App 违法违规收集使用个人信息

自评估指南

（App 专项治理工作组 二零一九年三月）

本指南主要用于 App 运营者对其收集使用个人信息的情况进行自查自纠。App 运营者应遵守《网络安全法》、《消费者权益保护法》等法律要求，参考个人信息保护国家标准，持续提升个人信息保护水平。

一、隐私政策文本

评估项 1：隐私政策的独立性、易读性

评估点	评估标准
1.是否有隐私政策	在App界面中能够找到隐私政策，包括通过弹窗、文本链接、常见问题（FAQs）等形式。
2.隐私政策是否单独成文	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。
3.隐私政策是否易于访问	进入 App 主功能界面后，通过 **4 次以内**的点击，能够访问到隐私政策，且隐私政策链接位置突出、无遮挡。
4.隐私政策是否易于阅读	隐私政策文本文字显示方式（字号、颜色、行间距等）不会造成阅读困难。

评估项 2：清晰说明各项业务功能及所收集个人信息类型

评估点	评估标准
5.是否明示收集个人信息的业务功能	隐私政策中应当将收集个人信息的**业务功能逐项列举**，不应使用“等、例如”字样。 **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、社区社交、网络支付、新闻资讯、网上购物、短视频、快递配送、餐饮外卖、交通票务等；。
6.业务功能与所收集个人信息类型是否一一对应	隐私政策中对每个业务功能都应说明其所收集的个人信息类型，不应出现多个业务功能对应一类个人信息的情况。
7.是否明示各项业务功能所收集的个人信息类型	每个业务功能在说明其所收集的个人信息类型时，应在隐私政策中逐项列举，不应使用“等、例如”等方式概括说明。
8.是否显著标识个人敏感信息类型	隐私政策应对个人敏感信息类型进行显著标识（如字体加粗、标星号、下划线、斜体、颜色等）。 **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）

评估项 3：清晰说明个人信息处理规则及用户权益保障

评估点	评估标准
9.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： 1、公司名称； 2、注册地址； 3、个人信息保护相关负责人联系方式。
10.个人信息存储和超期处理方式	隐私政策应对个人信息存放地域（国内、国外）；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。

11.个人信息的使用规则	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。
12.个人信息出境情况	如果存在个人信息出境情况，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、颜色等）。
13.个人信息安全保护措施和能力	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。
14.对外共享、转让、公开披露个人信息规则	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。
15.用户权利保障机制	隐私政策中应对以下用户操作方法提供明确说明： 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。
16.用户申诉渠道和反馈机制	隐私政策中至少提供以下一种投诉渠道： 1、电子邮件； 2、电话； 3、传真； 4、在线客服； 5、在线表格。
17.隐私政策时效	应明确标识隐私政策发布、生效或更新日期。
18.隐私政策更新	如果发生业务功能变更、个人信息出境情况变更、使用目的变更、个人信息保护相关负责人联络方式变更等情形时，隐私政策应进行相应修订，并通过电子邮件、信函、电话、推送通知等方式及时告知用户。

评估项 4：不应在隐私政策等文件中设置不合理条款

评估点	评估标准
19.隐私政策等文件是否存在免责等不合理条款	App 运营者不应在用户协议、服务协议、隐私政策等文件中出现**免除自身责任、加重用户责任、排除用户主要权利条款。** **注：免除自身责任**是指 App 运营者免除其依照法律规定应当负有的强制性法定义务; **加重用户责任**是指 App 运营者要求用户在法律规定的义务范围之外承担责任或损失; **排除用户主要权利**是指 App 运营者排除用户依照法律规定或者依照合同的性质通常应当享有的主要权利。

二、App 收集使用个人信息行为

评估项 5：收集个人信息应明示收集目的、方式、范围

评估点	评估标准
20.是否向用户明示收集、使用个人信息的目的、方式、范围	1、在用户安装、注册或首次开启 App 时，应主动提醒用户阅读隐私政策。。 2、当 App 打开系统权限时（不包括用户自行在系统设置中打开权限的情况），App 应当说明该权限将收集个人信息的目的。 3、收集个人敏感信息时，App 应通过弹窗提示等显著方式向用户明示收集、使用个人信息的目的、方式、范围。
21.若使用 Cookie 及其同类技术收集个人信息，是否向用户明示	当使用 Cookie 等同类技术（包括脚本、Clickstream、Web 信标、Flash Cookie、内嵌 Web 链接、sdk 等）收集个人信息时，应向用户明示所收集个人信息的目的、类型。
22.若存在嵌入第三方代码插件收集个人信息的功能，是否向用户明示	如果通过嵌入第三方代码、插件等方式将个人信息传输至第三方服务器，应通过弹窗提示等方式明确告知用户。

评估项 6：收集使用个人信息应经用户自主选择同意，不应存在强制捆绑授权行为

评估点	评估标准
23. 收集个人信息前是否征得用户自主选择同意	App 收集个人信息前应提供由用户主动选择同意或不同意的选项，不同意应仅影响与所拒绝提供个人信息相关的业务功能。
24.是否存在将多项业务功能和权限打包，要求用户一揽子接受的情形	1、不应通过捆绑 App 多项业务功能的方式，要求用户一次性接受并授权同意多项业务功能收集个人信息的请求。 2、根据用户主动填写、点击、勾选等自主行为，作为产品或服务的业务功能开启或开始收集个人信息的条件。

评估项 7：收集个人信息应满足必要性要求

评估点	评估标准
25.实际收集的个人信息类型是否超出隐私政策所述范围	各业务功能实际收集的个人信息类型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。
26.收集与业务功能有关的非必要信息，是否经用户自主选择同意	当 App 运营者收集的个人信息超出必要信息范围时，应向用户明示所收集个人信息目的并经用户自主选择同意。 **注 1：必要信息**指与基本业务功能直接相关，缺少该信息则基本业务功能无法实现的信息。 **注 2：自主选择同意**是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。
27.是否收集与业务功能无关的个人信息	App 不应收集与业务功能无任何关系的个人信息。
28.是否在用户明确拒绝后继续索要权限、打扰用户	对于用户明确拒绝使用、关闭或退出的特定业务功能，App 不应再次询问用户是否打开该业务功能或相关系统权限。
29.App更新是否更改系统权限设置	App 更新升级后，不应更改原有的系统权限设置。

三、App 运营者对用户权利的保障

评估项 8：支持用户注销账号、更正或删除个人信息

评估点	评估标准
30.是否支持用户注销账号	App 应提供注销账号的途径（如在线功能界面、客服电话等），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。
31.是否支持用户查询、更正或删除个人信息	App 应提供查询、更正、删除个人信息的途径。

评估项 9：及时反馈用户申诉

评估点	评估标准
32.是否及时反馈用户申诉	App 运营者应妥善受理并及时反馈用户申诉，原则上在 15 天内回复处理意见或结果。