ICS 13.310
A 91

团　体　标　准

T/ZJAF 5—2020

安全防范 人脸数据安全管理规范

Security protection —

Specifications for security management of face data

2020-09-15 发布　　2020-10-01 实施

浙江省安全技术防范行业协会 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。

本文件由浙江省安全技术防范行业协会提出并归口。

本文件起草单位：浙江昊阔物联科技有限公司、山西省综改示范区公安分局视频大数据实验室、广州像素数据技术股份有限公司、北京深醒科技有限公司、浙江大华技术股份有限公司、杭州海康威视数字技术股份有限公司、上海观安信息技术股份有限公司、浙江省公安科技研究所、浙江宇视科技有限公司、苏州科达科技股份有限公司、东方网力科技股份有限公司、浙江方正安防工程有限公司、温州市保安服务总公司、杭州平治科技有限公司、杭州宇泛智能科技有限公司、浙江省安全技术防范行业协会、杭州智衍科技有限公司。

本文件主要起草人：赵军、姚若光、杜云鹏、王树林、张兴明、廖双龙、应洪波、谢江、赵静岚、吴参毅、刘晓明、邹文艺、傅春、邓志吉、孔维生、朱志敏、马里剑、晋兆龙、黄琛泽、李伟、范绍富、林川江、李伟、郑东、李军、孙嘉、宋林、胡笑、骆晗、朱仁志、卢晓倩。

引　言

近年来，随着互联网应用的全面普及和人工智能技术的快速发展，人脸信息的采集、检测和识别技术在各行各业广泛使用，越来越多的组织收集、使用人脸数据，带来了人脸数据的非法采集、滥用和泄露等安全问题。人脸数据是个人信息数据的重要组成部分，有必要采取相应的安全管理策略，以保护人脸数据及个人信息安全。

本文件针对安全防范领域内人脸数据的安全管理，提出了人脸数据在不同场景下应用过程中安全策略，规范了人脸数据在采集、传输、存储、使用和销毁等全生命周期的安全管理行为，旨在遏制人脸数据的非法采集、滥用、泄露等乱象，最大程度地保护个人合法权益和社会公共利益。

安全防范 人脸数据安全管理规范

1 范围

本文件规定了人脸数据在安全管理中的基本要求、数据类型与安全防护等级、全生命周期管理、安全运营要求和安全管理要求。

本文件适用于安全防范领域内人脸数据所有者和使用者在采集、传输、存储、使用和销毁等环节的安全管理，其他行业也可参考使用。

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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 31488—2015 安全防范视频监控人脸识别系统技术要求

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 35275 信息安全技术 SM2密码算法加密签名消息语法规范

GB/T 37964 信息安全技术 个人信息去标识化指南

3 术语和定义

GB/T 31488-2015、GB/T 35273-2020界定的以及下列术语和定义适用于本文件。

3.1

人脸数据 face data

按照一定格式，以电子记录方式描述个人人脸信息的数据集合，包含人脸图像数据、人脸特征数据和人脸关联数据。

3.2

人脸图像数据 face image data

包含记录头部或人脸的单帧或视频图像的数据。

3.3

人脸特征数据 face feature data

从人脸图像数据中提取的代表该数据的特征信息或集合。

3.4

人脸关联数据 face-related data

与人脸相关的反映特定个人身份或者活动情况的各种数据或数据集合，例如：姓名、身份证件号码、联系方式、拍摄时间地点等。

4 基本要求

4.1 人脸数据的采集与使用应具有合法性、正当性和必要性。

4.2 应以清晰、合理的方式公开人脸数据的采集与使用范围、目的和规则，接受内外部监督。

4.3 应对人脸数据的采集、传输、存储、使用和销毁等环节采用全生命周期安全管理，从用户安全、网络安全、操作安全、环境安全等方面确保人脸数据的安全。

4.4 应遵循权责一致原则，谁建设、谁负责，谁使用、谁管理。

4.5 应具备相应的安全能力，构建合理的数据管理组织架构和数据架构体系，保护人脸数据的保密性、一致性、完整性、可用性和可追溯性。

4.6 应建立与人脸数据安全防护等级相符合的保护、监管、审计等要求的管理制度，对信息资产、运维人员、事件活动进行管理。

4.7 应采用必要的技术措施，保障人脸数据所在的信息系统的基本安全。

4.8 涉及人脸关联数据的信息系统，其数据安全防护等级属于 2 级的，应符合 GB/T 22239 中规定的二级及以上的安全等级保护要求；其数据防护等级属于 3、4 级的，应符合 GB/T 22239 中规定的三级及以上的安全等级保护要求。

5 数据类型与安全防护等级

5.1 数据类型

人脸数据根据产生的方式不同，可分为人脸图像数据、人脸特征数据和人脸关联数据，类型和特点见表1。

表 1 人脸数据类型

数据类型	数据特点
人脸图像数据	使用数码相机、手机、摄像机、执法记录仪或其他图像采集设备所获取的人脸图像，在数据全生命周期中不绑定任何身份和其他信息，仅存在有系统按顺序生成的编号和流水号。
人脸特征数据	由人脸图像数据提取的脸部特征数据，包括人脸特征项和人脸特征特性。
人脸关联数据	在人脸图像数据内加载了该人脸图像主体的相关身份信息、采集地点时间、财务信息、通信信息、人际关系信息，以及政治信仰信息等。

5.2 安全防护等级

根据人脸数据规模和人脸数据安全性遭受破坏后所造成的影响程度，将数据安全级别从低到高划分为1级、2级、3级、4级，见表2。

表 2　人脸数据安全级别划分

安全防护级别	数据定级要素		要求和影响
	数据类型	数据规模	
1级	人脸图像数据	≤499	1）人脸图像数据规模在499张以下时，或人脸特征数据在499条以下时，或无人脸关联数据时，其安全级别为1级。 2）数据的安全性遭到破坏后，对组织合法权益造成一定影响，但不影响国家安全、公众权益及个人隐私。
	人脸特征数据	≤499	
	人脸关联数据	0	
2级	人脸图像数据	500～4,999	1）人脸图像数据规模在500～4,999张时，或人脸特征数据在500～4,999条时，或人脸关联数据在1～499条时，其安全级别为2级。 2）数据的安全性遭到破坏后，对相关个人隐私造成轻微或中等影响，或对组织合法权益造成中等影响，但不影响国家安全和公众利益。
	人脸特征数据	500～4,999	
	人脸关联数据	1～499	
3级	人脸图像数据	5,000～99,999	1）人脸图像数据规模在5,000～99,999张时，或人脸特征数据在5,000～99,999条时，或人脸关联数据在500～9,999条时，其安全级别为3级。 2）数据的安全性遭到破坏后，对国家安全和公众权益造成轻微或中等影响，或对相关个人隐私和组织合法权益造成严重影响。
	人脸特征数据	5,000～99,999	
	人脸关联数据	500～9,999	
4级	人脸图像数据	≥100,000	1）人脸图像数据规模在100，000张以上时，或人脸特征数据在100，000条以上时，或人脸关联数据在10，000条以上时，其安全级别为4级。 2）数据安全性遭到破坏后，对国家安全和公众权益造成严重影响，或对相关个人隐私及组织合法权益造成非常严重影响。
	人脸特征数据	≥100,000	
	人脸关联数据	≥10,000	

6　全生命周期管理

6.1　人脸数据全生命周期管理体系见图 1。

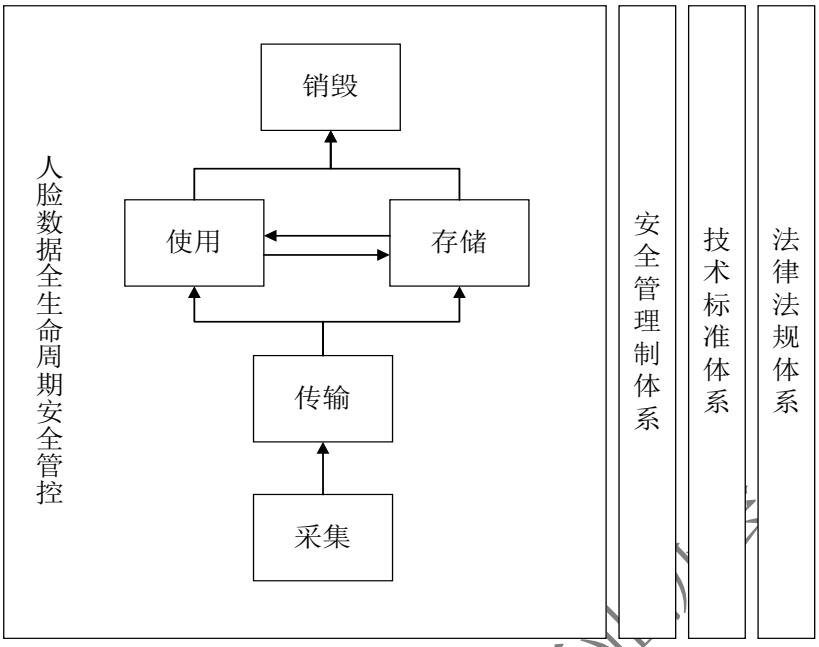

图 1　人脸数据全生命周期管理体系

6.2　人脸数据从采集、传输、使用、存储、销毁等全生命周期进行安全管控。

6.3　采集环节：使用数码相机、手机、摄像机、执法记录仪或其他图像采集设备采集人脸图像数据；使用智能摄像机或其他人脸分析与识别设备采集人脸特征数据；通过系统导入、手工录入或其他方式采集人脸关联数据。

6.4　传输环节：通过有线网络、无线网络或其他方式传输获取的人脸数据。

6.5　使用环节：直接使用或从存储系统调取使用人脸数据，支持增删改查、共享、复制、展示等使用方式。

6.6　存储环节：支持本地设备存储人脸数据，也支持云存储或分布式存储方式。

6.7　销毁环节：人脸数据在使用后直接销毁，或根据管理制度对存储系统中的人脸数据进行销毁。

7　安全运营要求

7.1　采集要求

7.1.1　采集人脸数据前，应向被采集人明确告知采集人脸事项。

7.1.2　采集设备/系统应定期更换密码，并采取病毒防范措施和及时修补漏洞。非系统控制的采集设备除外，如数码相机、手机等。

7.1.3　采集设备/系统宜对人脸数据进行数字签名，人脸关联数据的签名算法应符合 GB/T 35275 的规定。

7.1.4　采集设备宜获得其所在系统的认证。

7.2　传输要求

7.2.1　在传输过程中，应确保人脸数据不丢失、不泄漏，不被篡改、复制和伪造。

7.2.2 人脸数据传输时应采用加密算法。

7.2.3 人脸关联数据的加密算法应使用符合 GB/T 32907 的规定。

7.3 存储要求

7.3.1 应将人脸图像数据、人脸特征数据和人脸关联数据进行逻辑或物理隔离。

7.3.2 数据文件名称不应包含个人身份信息。

7.3.3 存储系统定期更改密码，并采取病毒防范措施和及时修补漏洞。

7.3.4 支持去标识化，应符合 GB/T 37964 的要求。

7.3.5 应防止未经授权的用户对人脸数据进行增、删、改等操作。

7.3.6 应具备数据备份和容灾备份的功能。

7.3.7 包含人脸数据的存储介质入库或出库应有授权/审批环节，并保留相应记录。

7.3.8 人脸数据存储时间应公示，且该时间应为实现目的所必需的最短时间。

7.3.9 人脸数据宜加密存储。

7.4 使用要求

7.4.1 数据访问

7.4.1.1 应建立内、外部审批制度，对人脸关联数据用户的访问目的、资质、保密条件等进行严格审核。

7.4.1.2 外部人员复制或提取使用时，外部人员及其单位即刻同时继承人脸数据的安全管理责任；

7.4.1.3 应严格控制数据访问范围，按照最小必要原则对用户访问进行授权。

7.4.1.4 应对人脸数据的录入/调取人员，调取内容、时间、用途以及去向等情况进行全流程记录。

7.4.1.5 在应用环境中访问人脸关联数据或移出到测试环境时，应进行脱敏处理。

7.4.2 数据展示

7.4.2.1 展示人脸数据前，应取得数据主体的同意，有规定的除外。

7.4.2.2 在公开展示人脸图像数据时，应与该数据关联的相关信息进行分离或去标识化，并同时对展示的数据叠加生物特征识别水印。

7.4.2.3 展示人脸数据时，所在场所宜受控，防止截屏、录屏以及其他非法获取人脸数据。

7.5 销毁要求

7.5.1 人脸数据应按照相关的法律法规及相关标准规定或公示的时间进行删除、销毁或匿名化处理。

7.5.2 人脸数据销毁时，应有授权/审批环节，并保留相应记录。

7.5.3 应确保存储、备份副本以及临时缓存的人脸数据一并销毁。

7.5.4 安全防护等级是 1、2 级时，应对存储介质进行格式化，或使用专用的工具在存储区域填入无用的信息进行覆盖；安全防护等级是 3、4 级时，应采用物理方式销毁存储介质，销毁后人脸数据应不可恢复。

7.5.5 销毁全过程应由专人负责和监督。

8 安全管理要求

安全管理制度和规程、安全管理机构、数据安全防护等级定级、安全防护与安全建设管理、安全监测与运行管理、全事件处置和应急响应等分级安全管理要求见表3。

表 3　人脸数据分级安全管理要求

管控域	安全要求项	安全防护等级			
		1 级	2 级	3 级	4 级
安全管理制度和规程	1）根据人脸数据安全防护等级要求制定安全管理策略，包括但不限于采集策略、加解密策略、脱敏策略、溯源策略、存储策略、使用策略、销毁策略等。	●	●	●	●
	2）制定安全管理规章制度和操作规程。	○	●	●	●
	3）指定或授权专人负责策略和规章制度的文档管理。	–	●	●	●
	4）安全管理策略和规章制度通过正式、有效的方式发布，并进行版本控制。	–	●	●	●
	5）定期对安全管理策略与规章制度的合理性和适用性进行论证和审定，对存在的不足进行修订。	–	○	●	●
	6）形成由管理策略、管理规章制度、操作规程、记录表单等构成的安全管理制度体系。	–	○	●	●
安全管理机构	1）设立人脸数据安全管理领导机构，并确定职责范围。	●	●	●	●
	2）明确法定代表人或主要负责人对人脸数据安全负全面领导责任。	–	–	●	●
	3）设定人脸数据安全管理的职能机构，设立安全主管、安全责任人，并明确各岗位的工作职责。	–	○	●	●
	4）明确内部涉及人脸数据处理工作的其他岗位的安全职责，以及发生安全事件的处罚机制。	–	○	●	●
	5）对接触、使用和管理人脸数据的相关人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	○	●	●	●
	6）与从事人脸数据处理岗位上的相关人员签署保密协议。	–	●	●	●
	7）明确可能访问人脸数据的外部人员应遵守的管理要求，与其签署保密协议。	–	●	●	●
	8）加强对外部人员和外协人员的安全管理，不得进行非授权操作，不得泄露、篡改、丢失和滥用数据。	–	○	●	●
	9）外部人员访问人脸数据信息系统前，应先提出书面申请，批准后由专人全程陪同，并登记备案。	–	●	●	●
	10)定期对接触人脸关联数据等重要数据的相关人员进行身份审查、背景、专业资质与资格审查，对其操作日志进行分析。一旦发现违规行为，应根据严重程度采取相应的惩戒措施。	–	○	●	●
	11）要求人脸数据处理岗位上的相关人员在调离岗位或终止劳动合同时，继续履行保密义务。	–	–	○	●
	12)定期开展针对各岗位人员的数据安全管理规章制度、操作流程的培训，并进行考核。	○	●	●	●
	13）定期（至少每年一次）或在隐私政策发生重大变化时，对人脸数据处理岗位上的相关人员开展人脸数据安全专业化培训和考核，确保相关人员熟练掌握隐私政策和相关规程。	–	●	●	●

管控域	安全要求项	安全防护等级			
		1级	2级	3级	4级
数据安全防护定级	1）以书面形式说明数据安全防护等级，以及确定等级的理由。	○	●	●	●
	2）将数据分级备案材料报主管部门备案。	-	●	●	●
	3）定期评审数据安全防护等级，如需要变更数据等级，应依据变更审批流程执行变更。	●	●	●	●
安全防护与安全建设管理	1）根据人脸数据安全防护等级选择基本数据安全防护措施，依据风险分析的结果补充和调整安全措施。	●	●	●	●
	2）确保人脸数据安全产品采购和使用符合国家的有关规定。	●	●	●	●
	3）制定或授权专门的部门或人员负责人脸数据安全保护建设工程实施过程的管理。	●	●	●	●
	4）对人脸数据安全产品和方案实施结果进行安全性测试验收。	●	●	●	●
	5）确保服务供应商的选择符合国家的有关规定。	●	●	●	●
	6）与选定的服务供应商签订与安全相关的协议，明确约定相关责任。	●	●	●	●
	7）根据被保护人脸数据对象的安全防护等级进行安全方案设计。	○	●	●	●
	8）组织安全专家对人脸数据安全保护方案进行论证和审定，经批准后才能正式实施。	○	●	●	●
	9)确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	○	●	●	●
	10）制定人脸数据安全保护工程实施方案，控制工程实施过程。	○	●	●	●
	11）制定人脸数据安全保护工程测试和验收方案，并根据方案进行验收，形成测试验收报告。	○	●	●	●
	12）提供人脸数据安全保护工程建设过程文档和运行维护文档。	○	●	●	●
安全监测与运行管理	1）制定安全检查的计划和方案，明确安全检查的范围、对象和方法等。	○	●	●	●
	2）对人脸数据安全相关的制度、策略、流程的落实情况进行监督，对发现的问题进行督促整改。	○	●	●	●
	3）梳理影响安全管理的关键要素，建立安全指标体系并进行监控。	-	●	●	●
	4）提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。	-	○	●	●
	5）定期检查恶意代码库的升级情况，对获得的恶意代码进行及时分析处理。	-	○	●	●
	6）定期对人脸数据所在信息系统和数据本身进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	○	●	●	●
	7）定期备份的人脸数据及软件系统等，应规定备份信息的备份方式、备份频度、存储介质、保存期等。	○	●	●	●
	8）分析安全监控数据，定期形成安全分析报告，包括但不限于状态分析、影响分析、趋势分析等。	-	○	●	●

管控域	安全要求项	安全防护等级			
		1级	2级	3级	4级
	9）制定安全检查表格并实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。	-	●	●	●
	10）明确并建立对数据采集、传输、存储、使用和销毁等相关操作的安全管理流程和审核机制。	●	●	●	●
	11）定期进行全面安全检查，检查内容包括但不限于制度体系建设情况、安全策略执行情况、数据安全防护状况等内容。	-	○	●	●
	12）在信息系统发生重大变更时，对当前的数据安全保护情况进行评估，对不符合或不适用情况进行整改。	-	-	●	●
	13）对高风险操作可能对平台和数据造成的影响进行评估，评估通过后才可进行相应操作。	-	-	-	●
安全事件处置和应急响应	1）及时向安全管理部门报告所发现的人脸数据的安全弱点和可疑事件。	●	●	●	●
	2）明确人脸数据的安全事件报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责。	-	●	●	●
	3）制定人脸数据安全事件应急响应机制、管理规范和流程，以及应急预案，包括应急处理流程、系统恢复流程等内容，明确人员分工，并定期开展应急演练。	-	●	●	●
	4）在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。	-	○	●	●
	5）建立态势感知系统，实现对平台或系统潜在安全风险的攻击行为的识别、分析和预警。	-	○	●	●
	6）发生安全事件后，根据应急响应机制进行处置。	○	●	●	●
注：●表示应支持；○表示宜支持；-表示不作要求。					

参 考 文 献

[1] GB/Z 28828 信息安全技术 公共及商用服务信息系统个人信息保护指南
[2] GA/T 1470 安全防范 人脸识别应用 分类
[3] General Data Protection Regulation(GDPR)