

通力合规评论 —— 2025 年 8 月 想要 APP 不被通报?做到这些就够了!

APP 已经日渐成为企业最重要的营销和获客渠道,但也因其可公开访问性,成为最容易被“盯上”的“合规黑洞”。除了消费者和竞争对手的举报外,各大监管部门对于 APP 的检测和通报也已经进入常态化。目前,工信(通管)、网信、公安、市监等各大监管部门,以及监管部门下属的事业单位(如国家病毒应急处理中心)均会不定期对 APP 进行检测,并对违法违规的 APP 进行通报。如果企业不对通报的问题进行及时整改,可能面临 APP 下架、断开网络接入、罚款甚至停业等处罚。

因此,APP 合规已经成为企业数据合规中的最高优先级。与其在 APP 被通报后再“亡羊补牢”,更有效的办法是在日常合规工作中做到未雨绸缪,提前做好 APP 合规工作,让监管挑不出下次。本月合规评论,我们就结合法律规定以及我们过往协助企业应对 APP 被通报的经验,为大家总结出避免 APP 被通报的合规要点。

1. 隐私政策

隐私政策已经成为 APP 的“脸面”,也是 APP 检测和通报中重点关注的对象。对于隐私政策,监管方面关注的主要问题为“未明示个人信息处理规则”。这项检测中,监管部门只需要简单地查看 APP 的隐私政策,就能发现是否存在问题。为了避免该方面的通报,企业应该注意以下问题:

- 1) 除非 APP 完全不收集个人信息,否则一定要设置隐私政策;
- 2) APP 首次运行时,应当通过弹窗等明显的方式展示隐私政策并提示用户阅读;
- 3) 用户注册、登录 APP 后仍然可以让用户查看隐私政策,且从 APP 主界面出发,点击 4 次以内可以访问到隐私政策;
- 4) 对于收集/处理敏感个人信息、数据出境、数据共享等情形,一定要设置单独同意,并妥善选择单独同意的展示机制(如单独的弹窗、勾选框等);
- 5) 对于隐私政策的内容本身,应当注意:
 - 将 APP 收集个人信息的目的与收集的个人信息类型及字段一一对应列出,避免杂糅在一起;
 - 对个人敏感信息类型进行显著标识(如字体加粗、下划线、斜体等);
 - 涉及到向第三方共享个人信息的,建议以列表的形式列出共享的个人信息以及接收方的信息;
 - 对于 SDK 信息,应以列表形式清晰告知用户 APP 中嵌入的第三方 SDK 名称、功能、收集的个人信息类型及其隐私政策链接;
 - 如果 APP 收集/处理 14 岁以下未成年人个人信息,应至少有专门的章节告知对于 14 岁以下未成年人个人信息的处理规则。

2. 违规收集个人信息

APP 通报中, 监管的第二大关注点是 APP 对于个人信息的收集行为是否合法、正当、必要。在这项检测中, 监管部门会对 APP 进行使用体验, 并辅以技术手段, 判断 APP 实际收取的个人信息的实际情况是否符合法律规定以及隐私政策的内容。为了避免被通报, 企业应当注意:

- 1) 避免在用户同意隐私政策之前就开始收集个人信息;
- 2) 避免实际收集的个人信息超过用户隐私政策中授权的范围, 或者收集后处理个人信息的范围、方式与隐私政策中告知的不符;
- 3) 避免对于隐私政策或弹窗等的默认勾选同意或捆绑式授权;
- 4) 即使有合规的隐私政策, 仍然应该注意收集/处理的个人信息的必要性。应避免收集与 APP 业务功能无关的个人信息, 或因用户不同意被收集非必要的个人信息, 而拒绝提供 APP 功能。此外, 仅以“改善服务质量”“提升用户体验”“研发新产品”等宽泛目的收集个人信息也在过往的通报中被视为违规收集个人信息。

3. 强制索权

“APP 强制、频繁、过度索取权限”也在各期 APP 通报中频繁出现。在此项检测中, 监管部门主要关注 APP 索取设备权限的时机、频率及合理性等问题。为了避免被通报, 企业应注意:

- 1) 调用用户设备权限前, 应通过弹窗等机制取得用户同意, 避免默认开启权限;
- 2) 应在 APP 提供服务或功能需要相关权限时, 即时申请所需权限, 避免提前索权;
- 3) 避免在用户拒绝提供授予某项权限后, 短期内再次要求相关权限;
- 4) 不应索取与 APP 提供的服务功能无关的权限(如天气预报功能索取通讯录权限);
- 5) 除 APP 运行或提供服务所必要的权限外, 不应因用户拒绝授权而不提供相关功能或服务。

4. 限制用户个人信息权利

用户个人信息权利方面, 监管目前关注的重点主要有“未妥善处理用户投诉”以及“账号注销难”。在这项检测中, 监管部门会以用户的视角, 体验 APP 响应用户权利的功能, 以判断企业是否合法、及时响应用户权利主张。具体而言:

1) 对于用户行权要求及投诉:

- 应在 APP 隐私政策中公布用户行使个人信息主体权利的渠道和方式;
- 建议可以设置可以直接通过 APP 提交用户行权主张或投诉, 如确实存在技术困难, 再考虑电话、邮件等方式;
- 如果响应用户行权或者投诉需要进行身份验证, 要求提供的身份验证信息应是注册、使用过程中已经收集过的个人信息;

- 对于收到的用户主张及投诉, 建议在 15 个工作日内进行反馈和解决。

2) 对于账户注销:

- 应在 APP 隐私政策中公布用户注销账户的方式, 并在 APP 中设置注销账户的功能;
- 如果注销账户进行身份验证, 要求提供的身份验证信息应是注册、使用过程中已经收集过的个人信息;
- 注销账户应该在 15 个工作日内完成, 且不应设置不合理的条件阻碍用户注销账户。

5. 其他关注点

除上述主要监管关注点外, 以下 APP 违规行为也在部分通报中被提及, 同样应该引起企业的重视:

- 1) 未成年人身份验证: 游戏、直播、聊天、社交、电商、教育等 APP 应关注是否设置了合理的未成年人身份验证机制;
- 2) 自启动和关联启动: 避免在用户没有操作的情况下, 通过系统机制自行启动 APP, 以及在用户未操作/授权的情况下, 从 APP 中启动、唤醒或者跳转其他 APP;
- 3) 信息窗口乱跳转/无法关闭: 避免点击信息窗口后跳转至任何无关的页面或 APP, 避免 APP 信息窗口无法关闭或需要停留一定的时长才能关闭;
- 4) 自动化决策: APP 涉及使用利用自动化决策处理个人信息的(例如使用算法进行个性化推荐), 应当提供不针对其个人特征的选项;
- 5) 加密等技术措施是否到位: 监管部门可以通过数据抓包、流量分析等方式检测 APP 传输数据是否进行了加密, 因此企业应对 APP 数据存储和传输采取必要的加密措施。

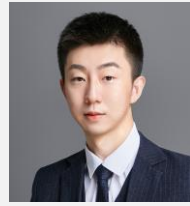
在 APP 合规领域, 我们可以为客户提供如下服务:

- APP 设计阶段的隐私保护设计与功能
- 隐私政策和用户协议制定
- APP 整体合规评估与合规提升
- APP 相关注册与备案
- APP 安全认证
- APP 安全技术检测
- APP 被通报后的评估、整改与政府沟通

如有需要, 请随时与我们联系:



潘永建
+86 21 3135 8701
david.pan@llinkslaw.com



朱晓阳
+86 21 3135 8683
nigel.zhu@llinkslaw.com



邓梓珊
+86 21 6043 3793
susan.deng@llinkslaw.com

往期文章:

[通力合规评论 \(2025 年 8 月\) - DPO 报送有风险? 关注点不该在这儿!](#)

[通力合规评论 \(2025 年 6 月\) - 买来的数据, 就没风险了?](#)

[通力合规评论 \(2025 年 6 月\) - 数据泄露莫要慌, 合规应对有保障](#)

[通力合规评论 \(2025 年 4 月\) - AI 合规](#)

[通力合规评论 \(2024 年 12 月\) - 2025 年了, 网数合规工作还要做啥?](#)

[通力合规评论 \(2024 年 11 月\) - 个人信息保护合规审计“风雨欲来”——你做好准备了吗?](#)

[通力合规评论 \(2024 年 10 月\) - 中国数据安全新规将于 2025 年 1 月 1 日起实施](#)

如您希望就其他问题进一步交流或有其他业务咨询需求, 请随时与我们联系: master@llinkslaw.com

上海

上海市银城中路 68 号
时代金融中心 19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

北京市朝阳区光华东里 8 号
中海广场中楼 30 层
T: +86 10 5081 3888
F: +86 10 5081 3866

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环遮打道 18 号
历山大厦 32 楼 3201 室
T: +852 2592 1978
F: +852 2868 0883

伦敦

1/F, 3 More London Riverside
London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: LlinksLaw

本土化资源 国际化视野

免责声明:

本出版物仅供一般性参考, 并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2025