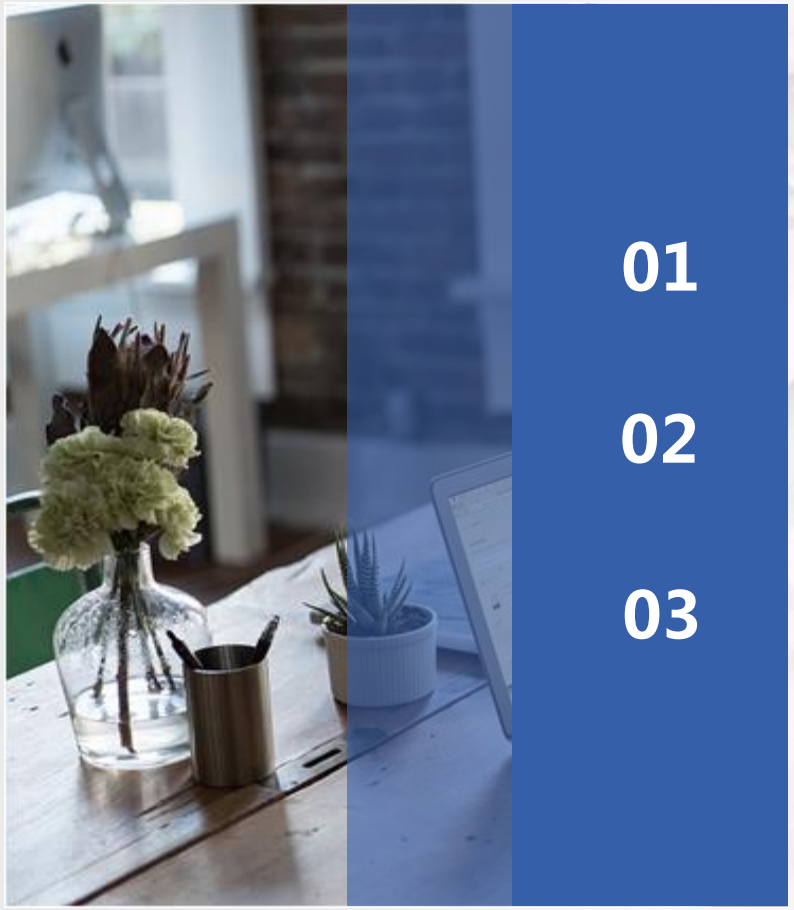
人脸识别信息和线下消费场景治理工作培训

目 录



1 工作背景

背景介绍

- 工作部署
  - 中央网信办会同公安部、市场监管总局等部门，于2025年6-10月开展公共场所违法违规收集使用人脸识别和线下消费场景违法违规收集使用个人信息专项治理行动。为落实相关工作要求，市委网信办联合市市场监管局、市商务局等部门联合开展我市专项治理行动。
- 法规依据
  - 依据《个人信息保护法》《网络数据安全管理条例》《人脸识别技术应用安全管理办法》等法规，明确公共场所与线下消费场景个人信息处理红线，为治理提供法律准绳。
- 治理目标
  - 健全完善个人信息保护监督管理工作体系，排查、整改、处置一批个人信息处理活动存在的安全问题和风险隐患，强化经营主体数据安全和个人信息保护责任意识。

背景介绍

- 人脸信息的特殊性

  人脸信息作为敏感个人信息（生物识别信息），具有独特性（如唯一性）、直接识别性、不可更改性、易采集性（如远距离、非接触、无感采集）、不可匿名性（无法去身份化）等特点 。其一旦泄露，后果难以逆转，可能伴随信息主体一生。

- 人脸识别技术应用安全管理办法

  规范应用人脸识别技术处理人脸信息活动，保护个人信息权益。

人脸识别技术应用安全管理办法主要内容

01 **明确应用人脸识别技术处理人脸信息的基本要求**，规定应用人脸识别技术处理人脸信息活动，应当遵守法律法规，尊重社会公德和伦理，遵守商业道德和职业道德等。

02 **明确应用人脸识别技术处理人脸信息的处理规则**，规定应用人脸识别技术处理人脸信息，应当具有特定的目的和充分的必要性，个人信息处理者应当履行告知、进行个人信息保护影响评估等义务。

03 **明确人脸识别技术应用安全规范**，规定实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，不得将人脸识别技术作为唯一验证方式，明确在公共场所安装人脸识别设备的具体要求。

04 **明确监督管理职责和法律责任**，规定个人信息处理者应当在应用人脸识别技术处理的人脸信息存储数量达到10万人之日起30个工作日内向所在地省级以上网信部门履行备案手续，明确违反本办法规定的法律责任。

人脸识别备案流程

个人信息处理者应当在应用人脸识别技术处理的人脸信息存储数量达到 10万人之日起 30 个工作日内，通过“个人信息保护业务系统”履行备案手续，系统网址为https://grxxbh.cacdtsc.cn。

查验个人信息处理者基本信息：包括提交的统一社会信用代码证件、经办人授权委托书、承诺书等是否符合要求。

查验备案材料：包括提交的个人信息处理者基本情况表、个人信息保护影响评估报告是否符合要求。

发放备案编号：省级网信办通过过备案系统向个人信息处理者发放备案编号。

省级网信办对已备案的人脸识别技术应用情况进行跟踪监督，如发现存在安全隐患、备案状态变更等情况，应及时督促整改。

个人信息处理者在系统中履行备案手续

省级网信办在备案系统中对个人信息处理者提交的备案信息进行审核

省级网信办对已备案的人脸识别技术应用情况进行跟踪监督。

治理范围

2.1 违规收集使用人脸识别信息治理

（1）应用人脸识别技术处理人脸信息的基本要求落实问题

治理要点	治理内容	查验方法	留存证据
具有特定的目的和充分的必要性	应用人脸识别技术处理人脸信息，应当具有特定的目的和充分的必要性，采取对个人权益影响最小的方式。	1）检查企业使用人脸识别技术的目的是否符合法律法规，是否用于合法的业务场景，如身份验证、安防监控等；提供明确、具体的人脸识别技术应用目的，如用于员工考勤、访客管理等，避免模糊表述。 2）检查是否存在其他非人脸识别技术方式可以达到相同目的或同等业务要求。例如，是否可以通过刷卡、密码登录、手机NFC等方式替代人脸识别；评估企业是否选择了对个人权益影响最小的方式。例如，是否仅在必要时采集人脸信息，且采集的信息量是否为实现目的所必需的最小范围。	1. 告知目的内容相关文档。

（1）应用人脸识别技术处理人脸信息的基本要求落实问题

治理要点	治理内容	查验方法	留存证据
履行合理明确的单独或书面告知同意等法律义务	个人信息处理者应用人脸识别技术处理人脸信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项： （一）个人信息处理者的名称或者姓名和联系方式； （二）人脸信息的处理目的、处理方式，处理的人脸信息保存期限； （三）处理人脸信息的必要性以及对个人权益的影响； （四）个人依法行使权利的方式和程序； （五）法律、行政法规规定应当告知的其他事项。	1）告知内容完整性：检查企业是否以显著方式、清晰易懂的语言向个人告知以下事项：个人信息处理者的名称或联系方式、处理目的、方式、保存期限、必要性及对个人权益的影响、个人依法行使权利的方式和程序等；对于残疾人、老年人等特殊群体，检查企业是否提供了符合无障碍环境建设规定的告知方式，如语音播报、大字体界面、手语视频等。 2）核实企业是否在充分告知的基础上，获得了个人自愿、明确作出的单独同意，而非捆绑在其他条款中。对于不满十四周岁未成年人的人脸信息处理，是否获得了监护人的同意。 3）验证个人依法行使权利的方式和程序，如查阅、复制、更正、删除等。检查企业是否在合理时间内响应个人的权利请求。 4）检查企业是否将人脸信息存储于人脸识别设备内，避免通过互联网传输。若企业确需通过互联网传输人脸信息，检查是否取得了个人单独同意或符合法定例外情形。	1.个人信息保护管理制度文件； 2.隐私政策文件 3.已经全面适当履行告知义务并获取个人单独同意的证明材料。
	基于个人同意处理人脸信息的，应当取得个人在充分知情的前提下自愿、明确作出的单独同意。		
	应建立保障个人信息主体权利的机制，保障个人信息主体查阅复制、更正补充、删除、知情选择、可携带等方面的权利，并及时响应个人信息主体请求。		
	除法律、行政法规另有规定或者取得个人单独同意外，人脸信息应当存储于人脸识别设备内，不得通过互联网对外传输。		

（1）应用人脸识别技术处理人脸信息的基本要求落实问题

治理要点	治理内容	查验方法	留存证据
依法开展个人信息保护影响评估	个人信息处理者应用人脸识别技术处理人脸信息，应当事前进行个人信息保护影响评估，并对处理情况进行记录。个人信息保护影响评估主要包括下列内容： （一）人脸信息的处理目的、处理方式是否合法、正当、必要； （二）对个人权益带来的影响，以及降低不利影响的措施是否有效； （三）发生人脸信息泄露、篡改、丢失、毁损或者被非法获取、出售、使用的风险以及可能造成的危害； （四）所采取的保护措施是否合法、有效并与风险程度相适应。 个人信息保护影响评估报告和处理情况记录应当至少保存3年。处理人脸信息的目的、方式发生变化，或者发生重大安全事件的，应当重新进行个人信息保护影响评估。	查验个人信息保护影响评估报告，是否对向其他个人信息处理者提供其处理的个人信息情形开展个人信息保护影响评估。	1.提供个人信息保护影响评估报告； 2.提供个人信息保护影响评估所需的其他佐证材料

（1）应用人脸识别技术处理人脸信息的基本要求落实问题

治理要点	治理内容	查验方法	留存证据
提供除人脸识别外的其他可选身份验证方式	实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，不得将人脸识别技术作为唯一验证方式。个人不同意通过人脸信息进行身份验证的，应当提供其他合理、便捷的方式。	1）调阅企业业务场景清单，确认刷脸的唯一目的是否仅为身份验证或门禁考勤等。是否可以用刷卡、密码、手机验证码、人工核对等方式达到同等目的。若存在替代方式，即不符合“唯一验证”豁免条件 2）现场测试：在刷脸闸机/考勤机/APP流程中，故意选择“拒绝刷脸”，观察系统是否立即提供其他验证入口。记录替代方案的实际耗时与便捷度，若明显繁琐或不可用，视为未提供“合理、便捷”方式； 3）检查是否有用户拒绝刷脸后的替代验证记录（日志、截图、纸质登记簿）。	1.验证记录； 2.业务场景清单； 3.隐私政策等。

案例解析

典型案例：

某物业公司为提升安全管理水平，在小区出入口安装人脸识别门禁系统，要求业主录入人脸信息后方可通行。部分业主质疑物业未明确告知人脸信息用途、存储方式，且未提供替代方案，侵犯其个人信息权益，随后该物业公司积极主动采取一系列整改行动：

（1）履行告知义务并征得个人单独同意：通过业主大会表决通过在该小区设置人脸识别技术应用的方案，明确向业主告知其人脸信息用途（仅限门禁识别）、处理规则（仅采集非原始图像的人脸特征值）、存储期限（1年）、退出机制等事项，并逐户逐员签署《人脸信息处理知情同意书》；

（2）提供替代方案：业主可选择刷卡或人工登记通行，避免“强制刷脸”；

（3）开展个人信息保护影响评估：针对人脸信息处理活动定期开展个人信息保护影响评估；

（4）维护业主个人权益的其他措施：开通线上渠道，允许业主随时查询、删除或撤回授权；设置严格的人脸数据访问权限，仅限安保负责人使用；委托合规第三方技术公司加密存储数据，定期进行安全检测等。

（2）公共场所人脸识别设备安装问题

治理要点	治理内容	查验方法	留存证据
明确为维护公共安全所必须	在公共场所安装人脸身份识别设备，其目的应当为维护公共安全所必需。其目的仅为维护公共安全为符合，否则为不符合。	1.查验公共场所安装图像采集、个人身份识别设备相关管理制度，是否明确安装目的，是否为维护公共安全所必需，是否用于商业目的； 2.查看在公共场所安装图像采集、个人身份识别设备的提示标识；查验提示标志的内容、大小、位置和可见度，确保公众可以轻易注意到；查验图像采集、个人身份识别设备本身是否清晰可见； 3.访谈了解公共场所安装图像采集、个人身份识别设备所收集的个人图像、身份识别信息的用途。	1.在公共场所安装图像采集、个人身份识别设备的，应当具备合法履行维护公共安全职责的身份资格证明； 2.已设置满足要求的显著提示标志的证明。如现场照片等。
设置显著提示标识	在公共场所安装人脸识别设备，应合理确定图像采集设备的安装位置、角度和采集范围，并设置显著的提示标识。		

案例解析

典型案例：

某城市轨道交通集团在其运营维护的地铁站部署人脸识别系统，应用于乘客刷脸快速进站（便利化服务用途）以及实时比对公安机关通缉人员数据库（公共安全防护用途）。针对公共场所中的公共安全防护这一用途，为严格履行法定义务采取了以下措施：

（1）显著告知：在地铁站入口处设置公告牌及电子屏，以充分显著的方式向乘客告知采集人脸信息目的、人脸信息存储期限、乘客个人权利以及行权方式与渠道等；

（2）规范用途：数据仅与公安机关共享，禁止用于商业用途或与其他用途混淆应用处理规则。

（3）人脸识别技术应用系统安全问题

治理要点	治理内容	查验方法	留存证据
人脸识别技术应用系统安全	人脸识别技术应用系统应当采取数据加密、安全审计、访问控制、授权管理、入侵检测和防御等措施保护人脸信息安全。 涉及网络安全等级保护、关键信息基础设施的，应当按照国家有关规定履行网络安全等级保护、关键信息基础设施保护义务。	1.查验安全文档，审核加密防篡改； 2.查看存储架构，查验数据隔离； 3.审核加密算法与密钥管理； 4.测试设备功能，确认数据可删； 5.查看处理记录； 6.检查支付策略，查验模板合规； 7.测试识别功能，确认本地优先； 8.审阅审计日志与策略； 9.审核传输加密与鉴别； 10.审查传出策略与记录。	1.安全方案、日志记录 2.存储架构图、配置文件 3.加密说明、密钥策略 4.功能报告、删除截图 5.删除日志、操作记录 6.支付方案、模板记录 7.测试报告、配置截图 8.审计日志、制度文件 9.传输方案、加密协议 10.传出策略、传输日志

案例解析

典型案例：

某游乐设施企业收集人脸信息后未对其运营的网站以及数据库采取充分的数据安全防护措施，遭恶意攻击泄露后导致数百万条信息泄露，其中包含人脸识别数据、身份证信息、实名信息以及客户住址等。

为防止此类涉及人脸信息等高敏感度个人数据安全事件再次发生，涉事企业后续完善内部数据安全管理制度，强化数据安全防护措施，针对人脸信息等敏感个人信息采取更高级别的数据安全技术，杜绝数据安全事件的再度发生。

（4）未成年人的人脸信息安全

治理要点	治理内容	查验方法	留存证据
未制定专门的处理规则	个人信息处理者应用人脸识别技术处理不满十四周岁未成年人人脸信息的，应当在存储、使用、转移、披露等方面制定专门的处理规则，依法保护未成年人个人信息安全。	1.访谈了解相关的未成年人工作机制，个人信息保护政策； 2.查验个人信息处理者的隐私政策和产品中是否有制定专门的不满十四周岁未成年人个人信息处理规则并予以发布。	1.不满十四周岁未成年人隐私政策等； 2.告知机制、告知文案、告知记录等。
取得父母或其他监护人同意	基于个人同意处理不满十四周岁未成年人人脸信息的，应当取得未成年人的父母或者其他监护人的同意。	1.查看个人信息保护管理制度，是否明确基于个人同意处理不满十四周岁未成年人的个人信息，事前需要取得未成年人的父母或者其他监护人的同意； 2.查看处理敏感个人信息情况说明，验证是否存在处理不满十四周岁未成年人的个人信息的情况（如抽查数据库存储个人信息）； 3.访谈了解相关的未成年人相关工作机制，未成年人保护政策； 4.访谈了解征得未成年人的父母或其监护人的明示同意的方式。	1.个人信息保护管理制度； 2.处理敏感个人信息情况说明； 3.个人单独同意记录、隐私政策、告知同意书、来往邮件等； 4.不满十四周岁未成年人父母或其他监护人同意的记录； 5.产品或服务上可以进行同意的按钮、选项的截图。 6.人脸信息台账相关记录。

案例解析

典型案例：

某省一中学基于加强学生进出校门和宿舍门的管理，统计学生的考勤情况等目的，在校内安装“智能人脸识别系统”，并向家长发送《致家长的一封信》，告知收集学生人脸信息的目的、用途以及资费等信息，获取家长的“确认”同意，就处理未成年人的人脸信息方面，学校的上述行为存在以下欠缺：

（1）制定未成年人个人信息处理规则：根据《个保法》相关规定，未满十四周岁未成年人的个人信息为敏感个人信息，未成年人的人脸信息更是“敏上加敏”，同时《管理办法》第七条亦对处理未成年人的人脸信息活动规则有所要求，然而学校未针对处理学生的人脸信息专门制定存储、使用、转移、披露等方面的处理规则，并将规则一并告知或公开。

（2）获取监护人同意：处理未成年人个人信息（含人脸信息）需取得监护人单独同意，并明确告知处理目的、方式、范围等内容，本案例中学校虽在形式上通过向家长发送《致家长的一封信》的方式履行了告知义务并取得了未成年人监护人的单独同意，但并未充分说明处理人脸信息的必要性，且未提供可实现上述目的可替代方案，实质上并不符合《个保法》意义上的自愿原则。同时，结合《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》第四条，在必要性不足的情况下，学校不得以已获取未成年人监护人的同意为由主张需处理人脸信息方可提供产品或者服务。

案例解析

健身房强制“刷脸”事件（2022年，江苏无锡）

某健身房强制要求会员使用人脸识别或指纹录入进入，且在会员拒绝后仍擅自使用其照片作为验证凭证，拒绝删除信息。检察机关介入调查后，督促整改并推动行业规范。

超市人脸识别“标签”事件（2022年，上海普陀）

多家超市在出入口安装人脸识别设备，未经消费者同意采集数据，并对部分消费者标注“疑似小偷”等标签，单日采集量超3000条。检察机关通过公益诉讼推动整改。

小鹏汽车违规采集人脸数据（2021年，上海）

小鹏汽车销售门店在6个月内非法采集43万张消费者人脸照片用于客流分析，被市场监管部门罚款10万元。

上海“亮剑浦江”专项行动（2024年）

上海市网信办联合多部门整治滥用人脸识别，覆盖健身房、商超、酒店等场景，推动600余家商超、6300余家酒店整改，并取消地铁站自动售货机“刷脸支付。

（5）人脸识别技术应用备案

治理要点	治理内容	查验方法	留存证据
按照《人脸识别技术应用安全管理办法》有关要求履行人脸识别技术应用备案手续	应用人脸识别技术处理的人脸信息存储数量达到10万人且向所在地省级以上网信部门履行备案手续。	1.判断人脸信息存储数量是否达到10万人； 2. 是否在https://grxxbh.cacdtsc.cn网站上提交备案材料。	1.材料上传相关截图

案例解析


— 人脸识别技术应用备案 —
当前用户：
返回首页
退出
人脸识别数据技术应用备案新增
附件上传
(注:请上传附件格式为PDF、OFD、PNG、IPG、JPEG、XLS、XLSX、ET的文件，每个文件大小不超过50MB。)
统一社会信用代码证件: 请上传《统一社会信用代码证件》原件扫描件（加盖公章）
* 统一社会信用代码证件:
删除
文件上传
法定代表人身份证件: 请上传《法定代表人身份证件》原件扫描件（加盖公章）
* 法定代表人身份证件:
删除
文件上传
经办人身份证件: 请上传《经办人身份证件》原件扫描件（加盖公章）
* 经办人身份证件:
删除
文件上传
经办人授权委托书: 请上传《经办人授权委托书》原件扫描件（加盖公章）
* 经办人授权委托书:
请上传格式为PDF、OFD、PNG、JPG、JPEG的文件
文件上传
模版下载
承诺书: 请上传《承诺书》原件扫描件（加盖公章）
* 承诺书:
请上传格式为PDF、OFD、PNG、JPG、JPEG的文件
文件上传
模版下载
个人信息保护影响评估报告: 请上传《个人信息保护影响评估报告》原件扫描件（加盖公章）
* 个人信息保护影响评估报告:
请上传格式为PDF、OFD、PNG、JPG、JPEG的文件
文件上传
模版下载
人脸识别技术应用情况备案表: 请上传《人脸识别技术应用情况备案表》电子版及原件扫描件（加盖公章）
* 人脸识别技术应用情况备案表:
请上传格式为XLS、XLSX、ET的文件
文件上传
模版下载
* 人脸识别技术应用情况备案表影印件:
请上传格式为PDF、OFD、PNG、JPG、JPEG的文件
文件上传
个人信息处理者基本情况表: 请上传《个人信息处理者基本情况表》电子版及原件扫描件（加盖公章）
* 个人信息处理者基本情况表:
删除
文件上传
模版下载
返回
暂存
全部完成

2.2 线下消费场景违规收集使用个人信息治理

（1）公开个人信息处理规则

治理要点	治理内容	查验方法	留存证据
公开展示个人信息处理规则	个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项： （一）个人信息处理者的名称或者姓名和联系方式； （二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限； （三）个人行使个人信息保护法规定权利的方式和程序； （四）法律、行政法规规定应当告知的其他事项。（依据《个人信息保护法》第十七条）	1）查验隐私政策及其他个人信息处理规则告知材料中是否包含上述内容； 2）查看处理敏感个人信息情况说明，验证存在哪些处理敏感个人信息的情况；查看处理敏感个人信息向个人告知处理敏感个人信息的必要性以及对个人权益的影响的方式；查看根据法律、行政法规规定，处理哪些敏感个人信息需要取得书面同意；访谈了解在处理敏感个人信息时取得书面同意的方式方法。 3）访谈了解是否存在想境外传输个人信息的情况，查验个人信息保护管理相关制度中是否说明向境外传输个人信息的情况； 4）访谈了解相关的未成年人工作机制，个人信息保护政策； 5）查验个人信息处理者的隐私政策和产品中是否有制定专门的不满十四周岁未成年人个人信息处理规则并予以发布； 6）访谈了解征得未成年人的父母或其监护人的明示同意的方式。	1.隐私政策或其他个人信息处理规则； 2.不满十四周岁未成年人隐私政策等； 3.告知机制、告知文案、告知记录等。
	处理敏感个人信息前应向用户告知个人信息处理者的名称或者姓名和联系方式；个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；个人行使权利的方式和程序；处理敏感个人信息的必要性以及对个人权益的影响以及法律法规规定应当告知的其他事项，并取得个人的单独同意。（依据《个人信息保护法》第二十八条、第二十九条《人脸识别技术应用安全管理办法》第五条、第六条）		
	应用程序向境外传输个人信息的，应向用户告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使权利的方式和程序等事项。		
	应用程序收集不满十四周岁未成年人个人信息的，应通过单独的个人信息处理规则明示应用程序运营者的名称和联系方式；未成年人个人信息的处理目的、处理方式；处理的个人信息种类、保存期限；用户行使个人信息权利的方式和程序；处理未成年人个人信息的必要性；对未成年人个人权益的影响。		

（1）公开个人信息处理规则

治理要点	治理内容	查验方法	留存证据
访问便捷、内容明确具体	个人信息保护政策应公开发布且易于访问，例如，在网站主页、移动互联网应用程序安装页等显著位置设置链接，进入App主界面后，少于4次点击等操作就能访问到	1）查看向用户提供的访问个人信息保护相关规则的界面，确保界面设计友好易于用户阅读。	1.隐私政策以及个人信息保护管理相关的制度； 2.查验用户访问隐私政策的方式或路径（截屏录屏）等。

（1）公开个人信息处理规则

治理要点	治理内容	查验方法	留存证据
易阅读理解	个人信息保护政策的内容应清晰易懂，符合通用的语言习惯，使用标准化的数字、图示等，避免使用有歧义的语言。	1）查阅个人信息保护相关的规则，确认是否存在不易于用户理解，存在歧义的描述干扰用户阅读个人信息保护相关的规则； 2）查看向用户提供的访问个人信息保护相关规则的界面，确保界面设计友好易于用户阅读； 3）查阅个人信息保护相关的规则，对于敏感信息收集使用个人信息的目的、范围等应显著标识。	1.隐私政策以及个人信息保护管理相关的制度； 2.用户访问隐私政策界面（截屏录屏）等。
	隐私政策等收集使用规则易于阅读，不存在文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等问题。		

（1）公开个人信息处理规则

案例展示：

未公开个人信息收集使用规则

隐私政策文字过小不易于阅读

未告知用户行使删除、撤回同意等权利的方式

1. Web 交易系统可以访问如下个人信息：

访问用户的个人信息：首页 – 账户信息页面可以查看用户的个人资产信息，首页 – 银证业务页面可以查看用户绑定的银行卡信息、余额等。

密码修改：系统设置 – 密码修改页面可以修改用户的交易密码和资金密码。

2. 官网首页右上角可以访问用户手机号，资金账号，身份证号

在以下情形中，按照法律法规要求，我们将无法响应您的更正、删除、注销信息的请求：

- 与国家安全、国防安全直接相关的；
- 与公共安全、公共卫生、重大公共利益直接相关的；
- 与犯罪侦查、起诉、审判和执行判决等直接相关的；
- 我们有充分证据表明您存在主观恶意或滥用权利的（如您的请求将危害公共安全和其他人合法权益，或您的请求超出了一般技术手段和商业成本可覆盖的范围）；
- 响应个人信息主体的请求将导致您或其他个人、组织的合法权益受到严重损害的；
- 涉及商业秘密的；
- 与我们履行法律法规规定的义务或者与我们履行与您之间的协议约定的

案例展示：

收集敏感信息时，未取得用户单独同意

（2）强制关注绑定

治理要点	治理内容	查验方法	留存证据
强制要求关注公众号、注册会员、绑定微信号	未将注册会员、绑定微信号、关注公众号作为使用应用程序的必要前置条件。	1）模拟未绑定微信/公众号的用户尝试使用基础服务，记录是否出现“必须绑定否则无法使用”的阻断提示，验证是否存在“捆绑同意”强制授权。 2）确认是否通过显著的方式征得用户同意（使用表意明确的按钮禁止采用“我知道了”等含糊不清的语句，采用“同意”“拒绝”等明确的语义），验证是否存在默认勾选、强制捆绑授权，用户拒绝授权后影响其他业务功能的正常使用。 3）查验隐私政策或第三方共享信息清单是否明确告知用户收集人脸信息的范围、使用方式、第三方共享情况。	1.个人信息保护相关的管理制度、第三方共享信息清单等； 2.征得用户明确同意的界面（截屏录屏等）。

（2）强制关注绑定

案例展示：

强制获取微信授权，否则无法使用

（3）强制收集个人信息

治理要点	治理内容	查验方法	留存证据
强制收集非必要的个人信息	个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。	1）遍历APP，确认是否存在欺诈、诱骗等不正当方式，比如赠送加分、话费诱导用户填写个人信息或打开可收集个人信息权限，隐瞒收集个人信息的真实目的。例如：参与红包、抽奖等活动向用户申请通讯录权限，与当前功能没有逻辑关系。 2）检测应用业务功能确认是否存在强制要求用户同意更新后的隐私政策并强制剥夺用户权益的行为；是否明确告知用户不同意更新后的隐私政策影响服务的范围。	1.个人信息保护管理制度； 2.隐私政策或用户协议。

（3）强制收集个人信息

治理要点	治理内容	查验方法	留存证据
误导、欺诈、胁迫用户提供个人信息	不得以改善服务质量、提升使用体验、研发新产品、增强安全性等为由，强制要求个人信息主体同意收集个人信息。	1.核查隐私政策，确认是否存在仅以改善服务质量或程序功能收集个人信息的行为；若存在是否提供了关闭收集个人信息的方式或途径； 2.验证关闭途径的有效性。	个人信息保护相关的管理制度。

（3）强制收集个人信息

案例展示：

强制收集与功能无关的的存储权限和位置信息

（4）违规处理未成年人个人信息

治理要点	治理内容	查验方法	留存证据
未经未成年人的父母或其他监护人同意	个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。（《个人信息保护法》第三十一条）	1）访谈了解相关的未成年人工作机制，个人信息保护政策； 2）查验个人信息处理者的隐私政策和产品中是否有制定专门的不满十四周岁未成年人个人信息处理规则并予以发布； 3.访谈了解征得未成年人的父母或其监护人的明示同意的方式； 4.核验个人信息处理者告知同意机制、告知文案和告知记录，是否采取不易绕过的方式向未成年人或其监护人告知未成年人个人信息的处理目的、处理方式、处理必要性及处理个人信息的种类、所采取的保护措施等。	1.不满十四周岁未成年人隐私政策等； 2.告知机制、告知文案、告知记录等。
未制定专门的个人信息处理规则	个人信息处理者应用人脸识别技术处理不满十四周岁未成年人人脸信息的，应当在存储、使用、转移、披露等方面制定专门的处理规则，依法保护未成年人个人信息安全。（《个人信息保护法》第三十一条）		

（4）违规处理未成年人个人信息

案例展示：

APP明确提供了《儿童个人信息保护准则》，并且独立成文的形式发布。

（5）违规处理人脸信息

治理要点	治理内容	查验方法	留存证据
未经个人单独同意	基于个人同意处理人脸信息的，应当取得个人在充分知情的前提下自愿、明确作出的单独同意。	1）检查人脸采集界面是否以弹窗/显著提示单独出现（非勾选框），需用户主动点击“同意”或“拒绝”按钮，且拒绝后仍可进入基本服务流程；拒绝后再次请求时未默认勾选同意（需用户主动点击确认）； 2）访谈了解并验证身份识别机制，是否采用人脸识别作为身份认证的唯一途径，用户是否可选择其他方式进行身份认证，测试人脸识别流程（记录步骤数、耗时）以及非人脸替代方案流程，比较两者操作复杂度差异（如替代方案是否需额外验证或多次跳转）； 3）拒绝授权后是否仍可完成基础功能；系统是否出现"必须同意否则无法使用"的强制提示；连续拒绝后是否限制后续服务（如24小时内禁止再次申请）。	1.收集用户人脸信息界面（截屏录屏）等； 2.访谈记录。
强制或超范围收集人脸	实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，不得将人脸识别技术作为唯一验证方式。个人不同意通过人脸信息进行身份验证的，应当提供其他合理、便捷的方式。		

（5）违规处理人脸信息

案例展示：

当前app在收集人脸信息时会以界面提示的方式告知并征求用户同意。

（6）非法公开或者擅自向他人提供个人信息

治理要点	治理内容	查验方法	留存证据
取得个人单独同意	个人信息处理者公开其处理的个人信息前，应取得个人单独同意。	1.查阅公开处理的个人信息情况说明，验证存在哪些公开处理个人信息的情形； 2.访谈了解个人信息控制者公开披露个人信息前征得个人信息主体单独同意的情况； 3.访谈了解个人信息公开取得个人单独同意的方式； 4.查看个人信息公开管理规范； 5.查看公开数据的内容； 6.查看对敏感个人数据公开记录；	1.公开处理的个人信息情况说明； 2.访谈记录； 3.公开管理规范； 4.敏感个人数据公开记录；

（6）非法公开或者擅自向他人提供个人信息

治理要点	治理内容	查验方法	留存证据
事前开展个人信息保护影响评估	委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息前，个人信息处理者应当事前进行个人信息保护影响评估。	1.查阅个人信息委托处理情况说明，验证有哪些提供、公开个人信息情形； 2.查验个人信息处理者在委托处理个人信息前是否开展了个人信息保护影响评估；查阅个人信息处理者在委托处理个人信息前开展个人信息保护影响评估的记录； 3.查看相关合同或其他文档，查验个人信息处理者是否通过合同等方式，与受托人约定个人信息委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等； 4.查看个人信息保护影响评估报告和委托处理合同文本，验证个人信息保护影响评估及合同文本是否存在错漏或不一致的情况，并核实原因。	1.个人信息委托处理情况说明; 2.查看相关合同或其他文档; 3.个人信息保护影响报告； 4.开展个人信息保护影响评估的记录。

（6）非法公开或者擅自向他人提供个人信息

治理要点	治理内容	查验方法	留存证据
未经同意直接向第三方提供个人信息	a)既未经用户同意，也未做匿名化处理，App客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息。（《个人信息保护法》第二十三条）	1) 通过App功能验证、查看文档资料及询问App提供者等方式，查看App提供者是否存在向第三方共享、转让个人信息的行为； 2) 查看App提供者的个人信息安全相关管理制度，是否明确规定告知用户共享、转让个人信息的目的、数据接收方的类型，并事先征得个人信息主体的授权同意； 3) 查看App的个人信息保护政策，其中是否向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型，并征得用户授权同意； 4) 通过技术检测App中共享给第三方的个人信息和第三方类型，判断是否与App个人信息保护政策中说明的一致； 5) 核查App服务端共享给第三方的个人信息和第三方类型，判断是否与App个人信息保护政策中说明的一致； 6) 询问App提供者是否存在向接入的第三方应用提供个人信息的行为，若存在则判断是否与App个人信息保护政策中说明的一致； 7) 询问并查看未告知的个人信息是否是经去标识化处理后且无法重新识别个人信息主体的个人信息。	1.个人信息安全相关管理制度； 2.访谈记录等。
	b)既未经用户同意，也未做匿名化处理，数据传输至App后台服务器后，向第三方提供其收集的个人信息。（《个人信息保护法》第二十三条）		
	c)App接入第三方应用，未经用户同意，向第三方应用提供个人信息。（《个人信息保护法》第二十三条）		

（6）非法公开或者擅自向他人提供个人信息

案例展示：

某应用通过检测存在腾讯TBS浏览器服务SDK获取IMEI等个人信息，在隐私政策中未告知用户。

第三方公司名称： 腾讯公司及其关联公司
产品/类型：腾讯TBS SDK
收集的信息：设备信息（操作系统版本、CPU类型、屏幕宽高、屏幕方向、屏幕像素）、应用信息（宿主应用包名，版本号）、存储信息
调用的权限：存储权限、网络权限
使用场景：用户使用APP相关业务时收集
使用目的：各种格式的文件浏览服务
收集方式：本机SDK
第三方隐私政策地址：第三方隐私政策
适用端：Android

（6）非法公开或者擅自向他人提供个人信息

案例展示：

在XXX功能向第三方共享个人信息时，通过弹窗的方式明确告知用户。

（7）安全保护措施

治理要点	治理内容	查验方法	留存证据
采取有效安全保护措施	a)制订了数据库账号权限管理、访问控制、日志管理、加密管理等制度并遵照执行。 b)制定了限制数据库管理、运维等人员操作行为的安全管理措施并遵照执行。 c)对逻辑存储系统中储存的敏感个人信息、重要数据进行加密存储。 d)敏感数据或个人隐私数据的查询、导出、更正、删除等操作有相关日志记录。 e)定期对逻辑存储系统进行安全漏洞排查和渗透测试。 f)设立个人信息保护责任人，开展定期审计和培训。	1）查阅个人信息处理者涉及个人信息的业务系统、数据库的权限管理机制及已有账号权限清单；访谈业务系统、数据库账号权限审批、审计岗位人员；查验有关人员在业务系统、数据库的查阅、复制、传输个人信息的授权审批记录，判断是否存在超出最小必要范围的授权。 2）访谈了解并查看相关业务系统是否对于敏感个人信息、重要数据进行加密存储； 3）查验敏感数据或个人隐私数据的查询、导出等相关日志记录是否完善； 4）查看定期进行渗透测试和安全漏洞排查的相关记录以及检测报告。 5）查阅个人管理制度，规定个人信息保护负责人及相关人员职责和考核评价要求；审阅开展个人信息保护安全教育和培训的规定，培训周期和参与培训的人员。	1.个人信息保护相关管理制度； 2.访谈记录； 3.渗透测试报告； 4.培训记录等。

（7）安全保护措施

治理要点	治理内容	查验方法	留存证据
存在个人信息泄露风险	及时修复等保测评、风险评估、渗透测试等安全测试过程中发现的风险隐患。 发生或可能发生个人信息泄露，应立即通知用户并向主管机关报告。	1）访谈了解是否会对业务系统进行安全测试，查验相关的安全评估报告，对于发现的风险漏洞是否完成修复，相关的复测报告。 2）测试业务系统是否存在安全漏洞。 3）访谈了解是否发生过个人信息泄露事件，查阅相关补救措施的记录；访谈了解个人信息安全事件通知所涉及个人并报告网信部门的情况；访谈了解个人信息保护负责人设置情况。	1.个人信息保护相关管理制度； 2.渗透测试报告等； 2.访谈记录； 3.个人信息泄露事件相关的记录文档（如有）。

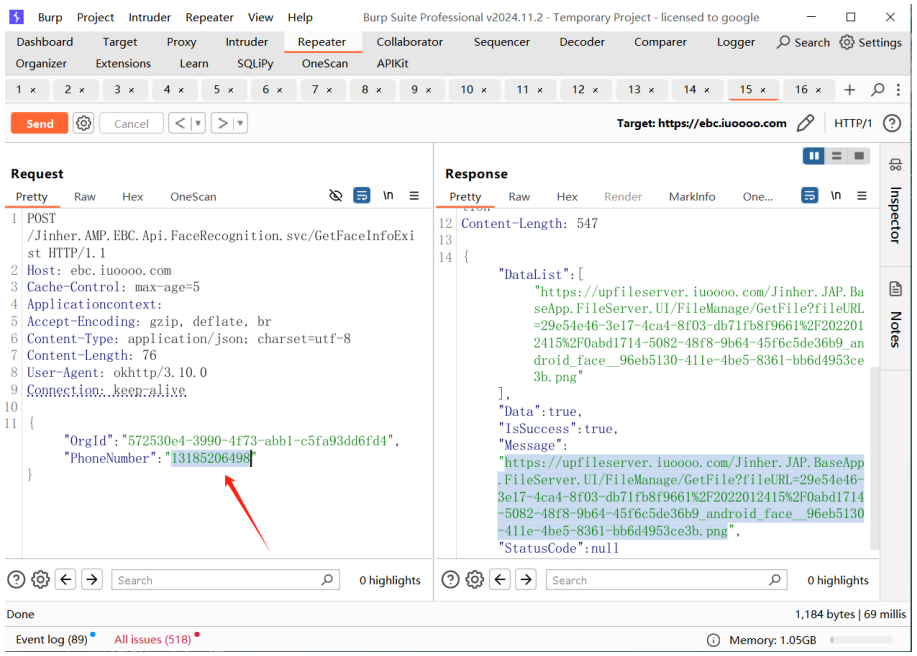
（7）安全保护措施

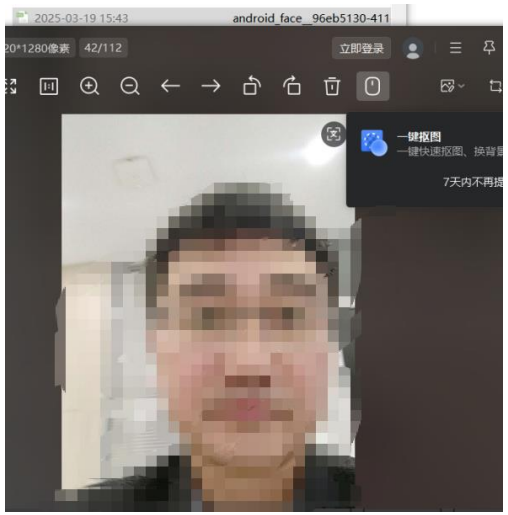
案例展示：

场景：

APP接口未实施严格的访问控制，导致所有用户的人脸信息泄露。

违法违规点：
未采取有效安全保护措施
存在个人信息泄露风险隐患



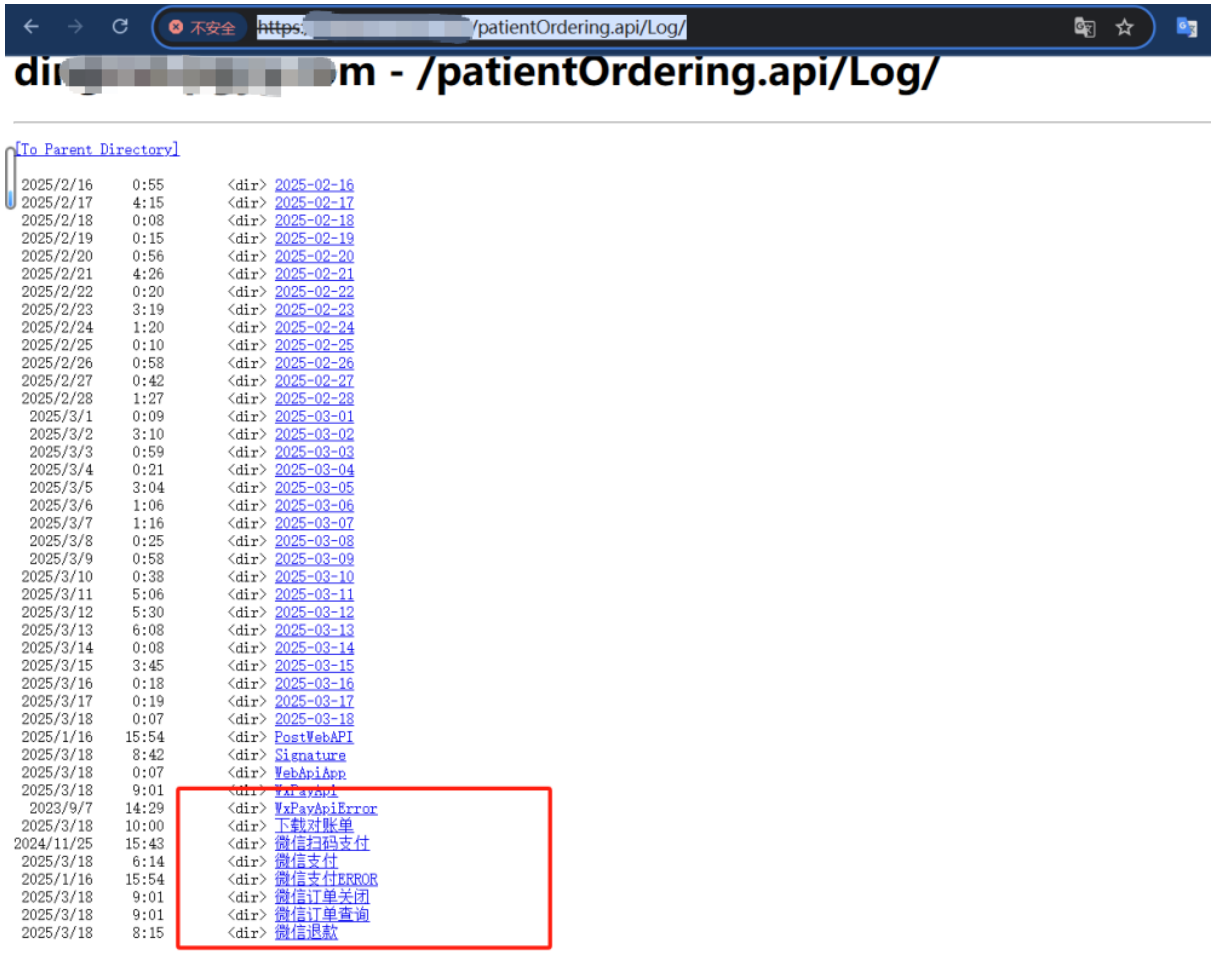


（7）安全保护措施

案例展示：

场景：
由于网站配置问题导致目录遍历，可获取敏感文件如全部日志文件、网站配置文件、微信支付记录、账单等，造成敏感信息泄露。

违法违规点：
未采取有效安全保护措施
存在个人信息泄露风险隐患



3 需企业配合的相关工作

自查清单填报

专项整治行动自查清单

标准应用

关于对《网络安全标准实践指南——扫码点餐个人信息保护要求（征求意见稿）》公开征求意见的通知

网安秘字〔2025〕93号

各有关单位：

为指导餐饮商家规范扫码点餐服务个人信息处理活动，减少因扫码点餐造成的个人权益损害问题，秘书处组织编制了《网络安全标准实践指南——扫码点餐个人信息保护要求（征求意见稿）》。

根据《全国网络安全标准化技术委员会<网络安全标准实践指南>文件管理办法》要求，秘书处现组织对《网络安全标准实践指南——扫码点餐个人信息保护要求（征求意见稿）》面向社会公开征求意见。如有意见或建议，请于**2025年8月4日前**反馈至秘书处。

联系人：王寒生 010-64102730 wanghs@cesi.cn

附件：《网络安全标准实践指南——扫码点餐个人信息保护要求（征求意见稿）》.pdf

全国网络安全标准化技术委员会秘书处

2025年7月22日

表 A.1 扫码点餐服务各方责任关系

情况	角色		
	小程序开发者	小程序运营者	个人信息安全责任承担者
A	餐饮商家或其委托的第三方	餐饮商家	餐饮商家
B		餐饮商家委托的第三方	餐饮商家，餐饮商家委托的第三方需要配合作为受托人的安全责任义务
C		小程序平台	餐饮商家，小程序平台提供技术支撑能力

表 B.1 扫码点餐服务必要个人信息范围

序号	个人信息类型	是否为实现扫码点餐服务所必需	所属功能
1	订单信息	是	点餐、结账
2	支付信息	是	结账
3	手机号	否	会员注册、点餐时核验餐饮用户身份
4	位置信息	否	识别餐饮用户所处店面
5	小程序账号信息	否	账号登录
注：订单信息包含订单号、桌号、所点菜品、菜品总价等。支付信息包含支付状态、支付时间、商品名称、商户名称、收单机构、支付方式、交易单号、商户单号等。小程序账号信息包含昵称、头像等。			

个人信息保护负责人填报

关于开展个人信息保护负责人信息报送工作的公告

网信中国 2025年07月18日 17:01 北京

根据《个人信息保护法》《个人信息保护合规审计管理办法》等法律法规规章规定，现就开展个人信息保护负责人信息报送工作有关事项公告如下：

一、信息报送要求

根据《个人信息保护法》第五十二条、《个人信息保护合规审计管理办法》第十二条规定，处理100万人以上个人信息的个人信息处理者，应当向所在地设区的市级网信部门履行个人信息保护负责人信息报送手续。

二、信息报送时间

（一）自本公告发布之日起，个人信息处理者处理个人信息达到100万人的，应当自数量达到之日起30个工作日内完成信息报送。

（二）本公告发布前，个人信息处理者处理个人信息数量已经达到100万人的，应当在2025年8月29日前完成信息报送。

（三）报送信息发生实质性变更的，应当在变更之日起30个工作日内办理信息变更手续。

三、信息报送方式

个人信息保护负责人信息报送工作采用线上方式。请直接访问“个人信息保护业务系统”（https://grxxbh.cacdtsc.cn），按照系统首页提供的《个人信息保护负责人信息报送系统

18210212136

huoran@bjcert.org.cn

感谢您的聆听！