ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 41819—2022

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

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：中国电子技术标准化研究院、中国科学院大学、中国信息安全研究院有限公司、北京理工大学、公安部第一研究所、公安部第三研究所、中国科学院自动化研究所、国家计算机网络应急技术处理协调中心、北京旷视科技有限公司、蚂蚁科技集团股份有限公司、国民认证科技(北京)有限公司、北京赛西科技发展有限责任公司、上海依图网络科技有限公司、北京市环球律师事务所、中国移动通信集团有限公司、杭州海康威视数字技术股份有限公司、阿里巴巴(北京)软件服务有限公司、复旦大学、杭州安恒信息技术股份有限公司、上海商汤智能科技有限公司、海信集团控股股份有限公司、华为技术有限公司、北京百度网讯科技有限公司、京东科技控股股份有限公司、浙江大华技术股份有限公司、北京眼神智能科技有限公司、云从科技集团股份有限公司、天融信科技集团股份有限公司、中国信息通信研究院、上海观安信息技术股份有限公司。

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、张堃博、钟陈、许晓耕、卢旗、朱雪峰、韩晗、周少鹏、邱勤、彭骏涛、成瑾、雷晓锋、高雪松、严敏瑞、李玲、张晓寒、李腾飞、王海棠、杨春林、傅山、谢江、李军、付昊。

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安全通用要求以及收集、存储、使用、传输、提供、公开、删除等具体处理活动的安全要求。

本文件适用于数据处理者安全开展人脸识别数据处理活动。

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　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 35273、GB/T 40660 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：人脸图像可从设备收集或通过视频、数字照片等获取，主要类型包括可见光图像、非可见光图像(如红外图像)、三维图像等。

3.2

人脸特征　face feature

从人脸图像提取的反映自然人脸部信息特征的参数。

3.3

人脸识别数据　face recognition data

可识别自然人身份的人脸图像或人脸特征。

3.4

人脸识别数据主体　face recognition data subject

人脸识别数据所标识或关联的自然人。

注：人脸识别数据主体简称数据主体。

4　概述

人脸识别数据主要用于识别自然人身份，典型应用包括机场、火车站使用人脸识别数据进行人证比

对，移动智能终端、应用程序使用人脸识别数据实现解锁、支付等功能，公园、居民小区等使用人脸识别数据核对人员身份。

5 安全通用要求

数据处理者处理人脸识别数据的安全通用要求如下：

a) 实现相同目的或达到同等安全要求可采用非人脸识别方式的，应优先选择使用非人脸识别方式。

b) 应仅在人脸识别方式比非人脸识别方式更具安全性或便捷性时，采用人脸识别方式进行身份识别；应同时提供人脸识别方式和非人脸识别方式，并由自然人选择使用。

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

c) 不应诱导自然人使用人脸识别方式，包括但不限于将人脸识别方式作为身份识别首选方式或默认方式，设置障碍使自然人难以选择使用非人脸识别方式等。

d) 在自然人拒绝使用人脸识别方式后，不应频繁提示以获取自然人对人脸识别方式的同意，例如，在 48h 内提示次数超过 1 次。

e) 应符合 GB/T 35273、GB/T 40660、GB/T 41479 的要求，以及 GB/T 37988 中数据安全能力成熟度等级 3 规定的要求。

f) 应在处理人脸识别数据前自行或委托第三方机构按照 GB/T 39335 规定的要求开展个人信息保护影响评估，评估内容包括但不限于：

1) 是否符合法律、行政法规和国家标准的强制性要求，是否符合公序良俗；

2) 是否具有特定的目的和充分的必要性；

3) 是否具备满足实现目的所需的准度、精度要求；

4) 是否采取了与面临的安全风险相适应的安全防护措施，以防范人脸识别数据泄漏、篡改、丢失、损毁或被非法获取、非法利用等安全风险；

5) 是否采取了措施以有效降低可能对数据主体权益带来的损害和不利影响。

g) 在发生以下情形时，应重新进行个人信息保护影响评估：

1) 人脸识别数据的处理目的、处理方式发生变化；

2) 人脸识别数据发生泄漏、篡改、丢失、损毁或被非法获取、非法利用等安全事件，表明已有安全措施难以有效防范安全风险。

h) 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的，应取得其监护人单独同意；应设置专门的未成年人个人信息保护规则和用户协议，并指定专人负责未成年人个人信息保护。

i) 除非经数据主体单独同意或书面同意，不应将人脸识别数据用于数据主体的评估或预测，包括但不限于评估或预测数据主体的工作表现、经济状况、健康状况、偏好、兴趣、消费行为和活动轨迹等。

j) 除非经数据主体单独同意或书面同意，不应存储人脸图像。

k) 应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：

1) 人脸识别数据的管理规定和操作规程；

2) 人脸识别数据的处理规则；

3) 人脸识别数据的处理权限，并定期对相关人员进行安全教育和培训；

4) 采取的安全防护措施，以防范人脸识别数据泄漏、篡改、丢失、损毁或被非法获取、非法利用等安全风险。

l) 对于处理超过 10 万人的人脸识别数据的数据处理者，应设置专门的个人信息保护机构和个人信息保护负责人，对个人信息保护负责人和关键岗位人员进行安全背景审查，并公开个人信息

保护负责人的联系方式。

m) 人脸识别数据处理规则应包括但不限于：

1) 收集、使用、存储人脸识别数据的目的、方式、范围，以及人脸识别数据的存储期限；

2) 可能对数据主体权益带来的损害和不利影响，以及拒绝提供的后果；

3) 数据主体自主管理其人脸识别数据的途径和方法，包括但不限于访问、更正、删除人脸识别数据及撤回同意；

4) 委托处理人脸识别数据的情况，以及相关保护义务和法律责任；

5) 发生人脸识别数据泄漏等安全事件的赔偿、处置规则；

6) 人脸识别数据处理规则的解释渠道，以及安全问题的询问、投诉、举报渠道。

n) 针对人脸识别数据泄漏、篡改、丢失、损毁或被非法获取、非法利用等安全风险，应制定应急预案并开展应急演练。

o) 当发生人脸识别数据泄漏、篡改、丢失、损毁或被非法获取、非法利用等安全事件时，应立即启动应急预案，采取相应处置或补救措施，包括但不限于：

1) 评估可能造成的安全风险，必要时暂停相关服务；

2) 24 h 内以电话、短信、邮件等方式向数据主体告知安全事件情况和防止、减轻损害的措施，确实无法单独告知数据主体的，可采用发布公告的方式告知；

3) 向相关主管部门报告。

p) 应建立保障数据主体权利的机制，保障数据主体知情同意、获取人脸识别数据处理情况、撤回同意、注销账号、投诉、获得及时响应等方面的权利，并及时响应数据主体的相关请求。

q) 在中华人民共和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。

r) 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 人脸识别数据收集要求

数据处理者收集人脸识别数据的要求如下：

a) 收集人脸识别数据时，应向数据主体告知人脸识别数据的相关事项，包括但不限于数据处理者的名称和联系方式、个人信息保护负责人的姓名和联系方式、处理规则、必要性依据等，并征得数据主体单独同意或书面同意；未取得数据主体单独同意收集的人脸图像应立即删除并确保不可恢复；

b) 数据主体不同意收集人脸识别数据的，不应拒绝数据主体使用基本业务功能；

c) 应采用需要数据主体主动配合的措施收集人脸识别数据；应在识别过程中持续告知数据主体验证目的，并通过语言、文字等向数据主体进行提示；

注：需要数据主体主动配合的措施包括要求数据主体直视收集设备并做出目光注视、特定姿势、表情，或者通过标注了人脸识别应用的文字、图示、图标或符号的专用收集通道等。

d) 应仅收集生成人脸特征所需的最小数量、最少图像类型的人脸图像；

e) 应采取安全措施保证人脸识别数据的真实性、完整性和一致性，防止人脸识别数据在收集过程中泄漏或篡改。

7 人脸识别数据存储要求

数据处理者存储人脸识别数据的要求如下：

a) 应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；
b) 应采取加密存储等安全措施存储人脸识别数据；
c) 数据主体个人所有且具备人脸识别功能的信息技术产品，包括但不限于移动智能终端、智能家居设备等，应将人脸识别数据存储在信息技术产品中，并可由数据主体删除。

8 人脸识别数据使用要求

数据处理者使用人脸识别数据的要求如下：

a) 应在使用人脸识别数据识别自然人身份后立即删除用于识别的人脸图像；
b) 人脸特征应具有可更新、不可逆、不可链接的特性；

注 1：可更新指当特定人脸特征泄漏或作废时，同一人脸图像可提取与该特征不同的人脸特征；不可逆指无法从人脸特征恢复出对应的人脸图像。不可链接指同一人脸图像提取的不同人脸特征之间不具备关联性。

c) 在本地和远程人脸识别方式均适用时，应优先使用本地人脸识别；

注 2：本地人脸识别是在终端设备中进行人脸识别数据收集、使用等处理活动的过程，该方式中人脸识别数据的处理均在终端设备完成。远程人脸识别是在终端设备收集人脸识别数据，在服务器端使用人脸识别数据的过程，该方式中人脸识别数据的处理在终端设备和服务器端分别进行。

d) 应对人脸识别数据使用行为进行审计。

9 人脸识别数据传输要求

数据处理者应采取双向身份鉴别、数据完整性校验、数据加密等措施保障人脸识别数据传输安全。

10 人脸识别数据提供、公开要求

数据处理者提供、公开人脸识别数据的要求如下：

a) 除非经数据主体单独同意或书面同意，不应公开人脸识别数据。
b) 不宜向第三方提供或委托处理人脸识别数据。因业务需要确需提供或委托处理的，应满足的安全要求包括但不限于：
   1) 按照 GB/T 39335 规定的要求对数据接收方开展安全评估，并通过合同等方式约定提供或委托处理的目的、期限、方式、保护措施等，并对数据接收方的处理活动进行监督；
   2) 在提供或委托处理前，单独告知数据主体人脸识别数据向数据接收方提供或委托的目的、数据接收方身份、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，并征得数据主体单独同意或书面同意；
   3) 数据接收方应按约定处理人脸识别数据，不得超出约定的目的、方式等处理人脸识别数据，不得转委托；数据接收方应采取安全措施保障所处理的人脸识别数据安全；委托不生效、无效、被撤销或终止的，数据接收方应将人脸识别数据返还，并予以删除，不得保留或恢复。
c) 因合并、分立等原因转移人脸识别数据的，应向数据主体告知数据接收方的身份、联系方式；数据接收方应继续履行数据处理者的保护义务；数据接收方变更处理目的、处理方式的，应重新向数据主体告知并取得数据主体单独同意或书面同意；没有数据接收方或未取得数据主体单独同意或书面同意的，应删除人脸识别数据并确保不可恢复。

11 人脸识别数据删除要求

数据处理者在发生以下情况时，应在15日内删除人脸识别数据并确保不可恢复：

a) 人脸识别数据处理目的已实现、无法实现或者为实现处理目的不再必要；

b) 人脸识别数据存储时间达到数据主体单独同意或书面同意的存储期限；

c) 数据主体撤回同意或明示停止使用；

d) 数据处理者停止提供人脸识别业务；

e) 数据主体一年未使用数据处理者提供的产品或服务；

f) 法律、行政法规规定的其他情形。

参 考 文 献

[1] GB/T 37036.3—2019 信息技术 移动设备生物特征识别 第3部分:人脸
[2] GB 37300—2018 公共安全重点区域视频图像信息采集规范
[3] GB/T 38671—2020 信息安全技术 远程人脸识别系统技术要求