

中华人民共和国国家标准

GB/T 43739—2024

网络安全技术 应用商店的移动互联网 应用程序(App) 个人信息处理规范性 审核与管理指南

Cybersecurity technology—Audit and management guide for personal
information processing normativeness of mobile internet applications in
App stores

2024-04-25发布

2024-11-01 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 I

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 应用商店中 App 的审核与管理流程 2

6 应用商店中 App 个人信息处理活动审核 3

 6.1 App 个人信息处理活动审核规则公示 3

 6.2 App 上架申请信息受理 3

 6.3 App 个人信息处理活动审核验证 3

 6.4 审核结果反馈与申诉处理 4

 6.5 存量 App 与版本更新审核 5

7 应用商店中 App 个人信息安全管理 5

 7.1 个人信息处理情况的展示 5

 7.2 个人信息安全相关标识 5

 7.3 App 运营者管理 6

 7.4 日常监督与问题处置 6

附录 A（资料性） App 个人信息处理活动审核材料参考模板 7

附录 B（资料性） App 下载页面展示内容示例 15

附录 C（资料性） 个人信息安全问题投诉举报渠道示例 18

参考文献 19

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。

本文件由全国网络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：中国移动通信集团有限公司、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、北京邮电大学、中国网络空间研究院、华为技术有限公司、OPPO 广东移动通信有限公司、北京小米移动软件有限公司、北京百度网讯科技有限公司、北京抖音信息服务有限公司、北京快手科技有限公司、北京三快在线科技有限公司、维沃移动通信有限公司、公安部第三研究所、中国网络安全审查技术与认证中心、中国电子科技集团公司第十五研究所、蚂蚁科技集团股份有限公司、长扬科技(北京)股份有限公司、北京时代新威信息技术有限公司、郑州信大捷安信息技术股份有限公司、武汉安天信息技术有限责任公司、北京指掌易科技有限公司。

本文件主要起草人：张滨、邱勤、何延哲、廖建新、袁捷、张峰、徐思嘉、杜雪涛、刘胜兰、赵蓓、张晨、金涛、胡影、任彦、江为强、于乐、周莹、刘畅、李文琦、白雪、姜伟、薛晨、周晨炜、郝春亮、邵冰、刘昊鑫、窦禹、王文磊、衣强、李实、路晓明、朱雪峰、付艳艳、杨明慧、汪定、李瑞卿、杜文博、郭建领、邓婷、王海荣、杨骁涵、赵乃萱、戴卓恒、黄厚瑞、张欢、王普、王昕、落红卫、李超然、祖岩岩、刘瑾、赵盈洁、贾科、张艳、申永波、鲁青、樊华、张磊、吴月升、徐天妮、易立、刘健、董晶晶、彭晋、林冠辰、白晓媛、赵华、王连强、杨玉忠、俞政臣、于海洋、刘献伦、彭婧、余丽娜、柳扬、刘冬、王光涛、彭根、蔡旭、赵峰、马丹、王雅莉、王璞、桂艳峰、王福海、张志远。

网络安全技术 应用商店的移动互联网 应用程序(App) 个人信息处理规范性 审核与管理指南

1 范围

本文件给出了应用商店运营者对移动互联网应用程序(App) 个人信息处理规范性审核与管理指南。

本文件适用于指导应用商店运营者开展 App 个人信息安全审核与管理，也为监管部门及第三方机构对应用商店运营者审核与管理 App 个人信息处理活动的的能力开展评估提供参考。

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 19011—2021 管理体系审核指南

GB/T 25069—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 41391—2022 信息安全技术 移动互联网应用程序(App) 收集个人信息基本要求

3 术语和定义

GB/T 19011—2021、GB/T 25069—2022、GB/T 35273—2020 和 GB/T 41391—2022 界定的以及下列术语和定义适用于本文件。

3.1

移动互联网应用程序 mobile internet application; App

运行在移动智能终端上向用户提供信息服务的应用程序。

注：包括移动智能终端预置、下载安装的应用程序和小程序。

[来源：GB/T 41391—2022, 3.1, 有修改]

3.2

移动互联网应用程序运营者 mobile internet application operator

移动互联网应用程序的所有者、管理者或提供者。

注：简称 App 运营者。

[来源：GB/T 41391—2022, 3.2]

3.3

应用商店 App store

提供移动互联网应用程序下载、安装、升级等分发服务的各类平台。

注：包括应用市场、分发网站、具有分发能力的移动互联网应用程序等。

3.4

应用商店运营者 App store operator
应用商店的所有者、管理者或提供者。

3.5

审核 audit
为获得客观证据并对其进行客观的评价，以确定满足准则的程度所进行的系统的、独立的并形成文件的过程。
[来源：GB/T19011—2021, 3.1, 有修改]

3.6

个人信息处理活动 personal information processing activity
个人信息的收集、存储、使用、加工、传输、提供、公开、删除等行为。

3.7

服务类型 service type
移动互联网应用程序提供的业务功能分类。
[来源：GB/T 41391—2022, 3.5, 有修改]

3.8

系统敏感权限 system sensitive permission
移动智能终端操作系统向移动互联网应用程序开放的，具有收集个人信息功能的系统权限。
注：简称系统权限或权限。
[来源：GB/T 41391—2022, 3.10, 有修改]

3.9

必要个人信息 necessary personal information
保障移动互联网应用程序基本业务功能正常运行所必需的个人信息，缺少该信息移动互联网应用程序即无法实现基本业务功能。
[来源：GB/T 41391—2022, 3.8]

4 缩略语

下列缩略语适用于本文件。
APK: 安卓系统软件安装包(Android Package)
IMEI: 国际移动设备识别码(International Mobile Equipment Identity)
IMSI: 国际移动用户识别码(International Mobile Subscriber Identity)
SDK: 软件开发工具包(Software Development Kit)

5 应用商店中 App 的审核与管理流程

应用商店运营者审核与管理 App 个人信息处理活动主要包括 App 进入应用商店前的个人信息处理活动审核和App 进入应用商店后的个人信息安全管理。
在 App 进入应用商店前，应用商店运营者对申请上架的App(含新申请上架的 App、版本更新需重新上架的 App) 以及存量App 的个人信息处理活动进行审核，并在App 通过审核后上架；在App 进入应用商店后，应用商店运营者对上架 App 进行安全管理，并在App 存在用户投诉举报及有关主管、监管部门通报的违法违规处理个人信息问题时督促其进行整改。

6 应用商店中App个人信息处理活动审核

6.1 App 个人信息处理活动审核规则公示

应用商店运营者制定简明、清晰、易于理解的 App 个人信息处理活动审核规则并公开发布，保证 App 运营者和社会公众可便捷获取。

6.2 App 上架申请信息受理

应用商店运营者在受理 App 进入应用商店的申请时，对 App 运营者所提交的 App 相关信息进行审核。对于未完整提交以下信息的，应用商店运营者应拒绝 App 上架。

- a) App 运营者信息，包括 App 运营者主体名称、App 运营者联系方式(联系邮箱选填，其他必填)(可参考附录A 的 A.1)。
- b)App 基本信息，包括名称、包名、版本号、更新日期、服务类型、安装文件(如 APK 文件)(可参考 A.1, 服务类型宜参照GB/T41391—2022 的附录 A并根据实际情况选择)。

注1:当App 服务类型不属于GB/T41391—2022 的附录A 给出的常见服务类型时，将实现用户主要使用目的的业务功能划分为App 的基本业务功能，将App 的基本业务功能所对应的服务类型确定为App 的服务类型。

- c) 个人信息保护政策(即隐私政策), 包括生效日期、全文文本、可查看全文的有效链接，面向不满14周岁的未成年人提供服务的还宜提交单独的未成年人个人信息保护政策(可参考A.1)。

注2:应用商店运营者可要求 App 运营者勾选是否对不满14周岁的未成年人提供服务，若勾选是，则 App 运营者提供相应的未成年人个人信息保护政策，并由应用商店运营者依据其提供的信息进行审核；若勾选否，则 App 运营者无需提供未成年人个人信息保护政策。

- d) 收集的个人信息范围，包括提供的服务类型、收集的个人信息类型(个人信息类型表述可参考 A.2)以及通过收集的个人信息所实现的业务功能/使用目的(可参考 A.3)。
- e) 申请的系统敏感权限列表，包括申请的系统敏感权限名称、相关业务功能/使用目的、用户可否拒绝授权(如不可拒绝则说明用户拒绝授权的影响)、是否仅本地化使用(可参考A.4)。
- f) 涉及收集个人信息的第三方 SDK 信息：包括名称、包名、SDK 运营者名称、嵌入目的、SDK 收集的个人信息类型、SDK 使用的系统敏感权限(可参考 A.5)。

6.3 App 个人信息处理活动审核验证

6.3.1 概述

应用商店运营者对 App 运营者提交的App 运营者信息、App 基本信息以及个人信息处理规则(如个人信息保护政策等)等上架申请信息进行审核，对App 运营者提供的 App 运营者信息进行核验，确保主体身份信息真实有效、联系方式畅通，并对App 个人信息处理活动进行验证。对于经审核发现提交信息不完整，或经验证发现个人信息处理活动存在问题的，应拒绝 App 上架请求。同时，应用商店运营者宜建立自动化处理能力，以提高审核和验证效率。

应用商店运营者因客观条件所限(如自动化审核技术不成熟等)无法在限定时间内完成部分内容审核的，可要求 App 运营者提供证明材料并存档，同时结合用户投诉举报情况对存档证明材料进行审核，处置措施参照7.4c)。

6.3.2 App 基本信息及个人信息处理规则审核

针对 App 运营者提交的上架申请信息，应用商店运营者进行审核后App 存在以下情形之一的，视为 App 未通过审核：

- a) App 基本信息中声明的服务类型与 App 实际提供的服务不相符;
- b) App 隐私政策链接无效、隐私政策未标注生效日期(如仅注明日期的视为生效日期);
- c) App 运营者身份信息不真实、联系方式虚假无效;
- d) 未明示收集的个人信息类型,未说明收集的必要性、通过收集的个人信息实现的相关服务或使用目的;
- e) 未明示申请权限所实现的业务功能/使用目的、用户可否拒绝授权(如不可拒绝需说明用户拒绝授权的影响);
- f) 未明示申请系统敏感权限时需同步告知的内容,未提交系统敏感权限申请时的屏幕截图;
- g) 未明示嵌入的涉及收集个人信息的第三方 SDK 名称、嵌入目的、收集的个人信息类型、使用的系统敏感权限。

6.3.3 App个人信息处理活动验证

针对 App 运营者的个人信息处理活动,应用商店运营者结合自身技术手段及 App 运营者提供的证明材料进行验证,验证发现 App 存在以下情形之一的,视为App 未通过审核:

- a) 未在 App 首次运行时通过弹窗等明显方式提示用户阅读隐私政策;
- b) 隐私政策存在默认勾选同意的情形;
- c) 处理敏感个人信息未征得用户的单独同意,如获取生物识别(人脸、指纹等)、医疗健康、金融账户、行踪轨迹等信息;
- d) 收集的个人信息超出实现业务功能/使用目的最小必要的范围,并且存在强制收集非必要个人信息的情形;
- e) 收集未在个人信息保护政策中告知的个人信息或打开未告知的可收集个人信息的权限;
- f) 强制要求用户一次性打开多个非必要权限;
- g) 在用户使用功能过程中,申请或者调用实现当前功能所必须权限范围之外的其他权限;
- h) 因用户不同意打开非必要权限或收集非必要个人信息而拒绝提供基本业务功能;
- i) 存在用户拒绝授权或拒绝收集非必要个人信息后,频繁征求用户同意干扰用户正常使用情况;
注:“频繁”的形式包括但不限于:单个场景在用户拒绝授权且选择不再提示后,仍然弹窗向用户索要授权;每当用户重新打开 App或使用无关的业务功能时,都会再次向用户索要授权或提示用户缺少相关授权。
- j) 在申请系统敏感权限时,未同步告知用户其目的,或者告知的目的与实际情况不符;
- k) 收集了隐私政策中声称的功能相关的个人信息,但不存在该功能;
- l) 未向用户提供有效的查询、更正、删除以及撤回同意收集个人信息的途径;
- m) 具有定向推送信息和个性化展示功能的,未向用户提供关闭的选项;
- n) 具有注册账号功能的,未提供有效的用户账号注销功能,或者为注销用户账号设置不必要或者不合理条件;
- o) 向第三方传输包含个人信息的数据,但未在隐私政策中说明相关情形;
- p) 首次打开App 时,未告知用户且未获得用户明示同意(如用户未点击同意隐私政策等收集个人信息规则)的情况下,就收集应用程序列表、用户唯一设备识别码等个人信息;
- q) 静默状态(包括后台运行)或自启动、被关联启动后,未告知用户且未获得用户明示同意的情况下,读取用户公共存储空间数据(如相册、文件、录音等),或读取用户个人信息(如短信、联系人、通话记录、日历数据、传感器数据、位置信息、设备信息等)。

6.4 审核结果反馈与申诉处理

应用商店运营者应记录App 审核结果,重点记录未通过审核的情况,审核记录在审核发生之后保

留至少6个月。

应用商店运营者应向App运营者说明未通过审核或拒绝上架的理由，并为App运营者提供意见反馈渠道，及时受理App运营者对审核结果的异议申诉，在5个工作日内完成对审核结果反馈、申诉的处理。

6.5 存量 App 与版本更新审核

对于已经进入应用商店的App，应用商店运营者在审核验证中若发现存在不满足要求的，对其进行通知限时整改，符合禁入情形且未按时完成整改的，将其从应用商店中下架。

应用商店中的App发生版本更新时，应用商店运营者应按照进入应用商店的程序对App更新版本进行审核，在App通过审核后下架App旧版本并上架App更新版本。

7 应用商店中App个人信息安全管理

7.1 个人信息处理情况的展示

应用商店运营者应在应用商店的App下载页面清晰、明确地展示和介绍以下App个人信息处理情况。

- a) App 基本信息：App 名称、App 版本号、涉及的服务类型。
- b)App 运营者信息：App 运营者主体名称、App 运营者联系方式(如联系邮箱等)。
- c) 隐私政策：隐私政策链接、个人信息处理活动规则。其中，个人信息处理活动规则的内容包括：
 - 1) 收集个人信息情况，包括个人信息类型(区分必要和可选个人信息)、相关业务功能/使用目的；
注1:展示方式参考附录 B的 B. 1。
 - 2) 系统权限申请情况，包括申请的系统权限名称(注明是否可拒绝)、相关业务功能/使用目的；
注2:展示方式参考 B. 2。
 - 3) 涉及收集个人信息的第三方 SDK 情况，包括 SDK 名称、相关业务功能/使用目的、收集的个人信息类型和使用的系统权限。
注3:展示方式参考 B. 3。

注4:打开隐私政策链接后显示隐私政策文本，且支持用户下载或可复制的隐私政策文本电子文档。

- d) 快速举报通道：包括个人信息问题投诉、举报渠道。
注5:举报通道的设计宜简便易操作，并将常见的个人信息处理问题设为选择项。

应用商店宜在App下载页面采用菜单折叠、表格、链接等方式显著展示a)~d) 中内容，方便用户下载App时查阅参考。

7.2 个人信息安全相关标识

应用商店运营者宜通过设置不同颜色、形状图标等方式对App进行显著标识，帮助用户快速了解App个人信息处理活动情况，宜提供包括但不限于以下标识。

- a) 认证标识：对通过个人信息保护、网络安全相关认证的App予以专属标识。
- b) 分类标识：对具有不同功能属性的App进行分类标识(如政务民生、医疗健康、生活娱乐等)。
注1:在适宜时按照用户搜索意图对带有“政务民生”标识的App予以优先展示。
- c) 负面信息标识：
 - 1) 对1年内被个人信息保护相关主管、监管部门公开通报存在个人信息处理问题的App进行特殊标识；

2) 对1年内曾因违法违规处理个人信息导致下架的App 进行特殊标识。

注2:上述标识信息包含次数、问题类型等要素,涉及的具体问题还能以点击链接等方式予以展示。

注3:将同一App运营者提供的不同App的负面信息进行汇总,形成标识在 App运营者的信息查询界面予以展示。

d) 年龄标识:提供App 运营者可自行选择年龄分级标识的功能。对于主要针对不满14周岁的未成年人提供服务的 App,予以未成年人专属标识。

7.3 App 运营者管理

应用商店运营者应指导督促 App 运营者提升个人信息保护的意识和能力,制定并公开发布 App 运营者管理制度,包括但不限于:

- a) 在与 App 运营者签署的相关协议中,明确 App 运营者遵循合法、正当、必要、诚信原则开展个人信息处理活动,履行个人信息安全的义务;
- b) 制定 App 运营者禁入/退出管理制度(即黑名单制度),对于App 运营者发布的 App 多次未通过审核的,可在一段时间内禁止其提交 App 上架申请;
- c) 对不同 App 运营者在审核标准、展示样式等个人信息保护方面的要求遵循一致性原则,不根据 App 运营者身份、影响力、市场地位等因素,在其申请系统权限等方面提供默认开启等便利条件;
- d) 宜对 App 运营者的相关开发人员进行个人信息保护相关的培训和考核,以增进其对审核标准和相关要求的理解。

7.4 日常监督与问题处置

应用商店运营者对App 个人信息处理活动进行日常监管,及时处理用户投诉举报和主管、监管部门通报的个人信息处理问题,包括但不限于:

- a) 根据下载量、举报记录、更新时间、历史违规记录等要素确定抽样审核的优先级,定期选取一定比例的 App 进行日常抽查,抽查过程宜参照第6章执行;
- b) 设立便捷的渠道接收用户关于 App 个人信息处理问题的投诉举报,并对用户投诉举报的本平台 App 违法违规个人信息处理活动的问题,在合理期间内向用户进行响应,使用户确认其举报已被接收受理;
注:投诉举报渠道示例参考附录C。
- c) 经核验用户反映问题属实的,按情况严重程度对 App 进行限时在架整改或立即下架处置,情况严重且拒不整改或者未在规定时间内按照要求整改的,予以下架处置;
- d) 按照主管、监管部门的监管要求,对典型举报问题、App 审核情况、问题 App 处置情况进行汇总分析并形成报告上报主管、监管部门;
- e) 定期将下架 App 的名单和问题上报主管、监管部门;
- f) 对主管、监管部门通报的存在违法违规个人信息处理问题的 App,配合采取督促整改、下架等措施;
- g) 对发现的违法违规线索,保存有关记录,及时报主管、监管部门。

附录 A
(资料性)

App 个人信息处理活动审核材料参考模板

A.1 App运营者及App 基本信息表

App 运营者及App 基本信息表见表 A.1。

表A.1 App 运营者及App 基本信息表

App运营者信息	
App名称	
App运营者主体名称	
App运营者联系电话	
App运营者联系邮箱	
App基本信息	
名称	
包名	
版本号	
更新日期	
服务类型	
安装文件	
隐私政策信息	
生效日期	
文档链接	
全文文本	(可设置上传按钮)

注：表中所有黑体突出显示的项目填写信息均不能为空，如涉及不存在该情形的情况，则通过设置“其他”“无”等选项或自定义方式进行填写。

A.2 App 收集的个人信息类型

App 收集的个人信息类型见表 A.2。

表A.2 App 收集的个人信息类型

类型	详细类别
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、港澳台通行证等证件号码、证件有效期、证件照片或影印件等
	个人姓名、生日、性别、民族、国籍、籍贯、婚姻状况、家庭关系、工作关系、社交关系等
生物识别信息	个人基因、指纹、声纹、掌纹、眼纹、耳廓、虹膜、笔迹、步态、面部识别特征等
账号信息	个人信息主体账号、IP地址、个人数字证书等
健康信息	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、吸烟史等，以及与个人身体健康状况相关的信息，如体重、身高、体温、肺活量、血压、血型等
履历信息	学历、学位、教育经历(如入学日期、毕业日期、学校、院系、专业等)、成绩单、资质证书、培训记录、奖惩信息、受资助信息等
	个人职业、职位、职称、工作单位、工作地点、工作经历、工资、工作表现、简历、培训记录等
财务信息	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、虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息等
通信信息	通信记录，短信、彩信、语音、电子邮件、即时通信等通信内容(如文字、图片、音频、视频、文件等), 以及描述个人通信的元数据(如通话时长)等
	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
联络信息	通讯录、好友列表、群列表、电子邮件地址列表等
	住址、个人电话号码、电子邮件地址等
上网记录	个人在业务服务过程中的操作记录和行为数据，包括网站浏览记录、软件使用记录、点击记录 Cookie、发布的社交信息、点击记录、收藏列表、搜索记录、服务使用时间、下载记录、访问时间(含登录时间、退出时间)等； 用户使用某业务的行为记录，如游戏业务：用户游戏登录时间、最近充值时间、累计充值额度、用户通关记录等
设备识别码	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/CPU ID/Boot ID/OAID/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
位置行踪	包括行踪轨迹、精准定位信息、住宿信息、经纬度等、基站信息、WiFi信息
综合信息	用户相册、应用列表、剪切板、第三方账号、日历行程信息、通知栏信息、运行中的进程
其他信息	婚史、宗教信仰、兴趣爱好、性取向、未公开的违法犯罪记录等

注：上述个人信息类型参考GB/T35273—2020的附录A和附录B进行梳理和扩充。

A.3 App 收集个人信息详情表(提交审核版)

App 收集个人信息详情表(提交审核版)见表 A.3。

表A.3 App 收集个人信息详情表(提交审核版)

个人信息详细类别	相关业务功能/使用目的	收集个人信息的方式	处理个人信息的方式	使用个人信息的频率	是否敏感个人信息	是否为实现功能或目的所必需
如：精准定位信息	如：用于确定用户位置，提供地图搜索展示和导航服务	如：用户触发功能获取、启动应用默认获取、后台不定期获取、关联启动获取等	如：单次读取、本地存储、上传到www.***.com域名服务器等。其中上传通讯录、通话记录、短信、应用列表、剪切板的，需要列明上传的详细字段	如：读取频率小于10次，小于100次，大于100次等	<input type="checkbox"/> 是 <input type="checkbox"/> 否	<input type="checkbox"/> 是 <input type="checkbox"/> 否

注：表中所有黑体突出显示的项目填写信息均不能为空；App 运营者需将获取详细类别个人信息的相关业务功能/使用目的进行逐项列举，便于应用商店按照业务场景进行App 违规判定。

A.4 App 申请系统敏感权限详情表(提交审核版)

安卓系统敏感权限，通常是安卓操作系统预定义保护级别(Protection Level)为危险(dangerous)级别的权限。此类权限与用户隐私和设备安全密切相关，需要 App 在运行时动态向用户申请。安卓11及以下版本的 App 申请系统敏感权限详情表(提交审核版)见表 A.4。

表 A.4 安卓 App 申请系统敏感权限详情表(提交审核版)

序号	权限分组	权限名	相关业务功能/使用目的	用户可否拒绝授权	是否仅本地化使用	备注(如不可拒绝的理由等)
1	CALENDAR 日历	READ_CALENDAR 读取日历	如：日程规划、事件提醒、票务预订等	<input type="checkbox"/> 是 <input type="checkbox"/> 否	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
2		WRITE_CALENDAR 编辑日历				

表A.4 安卓 App 申请系统敏感权限详情表(提交审核版)(续)

序号	权限分组	权限名	相关业务功能/使用目的	用户可否拒绝授权	是否仅本地化使用	备注(如不可拒绝的理由等)
3	CALL_LOG 通话记录	READ_CALL_LOG 读取通话记录	如：通话记录管理、备份与恢复，骚扰拦截、SOS紧急求助等			
4		WRITE_CALL_LOG 编辑通话记录				
5		PROCESS_OUTGOING_CALLS 呼出电话呼叫控制				
6	CAMERA 相机	CAMERA拍摄	如：拍摄照片视频、扫描二维码/条形码、人脸识别等			
7	CONTACTS 通讯录	READ_CONTACTS 读取通讯录	如：通讯录管理与备份、添加联系人等			
8		WRITE_CONTACTS 编辑通讯录				
9		GET_ACCOUNTS 获取App账户	如：账号登录场景等			
10	LOCATION 位置	ACCESS_FINE_LOCATION 访问精准定位	如：定位当前用户位置、拍照记录照片拍摄位置、社交分享位置、线上到线下上门服务定位用户位置等需要用户精准位置的场景			
11		ACCESS_COARSE_LOCATION 访问粗略位置	如：外卖、本地生活服务等分区域信息推荐、基于城市或地域进行新闻推送等基于粗略用户地理位置的场景			
12		ACCESS_BACKGROUND_LOCATION 支持后台访问位置	如：地图导航、网约车、运动健身等场景			
13	MICROPHONE 麦克风	RECORD_AUDIO 录音	如：语音即时通信、语音识别、音视频录制、直播等语音输入场景			

表A.4 安卓 App 申请系统敏感权限详情表(提交审核版)(续)

序号	权限分组	权限名	相关业务功能/使用目的	用户可否 拒绝授权	是否仅本 地化使用	备注(如不 可拒绝的 理由等)
14	PHONE 电话	READ_PHONE_STATE 读取设备信息	如：进行用户常用设备的标识，用于监测App账户异常登录、关联用户行为			
15		READ_PHONE_NUMBERS 读取本机电话号码	如：读取本机号码场景			
16		CALL_PHONE 拨打电话	如：在App内直接拨打商家、快递员、客服电话等			
17		ANSWER_PHONE CALLS接听电话	如：在驾驶模式下直接接听来电等			
18		ADD_VOICEMAIL 添加语音邮件	—			
19		USE_SIP 使用网络电话	如：接听、拨打网络电话等			
20		ACCEPT_HANDOVER 允许切换通话				
21	SENSORS 传感器	BODY_SENSORS 获取身体传感器信息	如：健康类App及可穿戴设备显示心率等状况			
22	SMS 短信	SEND_SMS 发送短信	如：便捷短信查询与服务订阅、短信优化编辑与发送、SOS紧急求助等			
23		RECEIVE_SMS 接收短信	如：便捷短信查询与服务订阅、短信优化编辑与发送、短信功能体验增强、骚扰拦截与上报垃圾短信、短信智能服务、SOS紧急求助等			
24		READ_SMS 读取文字讯息(短信或彩信)	如：短信管理、验证码便捷获取、骚扰拦截与上报垃圾短信等			
25		RECEIVE_WAP_PUSH 接收WAP推送	如：短信管理、WAP消息推送场景等			
26		RECEIVE_MMS 接收彩信	如：验证码便捷获取、便捷短信查询与服务订阅、短信功能体验增强、骚扰拦截、短信管理等			

表A.4 安卓 App 申请系统敏感权限详情表(提交审核版)(续)

序号	权限分组	权限名	相关业务功能/使用目的	用户可否拒绝授权	是否仅本地化使用	备注(如不可拒绝的理由等)
27	STORAGE 存储	READ_EXTERNAL_STORAGE 读取外置存储区	如：文件管理、阅读器等打开本地文件的场景等			
28		WRITE_EXTERNAL_STORAGE 写入外置存储区	如：存储拍摄的照片和视频，及下载文件、需要下载大量资源的游戏场景等			
29		ACCESS_MEDIA_LOCATION 读取照片位置信息	如：展示照片拍摄地点的场景等			
30	ACTIVITY_RECOGNITION 身体活动	ACTIVITY_RECOGNITION 识别身体活动	如：需要对用户的身体活动进行识别和分类的场景等			

注：表中所有黑体突出显示的项目填写信息均不能为空；App 运营者需将安卓 App 申请系统敏感权限的相关业务功能/使用目的进行逐项列举，便于应用商店按照业务场景进行 App 违规判定；应用商店运营者可根据对安装文件的检测结果，向 App 运营者列出仅涉及其所声明系统权限的系统权限申请使用情况表，供 App 运营者进一步填写。

iOS14 及以下版本的App 申请系统敏感权限详情表(提交审核版)见表 A.5,iOS 权限的使用场景宜参考表 A.4 的“相关业务功能/使用目的”。

表 A.5 iOS App申请系统敏感权限详情表(提交审核版)

序号	受保护的资源	权限名	相关业务功能/使用目的	用户可否拒绝授权	是否仅本地化使用	备注(如不可拒绝的理由等)
1	Calendar and Reminders日历与提醒事项	Calendars日历		<input type="checkbox"/> 是 <input type="checkbox"/> 否	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
2		Reminders提醒事项				
3	Camera and Microphone相机与麦克风	Camera相机				
4		Microphone麦克风				
5	Contacts通讯录	Contacts通讯录				

表 A.5 iOS App 申请系统敏感权限详情表(提交审核版) (续)

序号	受保护的资源	权限名	相关业务功能/使用目的	用户可否拒绝授权	是否仅本地化使用	备注(如不可拒绝的理由等)
6	Health 健康	Health Records健康记录				
7		Health Share读取 HealthKit健康数据				
8		Health Update更新 HealthKit健康数据				
9	Location 定位服务	Location Always and When In Use 始终访问位置				
10		Location访问位置				
11		Location When In Use 使用期间访问位置				
12		Location Temporary 临时访问位置				
13	MediaPlayer 媒体与 Apple Music	Media Library媒体库				
14	Motion 运动与健身	Motion运动与健身				
15	Photos 照片	Photo Library Additions 只写照片库				
16		Photo Library读取和写入照片库				

注：表中所有黑体突出显示的项目填写信息均不能为空；App运营者需将iOS App申请系统敏感权限的相关业务功能/使用目的进行逐项列举，便于应用商店按照业务场景进行App违规判定；应用商店运营者可根据对安装文件的检测结果，向App运营者列出仅涉及其所声明系统权限的系统权限申请使用情况表，供App运营者进一步填写。

A.5 App 内嵌第三方SDK 详情表(提交审核版)

App 内嵌第三方 SDK 详情表(提交审核版)见表 A.6。

表 A.6 App 内嵌第三方SDK 详情表(提交审核版)

序号	SDK名称	SDK包名	SDK运营者 主体名称	相关业务功能/ 使用目的	收集的个人信息 信息类型	处理个人 信息的方式	使用的系统 敏感权限
	×××				正在运行的应用列表、粗略地理位置信息、已安装应用列表、本机IMEI号、手机SIM卡序列号、本机IM-SI号等	单次读取、本地存储、上传到www.***.com域名服务器等。其中上传通讯录、通话记录、短信、应用列表、剪切板等，需要列明上传的详细字段	READ PHONE STATE读取电话状态、ACCESS COARSE LOCATION 访问粗略位置
2							

注：表中所有黑体突出显示的项目填写信息均不能为空。

附录 B
(资料性)
App 下载页面展示内容示例

B.1 App 收集个人信息详情表(下载页面展示版)

App 收集个人信息详情表(下载页面展示版)见表 B. 1, App 收集个人信息类型透明化展示示意图见图 B.1。

表 B.1 App 收集个人信息详情表(下载页面展示版)

个人信息类型	是否敏感个人信息	相关业务功能/使用目的	是否为实现功能或目的所必需
	<input type="checkbox"/> 是 <input type="checkbox"/> 否		<input type="checkbox"/> 是 <input type="checkbox"/> 否

注：表中所有黑体突出显示的项目填写信息均不能为空。



图 B.1 App 收集个人信息类型透明化展示示意图

B.2 App 申请系统敏感权限详情表(下载页面展示版)

安卓 App 申请系统敏感权限详情表(下载页面展示版)见表 B.2,iOS App申请系统敏感权限详情表(下载页面展示版)见表B.3,App 申请开启系统权限透明化展示示意图见图 B.2。

表 B.2 安卓 App 申请系统敏感权限详情表(下载页面展示)

序号	权限分组	权限名	相关业务功能/使用目的	用户可否拒绝授权	是否仅本地化使用
		×××		<input type="checkbox"/> 是 <input type="checkbox"/> 否	<input type="checkbox"/> 是 <input type="checkbox"/> 否
2	×××	×××			
3			

注：表中所有黑体突出显示的项目填写信息均不能为空。

表 B.3 iOS App 申请系统敏感权限详情表(下载页面展示版)

序号	受保护的资源	权限名	相关业务功能/使用目的	用户可否拒绝授权	是否仅本地化使用
		××××		<input type="checkbox"/> 是 <input type="checkbox"/> 否	<input type="checkbox"/> 是 <input type="checkbox"/> 否
2	×××	×××			
3	-	-			

注：表中所有黑体突出显示的项目填写信息均不能为空。



图 B.2 App 申请开启系统权限透明化展示示意图

B.3 App 内嵌第三方SDK 详情表(下载页面展示版)

App 内嵌第三方 SDK 详情表(下载页面展示版)见表 B.4,App 内嵌第三方 SDK 情况透明化展示示意图见图 B.3。

表 B.4 App 内嵌第三方 SDK 详情表(下载页面展示)

序号	SDK名称	相关业务功能/ 使用目的	收集的个人信息类型	使用的系统权限
1	xxx		正在运行的应用列表、粗略地理位置信息、已安装应用列表、本机IMEI号、手机SIM卡序列号、本机IMSI号等	READ_PHONE_STATE读取电话状态、ACCESS_COARSE_LOCATION访问粗略位置
2				

注：表中所有黑体突出显示的项目填写信息均不能为空。

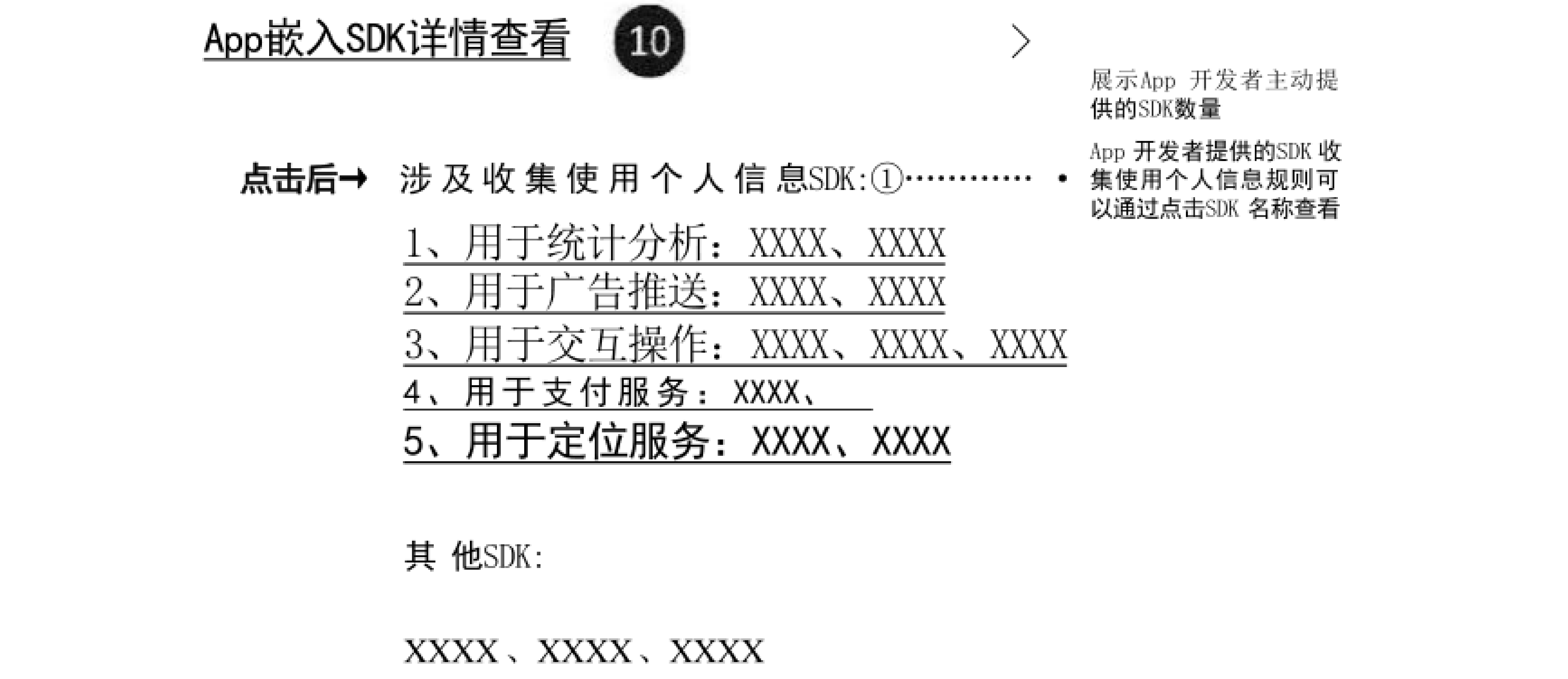


图 B.3 App 内嵌第三方 SDK 情况透明化展示示意图

附录 C
(资料性)
个人信息安全问题投诉举报渠道示例

个人信息安全问题投诉举报渠道示例见图C.1。

个人信息安全问题投诉举报入口

方条1: 点击云→

拨打电话/客服渠道 ①

应用商店运营者自行设置便捷的举报渠道, 包括电话、客服、在线表

方条2: 点击云→

填写举报信息

举报方式*

匿名举报

实名举报

姓名*

仅实名举报场景收集, 且严格保密不用于举报处签以外其他目的

请填写您的姓名

手机号*

请填写您的手机号码

APP 名称*

请填写APP 名称(20字以内)

问题描述*

请简要描述问题的基本情况, App的版本号, 来源的应用商店等, 必要时可提供相关截图。(1000字以内)

问题类别

超范围收集与功能无关个人信息

强制或频繁索要无关权限

默认捆绑功能并一揽子授权

骚扰我的通讯录好友

无隐私政策或隐私政策晦涩难懂

存在不合理免责条款

无法注销账号

无法删除或更正个人信息

无法退订基于个人喜好推送的新闻资讯

提供的申诉渠道无效

其他

上传图片

选传个文件

上传相关附件, 总大小10M内, 支持格式 [jpg/jpeg/png/gif]

仅实名举报场景收集, 且严格保密知信验证码本密不用于举报处置以外其他目的

获取短信验证码

提交

图 C.1 个人信息安全问题投诉举报渠道示例

18

参 考 文 献

[1] 中华人民共和国电信条例(2016年2月6日国务院发布)

[2] 网络安全审查办法(2022年1月4日国家互联网信息办公室等十三部门发布)

[3] 国家网络空间安全战略(2016年12月27日国家互联网信息办公室发布)

[4] 网络数据安全条例(征求意见稿)(2021年11月14日国家互联网信息办公室发布)

[5] App违法违规收集使用个人信息行为认定方法(2019年11月28日国家互联网信息办公室、工业和信息化部、公安部、市场监管总局发布)

[6] App违法违规收集使用个人信息自评估指南(2019年3月1日App专项治理工作组发布)

[7] 国务院关于大力推进信息化发展和切实保障信息安全的若干意见(国发〔2012〕23号)

[8] 关于加强国家网络安全标准化工作的若干意见(中网办发〔2016〕5号)

[9] 移动智能终端应用软件预置和分发管理暂行规定(工信部信管〔2016〕407号)

[10] 电信和互联网用户个人信息保护规定(工业和信息化部令第24号)

www.bzxz.net

免费标准下载网