



# 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

































































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

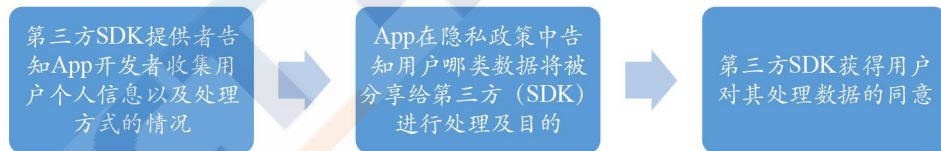
无法绕开 App，只能通过 App 才能进行。在这种情况下，对内可以分三步来完成：

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；

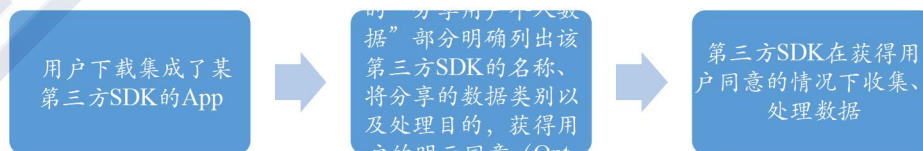
第二步：App 开发者在隐私政策的“与第三方分享数据”一节中说明，哪些数据将由第三方 SDK 提供者收集，或者哪些数据类型是由 App 共享给第三方 SDK 提供者以及该等处理的目的；或通过 App 的隐私政策中跳出 SDK 隐私声明的链接，由 SDK 发布单独的隐私声明来获取用户的同意；

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》<sup>9</sup>、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

<sup>9</sup> 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<sup>10</sup>，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

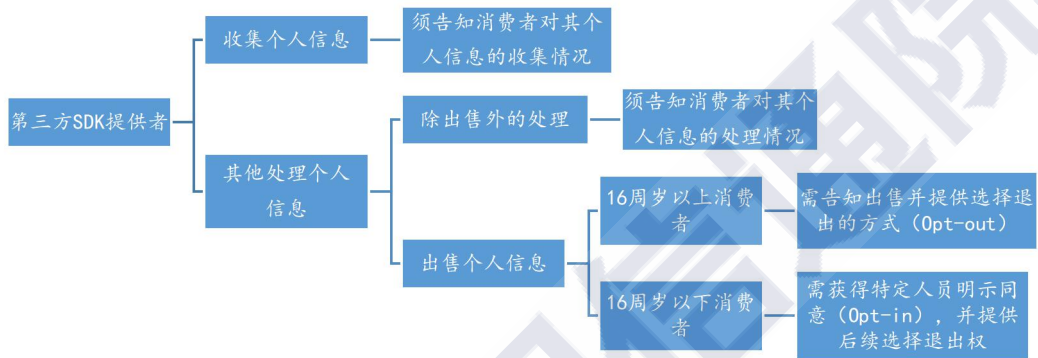
对于 16 周岁以下消费者个人信息的出售，CCPA 采取的是获得特定人员明示同意 (Opt-In) 的模式，即企业有请求用户明示授权的义务。<sup>11</sup> 故在 App-SDK 场景下，对于 16 周岁（含）以上的用户，第三

<sup>10</sup> 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。”

<sup>11</sup> 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

方 SDK 提供者仅需要通过 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；

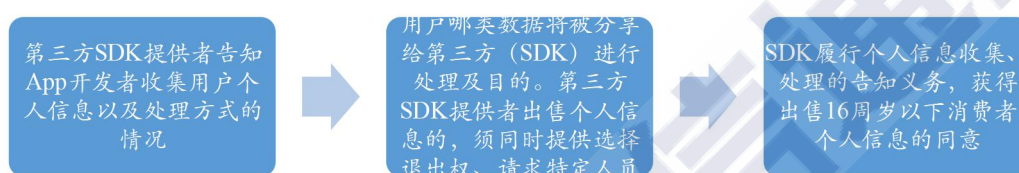
第二步：App 开发者在隐私政策的“与第三方分享个人信息”一节中告知或通过 App 的隐私政策中跳出 SDK 隐私声明的链接，由 SDK 发布单独的隐私声明来告知哪些个人信息将会由第三方 SDK 提供者收集，或者哪些信息类型是由 App 共享给第三方 SDK 提供者以及该

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。”

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：

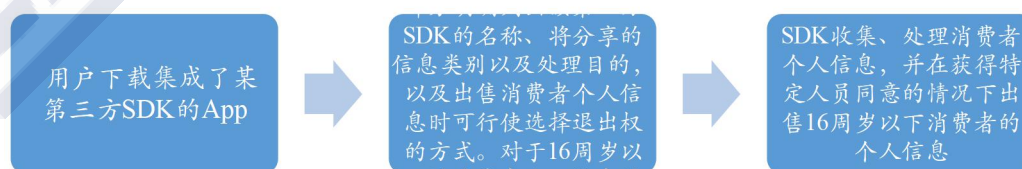


行描述：

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）》等法律和行政法规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》—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 数量没有那么庞大，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，询问用户是否“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。

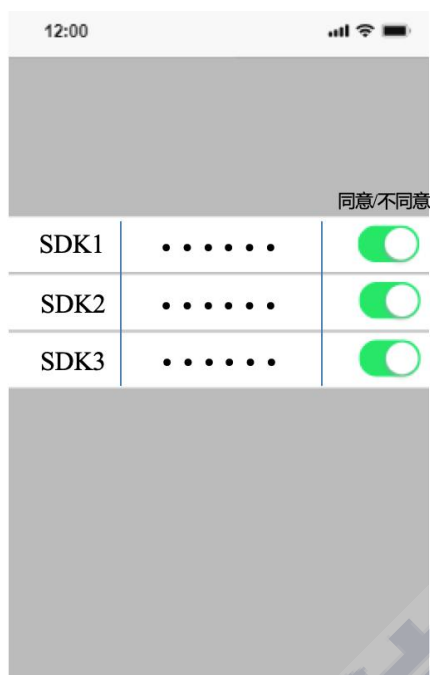


图 8 SDK 征得用户同意方式的示例

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“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：

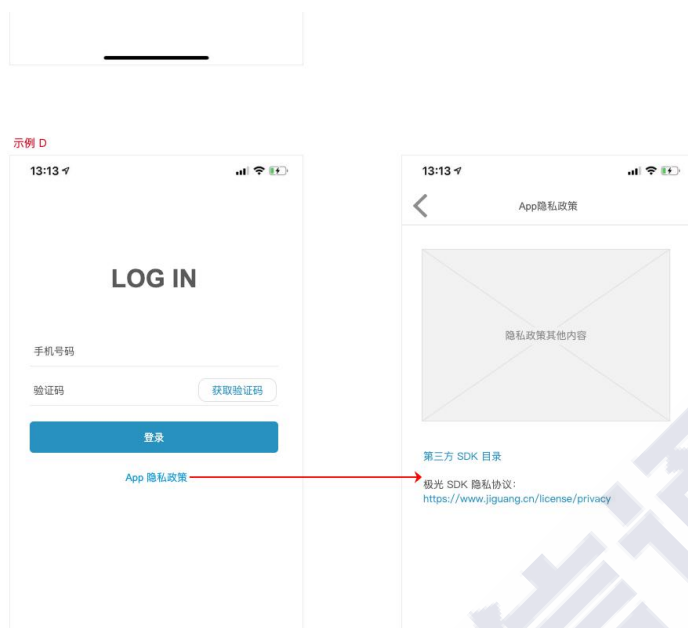


图 12 极光 SDK 展示隐私政策示例三

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：

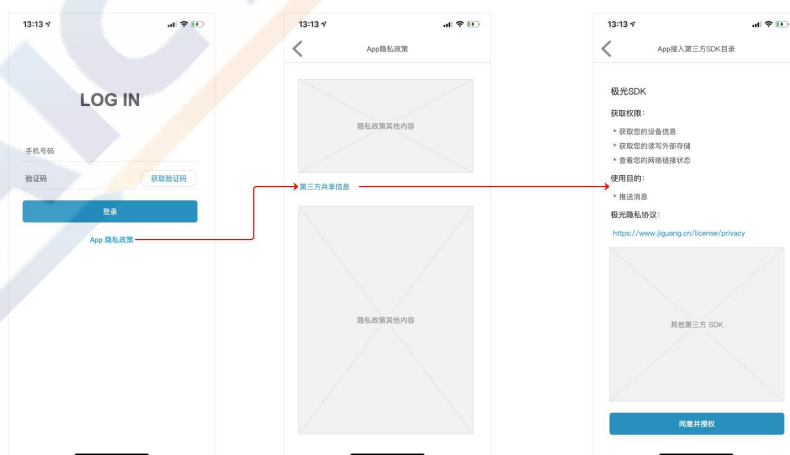


图 13 极光 SDK 展示隐私政策示例四

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。

CAICT 中国信通院

### （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 TalkingData 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别性数据。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](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](http://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](http://www.glo.com.cn)

