TC260-PG-20251A

网络安全标准实践指南

——人脸识别支付场景个人信息安全保护要求

（V1.0-202501）

全国网络安全标准化技术委员会秘书处

2025 年 1 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。

本文件起草单位：中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心北京分中心、蚂蚁科技集团股份有限公司、中国银联股份有限公司、国民认证科技（重庆）有限公司、北京友宝在线科技股份有限公司、深圳市丰宜科技有限公司、浙江嗨便利网络科技有限公司、武汉轻购云科技有限公司。

本文件主要起草人：姚相振、胡影、陈亮、郝春亮、陈舒、霍然、张雨桐、徐羽佳、高超、王寒生、黄晴、张立尧、林冠辰、展昭、李俊、晁华、单新宁、荆磊、卢文杰。

声　明

本《实践指南》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。

摘　要

依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规，指导开展人脸识别场景个人信息处理工作，制定本文件。

本文件给出了人脸识别支付场景数据收集、存储、传输、导出、删除等环节的安全要求，可为人脸识别支付服务提供方、人脸验证服务方、相关场所管理方、相关设备运营方处理个人信息提供参考。

目　录

1 范围

本文件给出了人脸识别支付场景数据收集、存储、传输、导出、删除等环节的安全要求，可为人脸识别支付服务提供方、人脸验证服务方、相关场所管理方、相关设备的运营方处理个人信息提供参考。

2 术语定义

2.1 人脸识别支付服务提供方

通过网络支付服务平台，提供人脸识别支付服务的组织。

2.2 人脸验证服务方

通过执行人脸识别的各个环节（包括人脸识别数据采集、人脸特征处理、人脸识别数据存储、人脸识别数据比对、人脸识别结果决策）提供身份验证服务的组织。

注：在人脸识别支付场景下，人脸验证服务方和人脸识别支付服务提供方存在为同一主体的情形，此时人脸识别支付服务提供方应当同时遵守本文件中对人脸验证服务方提出的要求。

2.3 场所管理方

对人脸识别支付场景的设置、应用、管理起到决定性作用的组织或个人。

示例：写字楼物业、园区物业、营业厅、小区居委会等。

2.4 设备运营方

通过布放人脸识别支付设备为用户提供支付服务的经营主体。

示例： 运营自动售货机提供自动售货服务的企业或个人。

2.5 相关方

本文件中人脸识别支付服务提供方、人脸验证服务方、场所管理方、设备运营方的统称。

2.6 用户

使用人脸识别支付服务的个人。

3 概述

本文件中人脸识别支付服务主要覆盖两大类场景：

a) 通过用户所拥有的设备（以下简称“用户设备”）提供的人脸识别支付服务，例如手机银行、手机支付的App、小程序等。在该类场景中，相关方包含人脸识别支付服务提供方、人脸验证服务方、用户，不涉及场所管理方及设备运营方。

b) 通过经营主体布放的设备（以下简称“经营主体布放设备”）提供的人脸识别支付服务，例如柜员机、售货机、售货车等。在该类场景中，相关方涉及人脸识别支付服务提供方、人脸验证服务方、场所管理方、设备运营方。

例1：银行在其营业厅内自有设备上提供人脸识别支付服务，此时人脸识别支付服务提供方、设备运营方以及场所管理方均为同一组织。

例2：公共场所布放的非自有售货机，售货机上的人脸识别支付服务由其他企业提供，此时设备运营方、场所管理方、人脸识别支付服务提供方三者均不相同。

例3：公共场所布放的自有售货机，售货机上的人脸识别支付服务由其他企业提供，此时设备运营方与场所管理方相同，但与人脸识别支付服务提供方不同。

例4：人脸识别支付服务提供方将其自有售货机摆放在其他企业管理的场所，此时人脸识别支付服务提供方与设备运营方相同，但与场所管理方不同。

4 基本要求

要求如下：

a) 相关方开展人脸识别支付相关工作，涉及网络安全、数据安全、个人信息安全、系统安全、密码应用等，应符合我国相关法律法规要求并参考有关国家标准实施。

注：相关标准见 GB/T 35273、GB/T 40660、GB/T 41819 以及 GB/T 42015 等。

b) 人脸验证服务方所采用的人脸识别技术，应实现人脸特征不可逆、不可链接等特性。

注：实现上述特性具体技术方案可参考 GB/T 40660。

c) 设备运营方、场所管理方不应处理因人脸识别支付产生的人脸识别数据。

d) 人脸识别支付服务提供方及人脸验证服务方应事前开展个人信息保护影响评估。

e) 人脸验证服务方提前取得个人单独授权同意后方可开展人脸数据处理活动：

1) 授权协议中应包含使用人脸识别技术处理人脸数据的必要性以及对个人权益的影响；

2) 授权协议应清晰易读，便于用户查阅。

f) 人脸验证服务方不应将人脸识别数据用于除验证该个人身份外的任何其他目的。

g) 人脸识别支付服务提供方如需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。

h) 人脸识别支付服务提供方如需集成人脸验证服务方提供的SDK或云服务进行人脸识别，应监督、核实人脸验证服务方满足本文件提出的要求。

i) 相关方应共同保障非人脸识别数据，包括拍摄时采集到的背景图像、其他个人的相关图像等，以及其经处理产生的数据，不传出设备。

5 人脸识别支付服务提供方

5.1 数据收集安全

用户通过用户设备或经营主体布放设备使用人脸识别服务，人脸识别支付服务提供方应满足：

a) 收集人脸识别数据时，应向用户告知收集人脸识别数据的相关事项以及可能影响，并取得个人的单独同意；因意外，未取得用户单独同意前收集到人脸图像的，应立即删除、不进行其他处理并确保不可恢复；

b) 应采取需要用户主动配合的措施收集人脸识别数据，并在获得人脸识别结果后及时停止收集。

注：需要用户主动配合的措施包括要求用户直视收集设备并做出目光注视、特定姿势、表情，或进入明确标注了人脸识别应用的专用收集通道等。

5.2 数据存储安全

不应存储人脸识别数据，按照法律法规明确要求进行留存的人脸识别相关存证数据除外，且不应将人脸识别相关存证数据用于存证外

其他用途。

6 人脸验证服务方

6.1 数据收集安全

用户通过用户设备或经营主体布放设备使用人脸识别服务，人脸验证服务方均应满足：

a) 应仅收集生成人脸特征所需的最小数据、最少图像类型的人脸图像；

b) 人脸识别支付摄像头只有在支付用户临近并进行了支付启动的相关操作后方可开启，不得在用户未启动支付相关操作前开启摄像头，用户人脸识别完成后应立即关闭摄像头；

c) 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露或篡改。

6.2 数据存储安全

用户通过用户设备或经营主体布放设备使用人脸识别服务，人脸验证服务方均应满足：

a) 进行人脸识别支付，应仅留存注册过程中具备不可逆、不可链接特性的人脸比对模板，不保留其他数据，有关管理部门有明确要求保留存证的除外；

b) 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；

c) 应采取加密存储等安全措施存储人脸识别数据；

d) 向用户征得人脸识别数据处理相关授权时，应明确告知人脸数据的保存期限；

e) 超过保存期限的，用户人脸识别数据应全部删除。

6.3 数据传输安全

用户通过用户设备或经营主体布放设备使用人脸识别服务，人脸验证服务方均应满足：

a) 如需将人脸识别数据传出设备，应仅传输具备不可逆、不可链接等特点的人脸识别数据，不应传输其他人脸识别相关数据，有关管理部门有明确要求保留存证的除外；

注：相关技术规范见GB/T 40660《信息安全技术 生物特征识别信息保护基本要求》。

b) 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。

6.4 数据导出安全

用户通过用户设备或经营主体布放设备使用人脸识别服务，人脸验证服务方均应满足：

a) 不应导出其留存的人脸识别数据，有关管理部门有明确要求的除外；

b) 不应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，应进行个人信息保护影响评估并按照法律要求取得相应的合法性基础。

6.5 数据删除安全

用户通过用户设备或经营主体布放设备使用人脸识别服务，人脸验证服务方均应满足：

a) 除注册时保留的人脸识别数据外，人脸识别全部过程数据在当次人脸识别结果产生后全部删除，以下数据除外：

1) 注册时保存的特征信息；

2) 为保证个人财产安全，相关主管部门明确要求必须保留的数据。

b) 对人脸识别数据的删除或匿名化处理效果进行评估，确保已删除或匿名化处理的人脸识别数据不具备还原能力。

7 场所管理方

用户通过经营主体布放设备使用人脸识别支付服务时，场所管理方应满足：

a) 应检查设备是否符合 8.1 要求，专门为公共安全管理定制的设备除外。

b) 应防止摄像头非正常调用，且使用于人脸识别的摄像头拍摄范围合理，包括：

1) 不朝向更衣室、厕所、浴室等隐私区域；

2) 不朝向个人进行敏感交互操作的区域，交互过程已被持续遮挡隐蔽的除外。

例：进行账号输入、口令输入等的区域。

8 设备运营方

8.1 数据收集安全

用户通过经营主体布放设备使用人脸识别支付服务时，设备运营方应满足：

a) 提前检查设备摄像头情况：

1) 安装高度选择、人脸采集摄像头参数设置等应遵循最小化采集人脸原则；

2) 用于人脸识别的摄像头开启时，设备应采用亮屏、亮灯、屏幕提示等方式对外提示摄像头已开启，该提示应明显易察觉；

3) 除用于人脸识别的摄像头外，设备上不应设置其他朝向设备周边环境的摄像头：

- 已安装相关硬件确实无法拆除的，应通过停止供电、软件禁用等方式停止该功能；
- 交易管理、货品管理等所需的摄像头不应朝向设备外；
- 可移动设备，因智能驾驶等设备移动需要布置的摄像头除外，但应通过该摄像头收集的视频、图像应仅用于帮助设备移动，实时进行删除，不应分析人脸特征，不传出设备。

b) 人脸采集摄像头应仅能被特定的支付 App 调用。

c) 人脸采集摄像头采集链路宜具备防止旁路或劫持的安全措施，可采取的手段包括但不限于数据加密传输等。

d) 内部货物摄像头应通过调整拍摄的角度和清晰度等，仅识别用户取货的动作，不得拍摄用户人脸及其他周边区域。

注：无法识别自然人身份的人脸局部区域的拍摄不包括在本条范围内。如因用户主动行为导致拍摄到人脸图像，企业应实时对人脸图像进行打码处理。

e) 用户通过经营主体布放设备使用人脸识别支付服务时，用户不同意收集人脸识别数据的，不应拒绝用户使用其他方式进行支付。

f) 不应强制要求用户在人脸识别支付过程中绑定手机号。

g) 设备运营方不应将人脸识别作为支付的默认选项。

h) 设备运营方不应通过关注公众营销账号等附加流程增加用户选择其他非人脸识别支付方式的难度。

i) 设备运营方为用户提供人脸识别支付及非人脸识别支付选择时，人脸识别支付选项的表现形式不应显著优于非人脸识别支付选项的表现形式，例如按钮更大、颜色更突出、点击更便捷等。

8.2 数据存储安全

用户通过经营主体布放设备使用人脸识别支付服务时，设备运营方不应存储人脸识别数据。

8.3 数据传输安全

用户通过经营主体布放设备使用人脸识别支付服务时，设备运营方不应通过旁路、镜像等方式获取人脸识别数据。

参考文献

[1] GB/T 35273 信息安全技术　个人信息安全规范

[2] GB/T 40660 信息安全技术　生物特征识别信息保护基本要求

[3] GB/T 41819 信息安全技术　人脸识别数据安全要求

[4] GB/T 42015 信息安全技术　网络支付服务数据安全要求