

快手安全手护者沙龙

隐私保护实践困境&破局

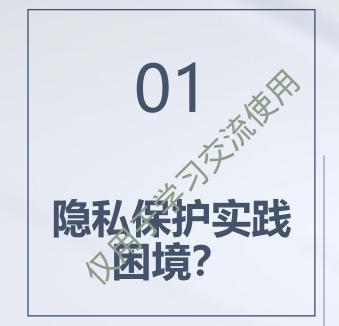
快手安全 邵华 2022年3月



隐私保护实践困境 目录 隐私合规框架 Contents 思考与展望











大环境



监管执法

21年度共计23批次共通报近 2000款、下架500+款



公众&媒体关注

啫喱iOS霸榜同时也陷入隐私 保护风波

网信办

公安部

市监局

举报

用户投诉

热点事件









小环境



怎么不断有新问题? 每次都要各业务自己改,成本太高了, 能不能统一改? 对业务影响太大了,怎么解?





同一个问题怎么又出现? 这个场景没有排查到啊? 整改不彻底,怎么还有漏过? 为什么新功能不同步合规评估?

. . .









隐私保护框架



合规、GR、法 务、PM 合规、业务 研发 GR、PR、客服 业务研发 法务、PR 合规 数据安全、业 务研发、合规 合规、PR、 GR、法务、 业务研发

PR、合规、 标准、GR

制度和协议

- 隐私保护规范
- 隐私政策
- 产品隐私指引
- 解决方案

DPIA

- 隐私评估机制
- 例行隐私巡检
- 数据跨境评估
- 年度隐私报告

用户权益

- 授权同意
- 敏感场景同意管理 (推荐、广告等)
- 自助注销账号
- 获取个人信息副本
- 双清单
- 逝者账号响应
- 申述机制

• ...

收集&共享

- 最小化收集
- 第三方获取
- 委托处理
- 边缘计算

安全保护措施

- 去标识化
- 个人信息服务化
- 访问控制
- 客户端存储、传输、 服务端加密
- 数据脱敏
- API网关
- 数据入境监测

应急响应

- 监管督办
- 舆论处置
- 热点事件跟踪
- 用户投诉
- 应用市场

运营

- 月报/双周报
- 媒体宣导
- 标准制修订
- 安全认证

团队/外部反向验证

• 外部机构合作

发展路径

体系化合规,提前发现问题

被动合规, 应急灭火, 效率低

- → 被动应对例行和突发检查
- →借助外部力量适配监管要求(不能复用既有成果)
- → 合规统一方案,统一口径。 顺利通过检查
- →跟进法规、政策、标准等 合规要求,及时差距分析 与解读
- → 基础安全认证补齐
- → 隐私合规问题检测发现、 例行评估等基础能力

创新合规,引领行业,安全与隐 私保护作为竞争力

- **主动合规**。与外部紧密合作
- → 微测跟进法规/政策/标准等 一 合规要求,与监管部门/测 评机构等建立紧密联系, 识别高风险合规事项。
- →内部:体系化建设合规能 力,并在某些领域主动适 配监管要求

- → 输出、引领前沿安全和隐 私技术研究和工程化
- →树立安全和隐私保护品牌 影响

隐私合规实践

用户出发

有据可依

收口应对

技术支撑

评估运营



建章立制

隐私合规能力 建设

提高业务 隐私保护水准 成立隐私保护小组, 收口建设隐私保护工作, 提升快手合规水位

梳理公司产品及相关业务团队,建立评估机制

自动化隐私合规检测能力

个人数据收集、使用管理能力

关注法律及监管要求,搭建内部App个人信息保护方案

持续开展内部App治理专项行动,识别内部产品潜在不合规问题

开展隐私评估,推进产品隐私设计,尊重用户权益

打开视野,了解行业隐私动向,查漏补缺







目标

怎么不断有新问题?

每次都要各业务自己改,成本太高了,能不能统一改?

对业务影响太大了

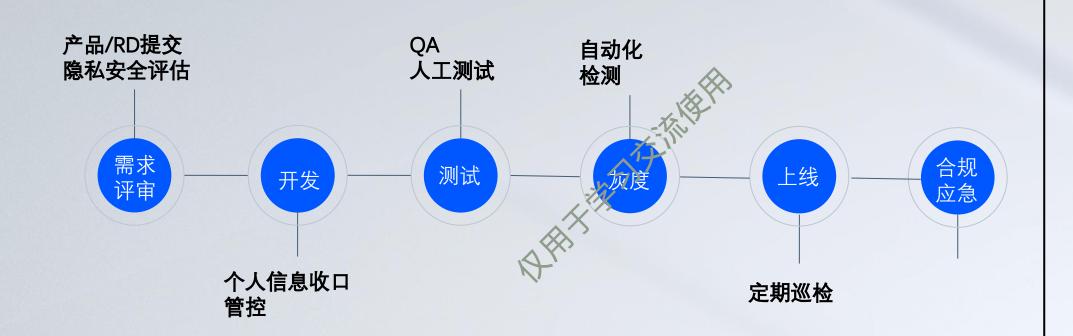
同一个问题怎么又出现?

这个场景没有排查到啊?整改不彻底,怎么还有漏过?

为什么新功能不同步合规评估?

安全合规 效率成本 业务收益

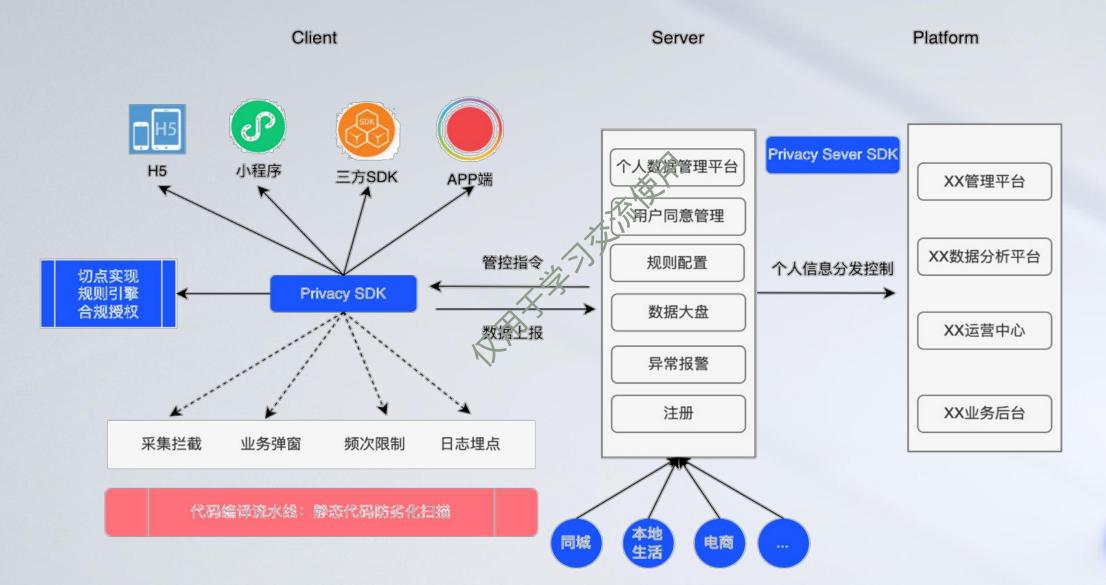
APP生命周期内的风险控制措施



机制保障

职责划分 团队协同 意识提升 合规问责

个人信息收口管控



个人信息收口管控

序号	字段		
1	应用列表	applist	
2	位置	纬度、经度、baseStation、 nearbyBaseStation(基站扇区)、 BSSID、SSID、RSSI及AP地址	
3	电话权限	android id、蓝牙MAC地址、MAC地址、 MSerialNumber/iccid、IP地址	
4	手机通讯录	手机号、姓名、邮箱、备注等	
5	第三方SDK		
6	剪切板	剪切板涉及内容,如可能保护账号、密码、地址等	
7	健康运动权限/身体活动		
8	相册&媒体文件读写	图片、视频以及图片和视频属性信息(如 位置,大小等)	
9	身份信息&面部识别(iOS	身份证号、护照、身份证照片,人脸识别	
10	手机号	sim_mobile, sim卡中手机号	

位置相关的

	3	J	
有 6 6 6 6	android.location.LocationManager	void	getCurrentLocation(String provider, CancellationSignal cancellationSignal, Executor executor, Consumer <location> consumer)</location>
	android.location.LocationManager	GpsStatus	getGpsStatus(GpsStatus status)
	android.location.LocationManager	Location	getLastKnownLocation(String provider)
	android.location.LocationManager	void	requestLocationUpdates(String provider, long minTimeMs, float minDistanceM, LocationListener listener)
	android.location.LocationManager	void	requestLocationUpdates(long minTimeMs, float minDistanceM, Criteria criteria, LocationListener listener, Looper looper)
	android.location.LocationManager	void	requestLocationUpdates(String provider, long minTimeMs, float minDistanceM, LocationListener listener, Looper looper)
	android.location.LocationManager	void	requestLocationUpdates(String provider, long minTimeMs, float minDistanceM, Executor executor, LocationListener listener)
	android.location.LocationManager	void	requestLocationUpdates(long minTimeMs, float minDistanceM, Criteria criteria, PendingIntent pendingIntent)
	android.location.LocationManager	void	requestLocationUpdates(long minTimeMs, float minDistanceM, Criteria criteria, Executor executor, LocationListener listener)







思考与展望







- •可算不可用 (识别)
- •可用不可见
- •可用不可得

- 去标识化/匿名化技术

- 司态技术
- 边缘计算







