TC260-PG-20203A

网络安全标准实践指南

—移动互联网应用程序（App）个人信息安全防范指引

（征求意见稿 v1.0-202003）

全国信息安全标准化技术委员会秘书处

2020 年 3 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）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。

声　明

技术支持单位

本《实践指南》得到中国电子技术标准化研究院、中国网络安全审查技术与认证中心、北京理工大学、公安部第一研究所、北京信息安全测评中心、中国移动通信集团有限公司等单位的技术支持。

摘　要

本实践指南依据法律法规和政策标准要求，基于相关评估工具数据统计和近期疫情防控App发现的问题，给出了当前App个人信息保护合规的常见问题和防范策略，建议App（含小程序）运营者和疫情防控App参考本实践指南，采取相应措施持续提升个人信息保护水平。

本实践指南给出的问题情形和防范策略仅反映常见情况，更详细的问题和策略可参见《App违法违规收集使用个人信息行为认定方法》（国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、国家市场监督管理总局办公厅）、GB/T 35273-2020《信息安全技术 个人信息安全规范》等文件。

目　录

问题 1：超范围收集

App[1]超范围收集个人信息的问题情形，包括但不限于:

情形一：收集无关信息。收集的个人信息类型或申请的系统权限[2]与 App 提供的业务功能无关。例如未提供短信相关功能的 App 申请短信权限。

情形二：强制收集非必要信息。因用户不同意收集非必要个人信息或打开非必要权限，App 拒绝提供业务功能。必要个人信息是指保障 App 业务功能正常运行所最少够用的个人信息，包括一旦缺少将导致 App 服务无法实现或无法正常运行的个人信息，以及法律法规要求必须收集的个人信息。例如浏览器 App 强制索要位置权限收集个人位置信息，用户拒绝提供位置权限则无法使用 App 任何功能。

情形三：收集频率不合理。收集个人信息的频率超出 App 业务功能实际需要。例如酒店预订 App 每 1 秒上传一次用户精确定位信息。

该问题的防范策略，包括但不限于:

1）不收集与 App 所提供服务无关的个人信息，不申请与 App 所提供服务无关的系统权限（即使用户可选择拒绝）。

2）遵循最小必要原则，仅收集/申请与 App 业务功能有直接关联的个人信息类型/系统权限。

3）App 收集个人信息前向用户明示收集信息的目的、方式和范

[1] 本实践指南中的 App，是指安装、运行在移动智能终端上的应用软件，包括在应用市场上架的软件、移动智能终端预装的软件、小程序等。
[2] 本实践指南的“系统权限”与“权限”，均指“可收集个人信息的权限”。

围，并征得用户同意，告知同意方式应符合相关法律法规、政策和标准的要求。

4）收集个人信息的频率应在 App 实现业务功能所必需的合理范围内。

5）App 尽量避免收集不可变更的设备唯一标识（如 IMEI 号、MAC 地址等），用于保障网络安全和运营安全的除外。

6）App 收集疫情联防联控所必需的个人信息坚持最小范围原则，收集对象原则上限于确诊者、疑似者、密切接触者等重点人群，一般不针对特定地区的所有人群。

7）针对一些没有高风险的区域、场所或不涉及高风险人群，疫情防控 App 宜尽可能缩小身份登记的个人信息填写范围，达到可追溯的目的即可。例如，收集个人信息可参考“前台匿名，后台实名”等方式，用户可提供手机号，无需填写身份证号或上传身份证图片。

问题 2：无法注销或设置不合理注销条件

App 无法注销或设置不合理条件的问题情形，包括但不限于：

情形一：无法注销或注销机制无效。例如：App 未提供注销功能；通过 App 界面、邮件、客服电话等渠道提交注销申请后未按相关要求或约定完成注销；注销成功后，未按相关要求或约定对其个人信息进行删除或匿名化处理等。

情形二：设置不合理注销条件。例如：注销过程进行身份核验时，要求用户提交超过 App 注册、使用时收集的个人信息类型，如提供手持身份证照片、绑定银行卡等；对于采用同一账号注册登录多个

App 的情形，用户注销单个 App 只能注销用户账号，导致用户无法使用其他相关 App; 要求用户填写精确的历史操作记录作为注销的必要条件等。

该问题的防范策略，包括但不限于:

1）提供简便易操作的注销功能，不设置不合理的注销条件。

2）及时响应用户注销请求，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）用户注销后停止对用户个人信息的收集和使用，并按照相关要求和约定删除其个人信息或匿名化处理。因法律法规规定需要留存个人信息的，不再将其用于日常业务活动中。

4）注销时因验证用户身份所收集的个人敏感信息，达成目的后立即删除或匿名化处理。

5）用户采用同一账号注册登录多个 App 时，可提供解除单个 App 用户账号使用关系的渠道。

6）明确疫情防控 App 收集个人信息的使用范围、保存时间和事后处置措施，确保为疫情防控、疾病防治收集的个人信息，不用于其他用途，并在疫情结束后能够及时删除或依法合理处置，涉及账号注册功能的，应提供注销功能。

问题 3：强制捆绑授权

App 强制捆绑授权的问题情形，包括但不限于:

情形一：必须同意开启 App 申请的所有权限，否则无法安装或使用。例如，用户安装 App 时，以捆绑打包形式申请其向操作系统

声明的所有权限，用户不同意则无法安装或使用，安装完成后申请的所有权限默认打开（如 Android 版 App 设置 targetSdkVersion 小于 23 所致）。

情形二：必须同意开启所有服务类型，否则无法使用。例如，当 App 提供多种服务类型的业务功能时，采用功能捆绑的方式强迫用户一次性接受多种或所有服务类型的业务功能收集个人信息/系统权限的请求，用户不同意则无法使用 App；又如，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个人信息/系统权限。

情形三：频繁索权。对于用户可选提供的系统权限，在用户拒绝后，每当其重新打开 App 或进入相应界面，都会再次向用户索要或以弹窗等形式提示用户缺少相关权限，干扰用户正常使用。

该问题的防范策略，包括但不限于：

1）Android 版 App 设置 targetSdkVersion 值应不小于 23，建议设置 targetSdkVersion 值不小于 26。

2）尽量避免强制索取权限等强制收集行为，尤其不以改善服务质量、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个人信息。

3）当用户同意 App 收集某服务类型的最小必要信息时，不因用户拒绝提供最小必要信息之外的个人信息而拒绝提供该类型服务。

4）用户不授权同意使用、关闭或退出特定业务功能的，不影响用户自主选择使用的其他业务功能的正常使用。

5）适当区分 App 基本功能与附加功能。对于仅为实现附加功能、个性化服务、提升用户体验，同时又并非 App 实现基本功能所必要的个人信息，可单独征得用户同意，并保障用户可拒绝的权利。用户拒绝此类信息后不影响其正常使用 App 基本功能。

6）合理设置系统权限的申请时机和频率，当用户拒绝权限申请后，除非该系统权限是用户主动触发的功能所必要，否则不应频繁申请或提示缺少相关权限，干扰用户正常使用。

问题 4：无隐私政策

App 无隐私政策的问题情形，包括但不限于：

情形一：未制定个人信息收集使用规则。例如通过 App、网站、小程序等收集使用个人信息，但未制定隐私政策，或隐私政策未包含收集使用个人信息规则。

情形二：未在 App 中公开隐私政策。例如在 App 界面中无法找到隐私政策，或者隐私政策链接无效、文本不能正常显示等。

该问题的防范策略，包括但不限于：

1）参考 GB/T 35273-2020《信息安全技术 个人信息安全规范》等标准，制定单独隐私政策，公开所收集个人信息的类型、收集目的、使用规则等，确保隐私政策链接正常有效。

2）疫情防控 App 宜以“简版隐私政策”、“个人信息保护声明”等方式，在注册、登录、填写个人信息等页面，以显著方式公开收集使用个人信息的关键规则，如收集个人信息的目的、类型，保存时间、安全措施及投诉渠道等。

问题 5：默认选择同意

App 默认选择同意的问题情形，包括但不限于:

情形一：默认勾选同意。例如，App 在注册/登录界面下方“我已阅读并同意服务许可协议及隐私政策”前的勾选框中提前替用户打钩；注册/登录界面下方只给出隐私政策链接，并未说明注册/登录后是否视为同意隐私政策。

情形二：诱导用户略过隐私政策。例如，以缩小字号、减淡颜色、遮挡等方式诱导用户略过隐私政策链接，或未能在用户首次使用或用户注册时主动提示用户阅读隐私政策。

该问题的防范策略，包括但不限于:

1）为用户提供主动选择同意、或显著提醒用户阅读后同意隐私政策的选项，对于通过勾选框形式征得同意的，不默认勾选同意。

2）征得用户同意前，不产生收集个人信息行为或私自打开系统权限。

3）在首次运行 App 或用户注册时，主动提示用户阅读隐私政策，宜通过弹窗等形式主动展示隐私政策的主要或核心内容，帮助用户理解收集个人信息的范围和规则进而做出决定。

问题 6：未充分明示个人敏感信息使用规则

App 未充分明示个人敏感信息收集使用规则的问题情形，包括但不限于:

收集身份证件号码、银行账户、个人生物识别信息等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解。例如

App 收集面部识别特征前未展示单独协议或进行显著特殊说明，在用户点击“继续”后，App 在无任何提示的情况下便开始采集用户的面部识别特征。

该问题的防范策略，包括但不限于：

1）收集个人生物识别信息前，应单独向用户告知收集、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，并征得用户的明示同意。

2）收集身份证号、银行账号、行踪轨迹等个人敏感信息时，同步告知用户其目的，目的应明确且易于理解。

3）疫情防控 App 收集详细地址、行程证明（如机票、船票、火车票）、个人健康生理信息（如体温信息）等个人敏感信息时，宜同步告知用户使用目的。

问题 7：申请权限目的不明

App 申请权限目的不明的问题情形，包括但不限于：

情形一：未告知申请目的。App 申请系统权限时未同步告知权限的申请目的，例如仅通过操作系统弹窗向用户申请系统权限，且未告知权限申请目的。

情形二：目的告知不明确。例如将目的描述为“需要您开启存储权限，以保证存储相关功能的正常使用”，未具体明确地说明权限的使用目的。

该问题的防范策略，包括但不限于：

Android 版 App 建议通过 App 弹窗提示等方式，向用户告知系统

权限的申请目的，目的应明确且易于理解；iOS 版 App 可在系统提供的权限申请弹窗中编辑具体明确的申请目的。

问题 8：未提供删除、更正或投诉举报的功能或渠道

App 未提供删除、更正或投诉举报的功能或渠道的问题情形，包括但不限于：

情形一：未按规定提供删除个人信息功能。例如，App 未提供有效的个人信息删除功能；为删除个人信息设置不合理条件；未按相关要求或约定时限响应用户删除个人信息请求等。

情形二：未按规定提供更正个人信息功能。例如，App 未提供有效的个人信息更正功能；为更正个人信息设置不合理条件；未按相关要求或约定时限响应用户更正个人信息请求；用户已完成更正个人信息操作，但 App 后台并未完成的等。

情形三：未提供个人信息安全投诉举报渠道。例如，未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（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）受理并处理的。

该问题的防范策略，包括但不限于：

1）提供有效的更正、删除个人信息的途径。

2）用户无法通过在线操作方式及时响应个人信息更正、删除请求的，App 运营者在承诺时限内（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。

3）更正和删除个人信息的过程应简单易操作，不设置不必要或

不合理的条件。

4）用户更正、删除个人信息等操作完成时，App 后台需同步执行完成相关操作，法律法规另有规定的除外。

5）建立并公布可受理个人信息安全问题相关的投诉、举报渠道，受理可采取在线操作、客服电话、电子邮件等方式。

6）妥善受理用户关于个人信息相关的投诉、举报，并在承诺时限内（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）受理并处理。

7）通过个人信息的大数据分析等自动化决策机制来判断用户个人健康状态的疫情防控 App，应提供反馈渠道及时处理因自动化决策机制而严重影响用户个人权益的问题。

问题 9：隐私政策内容与实际不符

App 隐私政策内容与实际不符的问题情形，包括但不限于:

情形一：实际收集个人信息超出隐私政策所述范围。即未完整告知所收集个人信息类型以及用于实现的功能或目的。

情形二：实际收集个人信息少于隐私政策所述范围。即声明了实际并未收集的个人信息或实际并未提供的功能。

情形三：隐私政策所述与实际情况存在明显偏差、错误。甚至出现大篇幅抄袭导致隐私政策内容不实等。

该问题的防范策略，包括但不限于:

1）隐私政策中所述内容应与 App 实际业务相符，并逐一说明各业务功能收集个人信息的目的、类型、方式，不使用“等、例如”等

方式不完整列举。

2）实际收集使用个人信息/系统权限的目的、方式、范围等，不超出隐私政策等个人信息收集使用规则的用户授权范围。

3）严格遵守收集使用规则，App 收集或使用个人信息的功能设计同隐私政策保持一致、同步调整。

4）收集使用个人信息的目的、方式、范围发生变化时，应更新隐私政策等收集使用规则并提醒用户阅读。

问题 10：未告知同意第三方 SDK 收集行为

未告知同意第三方 SDK 收集行为的问题情形，包括但不限于:

情形一：未明示第三方 SDK 收集行为。App 嵌入了收集用户个人信息的第三方 SDK，但未通过隐私政策或其他显著方式（如第三方 SDK 隐私政策链接）向用户明示第三方 SDK 的个人信息收集行为。

情形二：未经同意通过第三方 SDK 向第三方提供个人信息。未经用户同意，也未作匿名化处理，App 通过嵌入的第三方 SDK 向第三方提供个人信息。

该问题的防范策略，包括但不限于:

1）对嵌入的收集用户个人信息的第三方 SDK 进行披露，告知第三方 SDK 类型，及收集使用的个人信息的目的、方式和范围，如存在第三方 SDK 将个人信息传输至境外的，也需说明跨境传输个人信息的目的、类型和接收方等。

2）如 App 以嵌入第三方代码和插件（如 SDK）等方式向第三方提供个人信息，应在发送前征得用户同意的，或对个人信息进行匿名

化处理。

3）宜采取技术检测、安全审计等手段，确保第三方 SDK 收集、使用行为符合约定要求。

参考文献

[1] 国家标准《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》（征求意见稿）. 2020-01-20

[2] 中国电子技术标准化研究院. App 个人信息保护合规十大常见问题及处置策略. 2019-10-25

[3] App 专项治理工作组. App 申请权限时告知目的，是多此一举吗？. 2019-6-25

[4] App 专项治理工作组. 从天津专项治理通报看疫情联防联控应用程序个人信息保护要点. 2020-3-18