ICS 35.110
CCS L 79

T/CSAC

团　　体　　标　　准

T/CSAC 006—2023

移动互联网应用程序（App）接入软件开发工具包（SDK）个人信息安全指南

Personal information security guidelines for integrating software development kit to mobile internet applications

2023－9－22 发布　　2023－9－22 实施

中国网络空间安全协会　　发布

目　　次

前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由网络空间安全协会提出并归口。

本文件起草单位：北京抖音信息服务有限公司、北京市政务信息安全保障中心、国家计算机网络应急技术处理协调中心北京分中心、OPPO广东移动通信有限公司、深圳市和讯华谷信息技术有限公司、蚂蚁科技集团股份有限公司、北京百度网讯科技有限公司、小米科技有限责任公司、华为技术有限公司、三六零安全科技股份有限公司、阿里云计算有限公司、郑州云智信安安全技术有限公司、极客谷数字信息安全产业园、北京航空航天大学、北京邮电大学。

本文件主要起草人： 杜蕾、杨骁涵、安潇羽、李思凡、李昳婧、李若愚、王敏、赵乃萱、吴少卿、谷元坤、靳鑫亚、荣晓燕、李媛、程颖博、姚菲、秦世勉、史坤坤、陈光炎、马超、卢威、李娜、付艳艳、白晓媛、蒋思思、黄飞、杨智、彭铭、李实、吴汇洋、刘闯、黄天宁、关振宇、张熙。

移动互联网应用程序（App）接入软件开发工具包（SDK）个人信息安全指南

1 范围

本文件规定了App提供者和SDK提供者在App接入SDK的全生命周期内需遵循的信息安全指南，主要涵盖和涉及设计、开发、运营和退出四个阶段。

本文件适用于App提供者和SDK提供者对自身的信息安全防护和个人信息保护行为机制进行设计和评估，也适用于第三方评估机构和相关部门进行审查和评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022 信息安全技术 术语

GB/T 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

GB/T 42582—2023 信息安全技术 移动互联网应用程序（App）个人信息安全测评规范

3 术语和定义

GB/T 25069—2020界定的以及下列术语和定义适用于本文件。

3.1

移动互联网应用程序 mobile internet application：App

运行在移动智能终端上的应用程序。

注：包括移动智能终端预置、下载安装的应用程序和小程序。

[**来源**:GB/T 42582-2023，3.1]

3.2

移动互联网应用程序提供者 mobile internet application provider

移动互联网应用程序的开发者、运营者或所有者，简称App提供者。

3.3

软件开发工具包 software development kit

协助软件开发的软件库。

注：软件开发工具包通常包括相关二进制文件、文档、范例和工具的集合，简称SDK。

[**来源**:GB/T 41391-2022，3.14，有修改]

3.4

第三方软件开发工具包 third-party software development kit

由移动互联网应用程序运营者之外的其他法人实体提供的软件开发工具包。

[**来源**:GB/T 41391-2022，3.15]

3.5

软件开发工具包提供者 software development kit provider

软件开发工具包的开发者、运营者或所有者，简称 SDK 提供者。

3.6

自启动 self-startup

在用户没有直接操作某个 APP 的情况下，APP 内的 SDK 自行拉起自身进程并成功运行。

3.7

关联启动 coupling-startup

在用户没有直接使用某个 SDK 或 APP 对应的功能时，其进程已被另一个 SDK 或 APP 拉起并成功运行。

3.8

个人信息 personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

[**来源**：《中华人民共和国个人信息保护法》]

3.9

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息

注：敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

[**来源**：《中华人民共和国个人信息保护法》，有修改]

3.10

开源 open source

源代码公开，指软件的使用者可以获得其源代码。

3.11

闭源 closed source

源代码不公开，指软件的使用者无法获得其源代码。

4 缩略语

下列缩略语适用于本文件。

App：移动互联网应用程序（Mobile Internet Application）

API：应用程序编程接口（Application Programming Interface）

SDK：软件开发工具包（Software Development Kit）

5 概述

5.1 SDK 概述

SDK是一组工具集，提供独立、明确的功能，被广泛应用于各类App开发中，以提高App开发和运营的效率。其具体分类可参考TC260-PG-20205A 3.2。

5.2 SDK 使用场景与角色关系

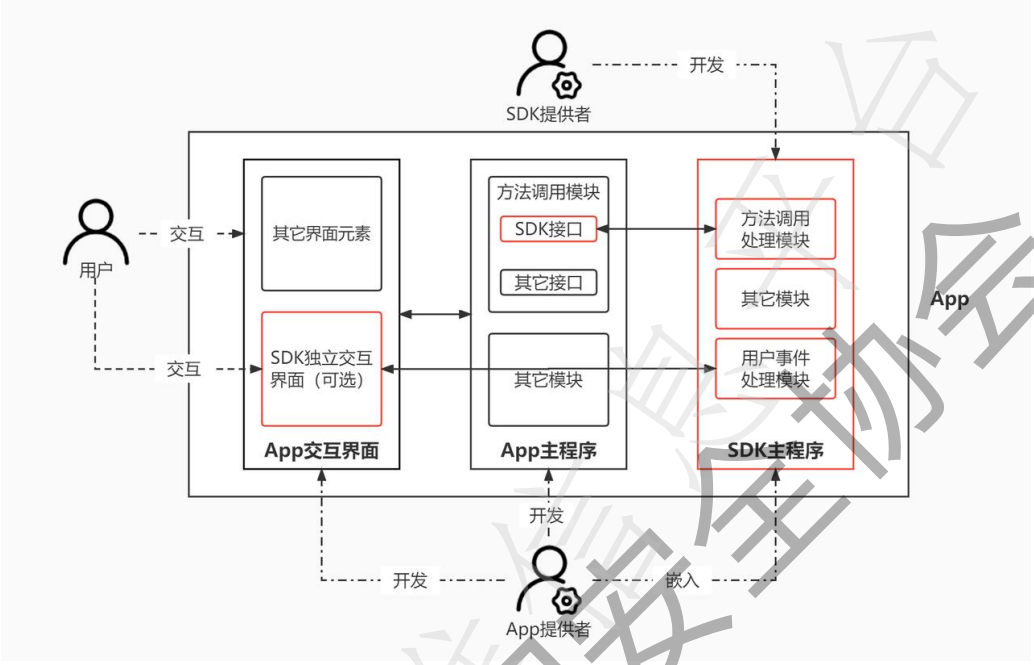


图 1 App接入SDK示意图

如图1所示，SDK的使用场景通常涉及到SDK提供者、App提供者和用户三方角色：

a) SDK提供者：作为SDK的设计和开发者，SDK提供者负责对SDK的功能代码封装成模块，并对外提供API接口、API文档、SDK接入文档、个人信息处理规则说明文档。

b) App提供者：作为App的设计和开发者，App提供者通过调用SDK所提供的接口来将其嵌入到App中，从而实现SDK相应功能的引入；另外，倘若SDK具有相对独立的交互界面（或界面元素），App提供者宜通过双方协商将将其嵌入到App的交互界面中。

c) 用户：作为App的最终使用者，用户一般通过App交互界面使用App的相应功能来间接使用SDK，SDK的嵌入对用户而言通常是没有感知的；但倘若SDK具有相对独立的交互界面（或界面元素），用户可能会感知到SDK的存在。

通常而言，SDK提供者和App提供者可能为同一方（即指App提供者使用自行开发的SDK），也可能分属不同法人实体。对于二者分属不同法人实体的情况，通常将所涉及的SDK称为第三方SDK。在未明确说明的情况下，本文中所提到的SDK均指的是第三方SDK。

5.3 App 与 SDK 责任划分

SDK提供者和App提供者需按照自身角色承担相应的责任和义务：

a) SDK提供者需对该SDK的安全防护负责，需详细告知App提供者安全使用和配置SDK的要求。

b) SDK提供者需对该SDK的个人信息保护负责，需向App提供者披露收集使用个人信息的相关情况。

c) App提供者需对SDK的引入负责，需整体把控SDK的使用和配置，具有审查和安全管理义务。

d) APP提供者需对其自身和第三方SDK的个人信息处理规则的公示负责，需向用户披露接入的第三方SDK的个人信息收集使用的情况，协助第三方SDK提供者取得APP用户的授权同意。

6 SDK 安全风险

6.1 SDK 安全漏洞

SDK自身可能存在安全漏洞并由此对App的安全性造成威胁，其常见分类和具体漏洞信息可参考TC260-PG-20205A 4.1。

6.2 SDK 恶意行为

SDK的主观恶意行为可能会破坏App的安全性、对用户的个人信息和合法权益造成威胁，其详细信息可参考TC260-PG-20205A 4.2。

6.3 SDK 违规处理个人信息

6.3.1 个人信息收集

SDK收集个人信息时，违法收集个人信息、过度收集个人信息、未充分告知处理目的及未经用户授权同意收集个人信息的风险。

6.3.2 个人信息存储

SDK存储个人信息时，未采取充分安全的保护措施及机制造成个人信息泄露的风险；存储时间超过个人信息主体授权使用目的所必需的最短时间。

6.3.3 个人信息使用

SDK提供者在使用个人信息时，超范围使用个人信息、展示的个人信息未做去标识化处理等导致数据个人信息等风险。

6.3.4 个人信息加工

SDK提供者在加工个人信息时，在不具备合法性基础的前提下对个人信息过度挖掘、造成用户焦虑恐慌的风险。

6.3.5 个人信息传输

SDK在传输个人信息时，未对个人信息进行加密或未采取充分安全的传输协议导致个人信息泄露的风险。

6.3.6 个人信息对外提供

SDK提供者对除了APP提供者之外的机构或个人提供个人信息时，在无其他合法性基础情况下，未对用户针对个人信息对外提供目的、期限、处理方式、个人信息种类以及可能产生的后果等进行充分告知的风险，以及未取得用户单独同意的风险。

SDK提供者委托第三方处理个人信息时，在无其他合法性基础情况下，未对用户针对个人信息处理的目的、期限、处理方式、个人信息种类以及可能产生的后果进行充分告知、未与受托方约定个人信息接收方的责任和义务的风险。

6.3.7 个人信息公开

SDK提供者在无其他合法性基础情况下，超出合理范围公开个人信息、未向用户告知公开披露个人信息的目的、类型，并征得其明示同意或公开个人信息给用户权益造成重大影响的风险。

6.3.8 个人信息删除

SDK完成业务功能及目的、用户撤回同意、SDK提供者停止提供产品或服务或超出最短存储期限后，在无其他合法性基础情况下，未及时删除或匿名化处理用户个人信息的风险。

6.3.9 个人信息跨境提供

SDK提供者未经用户同意、未履行法律规定的相关要求，向中华人民共和国境外提供个人信息的风险。

7 App 接入 SDK 安全原则

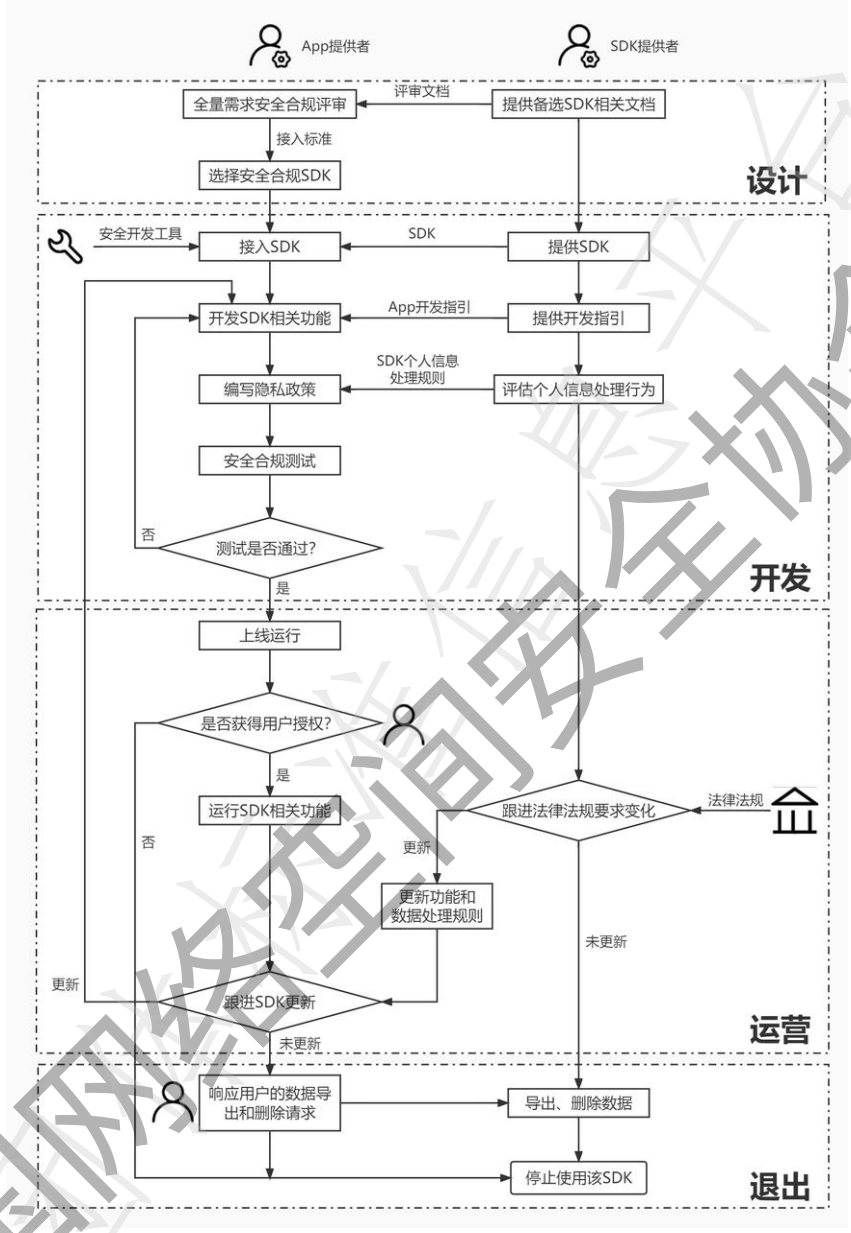
在App接入SDK的全流程中，App提供者和SDK提供者需遵循以下九项安全原则：

a) 全周期管理：针对所接入的SDK，App提供者需对其进行接入前审核、使用中监控、和退出时审计追溯，在发现违规行为时确保能够及时终止。
b) 权责一致：App提供者和SDK提供者需按照自身角色承担相应的责任和义务。
c) 目的明确：选用SDK时，App提供者需首先明确自身的业务需求并选择与此具有直接关联且个人信息处理目的合理、清晰、明确的SDK。
d) 最小必要：在选用SDK时，APP提供者需在满足自身业务需求的前提下选择最少够用的SDK。另外，SDK提供者需在实现相应业务功能的前提下申请最少够用的个人信息处理权限，不超范围、超频次申请权限。
e) 公开透明：SDK提供者需以合理清晰的方式向App提供者公开披露SDK处理个人信息的范围、目的和规则等，且其实际行为需与该声明保持一致。
f) 告知同意：App提供者需以合理清晰的方式向用户披露所嵌入的SDK及其处理个人信息的范围、目的、规则和SDK隐私政策等，且需征得用户授权同意。
g) 确保安全：在接入SDK的过程中，App提供者需使用足够的技术手段和管理措施来保证用户个人信息的安全性，且SDK提供者需在此过程中提供相应的帮助和支持。
h) 权限可控：App提供者需将SDK的所有个人信息处理权限申请和使用纳入管理范围，确保能够有效防止个人信息的非授权处理。
i) 主体参与：SDK提供者需保证用户的主体权益，向用户或APP提供者提供得以查询、更正、删除其个人信息以及进行撤回授权同意和投诉建议的有效方法，且App提供者需协助在交互界面上向用户明示SDK提供者实现用户权益相应的途径。

8 App 接入 SDK 安全指南

8.1 App 接入 SDK 生命周期

如图2所示，在瀑布模型的基础上，结合移动应用安全开发生命周期管理的特点，本文件将App接入SDK的生命周期划分为四个阶段：设计、开发、运营和退出。



注：这里的“退出”主要包含五种情况：（1）App下线；（2）SDK下线；（3）App停用SDK；（4）用户不再使用App；（5）用户不再使用SDK。

图 2 App接入SDK生命周期示意图

8.2 设计阶段

8.2.1 App 提供者

设计阶段App提供者需满足以下安全要求：

a） App提供者需明确自身业务需求并在此基础上充分评估接入SDK的必要性。若确有必要接入SDK，需在满足业务需求的前提下控制接入SDK的数量和在App中的应用范围。

b） App提供者需建立针对SDK引入的安全合规审核机制并制定明确的审核标准，且审核过程中需当严格把控，违法违规、基本信息不明确、来源不明、没有有效的沟通反馈渠道、没有风险控制能力、可能泄露用户个人信息、与业务需求无直接关联的SDK均不宜通过审核。

c） App提供者宜优先选用SDK的稳定或官方推荐版本。

d) 对于开源SDK，App提供者需根据其公开代码和文档自行对SDK进行充分的安全合规评估，明确SDK的功能、信息收集范围和安全要求等并据此形成用于安全合规审核的评审文档。
e) 对于闭源SDK，App提供者需利用SDK提供者所提供的的评审文档进行安全合规审核，如：信息安全资质、安全技术能力和管理水平、SDK信息处理规则、用户个人信息保护能力等。
f) 对于委托第三方定制开发的SDK，App提供者需根据自身业务需求明确SDK的功能、信息收集范围和安全要求并与SDK提供者签订委托合同；在SDK开发完成后，App提供者需利用SDK提供者所提供的的评审文档进行安全合规审核。
g) 若SDK涉及将数据对外共享或传输给任何App提供者以外的第三方机构或人员的行为，则App提供者需对其数据权限进行单独评估和审批，并取得用户的同意。
h) 对于涉及到个人信息处理的，App提供者需通过合同、合作协议等形式与SDK提供者达成合作约定，明确SDK的功能、信息收集范围和安全要求，约定双方在个人信息保护方面各自需要承担的责任、义务以及需要采取的安全措施等。当双方合作过程中发生重大变更时，需重新签订合同或合作协议。

8.2.2 SDK 提供者

设计阶段SDK提供者需满足以下安全要求：

a) SDK提供者需明确自身功能需求并在此基础上充分评估收集使用个人信息和申请敏感权限的必要性，其所收集使用的个人信息和申请的敏感权限不宜超出其业务功能的直接关联范围。若确有必要，需将收集使用个人信息和申请敏感权限的频率降低至实现自身业务功能所必需的最低频率。
b) SDK提供者需配合App提供者进行SDK的安全合规评审，在评审文档中以明确、易懂和合理的方式向App提供者完整、准确、及时地说明SDK的相关信息，不宜故意隐瞒和欺骗。宜包括的内容有：SDK提供者的基本信息和沟通反馈渠道；SDK的基本信息、功能和实现方式；SDK的隐私政策、收集使用的个人信息（及其目的）和申请的敏感权限（及其目的）；SDK的安全检测报告（包括数据安全存储、数据安全交互、关键组件安全配置、代码及资源文件安全等方面）；自启动和关联启动行为的合理性评估报告等。
c) 对于委托第三方定制开发的SDK，SDK提供者需根据App提供者所提出的功能、信息收集范围和安全要求进行SDK的设计和开发并签订委托合同，开发期间需配合App提供者进行SDK的修改和完善。
d) 对于涉及到个人信息处理的，SDK提供者需通过合同、合作协议等形式与App提供者达成合作约定，明确SDK的功能、信息收集范围和安全要求，约定双方在个人信息保护方面各自需要承担的责任、义务以及需要采取的安全措施等。当双方合作过程中发生重大变更时，需重新签订合同或合作协议。

8.3 开发阶段

8.3.1 App 提供者

开发阶段App提供者需满足以下安全要求：

a) App提供者需对SDK进行接入版本确认，包括但不限于：版本发布记录，版本名称，修订时间，修订说明等。
b) App提供者需确认根据自身业务需求，使SDK收集使用个人信息和申请敏感权限遵循合理、最小、必要原则。
c) App版本升级不得改变SDK系统权限设置。
d) App提供者需确认正确配置SDK，根据业务和场景需求对SDK声明的可选字段或权限功能进行选择使用或开启关闭。
e) App提供者需明确SDK初始化时机，无合理理由，不得在用户授权同意前初始化SDK。
f) App提供者宜审核监督SDK申请权限的时机、频率和必要性。

g) App提供者需确认调用SDK收集个人信息的频率是实现自身业务功能所必需的最低频率。在用户无操作以及无合理场景时，App不宜调用SDK能力收集任何个人信息。
h) App提供者需确认向用户告知所接入的SDK的相关信息，包括但不限于：SDK名称，SDK收集的个人信息类型、目的和方式，申请的敏感权限、申请目的、隐私政策链接等，并征得用户同意。
i) 若SDK需向用户单独告知收集使用个人信息的行为，App提供者需确认为其中无单独页面的SDK提供向用户告知的便捷渠道。

8.3.2 SDK 提供者

开发阶段SDK提供者需满足以下安全要求：

a) SDK提供者需配合App提供者进行SDK的接入版本确认，需要说明的内容包括但不限于：版本发布记录，版本名称，修订时间，修订说明，停止维护时间等；当SDK更新时，SDK提供者宜及时提醒和告知App提供者使用最新版本。
b) SDK收集使用个人信息和申请敏感权限需遵循合理、最小、必要原则。
c) 对于可选字段或权限，SDK提供者宜进行功能拆分或提供单独的开启关闭选项，允许App提供者根据业务和场景需求进行选择使用或开启关闭，不宜强制捆绑无关功能并以此为由申请无关权限或收集无关的个人信息。
d) SDK提供者需在隐私政策或接入文档中向App提供者声明合理的SDK初始化时机，无合理理由，不得在用户授权同意前初始化SDK。
e) 在用户或App提供者未使用SDK相关业务功能时，SDK不宜提前、频繁、强制申请权限。非由用户主动触发SDK功能，且没有该权限参与此业务功能无法实现的场景下，SDK不宜主动向用户申请权限。
f) SDK收集个人信息的频率宜为实现自身业务功能所必需的最低频率。在App用户或App提供者未使用SDK相关业务功能，或App未提供合理功能场景时，SDK不宜采集和回传任何个人信息。
g) SDK提供者需在隐私政策或接入文档中明确披露其收集的个人信息字段和收集目的以及申请的敏感权限和申请目的，并征得用户同意。
h) 在用户或App提供者未使用相应SDK功能时，SDK不宜提前申请权限或者通过自启动、关联启动等方式自行运行。
i) 在用户或App提供者未使用相应功能时，SDK不宜关联启动其它SDK或App。
j) SDK提供者需响应App提供者的请求和反馈，提供SDK接入技术指导及合规性建议，基于国家法律法规要求变化及时优化SDK功能代码、保护用户个人信息安全。

8.4 运营阶段

8.4.1 App 提供者

运营阶段App提供者需满足以下安全要求：

a) App提供者需履行对SDK的安全管理义务，确保用户在同意隐私政策之后再使用SDK相关业务功能。
b) App提供者需对所接入的SDK持续进行安全监测或定期进行安全检测，并建立预警机制；若发现新的安全漏洞，需及时通知SDK提供者并督促其进行修复。
c) App提供者需对所接入的SDK的实际运行行为进行持续动态监测，若发现其存在恶意行为，需及时停止使用；对于情节严重者，宜终止与SDK提供者的合作协议并向SDK提供者追究责任。
d) App提供者需遵守国家法律法规要求并持续跟进国家法律法规要求变化，在相关法律法规要求发生变化时，宜及时通知SDK提供者并提醒其进行更新。

e) App提供者需持续跟进SDK的功能和数据处理规则更新，及时修复个人信息相关问题、落实相应功能变化并更新隐私政策文本。若隐私政策文本发生实质性变化，需再次征求用户授权同意。若使用的SDK发生重大版本变更，需再次进行安全合规评估。

f) App提供者需在App界面上为所接入的SDK实现便捷的用户反馈和投诉建议访问途径。

8.4.2 SDK 提供者

运营阶段SDK提供者需满足以下安全要求：

g) SDK提供者需对自身SDK持续进行安全监测或定期进行安全检测，并建立预警机制；若发现新的安全漏洞，需立即告知App提供者并及时进行修复。

h) SDK提供者需遵守国家法律法规要求并持续跟进国家法律法规要求变化，在相关法律法规要求发生变化时，需及时遵照要求更新SDK功能代码、保护用户个人信息安全，还需同步更新个人信息处理规则和App开发指引并告知App提供者。

i) SDK提供者需根据业务所需的最小期限存储个人信息，法律法规另有规定的除外。

j) SDK提供者需对用户敏感个人信息采取加密等安全、技术措施进行保护，禁止对用户敏感个人信息进行明文存储和传输。

k) SDK提供者需建立完善的用户反馈和投诉建议机制并将相关信息明确告知App提供者，且需配合App提供者对用户的相关请求进行处理。

8.5 退出阶段

8.5.1 App 提供者

退出阶段App提供者需满足以下安全要求：

a) APP提供者宜建立第三方SDK服务终止和系统下线的相关机制。

b) App提供者需配合SDK提供者将查询、更正、删除个人信息和撤回授权同意的渠道展示在App的交互界面上，且访问该渠道的方法需尽可能便捷。

c) 当用户提出查询、更正、删除个人信息或撤回授权同意的请求与SDK相关时，App提供者需及时将其转达给SDK提供者并配合其进行处理。

d) 当SDK停止运营时，App提供者需及时从App中移除与该SDK相关的代码模块。

e) 有下列情形之一的，App提供者需敦促SDK提供者及时删除或匿名化处理从APP提供者处接收的个人信息，且立即停止与其共享信息：

1) 用户撤回授权同意；
2) App不再使用相应的SDK；
3) App停止运营，不再提供产品或服务；
4) SDK停止运营，不再提供产品或服务；
5) SDK提供者所保存的个人信息已超出约定的存储期限；
6) App提供者和SDK提供者所签订的合作合同中规定的相应情形；
7) 法律法规规定的其他情形。

f) 若SDK具有选择退出机制，App提供者需配合SDK提供者将其访问渠道展示在App的交互界面上，且提供便捷的访问该渠道的方法。

8.5.2 SDK 提供者

退出阶段SDK提供者需满足以下安全要求：

a) SDK提供者宜建立SDK服务终止和系统下线的相关机制。

b) 当SDK停止运营时，SDK提供者需提前告知使用该SDK的App提供者。

c) SDK提供者需为用户提供便捷有效的查询、更正、删除个人信息和撤回授权同意的渠道并将其告知App提供者。

d) 当从App提供者处收到用户所提出的查询、更正、删除个人信息或撤回授权同意的请求时，SDK提供者需及时响应其请求。

e) 有下列情形之一的，SDK提供者需主动删除或匿名化处理从APP提供者处接收的个人信息：

1) SDK停止运营，不再提供产品或服务；

2) SDK提供者所保存的个人信息已超出约定的存储期限；

3) App提供者和SDK提供者所签订的合作合同中规定的相应情形；

4) 法律法规规定的其他情形。

f) SDK提供者宜建立便捷有效的SDK选择退出机制并将其访问渠道告知App提供者，保障用户的自主选择权。

参 考 文 献

[1] TC260-PG-20205A 《网络安全标准实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引》

[2] 《中华人民共和国个人信息保护法》