ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 人脸识别数据安全要求

Information security technology — Security requirements of face recognition data

（征求意见稿）

（本稿完成时间：2021 年 04 月 22 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

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、北京赛西科技发展有限责任公司、中国科学院大学、中国信息安全研究院、北京理工大学、公安部第一研究所、公安部第三研究所、北京旷视科技有限公司、上海依图网络科技有限公司、蚂蚁科技集团股份有限公司、国民认证科技（北京）有限公司、环球律师事务所、杭州海康威视数字技术股份有限公司、杭州安恒信息技术股份有限公司、上海观安信息技术股份有限公司、中国移动通信集团有限公司。

本文件主要起草人：杨建军、孙彦、郝春亮、左晓栋、洪延青、梅敬青、刘亦珩、刘贤刚、姚相振、上官晓丽、何延哲、刘丽敏、胡影、李俊、刘军、林冠辰、孟洁、陈星、唐迪、朱雪峰、周少鹏、卢旗、谢江、邱勤。

信息安全技术 人脸识别数据安全要求

1 范围

本文件规定了人脸识别数据的基本安全要求、安全处理要求和安全管理要求。

本文件适用于数据控制者安全开展人脸识别数据相关业务。

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 信息安全技术 网络数据活动安全要求

GB/T BBBBB—BBBB 信息安全技术 生物特征识别信息保护基本要求

GB/T CCCCC—CCCC 信息安全技术 个人信息安全影响评估指南

3 术语和定义

GB/T 35273—2020、GB/T AAAAA—AAAA、GB/T BBBBB—BBBB和GB/T CCCCC—CCCC中界定的以及下列术语和定义适用于本文件。

3.1

人脸图像 face image

自然人脸部信息的模拟或数字表示。

注：人脸图像可通过设备收集，也可对视频、数字照片等进行处理后获得，主要包括可见光图像、非可见光图像(如红外图像)、三维图像等。

3.2

人脸特征 face feature

从数据主体的人脸图像提取的反映数据主体的参数。

3.3

人脸识别数据 face recognition data

人脸图像及其处理得到的，可单独或与其他信息结合识别特定自然人或特定自然人身份的数据。

3.4

数据主体 data subject

人脸识别数据所标识的特定自然人。

[来源：GB/T 35273-2020，3.3，有修改]

3.5

数据控制者 data controller

有能力决定人脸识别数据处理目的、方式等的组织或个人。

[来源：GB/T 35273-2020，3.4，有修改]

3.6

数据处理 process

对人脸识别数据进行收集、存储、使用、共享、转让、公开披露、删除的活动。

4 概述

本文件总结了涉及人脸图像处理的三类场景，包括：

a) 人脸验证：将采集的人脸识别数据与存储的特定自然人的人脸识别数据进行比对（1：1比对），以确认特定自然人是否为其所声明的身份。典型应用包括机场、火车站的人证比对，移动智能终端的人脸解锁功能等。此类场景应满足本文件的基本安全要求、安全处理要求和安全管理要求。

b) 人脸辨识：将采集的人脸识别数据与已存储的指定范围内的人脸识别数据进行比对（1：N比对），以识别特定自然人。典型应用包括公园入园、居民小区门禁等。此类场景应满足本文件的基本安全要求、安全处理要求和安全管理要求。

c) 人脸分析：不开展人脸验证或人脸辨识，仅对采集的人脸图像进行统计、检测或特征分析。典型应用包括公共场所人流量统计、体温检测、图片美化等。此类场景应遵循 GB/T 35273-2020、GB/T AAAAA-AAAA《网络数据活动安全要求》的要求处理人脸图像。

5 基本安全要求

数据控制者：

a) 应遵循 GB/T 35273-2020、GB/T AAAAA-AAAA《网络数据活动安全要求》、GB/T BBBBB-BBBB 《生物特征识别信息保护基本要求》的要求。

b) 处理人脸识别数据时应遵循最小必要原则。

c) 应采取安全措施确保数据主体权利，包括但不限于获取人脸识别数据使用情况、撤回授权、注销账号、投诉、获得及时响应等。

d) 不应收集未授权自然人的人脸图像。

e) 应具备与其所处理人脸识别数据的数量规模、处理方式等相适应的数据安全防护和个人信息保护能力。

f) 开展人脸验证或人脸辨识时，应至少满足以下要求：

1） 非人脸识别方式安全性或便捷性显著低于人脸识别方式。

示例：机场、火车站进行人证比对时，使用人脸识别以外的身份识别方式会导致相关服务便捷性的明显下降。

2） 原则上不应使用人脸识别方式对不满十四周岁的未成年人进行身份识别。

3） 应同时提供非人脸识别的身份识别方式，并提供数据主体选择使用。
4） 应提供安全措施保障数据主体的知情同意权。
5） 人脸识别数据不应用于除身份识别之外的其他目的，包括但不限于评估或预测数据主体工作表现、经济状况、健康状况、偏好、兴趣等。

6 安全处理要求

6.1 收集

数据控制者：

a） 收集人脸识别数据时，应向数据主体告知收集规则，包括但不限于收集目的、数据类型和数量、处理方式、存储时间等，并征得数据主体明示同意。
b） 在自然人拒绝使用人脸识别功能或服务后，不应频繁提示以获取自然人对人脸识别方式的授权同意。
c） 不应因数据主体不同意收集人脸识别数据而拒绝数据主体使用基本业务功能。
d） 用于采集人脸识别数据的设备应遵循相关标准要求。
示例：公共安全区域对人脸图像的采集应符合 GB 37300-2018、GB/T 38671-2020 的要求。
e） 在公共场合收集人脸识别数据时，应设置数据主体主动配合人脸识别的机制。
注：主动配合指要求数据主体直视收集设备并做出特定姿势、表情，或者通过标注“人脸识别”的专用收集通道等。
f） 在满足应用场景安全要求前提下，应仅收集用于生成人脸特征所需的最小数量、最少图像类型的人脸图像。

6.2 存储

数据控制者：

a） 在发生以下情况时，应删除人脸识别数据或进行匿名化处理：
1） 数据主体明示停止使用功能、服务，或撤回授权；
2） 数据主体授权的存储期限到期；
3） 数据控制者无法提供或停止提供服务；
4） 其他应删除人脸图像或进行匿名化处理的情况。
b） 应采取安全措施存储和传输人脸识别数据，包括但不限于加密存储和传输人脸识别数据，采用物理或逻辑隔离方式分别存储人脸识别数据和个人身份信息等。
c） 不应存储人脸图像，经数据主体单独书面授权同意的除外。
注：书面授权形式包括通过合同书、信件、电报、传真、电子数据交换和电子邮件方式进行授权。

6.3 使用

数据控制者：

a） 应在完成验证或辨识后立即删除人脸图像。
b） 应生成可更新、不可逆、不可链接的人脸特征。
注 1：可更新指从同一人脸图像可产生不同的人脸特征。当特定人脸特征泄露时，可重新生成不同的人脸特征。
注 2：不可逆指无法从人脸特征恢复人脸图像。
注 3：不可链接指根据同一人脸图像产生的不同人脸特征之间不具备关联性。
c） 应具备防护呈现干扰攻击的能力。

注 4：呈现干扰攻击主要包括使用人脸照片、纸质面具、人脸视频、人脸合成动画、仿真人脸三维面具等攻击和干扰人脸识别。

d) 在本地和远程人脸识别方式均适用时，应使用本地人脸识别。

注 5：本地人脸识别是在采集终端中完成人脸识别数据的采集和人脸识别。远程人脸识别是通过采集终端完成人脸识别数据采集，并在服务器端完成人脸识别。

6.4 委托处理、共享、转让、公开披露

数据控制者：

a) 不应公开披露人脸识别数据，原则上不应共享、转让人脸识别数据。因业务需要，确需共享、转让的，应按照 GB/T CCCCC《个人信息安全影响评估指南》开展安全评估，并单独告知数据主体共享或转让的目的、接收方身份、接收方数据安全能力、数据类别、可能产生的影响等相关信息，并征得数据主体的书面授权。

b) 原则上不应进行委托处理，确需委托处理的，应在委托处理前审核受委托者的数据安全能力，并对委托处理行为开展个人信息安全影响评估。

7 安全管理要求

数据控制者：

a) 应落实数据安全管理责任，在个人信息安全管理制度中明确人脸识别数据保护要求，包括但不限于保护策略、处理规则等。

b) 在发生或者可能发生人脸识别数据泄露、损毁、丢失的情况时，应立即采取补救措施，按照规定及时告知数据主体，并向相关主管部门报告。

a) 在我国境内收集或产生的人脸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。

参 考 文 献

[1] GB/T 37964—2019 信息安全技术 个人信息去标识化指南

[2] GB/T 26238—2010 信息技术 生物特征识别术语

[3] ISO/IEC 24745:2011 Information technology — Security techniques — Biometric information protection

[4] NIST SP 800-76-2 Biometric Specifications for Personal Identity Verification