CAICT 中国信通院

环球律师事务所
GLOBAL LAW OFFICE

软件开发包（SDK）安全与合规报告

（2020）

中国信息通信研究院安全研究所
北京市环球律师事务所

2020 年 9 月

版权声明

编 写 团 队

编写单位：

中国信息通信研究院安全研究所

北京市环球律师事务所

编写组成员：（姓氏笔画为序）

陈湉、张淑怡、孟洁、秦博阳、薛颖、覃庆玲、魏亮

联系人：

陈湉

电话：010-62308820

邮箱：chentian@caict.ac.cn

孟洁

电话：010-65846768

邮箱：mengjie@glo.com.cn

前　言

我国移动互联网市场经历了将近 20 年的快速发展，已经形成了庞大的产业规模，创造了可观的经济效益，并且在业务模式和商业模式创新方面引领全球。同时，移动互联网正在向传统产业加速渗透，人工智能、大数据、物联网等信息技术与实体经济持续深度融合，不断催生传统产业服务新业态，逐步改造着医疗、教育、交通、旅游、金融、传媒等传统行业的服务模式。在此过程中，移动应用软件，即 App，发挥了不可替代的入口作用，全天候、全方位深度参与到了广大网民日常生活的方方面面。

App 在提供各类便捷、高效、普惠服务的同时，也在无时不刻地收集、使用用户的个人信息，与 App 存在密切联系的第三方软件开发包（SDK）收集个人信息问题也已经进入各方视野。2019 年下半年起至 2020 年，不论是立法动态还是监管角度，均将 SDK 违法违规收集个人信息作为审查的重点之一。

僻如，在立法和国家标准制定方面，《数据安全管理办法（征求意见稿）》《GB/T 35273-2020 信息安全技术 个人信息安全规范》《网络安全标准实践指南 移动互联网应用程序（App）中的第三方软件开发工具包（SDK）安全指引（征求意见稿）》《信息安全技术 个人信息告知同意指南（征求意见稿）》等国家标准的研究也开始涉及第三方介入（包括 SDK）这一特定领域。

在监管方面，中央网信办、工业和信息化部、公安部、市场监督总局四部委组建的 App 专项治理工作组在全国范围开展较大规模的 App 的审查与治理行动，从曝光的结果来看，不难看出已对 App 中嵌入的违规 SDK 厂商，采取了包括但不限于约谈企业负责人、网上曝光、App 下架等措施。该治理工作组在今年 5 月发布的《App 违法违规收

集使用个人信息专项治理报告（2019）》，更是明确指出“第三方 SDK 自身的安全性，以及其收集使用个人信息行为，也成为移动生态中个人信息保护的风险点……建议将 SDK 收集使用个人信息行为纳入专项治理范围，以促进 SDK 行业加强数据收集使用规范性”。由此可见，2020 年，SDK 的合规性已经成为监管的重点。

并且，2020 年 3 月疫情期间爆出的 Zoom 接入 SDK 问题，2020 年 7 月“3．15”晚会曝光私自收集个人信息的 SDK 未经用户许可窃取个人信息问题，更是引发了公众对 SDK 安全与合规的极大关注。

特别地，2020 年 7 月中央网信办、工业和信息化部、公安部、国家市场监管总局四部门启动 2020 年 App 违法违规收集使用个人信息治理工作，提到今年年度的治理重点时专门提到了对第三方 SDK 的治理：制定发布 SDK 个人信息安全评估要点，对用户规模大、问题反映集中的小程序等进行深度评估。

本报告将在 2019 年版本的基础上，进一步梳理当前应用较为广泛的第三方 SDK 类型和市场情况，结合实际案例分析第三方 SDK 存在的主要安全问题以及第三方 SDK 提供者与 App 开发者合作过程中面临的法律合规问题。通过调研欧盟、美国的相关经验做法，从法律法规、企业责任、技术标准、行业自律等方面结合我国实际情况提出了有针对性的建议。

本报告 2020 年版比照 2019 年版的主要修订在于：

– 更新了 2019 年至今监管层面、国家标准层面针对 SDK 的规制；

– 更新了对 App 开发者嵌入第三方 SDK 的合规实践建议；

– 更新了第三方 SDK 自身的合规实践建议；

– 更新了第三方 SDK 产品最新的合规实践案例。

目 录

图 目 录

表 目 录

一、 第三方 SDK 的业内现状

据中国互联网络信息中心（CNNIC）统计数据显示，截至 2020 年 3 月，我国手机网民规模已达 9.04 亿，网民通过手机接入互联网的比例高达 98.6%。随着移动互联网的发展、智能手机的不断普及，移动互联网应用程序（App）得到广泛应用。据工信部统计数据显示，截至 2019 年 12 月，我国市场上监测到的 App 总量达到 367 万款，第三方应用商店分发累计数量超过 9502 亿次，游戏类、系统工具类、影音播放类、社交通讯类、日常工具类 5 类 App 下载量均超过千亿次。移动互联网服务便捷、即时、普惠的特点，在 App 应用中得到充分体现，部分 App 甚至已成为广大用户生活中的“必需品”。

由于移动互联网市场的快速迭代，高科技产品飞速更新，App 开发者为了提升效率、降低成本，往往会在开发过程中嵌入第三方代码（SDK 开发包）和插件等。本章将从常见类型、应用情况、主要特点等方面对 SDK 的业内现状进行介绍，详细分析其被广泛使用的原因。

（一）第三方 SDK 常见类型及应用情况

SDK 是 Software Development Kit 的缩写，即“软件开发工具包”。简单来看，它是辅助开发某一类应用软件的相关文档、范例和工具的集合。对 App 来说，为了提高开发效率，可以将某项功能交给第三方来开发，第三方服务提供商将服务封装为工具包（即 SDK）供开发者使用。目前，SDK 类型主要包括：第三方登录分享类、支付类、推送类、广告类、数据统计分析类、地图类、风控插件以及一些基础

库等。

1. 常见第三方 SDK 类型

按照第三方 SDK 能够帮助 App 开发者实现的具体功能不同进行区分，其中较为常见、与用户交互程度较强的主要有以下 6 类 SDK。

（1）第三方登录分享类

第三方登录分享类 SDK 主要用于简化用户登录流程，为用户使用已有的第三方帐号进行登录提供便利，同步帮助 App 构建自己的帐号登录体系。作为一种功能较为基础的 SDK，第三方登录分析类 SDK 被各类 App 广泛使用。

（2）支付类

据国家信息中心 2019 年发布的《中国移动支付发展报告》数据显示，截至 2018 年上半年，我国移动支付用户规模约为 8.9 亿，移动支付交易规模已超过 277 万亿元。随着移动支付的普及应用，支付功能越来越成为各类 App 的普遍需求。支付类 SDK 帮助开发者在 App 中进行了支付功能的集成，为用户提供购物、充值、付款、退款等相关功能。

（3）推送类

推送类SDK帮助App开发者向其用户实时推送通知或者消息，与用户保持互动，从而有效地提高用户留存率，提升用户体验。推送类SDK可实现基于用户活跃情况、设备属性、地理位置等不同用户群的推送。推送形式包括状态栏通知、自定义消息、本地通知等，内容可涵盖新闻资讯、日程提醒、活动预告、新版本更新等。

（4）广告类

据《中国互联网发展报告 2020》显示，2019 年网络广告市场规模达 4341 亿。随着移动广告红利时代的到来，App 开始接入广告相关 SDK 的情形越发普遍，广告类 SDK 对各类广告形式的支持情况也已成为影响移动开发者收入、操作等的关键因素之一。

（5）统计分析类

数据统计分析类 SDK 可以帮助 App 开发者统计和分析流量来源、内容使用、用户属性和行为数据等，以便 App 开发者利用数据进行产品、运营、推广策略的决策。

（6）地图类

地图类 SDK 帮助 App 集成地图显示、交互等相关服务，以便用户在使用 App 时在应用中访问相关地图数据，轻松实现相关功能，并在此基础上完成基于自身场景的更深层、更个性化的开发需求。

2. 常见第三方 SDK 应用情况统计

为了对第三方 SDK 的应用情况进行进一步了解，本章节按类别梳理、总结了一些常见第三方 SDK 类别的应用情况[1]。

（1）第三方登录分享类

第三方登录分享类 SDK 主要以主流即时通讯或社交类企业推出的 SDK 为主，常见的类型主要有微信登录分享、微博登录分享、QQ 登录分享等。嵌入此类 SDK 的 App 往往既包括 App 本身，也涉及 App 的同一母公司旗下其他产品，还包括其他各类 App（如新闻资讯、视频、

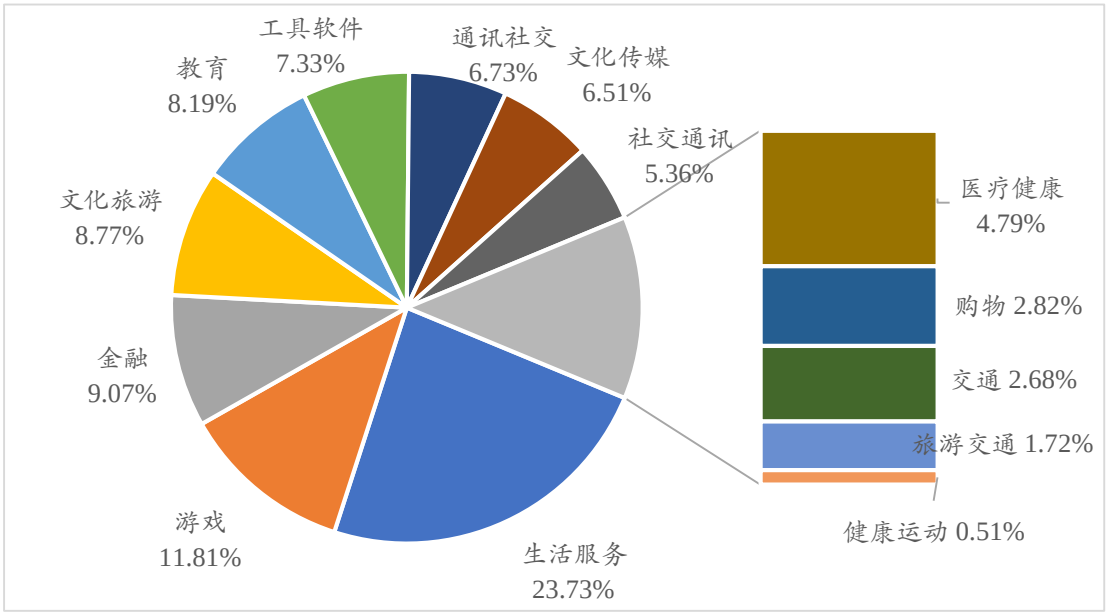
[1] 相关信息梳理来自各 SDK 官网或开发者平台。

旅游出行等），具体情况详见表 1。

表 1 常见第三方登录分享类 SDK 应用情况统计

SDK 名称	主要业务功能	简要介绍	嵌入此类 SDK 的 App
微信登录分享	使用微信帐号快速登录第三方平台或 App。	接入微信登录，实现微信帐号快速登录，一键连接。	普遍应用在各类 App 中。
微博登录分享	使用微博帐号快速登录网站或第三方 App，分享内容，同步信息。	满足了多元化移动终端用户随时随快速登录、分享信息的需求。	普遍应用在各类 App 中。
QQ 登录分享	使用 QQ 帐号快速登录网站或第三方平台。	用户使用已有的 QQ 号码即可登录移动应用，可减少登录交互操作，简化用户注册流程。	普遍应用在各类 App 中。

以新浪微博 SDK 为例，该 SDK 被广泛嵌入在各类 App 中，生活服务、游戏和金融行业 App 中嵌入该 SDK 的情况最为普遍，三者合计占比 44.61%。具体分布情况如图 1 所示：



（数据来源：北京智游网安科技有限公司（爱加密））

图1 嵌入新浪微博SDK的App分布情况

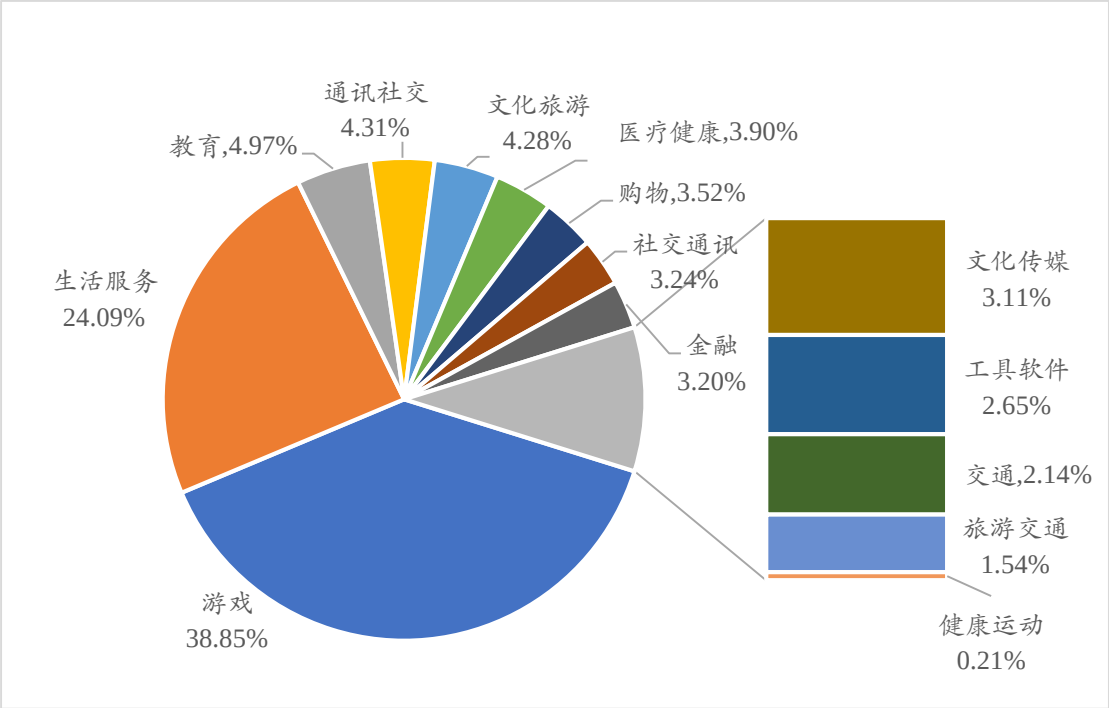
（2）支付类

支付类 SDK 通常提供的功能较为单一。目前常见的支付类 SDK 主要包括银联支付、支付宝支付、微信支付以及各个大银行自己独有的支付 SDK 等。嵌入此类 SDK 的，除了各类电商购物平台及相关旅游出行类 App 外，还包括其他设置了充值、付款、退款等功能的各类 App，具体情况详见表 2。

表 2 常见支付类 SDK 应用情况统计

SDK 名称	主要业务功能	简要介绍	嵌入此类 SDK 的 App
银联支付	跳转银联页面完成支付信息录入，最终完成支付。	综合性互联网支付工具，主要支持输入卡号付款、用户登录支付、网银支付、迷你付（IC 卡支付）等多种支付方式。	普遍应用在各类设置了支付场景的 App 中。
微信支付	通过点击微信付款码支付，或扫描二维码支付等功能。	综合性互联网支付工具。	普遍应用在各类设置了支付场景的 App 中。
支付宝支付	通过二维码面对面支付、小程序支付、花呗分期等多种支付功能。	综合性互联网支付工具。	普遍应用在各类设置了支付场景的 App 中。

以支付宝 SDK 为例，该 SDK 被广泛嵌入在各类设置了支付场景的 App 中，以游戏和生活服务行业最为广泛，分别有 38.85%与 24.09%的支付宝 SDK 嵌入了该类 App。具体分布情况如图 2 所示:



（数据来源：北京智游网安科技有限公司（爱加密））

图2 嵌入支付宝SDK的App分布情况

（3）推送类

推送类 SDK 因其多强调交互式体验的特点，广泛应用于与用户互动的场景中，目前常见的推送类 SDK 主要有小米推送、百度云推送、个推推送、极光推送、Mob 推送等。嵌入此类 SDK 的 App 包括新闻资讯、社交、地图、健康医疗、旅游出行类等 App，具体情况见表 3。

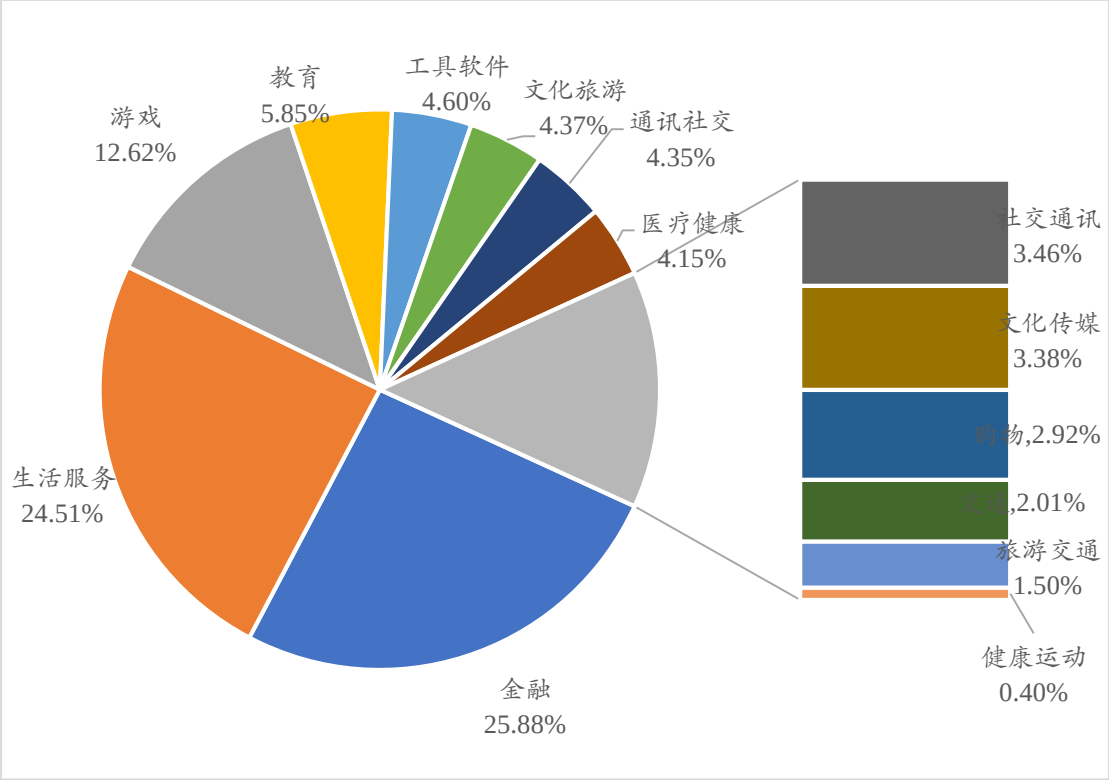
表 3 常见推送类 SDK 应用情况统计

SDK 名称	主要业务功能	简要介绍	嵌入此类 SDK 的 App
小米推送	主要实现消息推送功能。	通过在云端与客户端之间建立一条稳定、可靠的长连接，为开发者提供向客户端应用实时推送消息的服务，有效地帮助开发	百度地图、快手、今日头条、爱奇艺、淘宝、支付宝、UC 浏览器、QQ 音乐、高德地图、拼多多、

		者触达用户，提升App活跃度。	QQ浏览器、滴滴出行、酷狗音乐等。
百度云推送	推送聊天消息、日程提醒、活动预告、动态、新版本更新等功能。	一站式App信息推送平台，为企业和开发者提供免费的消息推送服务，开发者可以通过云推送向用户精准推送通知和自定义消息以提升用户留存率和活跃度。	手机百度、百度地图、爱奇艺、蚂蜂窝、聚美优品、我查查、虎嗅网、当当网等。
极光推送	多种消息类型、用户和推送统计、短信补充、A/B测试、可定制的私有云等功能。	为超过50万移动开发者和145.2万款移动应用提供服务，其开发工具包(SDK)安装量累计336亿，月度独立活跃移动终端13.6亿部。	珍爱网、酷狗铃声、浮浮雷达、福建移动（八闽生活)、格力、广州地铁、顺丰、土巴兔、探探、快看漫画、汽车之家、网易新闻、搬运帮、墨迹天气、翼支付、去哪儿、平安好医生、银联商务等。
个推推送	向其用户推送各类消息，结合精准的用户画像分析，给合适的用户在合适场景下推送合适的内容。	各行业提供大数据解决方案，服务于数十万App，覆盖数十亿移动终端。	人民日报、新华社、CCTV、新浪微博、京东、网易新闻、滴滴出行等。
Mob推送	Sharesdk、Smssdk、Moblink、Mobpush、秒验、mob云验证等	以数据应用为主导，融合大数据、云计算、人工智能等技术，	绿地集团、龙珠直播、无他相机、中国电

	功能。	SDK 下载数量超 370 万，日活用户超 2.5 亿。	信等。

以极光推送SDK为例，极光推送SDK嵌入的App主要集中在金融和生活服务类App，比例接近一半。具体分布情况如图3所示：



（数据来源：北京智游网安科技有限公司（爱加密））

图3 嵌入极光推送SDK的App分布情况

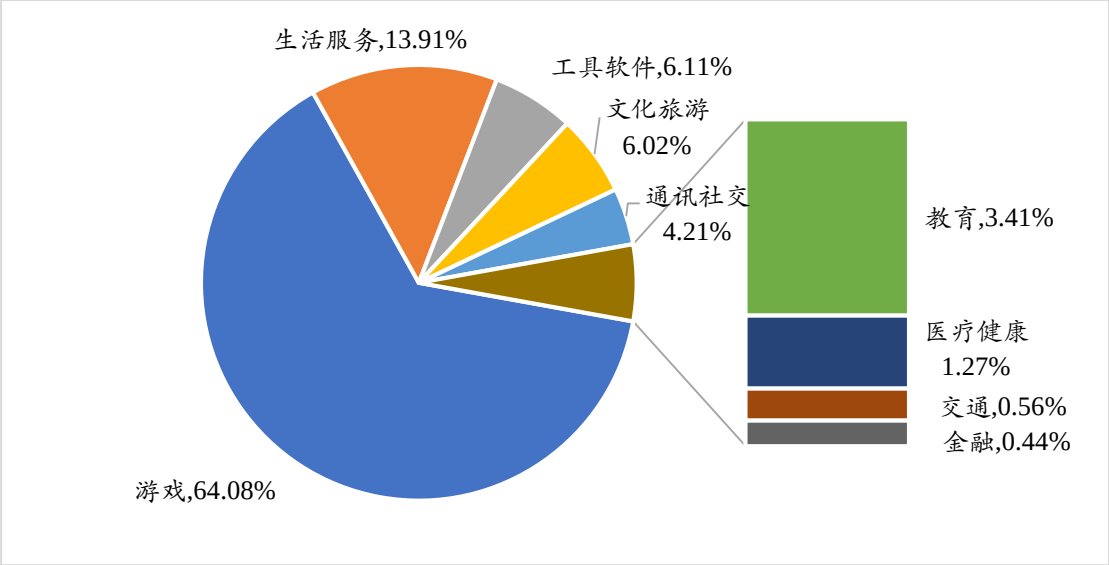
（4）广告类

广告类 SDK 提供的服务多为程序化广告，用以实现精准营销和推广。目前，国内市场上提供移动广告相关的 SDK 平台众多，主流的有广点通、多盟、TalkingData、有米等。由于 App 普遍具有广告投放推广需求，嵌入广告类 SDK 的 App 涵盖多个类别，具体情况见表 4。

表 4 常见广告类 SDK 应用情况统计

SDK 名称	主要业务功能	简要介绍	嵌入此类 SDK 的 App
广点通	主要实现广告投放相关功能。	为 App 开发者提供广点通投放系统，通过广点通，用户可在平台多个广告位上进行应用以及应用活动相关的精准推广。	欢乐淘、楚楚街、沪江教育、妈妈圈、十句话战仙、神仙道、时空猎人、美丽说等。
多盟	主要实现广告投放、营销等相关功能。	专注移动智能营销，提供程序化广告、数据营销、代理广告等服务。	中国银行、渣打银行、中国电信、招商银行、中国移动等。
TalkingData	主要实现应用统计分析、游戏运营分析、小程序统计分析等功能。	以 SmartDP 为核心的数据智能应用生态为企业赋能，帮助企业逐步实现以数据为驱动力的数字化转型。	腾讯、百度、网易、搜狐、360、Google 、 Yahoo 等。
有米	主要实现广告推广功能。	提供 App 推广、ASO 优化、出海营销、整合营销以及广告数据洞察等专业服务，满足游戏、电商、网服、教育、美妆等行业客户的推广需求。	封面新闻、晶报传媒、网易智造、Kappa 、 溢 米 辅 导、龙之谷等。
InMobi	主要实现个性化广告功能。	全球化的移动广告平台，覆盖超过 15 亿移动设备，每月广告请求超过 2000 亿。	天使纪元、少年三国志、狂暴之翼等。

以 InMobi SDK 为例，嵌入该 SDK 的 App 中，6 成以上分布在游戏行业；其次是生活服务行业，占有 13.91%。具体分布情况如图 4 所示：



（数据来源：北京智游网安科技有限公司（爱加密））

图4 嵌入 InMobi SDK的App分布情况

（5）统计分析类

数据统计分析类 SDK 作为一类较不易为用户感知的 SDK，对 App 的运营和统计分析提供支撑作用。目前，常见的数据统计分析类 SDK 包括友盟、海度云、贵士移动等。嵌入此类 SDK 的 App 也广泛来自各领域，且不乏各领域的头部 App，具体情况见表 5。

表 5 常见数据分析类 SDK 应用情况统计

SDK 名称	主要业务功能	简要介绍	嵌入此类 SDK 的 App
友盟	主要包括移动统计、应用统计、游戏统计、移动广告监测等功能。	结合实时更新的全域数据资源，挖掘出 15,000+客群标签、输出 300+应用或行业的分析指标，通过 AI 赋能的一站式互联网数据产品与服务体系。	微博、阿里云、Kantar Worldpanel、优酷、迈外迪、酷云互动、讯码科技、云房数据、飞猪、Marketin、淘

			票票、PP 助手、钉钉、豌豆荚、掌慧纵盈等。
贵士移动	TRUTH 移动互联网标准数据库系列、TRUTH-Plus 生态流量服务、DATA MINING 数据挖掘分析服务。	帮助客户了解市场发展趋势和行业竞争格局，通过理解用户特征和全景画像优化自身运营效率，另一方面也可以帮助客户前瞻性地发现市场机会，找到具有增长潜力的赛道和值得投资的领域。	百度、蚂蚁金服、中国平安、顺丰速运、腾讯、华为、苏宁易购等。
海度云	主要包括移动应用统计、网站统计、渠道分析等功能。	帮助客户了解市场发展趋势和行业竞争格局，优化自身运营效率，帮助客户发现市场机会，日接受移动数据量超过 150 亿。	YY、ME 直播、100 教育、环球网校、无忧英语、邢帅教育、闲趣网络等。

（6）地图类

地图类 SDK 帮助开发者实现地图数据的调用及相关服务的实现。目前，常见地图类 SDK 主要包括百度地图、高德地图、腾讯地图等。嵌入此类 SDK 的 App 多为旅游出行、电商购物、物流、外卖等，具体情况见表 6。

表 6 常见地图类 SDK 应用情况统计

SDK 名称	主要业务功能	简要介绍	嵌入此类 SDK 的 App
百度地图	主要有地图、定位、搜索、轨迹、导航、路线规	提供手机端、PC 端、智能穿戴设备的地图	摩拜单车、e 袋洗、点到、德

	划、路况等功能。	展示能力，在多个行业场景中可以配置个性的地图展示效果。	邦、苏宁易购、货拉拉、唯品会等。
高德地图	主要有地图、定位、导航、路线规划、搜索、自定义地图和数据可视化等功能。	LBS 服务提供商，服务超过三十万款移动应用，日均处理定位请求及路径规划数百亿次。	首汽约车、易到、神州专车、曹操专车、嘀嗒出行、饿了么等。
腾讯地图	主要有定位、地图展示、地点搜索、路线规划、导航和室内图等功能。	基于 Android 4.1 及以上版本设备的应用程序接口，通过该接口，可以轻松的使用腾讯地图定位服务。	京东、中国邮政、新达达、汇通天下、滴滴出行、美团外卖、快手等。

3. 第三方 SDK 的应用特点分析

从第三方 SDK 应用情况来看，主要呈现以下三个特点:

一是 App 使用第三方 SDK 已成为普遍现象。根据爱加密发布的 2020 年 Q1《全国移动 App 安全态势研究报告》，截至 2020 年 3 月底，爱加密大数据中心已收录 Android 应用超过 315 万款，iOS 应用超过 300 万款，其中 29.46%的应用嵌入了 SDK，近 5 成都是框架类 SDK。从嵌入第三方 SDK 的 App 所处行业类型来看，游戏类嵌入 SDK 的 App 数量最多，占比为 23.85%，其次是生活服务类 App，占比为 18.16%; 位列第三的是教育类 App，占比为 15.46%，详见图 52。可以说，SDK 已成为与 App 相生相依的重要伙伴，也同时成为了整个移动互联网生态中极其关键的一环。

[2] 爱加密 2020 年 Q1《全国移动 App 安全态势研究报告》。

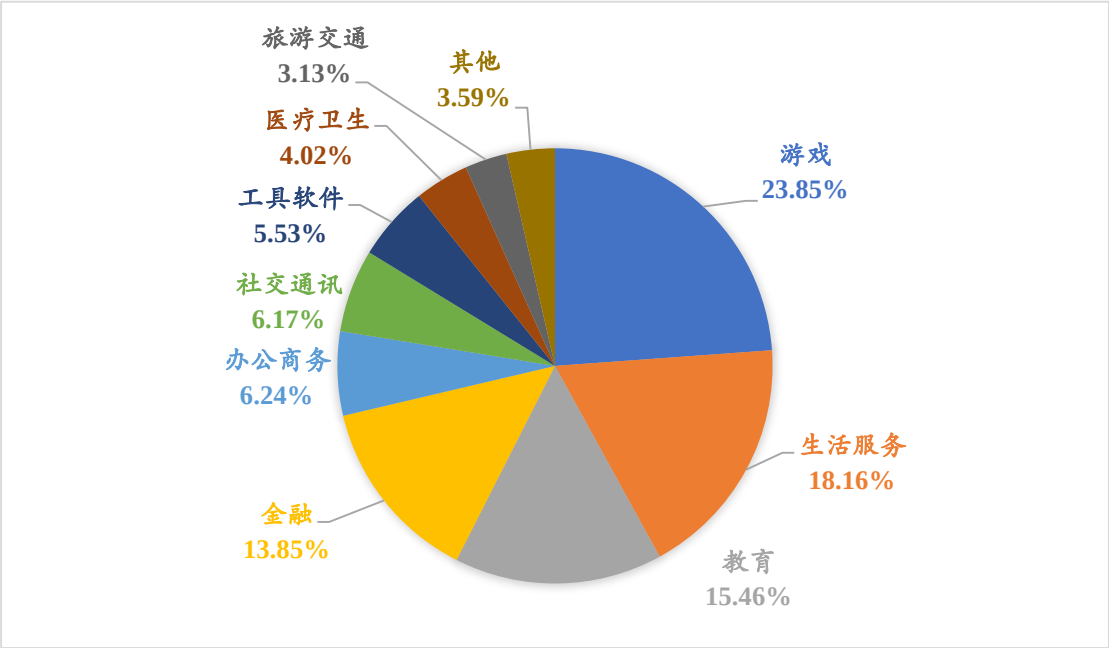
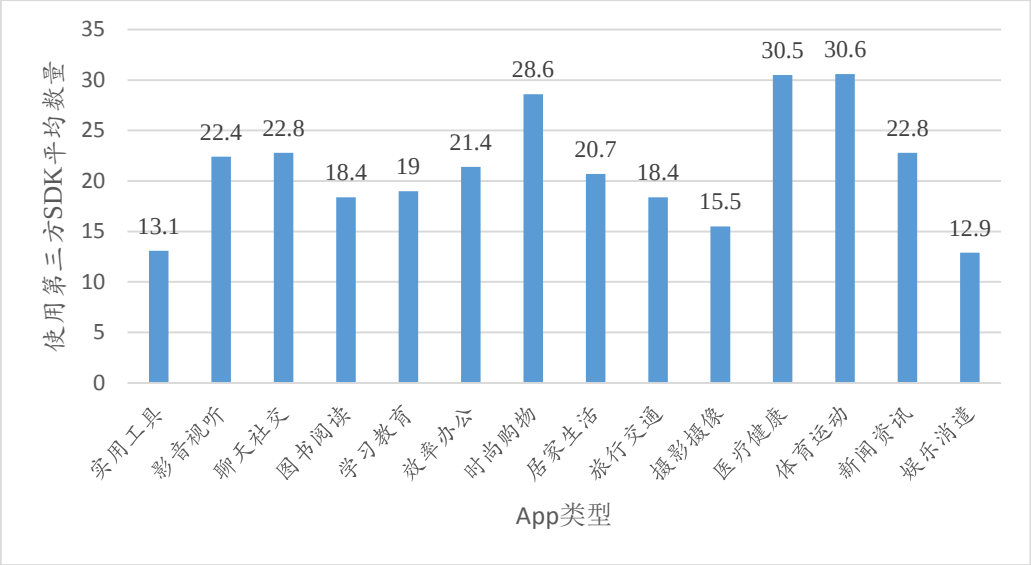


图5 各类型App嵌入SDK占比情况

二是各类别App平均使用第三方SDK的数量在10个以上。随着第三方SDK种类及数量的不断增多，不少App开发者由于开发时间和成本有限，大量使用第三方SDK进行代码集成。如图6所示，根据CSDN社区专业人士利用SDK分析工具，针对1000多款主流App使用SDK情况得出的统计数据[3]，各类别App使用第三方SDK平均在10个以上，最高可达平均30.6个/类。平均使用第三方SDK个数超过20个的App类型有8类。

[3] https://blog.csdn.net/rohsuton/article/details/78022158，最后访问时间 2019 年 7 月 20 日。



（数据来源：CSDN“IT东”博客的SDK分析工具）

图6　App中使用第三方SDK的数量分布图

三是第三方SDK功能逐渐多样化，应用于不同领域的大量App中。目前，市场上的第三方SDK提供者已不再局限于开发功能单一的SDK，而是将SDK功能从纵向和横向不断延伸，从而应用于不同领域的大量App中。以推送类SDK提供者为例，除了不断完善基于用户画像的实时、智能、多场景下的精准推送外，往往会同步对产品运营情况进行统计分析，帮助App进行产品优化升级，甚至部分SDK提供者还同步推出了登录验证功能。随着第三方SDK功能的不断强大并逐渐多样化，其应用市场的规模将持续扩大，市场前景持续看好。可以说，第三方SDK已成为事实上链接各类业务功能App的数据枢纽，有机会获取来自各类App不同业务场景下多类别的个人信息。

（二）第三方 SDK 安全标准化现状

1. 已发布标准情况

目前，涉及第三方SDK安全的，比较有代表性的标准包括国家标准《GB/T 35273-2020 信息安全技术 个人信息安全规范》，以及金融行业标准《JR/T 0171-2020 个人金融信息保护技术规范》。

国家标准《GB/T 35273-2020 信息安全技术 个人信息安全规范》第 9.6 条要求：“如个人信息控制者在提供产品或服务的过程中部署了收集个人信息的第三方插件（例如，网站经营者与在其网页或应用程序中部署统计分析工具、软件开发工具包 SDK、调用地图 API 接口），且该第三方并未单独向个人信息主体征得收集个人信息的授权同意，则个人信息控制者与该第三方在个人信息收集阶段为共同个人信息控制者”。

金融行业标准《JR/T 0171-2020 个人金融信息保护技术规范》第6.1.4.2条h）项要求使用外部嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）进行信息共享与转让时，应定期检查或评估信息共享工具、服务组件和共享通道的安全性和可靠性，并留存检查或评估结果记录；第6.1.4.4条f）项要求应对外部嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）开展技术检测，确保其个人金融信息收集、使用行为符合约定要求；并对其收集个人金融信息的行为进行审计，发现超出约定行为及时切断接入。第6.2.3条则对与个人金融信息相关的SDK应当符合的安全要求作出了规定：与个人金融信息相关的客户端应用软件

及应用软件开发工具包（SDK）应符合JR/T 0092-2019、JR/T 0068-2020客户端应用软件有关安全技术要求，并在上线前进行安全评估。

2020年3月信安标委秘书处发布的《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》中也强调根据《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”， App开发者则应“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”，特别是“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，以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。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。”而SDK作为目前市场上App中最为常见的第三方接入方式，也应适用于上述规范性文件中关于第三方的规定。

2. 在研标准情况

自去年以来，第三方SDK安全受到各方关注，专门研究第三方SDK安全的标准项目也相继启动。通信行业标准方面，2019年共立项两个相关行业标准项目，分别是《移动应用软件SDK安全技术要求和测试方法》和《移动应用SDK安全指南》，前者在移动应用软件SDK安全威胁的基础上，依据国家相关法规，结合移动应用软件和第三方SDK行业发展现状，制定移动应用软件SDK安全管理要求、技术要求及测试方法；后者从SDK应用安全角度出发，明确移动应用开发设计中使用

第三方SDK的安全原则，提供对移动应用中第三方SDK安全评估和安全监测的方法和手段，梳理常见SDK类型及其业务场景、功能和权限，增强App开发者对恶意SDK的识别、检测和防范能力。国家标准方面，TC260全国信息安全标准化技术委员会发布了《网络安全标准实践指南 移动互联网应用程序（App）中的第三方软件开发工具包（SDK）安全指引（征求意见稿）》，有望期待第三方SDK标准正式出台。

（三）第三方 SDK 普遍应用的原因分析

一是接入第三方 SDK 可以大幅度提升使用者的开发效率，明显降低开发成本。特别是推送类、广告类等 SDK，往往能够帮助 App 开发者在无需了解技术细节的情况下快速实现某一特定功能，从而提高开发效率，缩短开发周期。这样，App 开发者也可以将精力放在商业模式的制定与运营上，提高整体效率。

二是 SDK 的易用性和灵活性较强，为 App 提供流畅及定制化的用户体验。SDK 通过创造一种简单的模式，简化代码、优化繁琐的集成工作，实现 API 的有效调用，配置简便、友好、灵活。在实际中，开发者的需求各异，可以通过集成不同类型的 SDK 快速实现预期功能，构建自定义应用，并为其用户量身定制体验，大大增加应用程序的多样性，提高 App 的用户留存率和使用频率。

三是 SDK 能够帮助提高 App 的兼容性，扩大用户使用范围。SDK 的接入可以解决 App 具体功能与各厂商机型的兼容性问题，免去与各厂商机型繁琐的硬件适配工作，让使用各种机型的用户都能够使用

App 的某一特定功能，解决 App 在各应用市场的投放中可能存在的渠道兼容问题。

二、 第三方 SDK 的主要安全问题及分析

随着四部门App违法违规收集使用个人信息专项治理行动的持续深入推进，原本“隐藏”在App身后的第三方SDK进入了监管部门及公众视野，其目前存在的一些安全风险及收集使用个人信息的合规问题，也随之浮出水面。

（一）第三方 SDK 自身安全性不容乐观

目前，已经发现的SDK安全漏洞包括http误用、SSL/TLS不正确配置、敏感权限滥用、身份识别、本地服务、通过日志造成信息泄露、开发人员失误、远程任意文件读取漏洞、越权调用未导出组件、XML外部实体注入漏洞等。第三方SDK的应用模式决定了其自身安全问题往往产生放大效应，嵌入第三方SDK的App越多，其安全漏洞的波及范围就越广，严重时甚至能够影响Android生态系统安全。以2017年12月爆出的某消息推送类SDK漏洞为例，因其存在可越权调用未导出组件漏洞，利用该漏洞便可实现对嵌入了该SDK的App进行多种恶意攻击，包括远程窃取用户终端设备中的敏感数据（通讯录、照片、账号密码等）、向终端用户推送虚假诈骗信息等。据悉，该漏洞共影响了七千多款App[4]，其中不乏市场主流产品，影响范围极广。

[4] http://www.freebuf.com/articles/system/156332.html，最后访问时间 2019 年 7 月 23 日。

（二）第三方 SDK 成为病毒传播新途径

当前，App 普遍使用第三方 SDK 的现象也吸引了一些不法分子的注意。通过制作、发布、吸引 App 嵌入含有恶意代码的第三方 SDK，造成短时间、大范围的病毒传播和感染；并且使用代码分离、动态代码加载等技术，能够实现远程控制恶意代码的执行，具有很强的隐蔽性和对抗杀毒软件的能力。2018 年 4 月，腾讯安全反诈实验室曝光了一款推送类的恶意第三方 SDK——“寄生推”，它通过预留“后门”，云端动态更新下发恶意代码包，对感染手机进行 Root 提权，静默安装恶意应用，推送恶意广告，牟取不法收益。“寄生推”采用的云端控制下发恶意代码的方式，绕过了一些应用市场的 App 安装包检测和杀毒软件的蜜罐检测。据腾讯统计，共有 300 多款 App 嵌入了“寄生推”，潜在受影响用户数超 2000 万。

（三）第三方 SDK 隐蔽收集个人信息问题逐步显现

第三方SDK作为独立的软件开发工具包，和App一样，具备收集个人信息的能力。但第三方SDK收集了哪些个人信息，用户往往难以感知，App开发者也未必完全知悉。近年来，已经发生多起第三方SDK隐蔽收集个人信息的安全事件。例如，2019年2月《华尔街日报》曝光Facebook在未告知用户的情况下，利用App Events统计分析工具从11个应用程序中收集用户个人敏感信息。此前，卡巴斯基实验室研究人员Roman Unuchek也曾披露，某些第三方SDK会主动收集用户姓名、年龄、性别、电话号码、邮箱地址、位置信息、设备信息等众多个人信

息和个人敏感信息，并以明文方式上传至远程服务器，且不论用户是否知情同意，明文传输本身已经加剧了个人信息的泄露风险[5]。

2020年3月《Vice》在一份报告中指出，Zoom App嵌入的Facebook的SDK会向Facebook传输用户手机型号、城市、广告标识符、IP地址等用户个人信息。即使用户没有Facebook账号，其个人信息也依旧会传输给Facebook。Zoom 的隐私政策中也没有告知Facebook SDK收集个人信息或Zoom App向Facebook SDK共享个人信息的情况。事件曝光后，Zoom不仅遭受较大的负面舆论影响，市值蒸发58亿美元，股价下跌超6%[6]，而且在美国加利福尼亚州遭到起诉。

三、 第三方 SDK 的主要合规问题及分析

本章将主要讨论聚焦于第三方 SDK 收集使用个人信息在法律层面的合规问题，有别于上一章关于第三方 SDK 隐蔽收集个人信息的安全问题。对于第三方 SDK 被普遍使用、大量获取个人信息的现状形成鲜明对比的是，第三方 SDK 的个人信息收集使用行为经常缺少法律层面的正当性，因此存在合规风险。这些合规风险的产生，由于第三方 SDK 提供者在用户和 App 关系中起到的角色不同—在 App“背后”处理数据或通过 App 接入、以自己名义提供服务—而有所差异。

（一）第三方 SDK 作为数据处理者时，主要合规问题分析

在某种情况下，App 终端用户在使用 App 服务过程中虽然会被 SDK

[5] http://www.sohu.com/a/228862055_100066938，最后访问时间 2019 年 7 月 23 日。

[6] https://3g.163.com/news/article/FA83BC0Q05502ZGU.html，最后访问时间 2020 年 4 月 28 日。

直接收集个人信息，但用户自身对这类 SDK 的存在是无感知的，例如终端用户在使用 App 内的语音通话功能时被嵌入该 App 的语音分析 SDK 收集语音信息，用户是无法知悉其个人信息被哪家语音 SDK 企业收集、使用和存储了。

如果 App 与第三方 SDK 之间约定，App 开发者是数据控制者，第三方 SDK 提供者是受 App 委托的数据处理者，那么在私法层面上第三方 SDK 提供者将无法与用户直接建立“合同”关系，也就无法以自己的名义就收集使用用户个人信息的行为获得个人信息主体的同意。此时，第三方 SDK 提供者收集使用个人信息的正当性依据来自于：（a）App 开发者就该等数据的收集、使用和“分享”获得用户的同意；以及（b）App 开发者给予的委托处理数据之授权，条件（a）和（b）缺一不可。

然而，现实情况是，第三方 SDK 所收集和使用的个人信息及相关共享行为，很多 App 开发者并没有通过隐私政策或弹窗提示等方式获得用户的“同意”，显然也就无法满足（a）项条件；同时，为满足 App 的便利、便捷开发需求，第三方 SDK 提供者与 App 开发者往往通过第三方 SDK 提供者的开放平台，在线签署开发者服务协议来约定双方的权利义务，鲜少有关于委托处理数据方面的专门协议或特别规定，也就难以算作协议双方之间的有效“授权”，（b）项条件也未必满足。此外，目前大多数 App 开发者不会对第三方 SDK 收集了那些个人信息进行技术验证，此种情况下的第三方 SDK 的数据收集和处理活动对于 App 开发者而言相当于一个“黑盒子”，缺乏透明度，如果被诉侵犯个人用户隐私的， App 开发者或者 SDK 提供者将可能承担举证责任

倒置的风险。[7]

（二）第三方 SDK 作为数据控制者时，主要合规问题分析

在某些情况下，接入应用的 SDK 是以自己的名义向 App 用户提供服务的，比如 App 用户通过激活一个 SDK 接口而调用或者启动了该用户已安装的另一个 App 的服务功能。此时，第三方 SDK 提供者能够拥有独立的“数据控制者”身份，因为第三方 SDK 提供者有机会将自身品牌进行露出，用户对其使用的是哪家企业实际提供的特定服务是有明显感知的。此时应采用三重授权原则，即“【用户-平台 1】+ 【平台 1-平台 2】+ 【用户-平台 2】”可以解决 SDK 获取 App 用户个人信息的正当性问题。但是如果第三方 SDK 提供者在“同意”范围之外处理用户个人信息的，则该等数据处理的行为则显然不具备法律正当性，需要承担超出授权范围的相关责任。

现实情况中，也有少数第三方 SDK 提供者在 App 开发者合作委托其处理数据时，也坚持要求获得“数据控制者”身份，以此确保自身对数据使用目的、方式的“自主权”，并且在获取后也不会根据 App 开发者的指令进行销毁或者交还数据。其背后的动力来源于第三方 SDK 提供者汇聚多源数据后，更需要能够自主决定如何处理数据，进而实现数据变现。此时，即使第三方 SDK 有可能变成“数据控制者”

[7] 例如在庞理鹏诉北京趣拿信息技术有限公司、中国东方航空股份有限公司案件中，被告东航主张其通过与中航信签订《航空公司服务协议》，委托中航信为东航提供民航商务数据网络服务。由于原告（个体消费者）无法也没有能力拿到相关证据证明其个人信息是东航或趣拿公司泄露的，二审法院认为原告提供的证据已经足以表明其完成了“高度可能泄露”的举证责任，被告如果无法举证证明其不存在泄露庞理鹏个人隐私信息的，被告应该承担赔偿责任。因此，该案其实适用了举证责任倒置。

的身份，由于第三方 SDK 依然不直接面对用户，需要 App 开发者提供代为告知用户（如增加《第三方 SDK 收集个人信息情况》的单独页面、告知链接、弹窗告知变更隐私政策等）并获得用户“同意”，会增加 App 开发者的运营成本，多次弹窗还会影响用户体验。App 开发者还需要基于合同相对性，针对第三方 SDK 收集使用用户个人信息的情况，对用户承担合同法下的违约责任以及网络安全法下的行政责任，同时还有义务将各项合规义务传导至第三方 SDK 提供者。

四、 第三方 SDK 管理的域外经验

（一）欧盟的第三方 SDK 管理经验

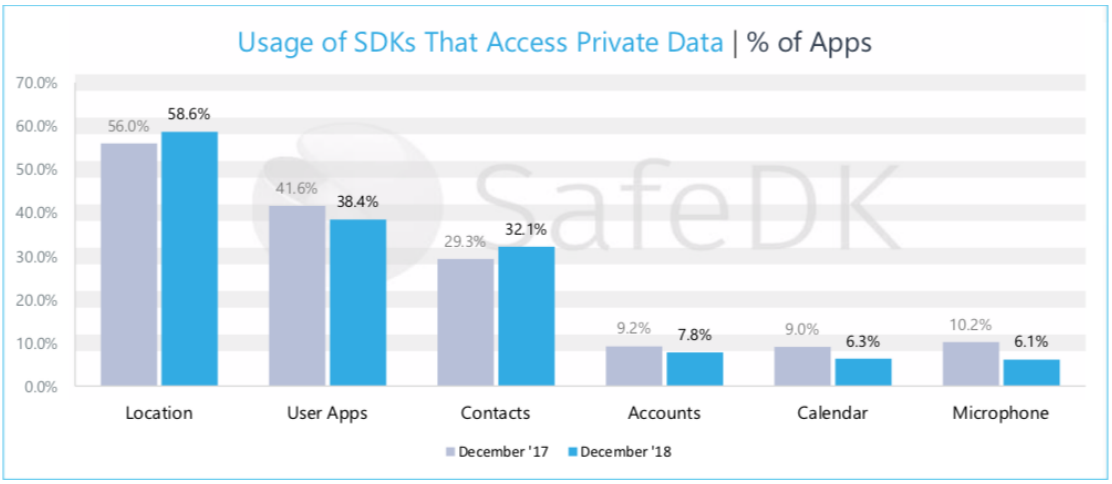
欧盟背景下对第三方 SDK 提供者收集、处理用户个人信息的行为是通过欧盟《通用数据保护条例》（General Data Protection Regulation,以下简称“GDPR”）进行规制的。[8]

1. 第三方 SDK 提供者在 GDPR 中的定位既可能是数据控制者也可能是数据处理者

现实中，根据本报告第一章对 SDK 数据收集使用情况的描述以及 SafeDK 调研 190000 个 App 后发布的《2018 SDK 数据使用趋势年度报告》中的数据，SDK 会通过调用 App 提供的数据，对用户个人信息（包括位置信息、联系方式、账户名称，见图 7）进行收集、缓存并上报至 SDK 服务端，即 SDK 提供者的行为构成对数据的收集和处理并应受

[8] 根据 GDPR 第 4（1）条的定义，“个人数据”是指任何已识别或可识别的自然人的相关信息，包括姓名、地理位置数据等。任何对该等数据的收集或处理均受到 GDPR 的规制。

到 GDPR 的规制。



（来源：SafeDK – 2018 SDK 数据使用趋势年度报告）

图 7 SDK 通过 App 收集的数据类型统计

GDPR 对于数据处理的义务与责任问题是通过各方在具体数据处理中担任的角色 – 数据控制者、数据处理者 – 来分配的。根据 GDPR 第 4 条的定义，数据控制者是指决定处理个人信息的目的和方式的自然人、法人、公共机构或者其他机构，数据控制者可以为多个。数据处理者是指代数据控制者处理个人数据的自然人、法人、公共机构或者其他机构。

在 App-SDK 关系中，App 开发者是数据控制者以及处理用户个人数据的首要责任人，SDK 提供者是 App 分享数据的第三方（即数据处理者）；也有可能 App 开发者与第三方 SDK 提供者均是以自己名义自行决定处理数据的目的与方式的数据控制者。第三方 SDK 提供者具体担任什么角色需要在个案中进行分析。

例如，欧洲法院在 2019 年 7 月 29 日发布的 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV 一案的指导建议中表示，网

站运营商在其网站上嵌入 Facebook 的点赞按钮，并将访问者个人数据收集、传输给 Facebook，可能与 Facebook 一同构成数据的共同控制者（joint-controllership），网站运营商原则上对 Facebook 之后对个人数据的单独处理行为不承担控制者的责任。

本案中的数据的收集和处理进程可以分为两个阶段：其一，Fashion ID 收集并传输给 Facebook 的阶段;其二,传输后由 Facebook 独立处理数据的阶段。就第一个阶段而言，Fashion ID 和 Facebook 共同决定了数据收集和处理的目的和方式(待德国杜鲁尔多夫高级地区法院进一步调查后确定相关细节），因此可以认定 Fashion ID 就本案中第一阶段的数据收集和传输行为与 Facebook 一同构成共同控制者。

根据 GDPR 的规定，不论第三方 SDK 提供者担任的是何种角色，其在个人数据的收集或处理之前，应取得 GDPR 第 6 条规定的处理个人数据的合法依据，并且，处理数据时应符合 GDPR 第 5 条规定的基本原则等要求。

（1）第三方 SDK 提供者处理个人数据前需获得数据主体的同意

GDPR 第 6 条第（1）款规定的处理的合法依据包括:

“只有满足至少如下一项条件时，处理才是合法的，且处理的合法性只限于满足条件内的处理:

（a）数据主体已经同意基于一个或多个特定目的而对其个人数据进行处理;

（b）处理对于履行某项数据主体为当事人的合同是必要的，或

者在签订合同前基于数据主体的请求而进行的处理;

（c）处理是为履行其法定义务所必需的;

（d）处理对于保护数据主体或另一个自然人的核心利益所必要的;

（e）处理是数据控制者为了公共利益或应官方机关要求而进行的;

（f）处理对于控制者或第三方所追求的正当利益是必要的，这不包括需要通过个人数据保护以实现数据主体的优先性利益或基本权利与自由，特别是儿童的优先性利益或基本权利与自由。”

此外，如果处理的数据涉及 GDPR 第 9 条规定的敏感数据（包括有关种族、宗教、政治观念、为识别特定自然人的基因、生物数据），则必须获得数据主体的明示同意。

如本报告第一章所介绍的，第三方 SDK 提供者收集、使用个人数据是为了提高自身或者 App 的服务，而非（b）-（f） 项规定的特殊情况。换言之，如果第三方 SDK 确有处理数据的行为，则只能根据第（a）项，即获得用户的同意。GDPR 在第 4（11）和 7 条规定了“同意”的构成要件: “自由做出、特定、知悉、不含混”，即告知用户哪些信息将被处理，被谁处理，以及基于什么目的被处理，且不得采取默认同意的方式。

（2）第三方 SDK 获得用户同意的方式

因为第三方 SDK 集成于 App 中，面对用户，更直接向其提供服务的是 App，而非第三方 SDK，故第三方 SDK 提供者想要获得用户同意

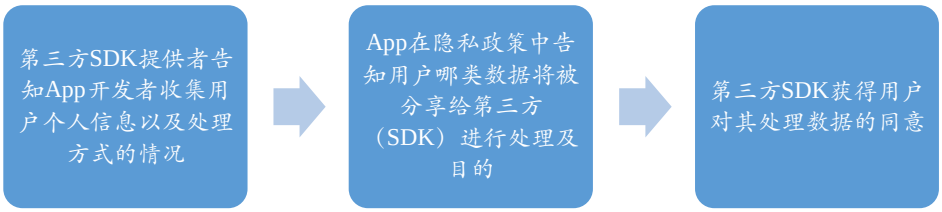
无法绕开 App，只能通过 App 才能进行。在这种情况下，对内可以分三步来完成：

第一步：第三方 SDK 提供者告知 App 开发者 SDK 将要处理用户哪些个人信息；

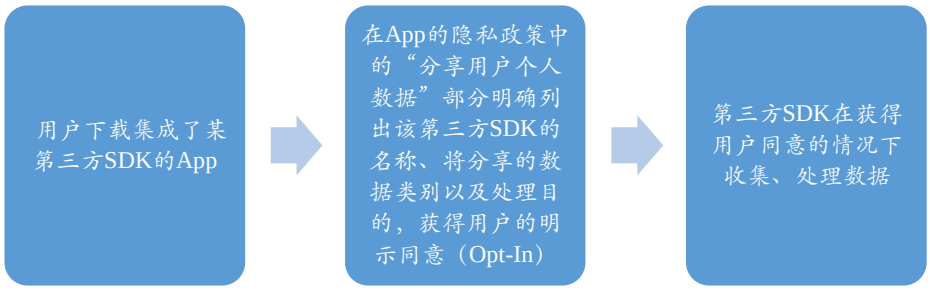
第二步：App 开发者在隐私政策的“与第三方分享数据”一节中说明，哪些数据将由第三方 SDK 提供者收集，或者哪些数据类型是由 App 共享给第三方 SDK 提供者以及该等处理的目的；或通过在 App 的隐私政策中跳出 SDK 隐私声明的链接，由 SDK 发布单独的隐私声明来获取用户的同意；

第三步：第三方 SDK 通过 App 获得用户对 SDK 处理数据的同意。

以下通过图例将第三方 SDK 获取用户同意的三个步骤更清晰、直观地进行描述：



对外呈现的形式为：



2. 第三方 SDK 提供者未获得用户同意收集数据将受到监管处罚

就监管机构设置而言，整体上，由欧盟数据保护委员会（European Data Protection Board, “EDPB”）制定指南性文件，确保 GDPR 在欧盟各国执法的统一性，协调各国数据保护机构，作为最高裁决者对涉及多国争议发布具有拘束力的决定；就各个国家而言，由各国设立的独立数据保护监管机构（DPA）依据 GDPR 对违规企业进行执法，例如英国信息专员办公室（Information Commissioner’s Office, “ICO”），法国信息监管委员会（Commission Nationale de l’Informatique, “CNIL”）等。因此，如果第三方 SDK 提供者未经用户同意自行处理用户个人数据，第三方 SDK 提供者将可能因违反 GDPR 第 6 条处理须有合法依据以及第 5 条规定的数据处理的合法性、透明性而承担法律责任，由各国的 DPA 进行执法，而 EDPB 可能会基于“一致性”原则进行统一协调。

（二）美国的第三方 SDK 管理经验

美国在联邦层面没有统一的个人信息保护法，而是呈现出行业化和各州分散立法的特点，如 1914 年针对损害消费者利益的商业行为颁布《联邦贸易委员会法案》[9]、1996 年颁布的《健康保险流通与责任法案》、1998 年针对未满 13 周岁的美国公民颁布的《儿童在线隐

[9] 1938 年《惠勒—利法》、1950 年《塞勒—凯弗维尔法》和 1980 年《反托拉斯诉讼程序改进法》对《联邦贸易委员会法》第 5 条、第 7 条进行修改。

私保护法案》、1999 年颁布的《金融服务现代化法案》等。2018 年 6 月颁布的《加州消费者隐私保护法案》（California Consumer Privacy Act，以下简称“CCPA”），从州层面上体现了民众对保护个人隐私的重视以及美国关于个人数据保护的一些最新理念。鉴于CCPA在美国有较大的影响力和代表性，以下将以 CCPA 为例，进行重点分析。

1. 第三方 SDK 提供者在 CCPA 的定位是收集或代为收集，并自行或与他人共同决定处理目的的“企业”

与 GDPR 不同，CCPA 并未区分数据控制者或数据处理者。根据CCPA第1798.140（c）的规定，只要第三方SDK提供者收集或代为收集消费者个人信息，并自行或与他人共同决定个人信息的处理目的，且满足年总收入超过 2500 万美元，或为商业目的购买、出售、分享超过50000条消费者、家庭或设备的个人信息，或通过销售消费者个人信息取得的年收入超过总收入的 50%，即为受到 CCPA 规制的“企业”，承担相应的义务并履行相应的责任。

CCPA对于个人信息（personal information）的定义比GDPR的个人数据（personal data）更为广泛，是指能够直接或间接识别、描述与特定的消费者或其家庭相关或合理相关的信息。但与 GDPR 对处理任何个人数据均需要获得明示同意（Opt-In）不同，CCPA对个人信息的出售、披露进行规制，且采用的是以Opt-Out为主、Opt-In为辅的模式。

（1）第三方 SDK 提供者收集消费者个人信息只需要告知，无需

获得同意

在 Opt-Out 机制下收集个人信息无需事先征得用户的同意只需要告知[10]，但在后续出售个人信息过程中需要让用户完全知情（透明性）以及给予用户更多的选择权（可控性）比如行使拒绝的权利。因此，第三方 SDK 提供者在收集个人信息前或收集时应当告知（inform）个人信息主体其所收集的个人信息的类别、内容和使用目的，但无需征得个人信息主体的明示同意。

（2）SDK 提供者向第三方出售个人信息需向消费者提供免于其个人信息被出售的选择退出权

CCPA 第 1798.120（a）规定：“消费者有权在任何时候指示一个拟将其个人信息出售的第三方，不得出售其个人信息”。因此，当存在 SDK 提供者出售消费者的个人信息时，CCPA 赋予消费者拒绝的权利（Opt-Out）。SDK 提供者在收到消费者的指示起即不得再出售该消费者的个人信息，除非随后得到该消费者就其个人信息出售的明示授权。

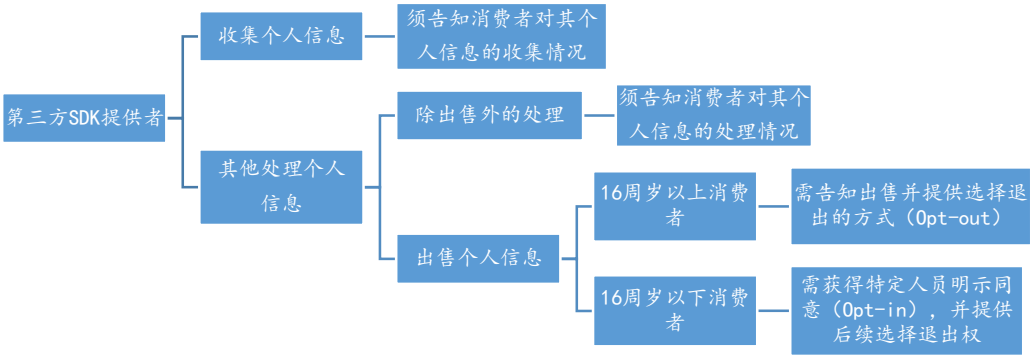
（3）第三方 SDK 提供者出售 16 周岁以下消费者的个人信息前需获得明示同意

对于 16 周岁以下消费者个人信息的出售，CCPA 采取的是获得特定人员明示同意（Opt-In）的模式，即企业有请求用户明示授权的义

[10] CCPA 第 1798.100（b）规定：“收集消费者个人信息的企业应当在收集时或者收集前告知消费者所收集个人信息的类别以及个人信息的使用目的。在未向消费者提供符合本节要求的告知情况下，企业不得收集其他类别的个人信息，或者将所收集个人信息用于其他目的。”

务。11 故在 App-SDK 场景下，对于 16 周岁（含）以上的用户，第三方 SDK 提供者仅需通过 App 告知用户将要出售其个人信息，并在后续出售信息时提供用户拒绝的方式即可，但对于 16 周岁以下的用户，则需要取得法案所规定人员的明示授权才能出售其个人信息。

以下通过图例将 CCPA 规定的告知义务和获得同意的义务更清晰、直观地进行描述：



（4）第三方 SDK 提供者告知以及获得同意的方式

如前所述，第三方 SDK 提供者想要告知或就出售行为获得特定消费者同意无法绕开 App，只能通过 App 来进行。在这种情况下，对内也需分三步来完成：

第一步：第三方 SDK 提供者告知 App 开发者 SDK 将要收集、处理消费者的哪些个人信息；

第二步：App 开发者在隐私政策的“与第三方分享个人信息”一节中告知或通过在 App 的隐私政策中跳出 SDK 隐私声明的链接，由

[11] CCPA 第 1798.120（d）项规定，“尽管有第（a）项规定，如果企业明知消费者年龄小于 16 岁，企业不应出售该消费者的个人信息，除非在 13 至 16 岁之间的消费者明示授权，或年龄小于 13 岁消费者的父母或监护人明示授权企业可以出售该消费者个人信息。企业任何故意忽视消费者年龄的行为应被视为其已明确知晓该消费者年龄。”

SDK 发布单独的隐私声明来告知哪些个人信息将会由第三方 SDK 提供者收集，或者哪些信息类型是由 App 共享给第三方 SDK 提供者以及该等处理的目的。

第三步：如涉及消费者个人信息的出售，则需要明确告知消费者的选择退出权和行使方式，如特别涉及 16 周岁以下消费者个人信息出售，则须在出售前获得 CCPA 规定的特定人员的明示同意。

以下通过图例将 SDK 获取用户同意的三个步骤更清晰、直观地进行描述：

对外呈现的形式为：

2. 第三方 SDK 提供者未履行告知义务、就出售未提供选择退出权或获得特定人员同意将受到监管处罚

就监管机构设置而言，对第三方 SDK 提供者的规制是联邦层面和

州层面双轨监督体系。在联邦层面，主要由联邦贸易委员会(Federal Trade Commission，“FTC”)依据《联邦贸易委员会法案》对离线和在线侵犯消费者隐私和数据安全问题进行概括监管;同时对其制定的《儿童在线隐私保护法案》等法案进行执法。在州层面，由各州的执法机构根据各州隐私保护法案（如有）进行执法，例如加利福尼亚州司法部（California Department of Justice）根据CCPA对相关企业进行执法。因此，如果第三方SDK提供者未履行告知义务、就出售消费者个人信息未提供选择退出权或获得特定人员同意，将会受到FTC根据联邦部门法,以及州司法部根据州隐私法案的双轨监管处罚。

五、 针对我国第三方SDK管理的相关建议

本报告通过分析第三方SDK存在的安全问题和法律合规问题，结合国外管理经验和实践做法，提出如下建议:

（一）尽快完善相关法律法规，明确相关主体的责任义务

从2019年至本报告发布期间的法律进程中，虽在国家互联网信息办公室发布的《数据安全管理办法（征求意见稿）》第三十条中提及“接入其平台的第三方应用”，看似对第三方接入开始从法规层面上做规制了，但是否包含App嵌入第三方SDK的情况尚不明确，有可能会被理解为仅涉及平台与第三方应用之间的关系，只是暗示平台需重视第三方SDK的管理。2019年3月，国家互联网信息办公室、工业和信息化部、公安部、市场监管总局（以下简称“四部委”）成立的App违法违规收集使用个人信息专项治理工作组发布的《App违法

违规收集使用个人信息自评估指南》第 21 条则较为明确地点明“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”；以及 2020 年 7 月 22 日，由全国信息安全标准化技术委员会发布的《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》第 21 条规定“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”均将整治目标直指 SDK 了。在 2019 年 11 月 App 违法违规收集使用个人信息专项治理工作组发布的《App 违法违规收集使用个人信息行为认定方法》同样规定，以下行为可被认定为“未明示收集使用个人信息的目的、方式和范围”：“1. 未逐一列出 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”；以下行为可被认定为“未经同意向他人提供个人信息”：“1. 既未经用户同意，也未做匿名化处理，App 客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息；2.既未经用户同意，也未做匿名化处理，数据传输至 App 后台服务器后，向第三方提供其收集的个人信息；3. App 接入第三方应用，未经用户同意，向第三方应用提供个人信息”。由此通过要求 App 逐一列出并明示所嵌入的第三方代码收集用户个人信息的目的、方式和范围并要求获得用户同意，更好地落实和规范 “三重授权”原则。

尽管上述法律进展相较于 2018、2019 年已经有显著的提升，但是，我国仍然欠缺现行有效的法律或者法规层级的文件，对第三方 SDK 的责任与义务、安全要求进行规定。建议在已经列入立法规划的《个人信息保护法》或正在公开征求意见的《数据安全法（草案）》《数据安全管理办法（征求意见稿）》等法律和行政规章中增加委托第三方处理数据或者共享数据给第三方（含 SDK 场景）进行关注（目前《数据安全法（草案）》中仅规定收集使用以及对国家机关委托他人存储、加工政务数据进行规定），参考国外实践，也明确在委托或者共享数据时的合规要求，如 App 开发者与第三方 SDK 提供者等网络运营者在获取、共享、使用用户个人信息时，需有具体的、清晰的和正当的目的，给予用户知情权和控制权，并且获得用户的同意；明确委托方与处理方或者数据共享方与数据接收方（如 App 开发者和第三方 SDK 提供者）分别的法律义务与责任。如 App 开发者作为网络运营者需对第三方 SDK 提供者数据请求的必要性进行评估，并且可以拒绝不必要的个人信息请求，在发现超出约定行为时及时采取措施，对第三方 SDK 提供者数据安全管理情况进行必要监督等。另外，建议在法律法规中引入惩罚性条款，比如须对 App 开发者超出 SDK 提供者的请求范围提供个人信息，以及 SDK 提供者超出授权范围和使用目的收集使用个人信息的行为进行处罚。

（二）App 开发者需要积极履行数据合规义务

1. 厘清 App 开发者与第三方 SDK 的合作关系，完善《隐

私政策》或者制定单独的《第三方 SDK 收集使用个人信息声明》

（1）完善《隐私政策》或者制定单独的《第三方 SDK 收集使用个人信息声明》

如前所述，App 开发者与第三方 SDK 的合作关系会根据不同功能的 SDK 以及其是否能实际得到在用户端的直接露出效果，而存在不同的身份认定。

当第三方 SDK 无法直接向用户露出自己，只是受 App 开发者委托，作为数据处理者时，在 App 的《隐私政策》一委托处理章节建议介绍 App 委托第三方处理个人数据的情况，此时的披露可以不具体到某个 SDK 的类型，但是最好可以说明委托哪类企业进行处理哪类数据，并需要承诺与 SDK 提供者之间签署了必要的保密协议与数据处理协议，以确保数据处理行为的安全可靠。

当第三方 SDK 可以直接透过 App 露出自己品牌时，App 开发者更容易让 SDK 提供方独自成为个人信息的数据控制者，故，应当在 App《隐私政策》的共享章节或者展示 SDK 的专门章节介绍 App 接入了哪些具体的第三方 SDK、向这些第三方 SDK 共享个人信息的目的、功能、范围、开启权限等情况、第三方 SDK 的隐私政策情况（如有）；如果在披露第三方 SDK 的隐私政策时，可实现跳转至第三方 SDK 官方服务页面的，建议向用户直接展示该第三方 SDK 的《隐私政策》。此时需要注意的是，披露的颗粒度建议具体到每个实际提供服务的 SDK。

另外还有一类特殊情况需要说明，即有些开发者自己既开发 App

也开发 SDK，并且自己的 App 还接入自己开发的 SDK 的，如果运营主体是同一个的（注意与 SDK 由 App 运营者的关联公司运营相区别），我们认为可以豁免在第三方 SDK 共享章节中对该 SDK 进行列举，因为他本质上不属于开发者向第三方共享数据，但建议应一并列入 App 收集使用个人信息章节中的各项功能处，此类由同一公司开发的 SDK 可以视为 App 业务功能的一种延伸，只是部分功能因使用频率高功能高度重合，因此提前封装好可以直接嵌入新开发的 App 而已。

（2）征得用户的同意

如果第三方 SDK 自己不能露出品牌的，此时考虑更多地是因其采用了委托处理的模式，那么则需要通过 App 征得用户的授权同意（如涉及个人敏感信息的，则须征得明示同意），即由 App 承担接入方的对外统一责任，然后 App 再根据数据处理协议的约定向第三方 SDK 追究合同违约责任。

如果第三方 SDK 自己可以直接露出品牌的，App 可在其隐私政策中将第三方 SDK 的身份以及其收集个人信息的情况全部列明，用户通过点击 App 隐私政策，实现对 App 隐私政策收集使用个人信息以及 SDK 收集使用个人信息进行一并同意，再通过 App 开发者与 SDK 提供方签署合同的方式，真正实现“三重授权”的机理。如果 App 开发者采用的是直接跳转链接至第三方 SDK 隐私政策的，那么在跳转过程中也可以设置弹窗等方式请用户选择是否同意 SDK 的隐私政策，由 App 提供方在后台做记录。如果用户不同意第三方 SDK 隐私政策的，那么需要切断对第三方 SDK 的接入，这种形式的授权同意相对更加明确，

并且可明晰不同主体间的责任。但后面一种模式，运营成本相对也会较高，多一次弹窗的出现将有可能出现用户流失率升高、SDK 被拒绝同意后相关功能无法使用等情况，企业可以做一个维持业务与符合合规之间的最大平衡。如果 App 开发者采用的是由第三方 SDK 自行征得用户同意的，则由第三方 SDK 保障用户同意机制有效以及记录同意行为。

（3）征得用户同意的方式

就 SDK 收集使用个人信息征得用户同意的方式而言，可以根据 SDK 的身份设计不同深浅度的同意方案，我们提出以下四种方案供大家参考:

方案一：可以直接露出自己服务/品牌的第三方 SDK，由 App 在隐私政策中展示每一个第三方 SDK 隐私政策的网址并通过跳转链接向用户进行展示，并且，如前所述，可以考虑通过弹窗征得用户对第三方 SDK 隐私政策的同意。这种做法的优点在于，用户对于同意 SDK 还是 App 隐私政策的区分能够比较清晰，缺点在于当接入的第三方 SDK 非常多时，需要用户逐一阅读并确认会比较不现实。因此，适中的做法为，当 1）App 接入的 SDK 数量没有那么庞多，2）第三方 SDK 都能够在自己的官网上展示隐私政策，并且 3）App 开发者有能力设计弹窗或单行页面时，在用户点击阅读某一第三方 SDK 链接时，问询用户是否“不同意”该 SDK 的隐私政策，以实现做“减法”的功能，没有点击的视为在勾选 App 隐私政策时一并同意 SDK 的隐私政策。只要用户同意了 App 隐私政策的，即视为一并同意 SDK 的隐私政策并可

以由 SDK 收集用户个人信息。

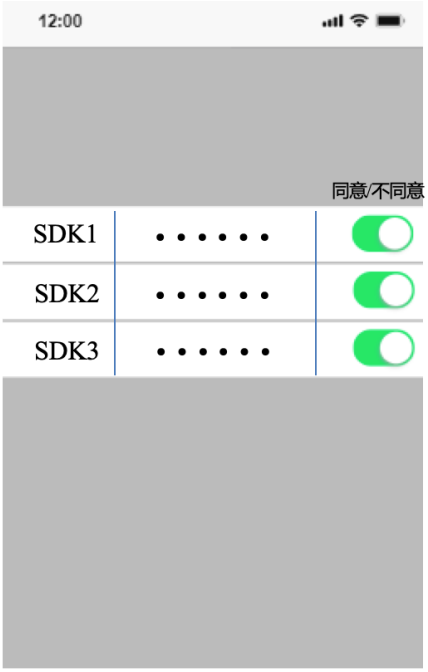


图 8 SDK 征得用户同意方式的示例

方案二:在 App 登录、注册页面，与 App 隐私政策平行放置《第三方 SDK 收集使用个人信息声明》,并设置单独勾选框(与下述第(3)点形成区分)，请求用户勾选同意。对于只勾选 App 隐私政策没有勾选第三方 SDK 隐私政策的，App 开发者不对第三方 SDK 进行接入，SDK 提供方也不收集用户个人信息。此做法的优点在于，可以实现 SDK 隐私政策与 App 隐私政策分开勾选，不搅裹在一起，让用户拥有更加自主、充分的选择权，也可以对信息的告知增强透明度。缺点在于，如果用户只勾选了 App 隐私政策而不勾选 SDK 隐私政策的，会对 SDK 提供方的业务有较大的影响与冲击。并且，如果 SDK 的类型较多时，如果用户不同意某一类第三方 SDK 接入的，却可能没有办法剔除不同意的这一类，不得不对整个 SDK 隐私政策的勾选框不选择，这样也会影响其他第三方 SDK 的接入。

方案三：在 App 登录、注册页面，通过弹窗或者一个勾选框，将第《三方 SDK 收集使用个人信息说明》与 App 的《用户服务协议》、《隐私政策》的所有文件，一并征得用户勾选同意。这种方式处理的优点是，可以克服第（2）点中所提到的，因用户不选择可能对 SDK 提供方业务有下滑的影响，但是缺点是，与 App 的《隐私政策》和《用户服务协议》放在一起让用户选择同意，也存在有“绑架”同意之嫌，让用户实现选择自主权又流于表面形式了。相反，如果用户因不同意个人信息被某一第三方 SDK 收集使用，因不可以分开授权，所以，如果一次性拒绝同意的情况下，有可能 App 也无法使用了。

方案四：将第三方 SDK 收集个人信息情况作为 App 隐私政策的一部分，列明所有第三方 SDK 的情况告知用户并征得同意。这种模式是目前各大企业比较常用的模式。区别于以前不批露，现在一些头部互联网企业以及合规实践遵守较好的中小企业，也已经将接入的第三方 SDK 在隐私政策中通过列表或者在单独静态页中放置列表的方式向用户详细告知第三方 SDK 的类型、名称、接入的目的、使用方式以及收集信息的范围。这种方式的好处在于，操作比较简便，也没有额外的开发工作，上线实施非常快。缺点在于，虽然用户对于 App 隐私政策的点击同意，视为获得到“三重授权”，但实际上用户不一定会去详细看冗长的隐私政策，即使看了也不一定再点击静态页去查看里面所列举的第三方 SDK 的信息。如果不同意第三方 SDK 接入收集其个人信息的，只能选择不使用 App，那么实际是对 App 开发者的业务损伤。因此，App 开发者可以考虑在隐私政策中区分并列举必需类 SDK；对

于非必需类 SDK 通过链接到 SDK 关闭的单行页面实现用户的撤回同意机制以弥补同意时的不足，确保用户同意是自由且具体的，具体可参见下述第五点建议提供的用户自主调控 SDK 的界面设计。

当且仅当用户明确、自由地表达同意后，该用户个人信息才可以被收集或共享给第三方 SDK 提供者。否则，App 开发者与第三方 SDK 提供者需要共同承担未经授权或者超出授权同意而收集使用用户个人信息的责任。

2. 完善合作协议，明确约定第三方 SDK 提供者能够直接采集或 App 共享的个人信息范围

在合作协议中应当:

-明确双方的身份（即第三方 SDK 承担的是数据控制者还是数据处理者的角色）;

-明确数据处理的范围及情况，包括但不限于收集信息的目的、方式、范围、数量、存储时间、个人信息进一步对外提供的情况、个人信息出境情况等，以便 App 开发者履行评估第三方 SDK 提供者收集个人信息清单中所列信息必要性的义务;

-明确处理个人信息的安全、合规机制，包括但不限于个人信息主体权利响应机制、对个人信息在存储和传输等环节采取的安全、加密措施、日志记录、权限控制等内容，以便 App 开发者评估第三方 SDK 的安全、合规性能;

-根据第三方 SDK 在收集处理个人信息时的身份不同，明确双方各自承担的法律义务与责任，包括但不限于第三方 SDK 提供者配合响

应个人信息主体的行权请求、在处理个人信息时应当提供的安全保护水平、数据泄露时的应急处理、合作结束后作为委托处理者的第三方SDK 配合 App 开发者删除从 App 处获取的个人信息等。

3. 强化第三方 SDK 收集、使用个人信息活动的安全管理

App 对合作第三方 SDK 的安全管理体现在事前审核、事中监督、事后保障三个环节。

事前审核，即在建立合作关系时、供应商入库环节中增加安全及合规审核，以及对第三方 SDK 提供者的尽职调查与数据安全能力评估、响应个人信息主体请求机制;

事中监督，是指在合作过程中如发现第三方 SDK 违规调取用户个人信息、出售用户个人信息的情况需要及时处置，落实惩罚机制;

事后保障，即在合作后期或合作终止但用户个人信息尚未被处置前，App 开发者仍需保障个人数据安全的连带义务和责任。此外，合作过程中，建议 App 开发者针对不同类型的第三方 SDK 提供者，建立SDK 收集、使用个人信息活动的评估机制，定期对第三方 SDK 提供者进行数据安全保护能力鉴定和技术检测，对第三方 SDK 收集、处理个人信息情况进行动态监测等。评估机制从技术方法上应重点关注 SDK 收集、使用个人信息范围的必要性、数量与评估 SDK 所收集的用户个人信息和向自己所提供服务的关联程度，对于与服务功能无关的收集和使用个人信息的类型，建议予以取消授权，并视严重情况终止与其合作。同时，根据技术可实现性，对第三方 SDK 提供者收集的信息与App 开发者收集的信息进行区分。

4. 定期对第三方 SDK 提供者的数据安全保障能力进行审计

建议 App 开发者指定独立的数据安全审计员或者第三方专业机构对第三方 SDK 提供者的数据安全保障能力进行定期检查，如是否采取完备的安全措施（如加密、脱敏、分类分级等）以保障数据处理过程中的安全性；是否建立严格的数据访问权限管理机制，降低人为泄密的风险；是否对数据处理活动进行记录，以检测不当访问处理数据的行为等。

5. 在 App 中加入用户自主调控 SDK 开启或者关闭的界面

当第三方 SDK 提供方为控制者时，建议 App 开发者在 App 内设计相关 SDK 的控制者和管理页面，使得用户可以自主调控、开启或关闭 App 中所嵌入的收集、处理用户个人信息的 SDK（在隐私政策中批露为非必需类的 SDK）。相关页面设计可以参考下图:

图 9 App 内设计相关 SDK 的控制者和管理页面

（三）第三方 SDK 提供者需要加快构建数据安全合规体系

1．理清 SDK 本身收集、处理个人信息的情况以及与 App 的合作关系，制定、公开隐私政策或其他个人信息收集使用规则

从前述分析来看，第三方 SDK 提供者不论作为数据控制者，还是作为数据处理者，都需要向 App 开发者及最终用户公开其个人信息收集使用规则，具体形式可以是除 App 开发者的隐私政策说明以外，在自己的网站或者开放平台中放置隐私政策。在隐私政策中，第三方 SDK 提供者需要准确说明其提供的 SDK 在个人信息处理过程中担任的角色、提供的功能，每类功能对应收集的个人信息类型，以及收集、使用个人信息的具体目的、方式、范围。关于隐私政策的具体要求，可以参考《GB/T 35273-2020 信息安全技术 个人信息安全规范》。

2. 制定开发者协议，要求 App 在接入 SDK 时在 App 的隐私政策中披露 SDK 收集、处理个人信息等情况

根据前述的分析，由于 SDK 是嵌入在 App 中，第三方 SDK 提供者作为数据处理者或共同数据控制者时，需要依赖 App 开发者获得收集、使用个人信息的法律正当性事由。为此，第三方 SDK 提供者与 App 开发者开展合作前，第三方 SDK 提供者需要通过开发者协议、服务协议，明确双方在个人信息保护及数据安全方面各自承担的义务和责任，特别是明确 App 开发者有义务通过隐私政策等形式明确告知个人用户第三方 SDK 收集个人信息的类型、目的、使用规则等，并获得个人用户同意。

3. 制定数据处理协议等合作协议，约定个人信息处理的范围以及双方责任

App 与 SDK 之间不同的角色定位决定了双方享有的权利义务不同。为此应当通过合同的形式约定双方的合作模式以及收集、处理个人信息时承担的角色。在合作协议中应当:

-明确双方的身份(即 SDK 是数据控制者还是数据处理者的角色);

-明确数据处理的范围及情况，包括但不限于收集信息的目的、方式、范围、数量、存储时间、个人信息进一步共享情况、个人信息出境中国大陆之外情况等，并约定不会超出用户的授权范围收集、处理个人信息;

-明确处理个人信息的安全、合规机制，包括但不限于个人信息主体权利响应机制、对个人信息在存储和传输等环节采取的安全、加

密措施、日志记录、权限控制等内容，以便 App 开发者评估第三方 SDK 的安全、合规性能；

-根据 SDK 在收集处理个人信息时担任的是控制者还是委托处理者的不同，明确双方各自承担的法律义务与责任，包括但不限于第三方 SDK 提供者配合响应个人信息主体的行权请求、在处理个人信息时应当提供的安全保护水平、数据泄露时的应急处理等。

4. 加强与 App 开发者合作数据合规管理

第三方 SDK 提供者可以建立对 App 开发者在合作前的数据合规尽职调查机制、合作过程中的合规巡查监测机制，审计 App 的用户协议、隐私政策是否披露了 SDK 的相关信息以及收集、使用个人信息的情况、征得用户同意机制是否合规、是否依法取得用户授权、是否符合 SDK 与 App 之间订立的合同要求等。对于未履行数据合规义务或者违反 SDK 与 App 合同义务的 App 开发者，尽快采取行动要求改正或终止合作。

5. 完善网络安全和数据安全防护措施

第三方 SDK 提供者在提供服务的过程中对个人信息的处理可以分为数据采集阶段、数据传输阶段、数据存储阶段、数据使用阶段以及数据销毁阶段。在每一阶段，第三方 SDK 提供者都需采取相应的技术措施以保障个人信息的安全，防止个人信息泄露或滥用风险。例如，在数据采集阶段，可以采用数据隔离、加密等方式保障缓存在终端本地的数据安全；在数据传输、存储阶段，采用数据隔离、加密、去标

识化等方式降低因数据泄露造成的用户损失，尽量按照最小化原则保存个人信息；在数据使用阶段，尽量消除个人信息的身份指向性，避免精准定位到特定个人，加强展示时的脱敏处理以及个人信息访问控制管理；在数据销毁阶段，及时响应个人用户要求以及 App 开发者代表个人用户发出的数据删除的请求。

此外，第三方 SDK 提供者还需要采取安全加固等安全措施并定期复检，保障自身 SDK 的安全性能，防止被逆向分析、二次打包、动态调试、进程注入、数据篡改等风险。同时第三方 SDK 提供者应采取必要措施保障基础设施、业务系统等方面的网络安全，完善安全应急响应机制和应急预案，防范因黑客攻击造成数据泄露等安全风险，同时强化自身安全事件应急处置能力。

（四）加快完善 SDK 安全管理的主体责任

如本报告第一章第（二）节和第五章第（一）节所述，从去年 2019 年白皮书发布至今，国家监管层面以及标准层面均开始对 SDK 的合规问题开始关注，但在细节规定上，例如从事 SDK 产品服务的主体资质、第三方 SDK 收集、使用个人信息符合合法、正当、必要、明确原则，SDK 与 App 之间角色和主体责任划分等等，目前对于上述问题仍缺乏落地性指导。第三方 SDK 作为移动互联网生态圈的重要一环，它的安全问题会对 App 开发者、整个移动互联网行业的稳健发展产生较大的影响，建议尽快完善与 SDK 相关的行业准入标准、安全标准及指南，以给予 App 开发者和 SDK 提供者可落地的指导与建议。

（五）鼓励第三方 SDK 企业开展行业自律

SDK 技术发展日新月异，第三方 SDK 安全问题也逐渐成为各方关注的焦点问题，建议鼓励相关 SDK 企业同步开展行业自律，作为立法与监管等国家公权力的补充力量，充分发挥专业性、经济型、灵活性等优势，共同营造 SDK 发展的良好生态。一方面，鼓励 SDK 企业自发或依托相关行业协会、社会组织平台，共同制定第三方 SDK 收集使用个人信息行为准则，签订行业自律公约，形成行业自治。另一方面，对当下法律规定不完善之处以及随着技术发展可能带来的全新问题，鼓励 SDK 企业共同探索安全实践和合规参考指南，推广宣传相关最佳实践，带动提升个人信息保护整体水平。

附录　第三方 SDK 产品的安全与合规实践

（一）极光 SDK 的安全与合规实践

1. SDK 开发者协议和隐私政策

（1）对开发者的要求

极光在其官方网站和用户注册界面均展示了开发者协议和隐私政策。访问者需同意极光开发者协议和隐私政策后才能注册成为极光开发者用户。为了方便 App 开发者向终端用户明确展示极光的隐私政策，并就极光 SDK 产品收集和使用终端用户个人信息的类型和目的明确告知终端用户用户并就在符合法律法规规定的范围内使用上述终端用户信息的事项征得您的终端用户同意，进一步做好合规工作，极光为 App 开发者提供以下 4 种方案建议:

A.在 App 使用或注册/登记界面以弹窗、页面提示方式显示极光的隐私政策、收集终端用户个人信息的类型和目的，并获得终端用户明示同意（即勾选“✓”），如图 10 所示。

图 10 极光 SDK 展示隐私政策示例一

B. 在 App 使用或注册/登记界面通过点击阅读 App 隐私政策时针对“第三方共享信息”条款部分，简要列明极光 SDK 收集终端用户个人信息的类型和目的，并获得终端用户明示同意（即勾选“✓”）。

参考示例图二：

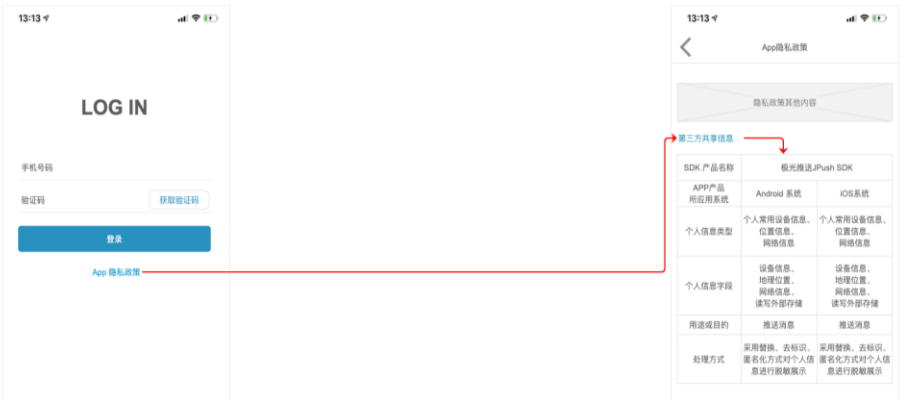


图 11 极光 SDK 展示隐私政策示例二

C. 在 App 使用或注册/登记界面通过协议在线展示的方式，即点击阅读 App 隐私政策时针对“第三方共享信息”条款部分，嵌入链接方式显示极光的隐私政策、收集终端用户个人信息的类型和目的，并获得终端用户明示同意（即勾选“✓”）。

参考示例图三：

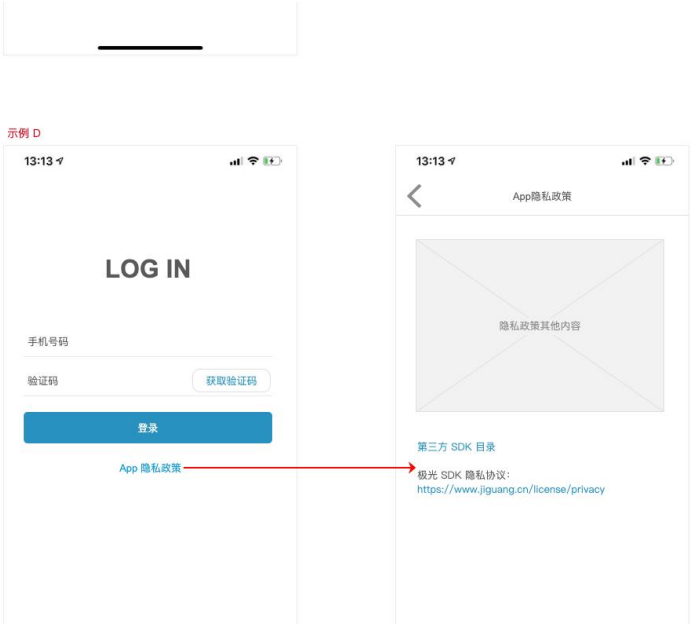


图 12 极光 SDK 展示隐私政策示例三

D. 在 App 使用或注册/登记界面点击阅读 App 隐私政策时针对“第三方共享信息”条款部分，披露 App 接入第三方 SDK 目录同时协议在线展示的方式，即嵌入链接方式显示极光的隐私政策、收集终端用户个人信息的类型和目的，并获得终端用户明示同意（即勾选“✓”）。

参考示例图四：

图 13 极光 SDK 展示隐私政策示例四

极光在其开发者协议和隐私政策中明确说明了其为开发者提供

服务的前提，包括但不限于（1）开发者已经遵守并将持续遵守适用的法律、法规和监管要求，包括但不限于制定和公布有关个人信息保护和隐私保护的相关政策；（2）对涉及需收集、存储、使用、共享来自于终端用户的个人信息，App 开发者须确认并承诺：其已经获得终端用户充分必要的授权、同意和许可；（3）App 开发者应向终端用户提供易于操作的选择机制，说明终端用户如何以及何时可以行使选择权，并说明行使选择权后如何以及何时可以修改或撤回该选择，使得终端用户可以选择同意或不同意为互联网定向广告目的而收集和使用其身份关联信息以及向第三方共享该信息。极光通过站内信、网站形式不时更新或发布极光合规指南、向 App 开发者提供隐私政策、使用方式以及参考模板，以帮助开发者避免因违反相关法律法规遭受损失。

（2）极光对 App 开发者的合规审查

为确保 App 开发者切实获得终端用户授权，极光更新了开发者隐私政策的 线上审核流程，保证极光获取终端用户个人信息的合法合规性。当开发者用户首 次创建应用或老用户未上传隐私政策时，极光会在“应用设置”界面自动提示开 发者上传隐私政策并进入系统审核流程，审查 App 开发者是否依法依规撰写隐 私政策、取得终端用户的授权。

对于收集用户个人信息不合规的开发者，极光会要求 App 开发者修订其隐 私政策。在隐私政策上传界面，极光还为开发者用户提供了一站式的隐私政策模 板服务，为开发者用户提供便捷的隐私合

规建议。同时，为提升线上审核的准确 性，我们会不定期地对已上传的隐私政策进行人工审核并比对审核结果，优化审 核程序。在与开发者合作过程中，极光会根据现行法律法规、国家标准以及官方 通报，定期调研或抽查有合作的开发者的隐私政策。对隐私政策不符合规定的开 发者，极光会发出整改通知要求开发者进行合规整改，直至符合合规要求。

（3）技术保障措施

极光非常注重终端用户的个人信息安全。极光通过物理安全、安全技术、安全管理等措施审慎保护终端用户的个人信息，防止丢失、误用、非授权存取、泄露和非授权更改。安全措施包括但不限于防火墙、信息加密、数据备份、访问权限控制、密级管理、雇员保密协议、利益冲突、安全管理和安全事件应急预案。极光已建立个人信息安全影响评估体系，评估并处置个人信息处理活动存在的安全风险。极光会定期和不定期举办信息安全和隐私保护培训课程，加强员工对于保护终端用户个人信息重要性的认识。

从数据处理生命周期角度来看，极光作为 SDK 提供者在提供服务过程中对个人信息的处理分为数据采集阶段、数据传输阶段、数据存储阶段、数据使用阶段、数据销毁阶段。每一个阶段极光推送 SDK 均采取了相应的技术措施以保障终端用户个人信息的安全性，防止终端用户个人信息泄露。

2. 标识用户方法及安全措施

数据在进入极光统计平台后，将立即进行去标识化或匿名化处理。

在个人信息第一次上报，通过系统的注册服务，结合设备标识与 App 标识，根据固定的算法加工生成 JDID（极光独有的标识符），使数据在不借助额外信息的情况下，无法识别或者关联到个人。

3. 数据存储安全措施

数据经客户端传输上报至服务端并经过缓存处理后，统一存储至统计平台待分析处理。存储时按照上报 App 进行单独隔离，个人信息与业务数据隔离存储，通过上述提及的 JDID 作为关联 ID，防止存储数据泄露之后的可逆操作，保证了数据安全。除此之外极光采取严格的数据访问控制，采用独立的鉴权方式，按需申请达到针对个人的最小化权限控制，防止人为操作原因导致的数据泄露。

4. 数据汇聚

极光推送 SDK 为提供推送服务而收集到的各类 App 数据，在数据传入统计平台后，会依据不同 App 要求进行隔离存储、加密传输、脱敏化，以保证数据的安全性。同时进入统计平台的数据，会依据不同的业务类型进行分级管理及存储和访问控制，以保证相关人员对数据的最小可见。

数据依托极光 JDID，对 SDK 收集的原始数据进行归类汇聚，并为客户提供基于时间、平台、客户自定义分类的归类和处理，处理完成后以网页呈现统计汇总及专属应用程序接口等方式提供给开发者，帮助开发者据此调整运营策略。

5. 数据删除环节的主要做法

（1）停止运营产品或服务

当停止运营某一产品或服务时，极光将停止运营的通知以逐一送达或公告的形式通知 App 开发者，同时停止收集个人信息并对其所持有的个人信息进行删除或匿名化处理。根据《网络安全法》的要求，涉及归档数据需要保存 6 个月，之后归档数据将自动删除。

（2）通过响应个人信息主体请求进行删除

由于极光的直接服务对象是 App 开发者，并不直接面对终端用户，因此极光支持个人用户行使删除权利的途径有两种:

A. 终端用户可以通过极光隐私政策预留的联系方式直接向极光提出个人信息主体请求。在响应请求前，极光会要求进行身份验证，在通过身份验证以及确认请求的合法性后，极光会立即响应个人用户的删除请求并进行回复;

B. 终端用户也可根据 App 开发者的隐私政策，将删除个人信息的请求直接发送给相关 App 开发者处理和寻求帮助，极光会配合 App 开发者对个人信息主体的删除请求进行响应。（对于个人信息主体请求的响应机制，除“删除”外，同样适用于个人信息主体关于“信息更正”、“撤回授权同意”、“注销账户”、“获取个人信息副本”等方面的请求。）

在确认响应信息主体关于删除的请求后，极光会立即对相关个人信息进行匿名化或删除处理。根据《网络安全法》的要求，归档数据需要保存 6 个月，之后归档数据将自动删除。

6. 对外合作情况

极光推送不向任何第三方提供能够单独或结合其他信息识别到终端用户个人身份的信息，也不允许任何第三方以任何形式访问这些数据。极光推送提供的用户和推送统计功能所形成的“推送报表”和“用户统计报表”，仅供开发者用来观察推送的效果和应用的发展趋势，不涉及终端用户的个人信息。同时，我们基于开发者服务协议合法收集的数据（对个人信息进行去标识化或匿名化处理）以及通过其他合法渠道获得的数据建立极光数据库，为开发者提供进一步的数据服务。数据服务中我们输出的数据仅为标签信息，该等标签信息是通过海量移动端受众数据的汇聚、匿名化处理、智能运算获得，最终以统计分析数据的形式体现，不含有任何个人的隐私或可识别个体的内容。

7. 新技术研发

极光推送作为极光开发者服务的核心产品，始终专注于为开发者提供更加优质的服务内容。基于推送服务的基本功能，结合业务统计信息，极光加入 AI 算法帮助开发者更加智能地重构业务信息分类，深度洞察用户，实现推送的“千人千面”。使开发者在为用户提供更加个性化/精准服务的同时，有效减少无效推送消息对用户的打扰，提升用户体验。

（二）小米推送 SDK 的安全与合规实践

1. SDK 开发者协议和隐私政策

（1）对开发者的要求

小米在其开发者协议中，设立专门的隐私保护章节，规范开发者对终端用户的个人信息保护。要求开发者或终端用户在使用小米推送提供的服务时，同意小米推送按照小米统一隐私政策收集、存储、使用、披露和保护个人信息。小米也强烈建议开发者按照小米推送建议，将关键条款（具体以网页公示为准）包含进开发者产品面向终端用户的隐私政策中，并保证链接准确有效，即开发者应保证事先获得终端用户同意以使小米推送有权收集并使用数据提供相应服务。如果终端用户未作出同意，则开发者不应继续使用小米推送服务。小米还要求开发者同意遵守适用的收集、使用、披露终端用户数据及保护终端用户相关的法律法规、政策和行业标准，并确保符合该等法律法规、政策及行业标准的规定适用小米推送服务。作为小米推送服务的使用者，开发者必须制定、发布其隐私政策并获得终端用户同意，且该政策应不低于小米推送的隐私保护标准。

小米推送开发者上线界面中会明示开发者阅读小米推送公示内容，并请开发者确认将推送所收集的信息部分集成进隐私政策中。开发者上线时须完成上述流程。

（2）技术保障措施

小米推送是小米开发的被集成于开发者产品或服务中于为用户提供推送服务的产品。在此场景中，开发者作为数据控制者决定用户

数据的处理目的、方式，小米推送在为用户提供推送服务过程中作为数据处理者，接受开发者委托并根据开发者指示处理用户数据。

小米非常重视个人信息安全，并采取一切合理可行的措施保护终端用户的个人信息。我们会采用符合业界标准的安全防护措施以及行业内通行的安全技术来防止终端用户的个人信息遭到未经授权的访问、修改，避免您的个人信息泄露、损坏或丢失。

2. 标识用户方法及安全措施

小米推送使用 regId 来唯一地标识一台设备上的一个应用（App）。regId 是 App 在初始化小米推送 SDK 时， 由 SDK 从服务器端获取的一个 base64 编码的字符串。此字符串是由（数字，应用 AppID，时间戳，数据中心编码）加密而成。不包含任何用户、设备相关的信息。

3. 数据传输安全措施

消息在传递过程中， 使用 SSL 和 AES 二次加密的方式对内容进行保护。应用在初始化推送 SDK 时， 在注册设备阶段使用 HTTPS 方式与小米推送服务进行数据交换。此时，使用 SSL 对报文进行加密。此阶段会交换应用的 SecretKey，做为下一阶段数据传输的公钥。

开发者向小米推送服务传递信息时，使用 HTTPS 来加密传输数据。小米推送服务向设备传递消息时，使用在注册阶段获得的 SecretKey，对所有报文以 AES 128 bit 方式进行第一次加密。报文进入传输通道后，通道还会使用自己的通道加密方式对密文再次加密，确保数据安全。

4. 数据使用情况

推送服务不对开发者提供的文本进行挖掘和使用，也不分析用户行为和偏好。 推送只作为消息通道，将消息从开发者侧传递到设备侧。收集的数据只满足标识设备以下发消息和统计需求。

为改善整体服务质量，小米推送会对 App 和设备，以消息、时间维度进行统计。具体来说，每个 App 在一段时间内，对发起的请求数、送达数、点击数进行统计。统计结果是汇总数据，不对应到任何一个用户。

5. 对外合作情况

推送的各类数据都没有提供给小米以外的合作方使用，包括原始数据、中间数据和统计结果。推送会为开发者提供与该开发者相关的后台统计数据，其中仅包括时间，消息维度的统计数据，不包括任何用户个人数据。

6. 数据删除的主要做法

小米推送作为 SDK，无界面与终端用户直接交互。用户相关信息的删除， 都通过集成的 App 来实施。小米推送 SDK 提供了反注册的方法和接口。调用此类方法，推送服务会将此 App 相关的数据和消息从数据库中删除。

当一台设备（以 UUID 标识）90 天都没有连接推送系统的记录，此设备相关的信息和消息，也会从数据库中删除掉。

除法律法规另有规定，未能下发的推送文本会在服务器中默认缓

存十四日后清除，其余信息，自开发者停止集成小米推送 SDK、要求推送停止服务时，小米推送会根据开发者指示清除所有个人信息。

（三）TalkingData SDK 的安全与合规实践

1. SDK 开发者协议和隐私政策

TalkingData SDK 的功能设置为按需定制，开发者可以自主选择产品线、平台类型和定制化提供方式。开发者选择的 TalkingData 产品服务功能所需收集的信息类型与其自身的系统权限匹配。

开发者在 TalkingData 官网上获取 SDK 时须主动勾选所需的 SDK 功能并选择 App 上架的平台。

（1）对开发者的要求

TalkingData 在其《服务条款》中，明确了对开发者对个人信息保护的相关要求。开发者在使用 TallkingData 数据服务时，应同意其产品（包括但不限于移动应用客户端、移动网站、应用平台及其他 TalkingData 确认可供提供服务的其他终端等）中使用 TalkingData 分析工具，并且通过开发者和其产品用户的服务协议/软件许可条款或其他形式的许可或授权（“用户授权”），获得开发者产品用户的必要同意以使得 TalkingData 分析工具有权收集有关开发者产品使用情况的原始数据及其他为提供服务所必须的用户个人信息。

（2）技术保障措施

TalkingData 已经建立健全数据安全管理体系，包括对用户信息进行分级分类、加密保存、数据访问权限划分，指定内部数据管理制度和操作规程，从数据的获取、使用、销毁都有严格的流程要求，避免用户隐私数据被非法使用。

TalkingData 还建立了定期举办安全和隐私保护的培训机制，提

高员工的个人保护意识。将不定期的审查、更新并公开 TalkingData 风险报告及个人信息安全影响评估报告。

2. 标识用户方法及安全措施

TalkingData SDK 基于分析服务所收集的数据，以及通过其他合法渠道获得的数据建立 TalkingData 数据库，通过汇聚、清洗、智能运算，形成 TalkingData 自有的用户标识符（TDID），来替代移动设备标识。TDID 采用 TalkingData 自有的 ID 生成逻辑及加密算法来生成，具体规则是：版本号 + 加密算法 F(设备 ID 因子 1,设备 ID 因子 2,设备 ID 因子 N, Salt)。

通过 SDK 在 App 第一次使用过程中所生成的 TDID，会保留在应用沙盒中(IOS 平台,对应存储于该应用自身的 Key Chain 中;Android 平台上，存储于应用自己的沙盒之中），从而确保 TDID 在设备端存储的安全性。

TalkingData 的 SDK 为每个 App 服务而收集的数据，首先在设备边缘侧先做了设备 ID 去标识化等预处理工作；收集的数据也采用加密方式存储和传输，通道加密方式回传。

3. 数据存储安全措施

TalkingData 将采用行业内通行的、合理的标准来保护其所储存的信息的安全性和保密性。包括但不限于：防火墙和数据备份措施；数据中心的访问权限限制；对移动终端的识别性信息进行加密处理等。

TalkingData SDK 所收集的数据，用于对应的业务分析或广告监

测业务服务线，并且在数据收集后，TalkingData 会按照“数据收集–存储–分析–利用–清理–归档”过程，严格追踪每一个数据使用的副本，在业务使用完成后，清除系统中所有相关的副本，同时，对需要保留的日志数据采用了包括：Hashing，映射、设定数据偏移量、混淆、加密等各种脱敏技术方案，实现数据泛化，以有效保障数据的安全。

内部存储方面，依据“1. 法律法规；2. 行业规范；3.商业机密；4.资产安全”的四大原则，对收集后的数据进行分级存储和管理。

内部管理机制方面，也通过物理多级隔离控制（如：访问设备接入的身份验证、安全控制网关、服务使用的登录堡垒机隔离，以及数据使用的专属提交机）、账号分级管理、多层事后审计机制等手段，确保存储数据的操作安全。

图 14 TalkingData 内部数据分级管理策略

4. 数据汇聚安全措施

TalkingData SDK 为每个 App 服务而收集的数据，在数据回传通道中，首先依据不同国家和地区，采用分地区落盘存储方式，确保数据收集符合当地法律法规政策。

进入内部的数据，依据不同产品业务服务、不同客户的数据也按照公司的数据分级管理体系，进行分级化存储和管理。

借助 TalkingData 设备标识 TDID，针对 SDK 收集回的原始数据进行归类，并基于时间、产品服务业务线及客户等进行分主题归类和预处理；预处理完成后，按照具体业务需求，以统计汇总、专属应用程序接口等方式供给开发者使用。

5. 数据使用安全措施

在 TalkingData 的数据中心内部，所有涉及数据使用的生产与治理全面采用了工具化方式管理，涵盖从研发工程(代码/配置/部署/任务/知识)、到生产领域(ETL)、数据资产管理、数据探索、及数据服务能力的使用及输出。

图 15 数据生产/加工/访问使用全流程工具化操作

通过工具化手段，杜绝数据处理中的人工参与，整个处理和使用流程通过系统来做到安全管控和事后审计监督。

在内部数据探索方面，TalkingData 也构建了数据沙箱运行环境，通过构建数据探索使用的安全沙箱；在安全沙箱中，部署自有的数据科学平台（Data Science Studio）；提供可视化建模工具，对存储

于沙箱中的数据进行目录查阅，工程建模、模型调优的探索工作。

6. 对外合作情况

在 SDK 数据服务能力对外服务提供方面，TalkingData 构建了移动端受众数据管理平台（TalkingData DMP 或称为 TalkingData 智能营销云），依托所累积和基于模型处理生产加工后所生成的第三方人群数据，这部分海量移动端受众数据的汇聚、匿名化处理，最终以统计分析数据形式展现，其中不包含任何个人信息和个人敏感性等可识性数据。通过受众管理平台提供客户群体构建、客群画像洞察和画像群体对接媒体进行基于群体的定向投放的数据支撑。

图 16 基于受众的群体画像能力输出

7.数据删除的主要做法

TalkingData SDK 收集的原始日志，基于国内法律规范，保留不少于 6 个月；业务使用过程中产生的数据副本，内部监控系统会时刻跟踪数据生产、加工处理过程中所产生的每一个数据副本，并依据事先的业务规则，在业务处理完成后，自动化删除每一个数据副本。

TalkingData 在为开发者提供的服务过程中或结束后，最终用户

均可以通过OPT-OUT渠道(http://www.talkingdata.com/optout.jsp?languagetype =zh_cn)随时向 TalkingData 提出撤回“同意”的申请，在收到申请后，TalkingData 将不再处理相应的信息，同时，可删除该申请用户在TalkingData 账户下相关业务的所有统计分析数据。

8.新技术研发

TalkingData SDK 能力建设方面，主要关注智能化在终端侧的实现。主要包括: 如何通过边缘结算和基于 AI 的模式识别能力，有效帮助开发者有效识别虚假作弊设备，帮助开发者判断设备使用，支持开发者统计和监测中的新模式分析等。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62308070

传真：010-62300264

网址：www.caict.ac.cn

北京市环球律师事务所

地　　址：北京市朝阳区建国路 81 号华贸中心 1 号写字楼 15&20 层

邮政编码：100025

联系电话：010-65846688

传　　真：010-65846666

网　　址：www.glo.com.cn