移动智能生态联盟个人信息保护标准

V2.0 版本

2020-8

1 背景

信息技术的发展和互联网应用的普及，给人们的生活带来了极大的便利，但同时，对个人信息的收集、使用等进行不当或不合法处理的现象也屡见不鲜。

因此，为提升互联网产品和服务的服务质量，增强用户对互联网产品和服务的信任，规范各组织、机构、单位收集、存储、使用、共享、转让、公开披露个人信息控制者所有的个人信息的行为，本标准依据《中国人民共和国网络安全法》、《信息安全技术-个人信息安全规范》、《App 违法违规收集使用个人信息行为认定方法》等相关法律法规、标准、指南，提出了最大程度地保障个人的合法权益和社会公共利益的隐私保护相关原则、条款和要求。

本标准中的具体事项，法律法规如另有规定，需遵照其规定执行。

2 适用范围

本标准适用于 Android 平台各类应用的个人信息保护水平和能力的衡量与判断。应用类型涉及：视频音乐、通讯社交、摄影美图、新闻阅读、购物优惠、生活服务、实用工具、教育学习、系统工具、金融理财、旅游出行、娱乐消遣、育儿母婴、健康美容、效率办公等。

本标准主要包含个人信息安全基本原则，个人信息的收集，个人信息的存储，个人信息的使用，个人信息主体的权利，个人信息的委托处理、共享、转让，共六部分内容。

3 术语和定义

3.1 个人信息

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注 1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2：关于个人信息的判定方法和类型参见附录 A。

注 3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，属于个人信息。

3.2 个人敏感信息

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。

注 2：关于个人敏感信息的判定方法和类型参见附录 B。

注 3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，属于个人敏

感信息。

3.3 个人信息主体

个人信息所标识或者关联的自然人。

3.4 个人信息控制者

有能力决定个人信息处理目的、方式等的组织或个人。

3.5 收集

获得个人信息的控制权的行为。

注 1：包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集行为，以及通过共享、转让、搜集公开信息等间接获取个人信息等行为。

注 2：如果产品或服务的提供者提供工具供个人信息主体使用，提供者不对个人信息进行访问的，则不属于本标准所称的收集。例如，离线导航软件在终端获取个人信息主体位置信息后，如果不回传至软件提供者，则不属于个人信息主体位置信息的收集。

3.6 明示同意

个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。

注：肯定性动作包括个人信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

3.7 授权同意

个人信息主体对其个人信息进行特定处理作出明确授权的行为。

注：包括通过积极的行为作出授权（即明示同意），或者通过消极的不作为而作出授权（如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域）。

3.8 用户画像

通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，形成其个人特征模型的过程。

注：直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

3.9 个人信息安全影响评估

针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。

3.10 删除

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

3.11 公开披露

向社会或不特定人群发布信息的行为。

3.12 转让

将个人信息控制权由一个控制者向另一个控制者转移的过程。

3.13 共享

个人信息控制者向其他控制者提供个人信息，且双方分别对个人信息拥有独立控制权的过程。

3.14 匿名化

通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

3.15 去标识化

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

3.16 个性化展示

基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息， 向该个人信息主体展示信息内容、提供商品或服务的搜索结果等活动。

4 个人信息安全基本原则

个人信息控制者开展个人信息处理活动应遵循合法、正当、必要的原则，具体包括：

权责一致——采取技术和其他必要的措施保障个人信息的安全，对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任；

目的明确——具有明确、清晰、具体的个人信息处理目的；

选择同意——向个人信息主体明示个人信息处理目的、方式、范围等规则，征求其授权同意；

最小必要——只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时删除个人信息；

公开透明——以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督；

确保安全——具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性；

主体参与——向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法。

5 个人信息的收集

5.1 收集个人信息的合法性

标准描述	对个人信息控制者的要求包括： 1、不应以欺诈、诱骗、误导的方式收集个人信息； 2、不应隐瞒产品或服务所具有的收集个人信息的功能； 3、不应从非法渠道获取个人信息。
评估标准	**1、是否以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限** 个人信息控制者所明示收集使用个人信息的目的应真实、准确，不应故意欺瞒、掩饰收集使用个人信息的真实目的。如以红包、金币、抽奖等方式诱骗用户打开可收集个人信息的通讯录权限后， 立即上传所有通讯录信息。

5.2 收集个人信息的最小必要

标准描述	对个人信息控制者的要求包括： 1、收集的个人信息的类型应与实现产品或服务的业务功能有直接关联；直接关联是指没有上述个人信息的参与，产品或服务的功能无法实现； 2、自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率； 3、间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。
评估标准	**1、是否收集与业务功能无关的个人信息** 1.1 不应收集与业务功能无关的个人信息。 1.2 个人信息控制者不应申请打开与业务功能无关的可收集个人信息的权限。 **2、收集个人信息的频度是否超出业务功能实际需要** 2.1 个人信息控制者收集个人信息的频度不应超出业务功能实际需要，在使用 App 某业务功能过程中，应仅收集与当前业务功能相关的个人信息。 2.2 在未打开个人信息控制者的 App 或后台运行 App 时，个人信息控制者不应收集用户个人信息，除非 App 业务功能需要后台运行时继续提供服务，如导航功能。

	2.3 个人信息控制者存在接入第三方应用时，应提醒用户关注第三方应用收集使用个人信息的规则，不得私自截留第三方应用收集的个人信息。

5.3 多项业务功能的自主选择

标准描述	当产品或服务提供多项需收集个人信息的业务功能时，个人信息控制者不应违背个人信息主体的自主意愿，强迫个人信息主体接受产品或服务所提供的业务功能及相应的个人信息收集请求。对个人信息控制者的要求包括： 1、不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求； 2、应把个人信息主体自主作出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件。个人信息控制者应仅在个人信息主体开启该业务功能后，开始收集个人信息； 3、关闭或退出业务功能的途径或方式应与个人信息主体选择使用业务功能的途径或方式同样方便。个人信息主体选择关闭或退出特定业务功能后，个人信息控制者应停止该业务功能的个人信息收集活动； 4、个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应频繁征求个人信息主体的授权同意； 5、个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应暂停个人信息主体自主选择使用的其他业务功能，或降低其他业务功能的服务质量； 6、不得仅以改善服务质量、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。
评估标准	**1、是否以非正当方式强迫收集用户个人信息** 1.1 根据用户主动填写、点击、勾选等自主行为，作为 App 的各个业务功能打开或开始收集使用个人信息的条件。 1.2 App 新增业务功能申请收集的个人信息超出用户原有同意范围时，不应因用户拒绝新增业务功能收集个人信息的请求， 拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外。 1.3 不应仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集其个人信息并以此作为提供服务的条件。 1.4 个人信息控制者不得以捆绑方式强制要求用户一次性同意打开多个可收集个人信息权限。如将安卓版 App 的 targetSdkVersion 值设置低于 23，通过声明机制，在安装 App 时要求用户一次性同意打开多个可收集个人信息权限。 **2、是否以默认选择同意隐私政策等非明示方式征求用户同意**

	2.1 在首次运行 App 或用户注册时，不应采用默认勾选隐私政策等非明示方式征求用户同意； 2.2 注册（包括登录即代表注册）的选项与同意隐私政策等的因果逻辑关系应清楚，且主动提示用户阅读以显著方式展示的隐私政策等收集使用规则后，执行下一步注册/登录等动作。 **3、用户明确表示不同意收集后是否仍收集个人信息或打开可收集个人信息的权限** 用户通过拒绝提供个人信息、不同意收集使用规则、拒绝提供或关闭权限等操作，明确拒绝 App 收集某类个人信息后，不应以任何形式收集该类个人信息或打开可收集个人信息的权限。 **4、用户明确表示不同意收集后是否频繁征求用户同意、干扰用户正常使用** 4.1 用户明确表示不同意收集后，不应在每次重新打开 App、或使用某一业务功能时，向用户频繁（如 48 小时内）询问是否同意收集个人信息。 4.2 用户明确表示不同意收集后，不应在每次重新打开 App、或使用某一业务功能时，向用户频繁（如 48 小时内）询问是否同意打开可收集个人信息的权限。 注：用户选择使用 App 的某一具体功能触发征得同意的动作，不属于频繁干扰情形。如用户自行选择使用拍摄、扫码等功能，App 需获取“相机”权限。

5.4 收集个人信息时的授权同意

标准描述	对个人信息控制者的要求包括： 1、收集个人信息，应向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则，并获得个人信息主体的授权同意； 注 1：如产品或服务仅提供一项收集、使用个人信息的业务功能时，个人信息控制者可通过个人信息保护政策的形式，实现向个人信息主体的告知；产品或服务提供多项收集、使用个人信息的业务功能的，除个人信息保护政策外，个人信息控制者宜在实际开始收集特定个人信息时，向个人信息主体提供收集、使用该个人信息的目的、方式和范围，以便个人信息主体在作出具体的授权同意前，能充分考虑对其的具体影响。 2、收集个人敏感信息前，应征得个人信息主体的明示同意，并应确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示； 3、收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生

	物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意； 注：个人生物识别信息包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。 4、收集年满 14 周岁未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意； 5、间接获取个人信息时： 应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认； 应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露、删除等； 如开展业务所需进行的个人信息处理活动超出已获得的授权同意范围的，应在获取个人信息后的合理期限内或处理个人信息前，征得个人信息主体的明示同意，或通过个人信息提供方征得个人信息主体的明示同意。
评估标准	**1、收集个人信息或打开可收集个人信息的权限前是否征得用户同意** 1.1 App 收集个人信息前应提供由用户主动选择同意或不同意（包括退出、上一步、关闭、取消等）的选项。 1.2 未征得用户同意时，不应收集个人信息或打开可收集个人信息权限。如 App 首次打开时，在用户未得知收集个人信息的目的前，App 就开始收集个人信息。 1.3 不应在征得用户同意前，利用 Cookie 等同类技术、或私自调用可收集用户个人信息的权限等方式收集个人信息。 **2、是否逐一列出 App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等** 2.1 完整、清晰、区分说明各业务功能所收集的个人信息。隐私政策中所述内容应与 App 实际业务相符，并逐项说明各业务功能收集个人信息的目的、类型、方式，不应使用“等、例如”等方式不完整列举。 2.2 如 App 使用 Cookie 等同类技术（包括脚本、Clickstream、Web 信标、Flash Cookie、内嵌 Web 链接等）收集个人信息，应向用户说明使用该类技术收集个人信息的目的、类型、方式。 2.3 如 App 嵌入了第三方代码、插件（如 SDK）收集个人信息，应说明第三方类型，及收集个人信息的目的、类型、方式，说明方式包括隐私政策、弹窗提示、文字备注、文本链接等。

	2.4 如委托的第三方或嵌入的第三方代码、插件直接将个人信息传输至境外的，应明确说明跨境传输个人信息的目的、类型和接收方等。 **3、实际收集的个人信息或打开的可收集个人信息权限是否超出用户授权范围** App 收集使用个人信息的过程应与其所声明的隐私政策等收集使用规则保持一致。如实际收集的个人信息类型、申请打开的可收集使用个人信息的系统权限、调用系统权限函数的行为应与隐私政策所描述内容一致，不应超出隐私政策所述范围。 **4、是否同步告知申请打开权限和要求提供个人敏感信息的目的** 4.1 在申请打开可收集个人信息的权限时，App 应通过显著方式（如弹窗提示等）同步告知用户其目的，对目的的描述应明确、易懂。 4.2 在要求用户提供个人敏感信息（用户身份证号、银行账号、行踪轨迹等）时，App 应通过显著方式（如文字加粗、弹窗提示、文字备注、文本链接等）同步告知用户其目的，对目的的描述应明确、易懂。 **5、收集使用规则是否易于理解** 有关收集使用规则的内容应简练、结构清晰、重点突出，避免使用晦涩难懂的词语（如使用大量专业术语）和冗长繁琐的篇幅。 **6、是否未经用户同意更改其设置的可收集个人信息权限状态** 6.1 未经用户同意，不应私自更改用户设置的收集个人信息权限。 6.2 App 更新升级后，不应自动将用户设置的权限恢复到默认状态。

5.5 个人信息保护政策

标准描述	对个人信息控制者的要求包括： 1、应制定个人信息保护政策，内容应包括但不限于： 个人信息控制者的基本情况，包括主体身份、联系方式； 收集、使用个人信息的业务功能，以及各业务功能分别收集的个人信息类型。涉及个人敏感信息的，需明确标识或突出显示； 个人信息收集方式、存储期限、涉及数据出境情况等个人信息处理规则； 对外共享、转让、公开披露个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及各自的安全和法律责任；

	个人信息主体的权利和实现机制，如查询方法、更正方法、删除方法、注销账户的方法、撤回授权同意的方法、获取个人信息副本的方法、对信息系统自动决策结果进行投诉的方法等； 提供个人信息后可能存在的安全风险，及不提供个人信息可能产生的影响； 遵循的个人信息安全基本原则，具备的数据安全能力，以及采取的个人信息安全保护措施，必要时可公开数据安全和个人信息保护相关的合规证明； 处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式。 2、个人信息保护政策所告知的信息应真实、准确、完整； 3、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； 4、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； 5、个人信息保护政策应逐一送达个人信息主体。当成本过高或有显著困难时，可以公告的形式发布； 6、在 1）所载事项发生变化时，应及时更新个人信息保护政策并重新告知个人信息主体。 注 1：组织会习惯性将个人信息保护政策命名为“隐私政策”或其他名称，其内容宜与个人信息保护政策内容保持一致。 注 2：在个人信息主体首次打开产品或服务、注册账户等情形时，宜通过弹窗等形式主动向其展示个人信息保护政策的主要或核心内容，帮助个人信息主体理解该产品或服务的个人信息处理范围和规则，并决定是否继续使用该产品或服务。
评估标准	**1、是否有隐私政策等收集使用规则** 1.1 在 App 界面中能够找到隐私政策，包括通过弹窗、文本链接、附件、常见问题（FAQs）等形式，且隐私政策可正常显示。 1.2 隐私政策中需包含收集使用个人信息规则的相关内容。 1.3 隐私政策文本链接有效，且文本可正常显示。 **2、是否公开收集使用个人信息的其他规则** 2.1 隐私政策应说明发布、生效或更新日期。 2.2 隐私政策应对个人信息存放地域（境内、境外哪个国家或地区）、存储期限（法律规定范围内最短期限或明确的期限）、超期处理方式进行明确说明。

	2.3 如果 App 运营者将个人信息用于用户画像、个性化展示等，隐私政策中应说明其应用场景和可能对用户产生的影响。 2.4 如果存在个人信息出境情形，隐私政策中应将出境个人信息类型逐项列出并显著标识（如字体加粗、标星号、下划线、斜体、不同颜色等）；如果不存在个人信息出境情形，则明确说明。 2.5 隐私政策中应对 App 运营者在个人信息保护方面采取的措施和具备的能力进行说明，如身份鉴别、数据加密、访问控制、恶意代码防范、安全审计等。 2.6 如果存在个人信息对外共享、转让、公开披露等情况，隐私政策中应明确以下内容：①对外共享、转让、公开披露个人信息的目的；②涉及的个人信息类型；③接收方类型或身份。 2.7 隐私政策中应对以下用户权利和相关操作方法进行明确说明：①个人信息查询；②个人信息更正；③个人信息删除；④用户账户注销；⑤撤回已同意的授权。 2.8 隐私政策中至少提供以下一种申诉渠道：①电子邮件；②电话；③在线客服；④在线表单。 **3、是否提示用户阅读隐私政策等收集使用规则** 3.1 App 需在首次运行或用户注册时通过弹窗等明显方式，提示用户阅读隐私政策。 3.2 避免使用灰色字体、缩小字号、键盘遮挡、置于边缘等方式未突出显示隐私政策链接。 **4、隐私政策等收集使用规则是否易于访问** 4.1 用户进入 App 主功能界面后，通过 4 次（含）以内的点击，能够访问到隐私政策。 4.2 在 App 常规交互界面展示隐私政策链接，避免仅在注册/登录界面展示隐私政策链接，或只能以咨询客服等方式查看隐私政策的情形。 4.3 隐私政策以单独成文的形式发布，而不是作为用户协议、用户说明等文件中的一部分存在。 **5、隐私政策等收集使用规则是否易于阅读** 5.1 隐私政策文本文字显示方式（字号、颜色、行间距、清晰度等）不会造成阅读困难。

	5.2 需提供简体中文版隐私政策。 5.3 隐私政策的内容需符合通用的语言习惯，使用标准化的数字、图示，避免出现错别字或有歧义的语句。 **6、是否公开 App 运营者的基本情况** 隐私政策应对 App 运营者基本情况进行描述，至少包括组织或公司名称、注册地址或常用办公地址、个人信息保护工作机构或相关负责人联系方式。 **7、是否以适当的方式通知用户收集使用个人信息的目的、方式、范围发生的变化** 收集使用个人信息的目的、方式和范围发生变化时，应以适当方式通知用户，适当方式包括更新隐私政策并以信息、邮件、弹窗等方式提醒用户阅读发生变化的条款等。

6 个人信息的存储

6.1 个人信息存储时间最小化

标准描述	对个人信息控制者的要求包括： 1、个人信息存储期限应为实现个人信息主体授权使用的目的所必需的最短时间， 法律法规另有规定或者个人信息主体另行授权同意的除外； 2、超出上述个人信息存储期限后，应对个人信息进行删除或匿名化处理。
评估标准	**1、个人信息存储期限是否合理** 1.1 为实现业务目的，需要个人数据做判断，但没有存储和后续数据处理需求的，不对个人信息进行存储。 1.2 为实现业务目的，需要存储个人数据，获得个人信息主体授权后，并告知个人信息主体信息的存储期限，同时业务目的在可预见时间内完成的，存储期限一般不超过 1 年（如法律有明确约定的，以法律约定为准）。 1.3 为实现业务目的，需要存储个人数据，且用户将长期使用的，在用户注销服务或者业务目的完成后，应对个人信息数据进行删除或匿名化处理。 **2、是否在超出个人信息存储期限后对其进行删除或匿名化处理** 超出法律法规中明确的保存时间后，或超出用户授权同意的存储期限后，应对个人信息数据进行删除或匿名化处理。

6.2 去标识化处理

标准描述	收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。
评估标准	**1、是否采用合理方式对个人信息进行去标识化处理** 以特定的规则对个人信息中的敏感信息进行变形，实现对敏感个人信息的保护，让其可以正常使用而不被非法利用。 从应用场景、业务层面确定可能涉及个人信息； 应根据业务需求识别出个人信息所面临的风险，确定需要进行脱敏的个人信息及具体实现方式； 应保留脱敏前的有意义信息并能防止恶意攻击者进行破解； 宜采用自动化工具对个人信息字段进行指定的脱敏处理，以保持组织内部脱敏方式的统一与规范； 宜对个人信息脱敏设计过程进行文档记录，以便于后期的维护和追溯。

6.3 个人敏感信息的传输和存储

标准描述	对个人信息控制者的要求包括： 1、传输和存储个人敏感信息时，应采用加密等安全措施； 注：采用密码技术时宜遵循密码管理相关国家标准。 2、个人生物识别信息应与个人身份信息分开存储； 3、原则上不应存储原始个人生物识别信息（如样本、图像等），可采取的措施包括但不限于： 仅存储个人生物识别信息的摘要信息； 在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能； 在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。 注 1：摘要信息通常具有不可逆特点，无法回溯到原始信息。 注 2：个人信息控制者履行法律法规规定的义务相关的情形除外。
评估标准	**1、是否对个人敏感信息加以安全控制** 1.1 用户个人数据需以假名化的方式进行存储，标识用户类的数据应当加密存储。使用安全的哈希或加密算法，如 SHA2 等。 1.2 传输时应当使用加密的通信协议，如 HTTPS 等。 1.3 不得将匿名化或假名化的数据进行还原，也不得进行任何 ID 之间的组合或匹配。 **2、是否将个人生物识别信息与个人身份信息分开存储**

	存储个人生物识别信息和个人身份信息时，应当将二者存储至不同的位置，并对存储环境进行加密管理，其数据访问的安全性应当得到保障。

7 个人信息的使用

7.1 个人信息访问控制措施

标准描述	对个人信息控制者的要求包括： 1、对被授权访问个人信息的人员，应建立最小授权的访问控制策略，使其只能访问职责所需的最小必要的个人信息，且仅具备完成职责所需的最少的数据操作权限； 2、对个人信息的重要操作设置内部审批流程，如进行批量修改、拷贝、下载等重要操作； 3、对安全管理人员、数据操作人员、审计人员的角色进行分离设置； 4、确因工作需要，需授权特定人员超权限处理个人信息的，应经个人信息保护责任人或个人信息保护工作机构进行审批，并记录在册； 5、对个人敏感信息的访问、修改等操作行为，宜在对角色权限控制的基础上，按照业务流程的需求触发操作授权。例如，当收到客户投诉，投诉处理人员才可访问该个人信息主体的相关信息。
评估标准	**1、是否对个人信息的访问进行合理控制并实施有效的措施** 确保个人信息安全的防护策略和规范被有效的执行和落地，确保快速发现潜在的风险和行为。 对现有涉及个人信息的账号和权限进行统一梳理； 账号的调整必须遵循企业规章制度等合规性保障； 应对所有涉及个人信息的账号和权限变化进行监控，出现违规变化应告警； 应对涉及个人信息的所有操作进行日志记录并定期审计，包括账号、操作时间、IP、会话、操作、对象、结果、耗时等； 宜具备对涉及个人信息的操作返回数量设置阈值的能力，超过一定阈值触发告警； 应具备对异常行为的监测与分析能力，如高频查询个人信息的账号或权限、高频被查询的个人信息、被高频修改的个人信息等。

7.2 个人信息的展示限制

标准描述	涉及通过界面展示个人信息的（如显示屏幕、纸面），个人信息控制者宜对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。例如，在个人信息展示时，防止内部非授权人员及个人信息主体之

	外的其他人员未经授权获取个人信息。
评估标准	**1、是否对个人信息的展示和访问进行安全控制** 1.1 对被授权访问用户个人数据的人员，应建立最小授权的访问控制策略，使其只能访问职责所需的最少够用的用户个人数据，且仅具备完成职责所需的最少的数据操作权限。 1.2 对个人信息的重要操作设置内部审批流程，如进行批量修改、拷贝、下载等重要操作；对于导出的数据，需明确授权使用人员，并限制未授权人员的访问，并于使用目的实现后立即销毁。 1.3 确保人员离职、转岗后删除其数据处理系统的访问权限，并定期清理过期账号。 1.4 对安全管理人员、数据操作人员、审计人员的角色进行分离设置。 1.5 对个人敏感信息的访问、修改等操作行为，应当在对角色的权限控制的基础上，根据业务流程的需求触发操作授权。例如，因收到客户投诉，投诉处理人员才可访问该用户的相关信息。 1.6 业务的管理后台界面，不提供展示个人数据的功能，如若需要，应对个人信息限制展示，如对电话号码进行打码处理等。

7.3 个人信息使用的目的限制

标准描述	对个人信息控制者的要求包括： 使用个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意； 注：将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内。但对外提供学术研究或描述的结果时，需对结果中所包含的个人信息进行去标识化处理。 如所收集的个人信息进行加工处理而产生的信息，能够单独或与其他信息结合 识别特定自然人身份或者反映特定自然人活动情况的，应将其认定为个人信息。对其处理应遵循收集个人信息时获得的授权同意范围。 注：加工处理而产生的个人信息属于个人敏感信息的，对其处理需符合对个人敏感信息的要求。
评估标准	**1、是否违反其所声明的收集使用规则，收集使用个人信息** App 应严格遵循其披露的隐私政策等收集使用规则，开展个人信息处理活动，如个人信息使用目的发生变化的，应再次征得用户同意。

7.4 用户画像的使用限制

标准描述	对个人信息控制者的要求包括： 1、用户画像中对个人信息主体的特征描述，不应： 包含淫秽、色情、赌博、迷信、恐怖、暴力的内容； 表达对民族、种族、宗教、残疾、疾病歧视的内容。 2、在业务运营或对外业务合作中使用用户画像的，不应： 侵害公民、法人和其他组织的合法权益； 危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序。 3、除为实现个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。例如，为准确评价个人信用状况， 可使用直接用户画像，而用于推送商业广告目的时，则宜使用间接用户画像。
评估标准	**1、用户画像的使用是否合理合法** 特征描述是否包含违法、歧视内容；是否侵害他人合法权益；是否威胁国家安全；是否扰乱国家和社会秩序；是否精准定位到个人。

7.5 个性化展示的使用

标准描述	对个人信息控制者的要求包括： 1、在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容； 注：显著区分的方式包括但不限于：标明“定推”等字样，或通过不同的栏目、版块、页面分别展示等。 2、在向个人信息主体提供电子商务服务的过程中，根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项； 注：基于个人信息主体所选择的特定地理位置进行展示、搜索结果排序，且不因个人信息主体身份不同展示不一样的内容和搜索结果排序，则属于不针对其个人特征的选项。 3、在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应： 为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项； 当个人信息主体选择退出或关闭个性化展示模式时，向个人信息主体提供删

	除或匿名化定向推送活动所基于的个人信息的选项。 4、在向个人信息主体提供业务功能的过程中使用个性化展示的，宜建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制， 保障个人信息主体调控个性化展示相关性程度的能力。
评估标准	**1、App 利用用户个人信息和算法定向推送信息时，是否提供非定向推送信息的选项** App 存在利用用户个人信息和算法定向推送信息情形（包括利用个人信息和算法推送新闻和信息、展示商品、推送广告等），应提供拒绝接受定向推送信息，或者停止、退出、关闭相应功能的机制，或者不基于个人信息、用户画像等推送的模式、选项。

7.6 基于不同业务目的所收集个人信息的汇聚融合

标准描述	对个人信息控制者的要求包括： 1、应遵守 7.3 的要求； 2、应根据汇聚融合后个人信息所用于的目的，开展个人信息安全影响评估，采取有效的个人信息保护措施。
评估标准	——

7.7 信息系统自动决策机制的使用

标准描述	个人信息控制者业务运营所使用的信息系统，具备自动决策机制且能对个人信息主体权益造成显著影响的（例如，自动决定个人征信及贷款额度，或用于面试人员的自动化筛选等），应： 1、在规划设计阶段或首次使用前开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施； 2、在使用过程中定期（至少每年一次）开展个人信息安全影响评估，并依评估结果改进保护个人信息主体的措施； 3、向个人信息主体提供针对自动决策结果的投诉渠道，并支持对自动决策结果的人工复核。
评估标准	**1、是否对个人信息安全影响进行评估** 应当对自动化决策机制给个人信息主体权益造成的影响进行安全影响评估，并定期进行核查。安全影响评估包括但不限于对个人信息主体数据的安全性影响评估、对个人信息主体权利实现的影响评估等。 **2、是否提供个人信息主体针对自动决策结果的投诉渠道** 个人信息控制者应当建立简单、方便、合理、合法的投诉渠道，供个人信息

	主体针对自动决策结果进行投诉或反馈，并应当在法律允许的条件下和范围内向个人信息主体提供自动决策的机制和依据。

8 个人信息主体的权利

8.1 个人信息查询

标准描述	个人信息控制者应向个人信息主体提供查询下列信息的方法： 1、其所持有的关于该主体的个人信息或个人信息的类型； 2、上述个人信息的来源、所用于的目的； 3、已经获得上述个人信息的第三方身份或类型。 注：个人信息主体提出查询非其主动提供的个人信息时，个人信息控制者可在综合考虑不响应请求可能对个人信息主体合法权益带来的风险和损害，以及技术可行性、实现请求的成本等因素后，作出是否响应的决定，并给出解释说明。
评估标准	**1、是否提供有效的查询个人信息的途径** 1.1 App 应提供有效的查询个人信息的途径。 1.2 用户无法通过在线操作方式及时响应个人信息查询请求的，App 运营者应在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理。 1.3 查询个人信息的过程应简单易操作，不应设置不必要或不合理的条件。

8.2 个人信息更正

标准描述	个人信息主体发现个人信息控制者所持有的该主体的个人信息有错误或不完整的， 个人信息控制者应为其提供请求更正或补充信息的方法。
评估标准	**1、是否提供有效的更正个人信息的途径** 1.1 App 应提供有效的更正个人信息的途径。 1.2 个人信息主体无法通过在线操作方式及时响应个人信息更正请求的，App 运营者应在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理。 1.3 更正个人信息的过程应简单易操作，不应设置不必要或不合理的条件。 1.4 个人信息主体更正个人信息等操作完成时，App 后台应同步执行完成相关操作。

8.3 个人信息删除

标准描述	对个人信息控制者的要求包括：

	1、符合以下情形，个人信息主体要求删除的，应及时删除个人信息： 个人信息控制者违反法律法规规定，收集、使用个人信息的； 个人信息控制者违反与个人信息主体的约定，收集、使用个人信息的。 2、个人信息控制者违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止共享、转让的行为，并通知第三方及时删除； 3、个人信息控制者违反法律法规规定或违反与个人信息主体的约定，公开披露个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。
评估标准	**1、是否提供有效的删除个人信息的途径** 1.1 App 应提供有效的删除个人信息的途径。 1.2 用户无法通过在线操作方式及时响应个人信息删除请求的，App 运营者应在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理。 1.3 删除个人信息的过程应简单易操作，不应设置不必要或不合理的条件。 1.4 用户删除个人信息等操作完成时，App 后台应同步执行完成相关操作。

8.4 个人信息主体撤回授权同意

标准描述	对个人信息控制者的要求包括： 1、应向个人信息主体提供撤回收集、使用其个人信息的授权同意的方法。撤回授权同意后，个人信息控制者后续不应再处理相应的个人信息； 2、应保障个人信息主体拒绝接收基于其个人信息推送商业广告的权利。对外共享、转让、公开披露个人信息，应向个人信息主体提供撤回授权同意的方法。 注：撤回授权同意不影响撤回前基于授权同意的个人信息处理。
评估标准	**1、是否向用户提供撤回同意收集个人信息的途径、方式** 1.1 App 应向用户提供撤回同意收集个人信息的途径、方式，并在隐私政策等收集使用规则中予以明确。 1.2 如用户拒绝或撤回特定业务功能收集个人信息的授权时，App 不应暂停提供其他业务功能，或降低其他业务功能的服务质量（如用户撤回的为业务基本功能的除外）。 1.3 如用户拒绝或撤回可收集个人信息的权限时，不得影响用户正常使用与该权限无关的功能，除非该权限是保证 App 正常运行所必需。

8.5 个人信息主体注销账户

标准描述	对个人信息控制者的要求包括： 1、通过注册账户提供产品或服务的个人信息控制者，应向个人信息主体提供注销账户的方法，且方法简便易操作； 2、受理注销账户请求后，需要人工处理的，应在承诺时限内（不超过 15 个工作日） 完成核查和处理； 3、注销过程如需进行身份核验，要求个人信息主体再次提供的个人信息类型不应多于注册、使用等服务环节收集的个人信息类型； 4、注销过程不应设置不合理的条件或提出额外要求增加个人信息主体义务，如注销单个账户视同注销多个产品或服务，要求个人信息主体填写精确的历史操作记录作为注销的必要条件等； 注 1：多个产品或服务之间存在必要业务关联关系的，例如，一旦注销某个产品或服务的账户，将会导致其他产品或服务的必要业务功能无法实现或者服务质量明显下降的，需向个人信息主体进行 详细说明。 注 2：产品或服务没有独立的账户体系的，可采取对该产品或服务账号以外其他个人信息进行删除，并切断账户体系与产品或服务的关联等措施实现注销。 5、注销账户的过程需收集个人敏感信息核验身份时，应明确对收集个人敏感信息后的处理措施，如达成目的后立即删除或匿名化处理等； 6、个人信息主体注销账户后，应及时删除其个人信息或匿名化处理。因法律规规定需要留存个人信息的，不能再次将其用于日常业务活动中。
评估标准	**1、是否提供有效的注销用户账号功能** 1.1 App 应提供有效的注销账号的途径（如在线操作、客服电话、电子邮件等），并在用户注销账号后，及时删除其个人信息或进行匿名化处理，法律法规另有规定的除外。 1.2 受理注销账号请求后，App 运营者应在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限） 完成核查和处理。 1.3 注销账号的过程应简单易操作，不应设置不必要或不合理的注销条件，如提供额外的个人敏感信息用于身份验证，或未明确注销所需个人敏感信息在注销成功后是否会删除等。

8.6 个人信息主体获取个人信息副本

标准描述	根据个人信息主体的请求，个人信息控制者宜为个人信息主体提供获取以下类型个人信息副本的方法，或在技术可行的前提下直接将以下类型个人信息的副本传输给个人信息主体指定的第三方：

	1、本人的基本资料、身份信息； 2、本人的健康生理信息、教育工作信息。
评估标准	**1、是否能够按需提供个人信息副本** 当个人信息主体提出相关需求后，个人信息控制者应当在合理期限内将个人信息主体所主张的个人信息副本完整地以合理的方式提供给个人信息主体。

8.7 响应个人信息主体的请求

标准描述	对个人信息控制者的要求包括： 1、在验证个人信息主体身份后，应及时响应个人信息主体基于8.1~8.6提出的请求，应在三十天内或法律法规规定的期限内作出答复及合理解释，并告知个人信息主体外部纠纷解决途径； 2、采用交互式页面（如网站、移动互联网应用程序、客户端软件等）提供产品或服务的，宜直接设置便捷的交互式页面提供功能或选项，便于个人信息主体在线行使其访问、更正、删除、撤回授权同意、注销账户等权利； 3、对合理的请求原则上不收取费用，但对一定时期内多次重复的请求，可视情收取一定成本费用； 4、直接实现个人信息主体的请求需要付出高额成本或存在其他显著困难的，个人信息控制者应向个人信息主体提供替代方法，以保障个人信息主体的合法权益； 5、如决定不响应个人信息主体的请求，应向个人信息主体告知该决定的理由，并向个人信息主体提供投诉的途径。
评估标准	**1、是否能够合理响应个人信息主体的请求** 应当尽可能提供交互式页面，供个人信息主体实现相关权利；不能提供交互式页面的，能够以合理合法的方式，响应个人信息主体的请求。

9 个人信息的委托处理、共享、转让

9.1 委托处理

标准描述	个人信息控制者委托第三方处理个人信息时，应符合以下要求： 1、个人信息控制者作出委托行为，不应超出已征得个人信息主体授权同意的范围； 2、个人信息控制者应对委托行为进行个人信息安全影响评估，确保受委托者达到数据安全能力要求； 3、受委托者应：

	严格按照个人信息控制者的要求处理个人信息。受委托者因特殊原因未按照个人信息控制者的要求处理个人信息的，应及时向个人信息控制者反馈； 受委托者确需再次委托时，应事先征得个人信息控制者的授权； 协助个人信息控制者响应个人信息主体基于8.1~8.6提出的请求； 受委托者在处理个人信息过程中无法提供足够的安全保护水平或发生了安全事件的，应及时向个人信息控制者反馈； 在委托关系解除时不再存储相关个人信息。 4、个人信息控制者应对受委托者进行监督，方式包括但不限于： 通过合同等方式规定受委托者的责任和义务； 对受委托者进行审计。 5、个人信息控制者应准确记录和存储委托处理个人信息的情况； 6、个人信息控制者得知或者发现受委托者未按照委托要求处理个人信息，或未能有效履行个人信息安全保护责任的，应立即要求受托者停止相关行为，且采取或要求受委托者采取有效补救措施（如更改口令、回收权限、断开网络连接等） 控制或消除个人信息面临的安全风险。必要时个人信息控制者应终止与受委托者的业务关系，并要求受委托者及时删除从个人信息控制者获得的个人信息。
评估标准	**1、个人信息控制者委托第三方处理个人信息是否征得个人信息主体授权同意** 个人信息控制者委托第三方处理个人信息前，应以书面或用户授权交互界面的形式征得用户同意； 个人信息控制者所提供的隐私政策文本中应准确描述委托第三方处理个人信息的目的、方式、安全性控制措施。 **2、个人信息控制者应当对第三方进行安全性评估** 个人信息控制者在委托第三方前，应当对第三方进行全面的安全性评估。其中包括但不限于第三方是否通过安全与隐私相关的国内外权威认证、是否建立了全面的安全管理制度、是否配备有专职的信息安全员工、是否对人员安全进行保密性控制、是否对员工进行安全意识及相关的安全技术培训、是否对访客进行安全性控制、是否对信息数据进行访问控制和审计、是否有代码的安全评审机制、是否会定期对产品或服务进行安全检查、是否对办公环境进行定制安全扫描、是否制定了漏洞修复的服务等级协议、是否有应急预案或事故处理流程、是否会定期进行人员应急培训和演练、是否建立了完善的安全信息事件通报机制、是否对办公网络和生产环境网络进行了区隔、是否

	在网络层面上建立了 ACL 或防火墙、是否对主机安全建立了安全性控制机制和审计机制、是否对用户敏感数据进行加密存储、是否适用 https 加密传输数据、员工的终端设备是否设置了安全性保护措施。 **3、第三方委托时，若发生风险或问题，是否能够立即停止委托处理** 是否建立了严格且完整的第三方风险监控和处理机制，能够及时应对第三方不满足委托要求时的处理和管控需求。

9.2 个人信息共享、转让

标准描述	个人信息控制者共享、转让个人信息时，应充分重视风险。共享、转让个人信息， 非因收购、兼并、重组、破产原因的，应符合以下要求： 1、事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施； 2、向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型以及可能产生的后果，并事先征得个人信息主体的授权同意。共享、转让经去标识化处理的个人信息，且确保数据接收方无法重新识别或者关联个人信息主体的除外； 3、共享、转让个人敏感信息前，除 2）中告知的内容外，还应向个人信息主体告知涉及的个人敏感信息类型、数据接收方的身份和数据安全能力，并事先征得个人信息主体的明示同意； 4、通过合同等方式规定数据接收方的责任和义务； 5、准确记录和存储个人信息的共享、转让情况，包括共享、转让的日期、规模、目的，以及数据接收方基本情况等； 6、个人信息控制者发现数据接收方违反法律法规要求或双方约定处理个人信息的，应立即要求数据接收方停止相关行为，且采取或要求数据接收方采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险；必要时个人信息控制者应解除与数据接收方的业务关系，并要求数据接收方及时删除从个人信息控制者获得的个人信息； 7、因共享、转让个人信息发生安全事件而对个人信息主体合法权益造成损害的， 个人信息控制者应承担相应的责任； 8、帮助个人信息主体了解数据接收方对个人信息的存储、使用等情况，以及个人信息主体的权利，例如，访问、更正、删除、注销账户等； 9、个人生物识别信息原则上不应共享、转让。因业务需要，确需共享、转让的， 应单独向个人信息主体告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等，并征得个人信息主体的明示同意。

评估标准	**1、向他人提供个人信息前是否征得用户同意** 1.1 如App存在从客户端直接向第三方发送个人信息的情形，包括通过App客户端嵌入第三方代码、插件（如SDK）等方式，应事先征得用户同意，经匿名化处理的除外。 1.2 如个人信息传输至App服务器后，App运营者向第三方提供其收集的个人信息，应事先征得用户同意，经匿名化处理的除外。 1.3 如App接入第三方应用，当用户使用第三方应用时，应事先征得用户同意后，再向第三方应用提供个人信息，用户获知应用为第三方且在知悉收集使用个人信息规则后，自行同意提供给第三方的除外。

9.3 共同个人信息控制者

标准描述	对个人信息控制者的要求包括： 1、当个人信息控制者与第三方为共同个人信息控制者时，个人信息控制者应通过合同等形式与第三方共同确定应满足的个人信息安全要求，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，并向个人信息主体明确告知； 2、如未向个人信息主体明确告知第三方身份，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，个人信息控制者应承担因第三方引起的个人信息安全责任。 注：如个人信息控制者在提供产品或服务的过程中部署了收集个人信息的第三方插件（例如，网站经营者与在其网页或应用程序中部署统计分析工具、软件开发工具包 SDK、调用地图 API 接口）， 且该第三方并未单独向个人信息主体征得收集个人信息的授权同意，则个人信息控制者与该第三方在个人信息收集阶段为共同个人信息控制者。
评估标准	**1、是否向个人信息主体明示共同个人信息控制者的相关信息，并征得用户同意** 个人信息控制者所提供的隐私政策文本中应准确描述共同个人信息控制者的相关信息，并明确与共同个人信息控制者的责任和义务。与共同个人信息控制者共同控制个人信息主体的数据前，应当获得用户授权。 **2、是否对共同个人信息控制者进行安全性评估** 个人信息控制者在与共同个人信息控制者共同控制个人信息主体的数据前，应当对共同个人信息控制者进行全面的安全性评估。其中包括但不限于共同个人信息控制者是否通过安全与隐私相关的国内外权威认证、是否建立了全面的安全管理制度、是否配备有专职的信息安全员工、是否对人员安全进行

	保密性控制、是否对员工进行安全意识及相关的安全技术培训、是否对访客进行安全性控制、是否对信息数据进行访问控制和审计、是否有代码的安全评审机制、是否会定期对产品或服务进行安全检查、是否对办公环境进行定制安全扫描、是否制定了漏洞修复的服务等级协议、是否有应急预案或事故处理流程、是否会定期进行人员应急培训和演练、是否建立了完善的安全信息事件通报机制、是否对办公网络和生产环境网络进行了区隔、是否在网络层面上建立了 ACL 或防火墙、是否对主机安全建立了安全性控制机制和审计机制、是否对用户敏感数据进行加密存储、是否适用 https 加密传输数据、员工的终端设备是否设置了安全性保护措施。

9.4 第三方接入管理

标准描述	当个人信息控制者在其产品或服务中接入具备收集个人信息功能的第三方产品或服务且不适用 9.1 和 9.3 时，对个人信息控制者的要求包括： 1、建立第三方产品或服务接入管理机制和工作流程，必要时应建立安全评估等机制设置接入条件； 2、应与第三方产品或服务提供者通过合同等形式明确双方的安全责任及应实施的个人信息安全措施； 3、应向个人信息主体明确标识产品或服务由第三方提供； 4、应妥善留存平台第三方接入有关合同和管理记录，确保可供相关方查阅； 5、应要求第三方根据本标准相关要求向个人信息主体征得收集个人信息的授权同意，必要时核验其实现的方式； 6、应要求第三方产品或服务建立响应个人信息主体请求和投诉等的机制，以供个人信息主体查询、使用； 7、应监督第三方产品或服务提供者加强个人信息安全管理，发现第三方产品或服务没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入； 产品或服务嵌入或接入第三方自动化工具（如代码、脚本、接口、算法模型、软件开发工具包、小程序等）的，宜采取以下措施： 开展技术检测确保其个人信息收集、使用行为符合约定要求； 对第三方嵌入或接入的自动化工具收集个人信息的行为进行审计，发现超出约定的行为，及时切断接入。
评估标准	**1、对第三方插件/SDK 进行安全性和合理性评估** 1.1 合理性原则：涉及第三方 SDK 申请及使用的所有权限，均应且只应满足宿主产品所需要的功能。 1.2 必要性原则：超出宿主产品所使用的功能，即使功能合理，也应当进行裁剪。

	1.3 辅助性原则：如果有替代方案可通过不采集个人信息或不使用敏感权限的前提下也能够实现所需功能，应当采取替代方案。 1.4 最小化原则：在满足以上三个原则的情况下，针对宿主产品无使用场景，需要单独为第三方 SDK 申请的隐私敏感权限，应进行严格控制。 1.5 第三方插件/SDK 应进行代码审计和漏洞检测。 1.6 对 SDK 所申请的敏感隐私权限、采集用户个人信息的字段、频率、回传服务端场景等进行安全评估。 1.7 对第三方插件/SDK 的权限的申请及获取进行限制，如安卓系统统一通过宿主 APP 进行权限声明、禁止 SDK 热更新等。

9.5 个人信息跨境传输

标准描述	在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，个人信息控制者应遵循国家相关规定和相关标准的要求。
评估标准	**1、个人信息的跨境传输是否合理合规** 个人信息控制者向境外传输的数据，及传输的方式、安全性控制措施、目的等是否符合国家相关规定和相关标准的要求。

附 录 A
（资料性附录） 个人信息示例

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，如姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

判定某项信息是否属于个人信息，应考虑以下两条路径：一是识别，即从信息到个人，由信息本身的特殊性识别出特定自然人，个人信息应有助于识别出特定个人。二是关联，即从个人到信息，如已知特定自然人，由该特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录等）即为个人信息。符合上述两种情形之一的信息，均应判定为个人信息。

表 A.1 给出了个人信息举例。

表 A.1 个人信息举例

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书等
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
个人财产信息	银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
个人常用设备信息	指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如 IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等）等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

附 录 B

（资料性附录） 个人敏感信息判定

个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。通常情况下，14 岁以下（含） 儿童的个人信息和涉及自然人隐私的信息属于个人敏感信息。可从以下角度判定是否属于个人敏感信息：

泄露：个人信息一旦泄露，将导致个人信息主体及收集、使用个人信息的组织和机构丧失对个人信息的控制能力，造成个人信息扩散范围和用途的不可控。某些个人信息在泄漏后，被以违背个人信息主体意愿的方式直接使用或与其他信息进行关联分析，可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，个人信息主体的身份证复印件被他人用于手机号卡实名登记、银行账户开户办卡等。

非法提供：某些个人信息仅因在个人信息主体授权同意范围外扩散，即可对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，性取向、存款信息、传染病史等。

滥用：某些个人信息在被超出授权合理界限时使用（如变更处理目的、扩大处理范围等），可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，在未取得个人信息主体授权时，将健康信息用于保险公司营销和确定个体保费高低。

表 B.1 给出了个人敏感信息举例。

表 B.1　个人敏感信息举例

个人财产信息	银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等