TC260-PG-20202A

网络安全标准实践指南

—移动互联网应用程序（App）收集使用个人信息自评估指南

全国信息安全标准化技术委员会秘书处

2020 年 7 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

本《实践指南》版权属于信安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国信息安全标准化技术委员会秘书处”。

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、中国信息通信研究院、公安部第一研究所、中国网络空间安全协会、中国电子科技集团公司第三十研究所、国家计算机病毒应急处理中心等单位的技术支持。

摘　要

2016 年《网络安全法》颁布，明确我国网络安全保护的基本要求和制度，并将个人信息保护问题作为网络安全的重要内容予以规定。

本《实践指南》依据《网络安全法》等法律法规要求，参照《App违法违规收集使用个人信息行为认定方法》和相关国家标准，结合检测评估工作经验，归纳总结出App收集使用个人信息的六个评估点：是否公开收集使用个人信息的规则；是否明示收集使用个人信息的目的、方式和范围；是否征得用户同意后才收集使用个人信息；是否遵循必要原则，仅收集与其提供的服务相关的个人信息；是否经用户同意后才向他人提供个人信息；是否提供删除或更正个人信息功能，或公布投诉、举报方式等信息，供App运营者自评估参考使用。小程序、快应用等运营者也可参考其中的适用条款进行自评估。

目 录

评估点一：是否公开收集使用个人信息的规则

1.1 是否公开隐私政策等收集使用规则

a) 隐私政策通过弹窗、文本链接、附件、常见问题（FAQs）等界面或形式展示。

b) 隐私政策中包含收集使用个人信息规则的相关内容。

c) 隐私政策文本链接有效，文本可正常显示。

d) 如存在涉及收集使用儿童个人信息相关业务功能的，需制定针对儿童的个人信息保护规则。

注 1: 详见 2019 年国家互联网信息办公室令（第 4 号）《儿童个人信息网络保护规定》。

注 2: 例如收集不满十四周岁的未成年人个人信息的教育类App，需制定针对儿童的个人信息保护规则。

1.2 是否提示用户阅读隐私政策等收集使用规则

a) 在App首次运行或用户注册时主动提示用户阅读隐私政策。

注：例如可采用通过弹窗、突出链接等主动方式提示用户阅读隐私政策。

b) 避免使用不明显的方式展示隐私政策链接，导致用户不易发现隐私政策。

注：例如采用与背景颜色相近的字体、刻意缩小字号、弹出键盘遮挡、置于边缘等为不明显方式展示隐私政策链接。

1.3 隐私政策等收集使用规则是否易于访问

a) 用户进入主功能界面后，通过 4 次（含）以内的点击等操作，能够访问到隐私政策。

b) 尽可能在界面的固定路径展示隐私政策（或其链接），以便用户随时访问和获取，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找隐私政策等情形。

注 1：例如通过“我--设置--关于”或者“我的--设置--隐私”等用户熟悉路径展示隐私政策，不频繁变更展示隐私政策的路径。

注 2：在首次展示隐私政策时，宜说明查找隐私政策的方法、路径。

c) 隐私政策以单独成文的形式发布，而不是作为用户协议、用户须知等文件中的一部分存在。

注：如果因展示条件等特殊原因使用用户协议、用户须知等文件描述个人信息收集使用规则，则尽可能显著标识并以连续篇幅呈现。

1.4 隐私政策等收集使用规则是否易于阅读

a) 隐私政策文本文字显示方式不会造成阅读困难。

注 1：例如可采取与App其他界面等同的样式。

注 2：例如文本字号过小、颜色与背景色相近、行间距过密、字迹模糊、列宽大于手机屏幕等易造成阅读困难。

b) 提供简体中文版隐私政策。

c) 隐私政策内容使用标准化的数字、图示，采用通用的语言习惯，避免误用概念、术语或存在有歧义的语句等。

1.5 公开的收集使用规则是否完整

a) 对App运营者基本情况进行描述，至少包括组织名称、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。

b) 说明隐私政策的发布、生效或更新日期。

c) 说明收集使用个人信息的目的、方式、范围。

注：详见本《实践指南》2.1 节。

d) 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）、超期处理方式进行说明。

e) 如果将个人信息用于用户画像、个性化展示等，说明其应用场景和可能对用户权益产生的影响。

注：如部分业务功能不涉及用户画像、个性化展示，可在规则中明确说明。

f) 如果存在个人信息出境情形，说明出境个人信息类型并显著标识。

注：例如可采用字体加粗、标星号、下划线、斜体、不同颜色等显著标识方式。

g) 对个人信息保护方面采取的措施和具备的能力进行说明。

h) 如果存在个人信息对外共享、转让、公开披露的情况，说明以下内容：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。

i) 对以下用户权利和相关操作方法进行说明：①个人信息查询；②个人信息更正；③个人信息删除；④用户账号注销；⑤撤回已同意的授权。

j) 至少说明以下一种投诉、举报渠道：①电子邮件；②电话；③在线客服；④在线表单；⑤即时通信账号。

注：本节相关定义和内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》5.5 节。

评估点二：是否明示收集使用个人信息的目的、方式和范围

2.1 是否逐一列出收集使用个人信息的目的、方式、范围等

a) 完整、清晰、区分说明各业务功能所收集的个人信息。宜根据用户使用习惯逐项说明各业务功能收集个人信息的目的、类型、方式，避免使用“等、例如”等方式不完整列举。

注：业务功能通常是指App为面向用户的具体使用需求所提供的一类完整的服务类型，如地图导航、网络约车、即时通信、网络支付、新闻资讯、网上购物、短视频、快递物流、餐饮外卖、交通票务、婚恋相亲、房屋租售、求职招聘、网络借贷等。

b) 使用Cookie等同类技术（包括脚本、Clickstream、Web 信标、Flash Cookie、内嵌 Web 链接等）收集个人信息时，简要说明相关机制，以及收集个人信息的目的、类型。

c) 如嵌入的第三方代码、插件（如SDK）收集个人信息，说明第三方代码、插件的类型或名称，及收集个人信息的目的、类型、方式。

注：例如可采用隐私政策、弹窗提示、文字备注、文本链接等方式说明。

2.2 收集使用个人信息的目的、方式、范围发生变化时是否通知用户

a) 收集使用个人信息的目的、方式和范围发生变化时，以适当方式通知用户。

注：例如可采用更新隐私政策等收集使用规则并以推送消息、邮件、弹窗、红点提示等方式提醒用户阅读发生变化的条款。

2.3 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

a) 在申请打开可收集个人信息权限时，通过显著方式同步告知用户其目的，对目的的描述明确、易懂。

注 1：常见可收集个人信息权限类型有：

iOS系统:定位、通讯录、日历、提醒事项、照片、麦克风、相机、健康等;

Android系统:日历、通话记录、相机、通讯录、位置、麦克风、电话、传感器、短信、存储等。

注 2：例如可采用弹窗提示、用途描述等显著方式告知。

b) 在要求用户提供个人敏感信息时，通过显著方式同步告知用户其目的，对目的的描述明确、易懂。

注 1：个人敏感信息定义见GB/T 35273-2020《信息安全技术 个人信息安全规范》3.2 节。

注 2：例如可采用弹窗提示、用途描述等显著方式告知。

2.4 收集使用规则是否易于理解

a) 有关收集使用规则的内容需简练、结构清晰、重点突出。

注：例如使用晦涩难懂的词语、冗长繁琐的篇幅、大量专业术语、逻辑结构混乱等易造成用户难以理解。

评估点三：是否征得用户同意后才收集使用个人信息

3.1 收集个人信息或打开可收集个人信息权限前是否征得用户同意

a) 收集个人信息前提供可由用户自主作出同意或不同意的选项。

注：例如提供“退出”“上一步”“关闭”“取消”的按钮等方式供用户作出不同意的选项。

b) 未征得用户同意前，不收集个人信息或打开可收集个人信息权限。

注 1：例如用户首次使用App时，在未得知收集个人信息的目的并作出同意前，App就开始收集个人信息的行为属于未征得用户同意收集个人信息。

注 2：相关定义和内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》5.4 节。

c) 未征得用户同意前，不利用Cookie等同类技术或通过调用可收集用户个人信息的权限、接口等方式收集个人信息。

3.2 用户明确表示不同意收集后是否仍收集个人信息

a) 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，明确表示不同意收集某类个人信息后，不以任何形式收集该类个人信息或打开该类可收集个人信息权限。

3.3 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

a) 用户明确表示不同意收集后，不在每次重新打开App、或使用某一业务功能时，向用户频繁询问（如 48 小时内询问超过一次）是否同意收集该类个人信息。

b) 用户明确表示不同意打开某类可收集个人信息权限后，不在每次重新打开App、或使用某一业务功能时，向用户频繁询问（如48 小时内询问超过一次）是否同意打开该类可收集个人信息权限。

注：为支持App正常运行，或用户主动选择使用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。例如用户拒绝授权“相机”权限后的 48 小时内，主动选择使用拍摄、扫码等功能时，App再次申请打开该权限的情形不属于频繁干扰。

3.4 实际收集的个人信息是否超出用户授权范围

a) 收集使用个人信息的过程需与其所声明的隐私政策等收集使用规则保持一致。实际收集的个人信息类型、申请打开可收集使用个人信息的权限等与隐私政策等收集使用规则中相关内容一致，不超出隐私政策等收集使用规则所述范围。

3.5 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

a) 在首次运行、用户注册等时，可通过弹窗、突出链接等明示方式提醒用户阅读隐私政策后征求用户同意，不采用默认勾选隐私政策等非明示方式。

b) 通过设置“下一步”“注册”“登录即代表同意”等方式征求用户同意的情形，除以显著方式展示隐私政策等收集使用规则外，还需明确执行上述动作与同意隐私政策之间的逻辑关系，以达到主动提醒用户主动阅读隐私政策后征求用户同意的效果。

注：隐私政策等收集使用规则未发生变化时无需反复征求用户同意。如App更新后，隐私政策无变化时，无需再次征求用户同意隐私政策。

3.6 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

a) 未经用户同意，不私自更改用户设置的可收集个人信息权限和收集使用个人信息相关功能的状态。

注：例如未经用户同意，在更新升级后，将用户设置的可收集个人信息权限恢复到默认状态，或将用户已关闭的使用通讯录匹配好友等功能重新打开。

3.7 存在定向推送信息情形的是否提供非定向推送信息的选项

a) 存在利用用户个人信息和算法定向推送信息情形时（包括利用个人信息和个性化推荐算法等推送新闻和信息、展示商品、推送广告等），需为用户提供拒绝接收定向推送信息，或停止、退出、关闭相应功能的机制，或不基于个人信息和个性化推荐算法等推送的模式、选项。

注：相关定义和内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》7.5 节。

3.8 是否以不正当方式误导用户同意收集个人信息

a) 明示收集使用个人信息的目的需真实、准确。不故意欺瞒、掩饰收集使用个人信息的真实目的，不诱骗用户同意收集个人信息或打开可收集个人信息权限。

注：例如App提示用户打开通讯录权限以参与红包、金币、抽奖等活动。事实上，通讯录权限与上述活动之间毫无关联，App诱骗用户打开通讯录权限后，立即上传用户通讯录信息，并将该类信息用于发送商业广告或其它目的。

3.9 是否向用户提供撤回同意收集个人信息的途径、方式

a) 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。

b) 如用户拒绝或撤回特定业务功能收集个人信息的同意时，除非用户拒绝或撤回的个人信息是其他业务功能所必需，否则不暂停其他业务功能，或降低其他业务功能的服务质量。

c) 如用户拒绝或关闭可收集个人信息权限时，不影响用户正常使用与该权限无关的业务功能，除非该权限是保证App正常运行所必需。

注 1：相关定义和内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》8.4 节。

注 2: 如用户需要撤回对同意App收集使用其所有个人信息的授权，可采取注销账号等方式执行。

3.10 是否违反其所声明的收集使用规则

a) 开展个人信息处理活动需严格遵循所公开的隐私政策等收集使用规则，并遵守与用户的约定；如个人信息使用目的、方式、范围等发生变化的，需再次征得用户同意。

评估点四：是否遵循必要原则，仅收集与其提供的服务相关的个人信息

4.1 是否收集与业务功能无关的个人信息

a) 不收集与业务功能无关的个人信息。

b) 不申请打开与业务功能无关的可收集个人信息权限。

4.2 用户是否可拒绝收集非必要信息或打开非必要权限

a) 收集与业务功能相关但非必要的个人信息或申请打开相关但非必要的可收集个人信息权限时，需由用户自主选择同意，如用户不同意，不影响其使用现有业务功能或相关服务。

b) 不将同意收集其他业务功能所需的个人信息或同意打开其他业务功能所需的可收集个人信息权限，作为用户使用当前业务功能的前提条件。

c) 如提供无需注册即可使用的服务模式（如仅浏览、游客模式），当用户拒绝同意该类服务模式以外的个人信息收集行为时，不影响其使用仅浏览等功能。

注 1：必要信息指与业务功能直接相关的个人信息，缺少该个人信息则无法提供最基本的服务。必要信息范围可参考《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》，如果服务类型不在该标准内，则可根据其业务特点，参考该标准相关定义和理念自行分析。

注 2：相关内容和实践案例可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》5.3 节及其附录C。

4.3 是否以非正当方式强迫收集用户个人信息

a) 根据用户主动填写、点击、勾选等自主行为，作为各个业务功

能收集使用个人信息的前提条件。

b) 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。

c) 不仅以改善服务质量、提升使用体验、研发新产品、定向推送信息、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。

d) 不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。

注：例如将安卓版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属于捆绑方式。

4.4 收集个人信息的频度是否超出业务功能实际需要

a) 收集个人信息的频度不超出业务功能实际需要，在用户使用某业务功能过程中，仅收集与当前业务功能相关的个人信息。

b) 在App未打开或处于后台运行状态时，不收集用户个人信息，除非业务功能需要后台运行时继续提供服务，如导航功能等。

注：在用户主动关闭App后，未经用户同意不采用自启动、关联启动方式收集个人信息。

c) 接入第三方应用时，不私自截留第三方应用收集的个人信息。

注：例如信息查询类App，在用户向第三方应用提交相关个人信息时，截留用户个人信息并上传至其后端服务器的行为属于私自截留个人信息。

评估点五：是否经用户同意后才向他人提供个人信息

5.1 向他人提供个人信息前是否征得用户同意

a) 如存在从客户端直接向第三方发送个人信息的情形，包括通过客户端嵌入第三方代码、插件（如SDK）等方式向第三方发送个人信息的情形，需事先征得用户同意，经匿名化处理的除外。

b) 如个人信息传输至服务器后，App运营者向第三方提供其收集的个人信息，需事先征得用户同意，经匿名化处理的除外。

c) 如向第三方传输的个人信息类型、接收数据的第三方身份等发生变更的，需以适当方式通知用户，并征得用户同意。

注：“匿名化”的定义可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》3.14 节。

5.2 向接入的第三方应用提供个人信息前是否经用户同意

a) 如App接入第三方应用，当用户使用第三方应用时，需在征得用户同意后，再向第三方应用提供个人信息；当用户获知应用为第三方提供后，自行以主动填写等方式向第三方直接授权的除外。

b) App运营者宜对于接入的第三方应用收集个人信息的合法、正当、必要性等方面进行审核，明确标识相关业务功能为第三方提供，并提醒用户关注第三方应用收集使用个人信息的规则。

注：第三方接入管理相关内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》9.7 节。

评估点六：是否提供删除或更正个人信息功能，或公布投诉、举报方式等信息

6.1 是否提供有效的注销用户账号功能

a) 提供有效的注销账号途径，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。

注：例如可提供在线操作、客服电话、电子邮件等注销账号的途径。

b) 受理注销账号请求后，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。

c) 注销账号的过程简单易操作，不设置不必要或不合理的注销条件。

注：不必要或不合理的注销条件相关内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》8.5节。

6.2 是否提供有效的更正或删除个人信息途径

a) 提供有效的查询、更正、删除个人信息的途径。

注：隐私政策中注明的，经证实无法完成相关操作的，视为无效途径。

b) 无法通过在线操作方式及时响应个人信息查询、更正、删除请求的，在承诺时限内（承诺时限不超过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。

c) 查询、更正和删除个人信息的过程简单易操作，不设置不必要或不合理的条件。

d) 用户更正、删除个人信息等操作完成时，后台需及时执行完成相关操作。

6.3 是否建立并公布个人信息安全投诉、举报渠道

a) 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。

注：例如可采取电子邮件、电话、在线客服、在线表单、即时通讯账号等受理方式。

b) 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。