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

（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、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信息安全的重要内容予以规定。App运营者作为典型的网络运营者，在其收集、使用个人信息时，应当遵守《网络安全法》等法律法规有关个人信息保护的要求。2019年1月，中央网信办、工业和信息化部、公安部、市场监管总局发布《关于开展App违法违规收集使用个人信息专项治理的公告》，公告中指出，由全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会，依据法律法规和国家相关标准，编制大众化应用基本业务功能及必要信息规范、App违法违规收集使用个人信息治理评估要点，组织相关专业机构，对用户数量大、与民众生活密切相关的App隐私政策和个人信息收集使用情况进行评估。2019年3月1日，App专项治理工作组结合2017年和2018年“隐私条款专项评审”等工作经验，对外发布第一版《App违法违规收集使用个人信息自评估指南》技术文件，提出评估点，以便于指导App运营者自查自纠。2019年12月30日，中央网信办、工信部、公安部、市场监管总局联合制定的《App违法违规收集使用个人信息行为认定方法》正式发布，认定方法的内容结合了一年来关于App违法违规收集使用个人信息检测评估工作的经验和规律，为监督管理部门认定App违法违规收集使用个人

信息行为提供参考，为App运营者自查自纠和网民社会监督提供指引。

本实践指南在2019年3月1日版《App违法违规收集使用个人信息自评估指南》的基础上，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收集使用个人信息评估点，供App运营者自评估参考，帮助其持续提升个人信息保护水平。

目 录

评估点一：是否公开收集使用个人信息的规则

《网络安全法》第41条规定，网络运营者收集、使用个人信息，应当公开收集、使用规则。

《消费者权益保护法》第29条规定，经营者收集、使用消费者个人信息，“应当公开其收集、使用规则”。

1.1 是否有隐私政策等收集使用规则

a) 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。

b) 隐私政策中需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，且文本可正常显示。

1.2 是否提示用户阅读隐私政策等收集使用规则

a) 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。

b) 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。

1.3 隐私政策等收集使用规则是否易于访问

a) 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。

b) 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。

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

户说明等文件中的一部分存在。

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（字号、颜色、行间距、清晰度等）不会造成阅读困难。

b) 需提供简体中文版隐私政策。

c) 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。

1.5 是否公开App运营者的基本情况

a) 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。

1.6 是否公开收集使用个人信息的其他规则

a) 隐私政策应说明发布、生效或更新日期。

b) 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。

c) 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。

d) 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。

e) 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。

f) 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。

g) 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。

h) 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。

注：相关定义和内容可参考GB/T 35273《个人信息安全规范》。

评估点二：是否明示收集使用个人信息的目的、方式和范围

《网络安全法》第41条规定，网络运营者收集、使用个人信息，应当公开收集、使用规则。

《消费者权益保护法》第29条规定，经营者收集、使用消费者个人信息，“应当公开其收集、使用规则”。

2.1 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

a) 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。

注：**业务功能**是指App面向个人用户所提供的一类完整的服务，如地图导航、网络约车、即时通讯、网络社区、网络支付、新闻资讯、网上购物、短视频、快递配送、餐饮外卖、交通票务、婚恋相亲、房屋租售、求职招聘、二手车交易、金融借贷等。

b) 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。

c) 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。

d) 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。

2.2 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

a) 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。

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。

注：常见可收集个人信息的系统权限有：
iOS系统：定位、通讯录、日历、提醒事项、照片、麦克风、相机、健康；

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。

b) 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。

注：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、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）未成年人的个人信息等。（该定义见GB/T 35273《个人信息安全规范》3.2 节）

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。

评估点三：收集使用个人信息是否征得用户同意

《网络安全法》第 41 条规定网络运营者收集、使用个人信息，应“经被收集者同意”且“不得违反法律、行政法规的规定和双方的约定收集、使用个人信息”。

《消费者权益保护法》第 29 条规定经营者收集、使用消费者个人信息，应“经消费者同意”且“不得违反法律、法规的规定和双方的约定收集、使用信息”，“经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。”

3.1 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

a) 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。

b) 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。

注：**征得同意**，指个人信息主体通过书面声明或主动做出肯定性动作，对其个人信息进行特定处理做出明确授权的行为。肯定性动作包括个人信息主体主动作出声明(电子或纸质形式)、主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

c) 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。

3.2 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

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。

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。

b) 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。

3.4 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

a) 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。

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；

b) 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。

3.6 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，不应私自更改用户设置的收集个人信息权限。

b) 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。

3.7 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

a) 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。

注：相关定义和内容可参考GB/T 35273《个人信息安全规范》。

3.8 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

a) App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。

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) 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。

b) 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。

c) 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。

3.10 是否违反其所声明的收集使用规则，收集使用个人信息

a) 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。

评估点四：是否遵循必要原则，仅收集与其提供的服务直接相关的个人信息

4.1 是否收集与业务功能无关的个人信息

a) 不应收集与业务功能无关的个人信息。

b) App不应申请打开与业务功能无关的可收集个人信息的权限。

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) App收集业务功能非必要的个人信息或申请打开非必要权限时，应征得用户同意，用户不同意不得拒绝提供相应业务功能。

b) App不应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可收集个人信息权限，作为业务功能打开的前提条件。

c) 如App提供无需注册即可使用（如浏览、游客模式）的业务模式，当用户拒绝支撑浏览、游客等模式以外的个人信息收集行为，App不应拒绝提供服务。

注：**必要信息**指与基本业务功能直接相关的个人信息，缺少该个人信息则基本业务功能无法实现。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》（征求意见稿），如果业务类型不在该标准内，则应根据其业务特点，参考该规范相关定义和理念自行判定。

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App的各个

业务功能打开或开始收集使用个人信息的条件。

b) 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。

c) 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。

d) App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。

4.4 收集个人信息的频度是否超出业务功能实际需要

a) App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。

b) 在未打开App或后台运行App时，App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。

c) App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。

评估点五：是否未经同意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。

b) 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。

c) 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。

评估点六：是否按法律规定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) 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。

b) 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。

c) 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。

注：相关内容可参考GB/T 35273《个人信息安全规范》。

6.2 是否提供有效的更正或删除个人信息

a) App应提供有效的查询、更正、删除个人信息的途径。

b) 用户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，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。

c) 查询、更正和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。

d) 用户更正、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。

6.3 是否建立并公布个人信息安全投诉、举报渠道

a) App运营者应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。

b) App运营者应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。