知情同意书的副本，下面包含我和主要研究者的签名。</p> <p>参与者签名：_____ 日期：_____</p> <p>联系电话：_____</p> <p>（注：如果受试者无行为能力/限制行为能力时，则需法定代理人签名和签署日期）</p> <p>法定代理人签名：_____ 日期：_____</p> <p>联系电话：_____</p> <p>（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）</p> <p>独立见证人签名：_____ 日期：_____</p> <p>联系电话：_____</p> <p>主要研究者签名：_____ 日期：_____</p> <p>联系电话：_____</p>	<p>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。</p>

## 参 考 文 献

- [1] 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）
  - [2] GB/T 37964-2019 信息安全技术 个人信息去标识化指南
  - [3] GB/T 35114-2017 公共安全视频监控联网信息安全技术要求
  - [4] GA/T1400-2017 公安视频图像信息应用系统
-