ICS 33.050
CCS M 30

团　体　标　准

T/TAF 189—2023

软件开发工具包（SDK）用户权益保障基本要求

Basic requirements for user rights protection of Software Development Kit（SDK）

2023-10-31 发布　　2023-10-31 实施

电信终端产业协会　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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、每日互动股份有限公司、友盟同欣（北京）科技有限公司、华为技术有限公司、北京抖音信息服务有限公司、维沃移动通信有限公司、北京快手科技有限公司、荣耀终端有限公司、阿里巴巴(中国)有限公司、北京奇虎科技有限公司、小米通讯技术有限公司、蚂蚁科技集团股份有限公司、OPPO广东移动通信有限公司、上海兆言网络科技有限公司、科大讯飞股份有限公司、网易（杭州）网络有限公司、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：常浩伦、李鑫、臧磊、汤立波、郭文双、方毅、董霖、叶新江、李颖莹、郄世杰、姚栋、贾紫薇、李实、衣强、安潇羽、赵乃萱、姜宇栋、杜蕾、徐曼、落红卫、王昕、李辰淑、赵晓娜、黄天宁、姚一楠、张向拓、汪坤、石玉珍、杨晓丹、郑云、余明明、罗文广、朱星星、刘献伦。

软件开发工具包（SDK）用户权益保障基本要求

1 范围

本文件规定了第三方SDK向SDK使用者和最终用户提供服务全生命周期的用户权益和个人信息保护相关保障要求。

本文件适用于第三方SDK开发者规范自身向SDK使用者和最终用户提供服务过程，同时也适用于主管部门、第三方评估机构等对SDK用户权益保护能力进行监督和评估。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

软件开发工具包 software development kit；SDK

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。

3.2

软件开发工具包使用者 software development kit user

集成使用软件开发工具包的移动应用程序（APP、小程序等）开发者，简称SDK使用者。

3.3

最终用户 end user

在终端设备上使用移动应用程序的个人用户。

4 SDK 服务提供前的保障要求

4.1 SDK 个人信息处理规则

SDK应简洁、清晰、易懂地公开展示其个人信息处理规则，并满足以下要求：

a） 个人信息处理规则中应包括以下内容：

1） 个人信息处理者的名称或者姓名和联系方式；

2） 收集、存储、使用、加工、传输、提供、公开、删除等个人信息处理各环节规则，包括处理个人信息的种类、目的、方式、范围及保存期限；

3） 最终用户行使其决定、查阅、复制、转移、更正、补充、删除等权利的方式和程序；

4） 法律、行政法规规定应当告知的其他事项。

b） SDK 应单独制定个人信息处理规则，并明示其对应的 SDK 名称，不应与公司内其他 APP、网站、小程序等产品服务共用同一个人信息处理规则；

c） 同一 SDK 开发者主体包含多个 SDK 产品的，宜分别制定个人信息处理规则，共用同一个人信息处理规则的，应显著区分不同 SDK 产品对应的各环节个人信息处理规则（如：单独成章、SDK 名称加粗等方式）；

d） 个人信息种类应具体明确信息名称，不应采用概况性描述，如仅描述设备标识符，未明确 IMEI、IMSI、OAID 等具体信息名称；

e） 应明确 SDK 基本业务功能和扩展业务功能，区分描述对应所需必要个人信息、可选个人信息，以及需向最终用户申请的系统权限；

f） 涉及敏感个人信息的名称应采用字体加粗、字号增大、下划线等方式突出显示；

g） 处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则；

h） 向中华人民共和国境外提供个人信息的，应明示境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及最终用户向境外接收方行使权利的方式和程序等事项；

i） 处理个人信息进行个性化推荐或大数据分析业务功能的，应告知其业务功能所使用的个人信息种类、目的意图、主要运行机制等；

j） 集成使用第三方 SDK 或因业务需要将个人信息传输至其他第三方的，应告知第三方产品名称、主体名称、第三方处理个人信息种类及目的、第三方个人信息处理规则等。

4.2 SDK 合规使用说明

SDK应简洁、清晰、易懂地向SDK使用者提供合规使用说明，满足以下要求：

a） 合规使用说明中应包括以下内容：

1） SDK 各项扩展业务功能介绍及对应关闭的配置方式、示例；

2） SDK 各项可选个人信息使用目的、场景及对应关闭的配置方式、示例；

3） SDK 收集个人信息频次、精度可配置的，应明确不同频次、精度使用目的、场景及对应选择的配置方式、示例；

4） SDK 所需的系统权限与各业务功能间的关系，并说明权限申请时机；

5） SDK 初始化及各项业务功能接口合规调用时机，如最终用户选择使用第三方登录方式后，初始化某第三方登录 SDK；

6） 提供向最终用户披露条款的示例，包括自身 SDK 名称、公司名称、处理个人信息种类及目的、自身个人信息处理规则文本下载或展示链接等；

7） 获取最终用户授权同意的建议方式，其中需要取得最终用户单独同意的，应显著提示并给出示例；

8） 以嵌入接口形式向最终用户提供行使权利的，应提供接口调用方式、示例；

9） 其他相关法律法规规章的合规要求对应的配置方式、示例。

b） 文本中应客观描述各项配置功能及其效果，不应通过扩大配置选项对业务功能影响等方式，诱导 SDK 使用者接受默认配置选项；

c） 合规使用说明应单独制定，或在 SDK 集成接入文档中设立单独章节，明示其对应的 SDK 名称。

4.3 其他要求

SDK提供服务前还应满足以下要求；

a） 应向 SDK 使用者提供 SDK 包名、工程文件摘要值等唯一性标识，便于 SDK 使用者验证 SDK 唯一性、完整性；

b) 应在 SDK 文件下载同一页面，公开展示 SDK 名称、开发者、版本号、主要功能、个人信息处理规则、合规使用说明等信息，未公开提供下载页面的，应在 SDK 产品介绍页面公开展示上述信息；
c) 宜向 SDK 使用者提供 SDK 个人信息保护能力评估报告（自评估或第三方检测机构报告）。

5 SDK 提供服务过程中的保障要求

SDK提供服务过程中应满足以下要求：
a) 个人处理规则变更应及时告知 SDK 使用者，不应使用热更新等远程控制方式擅自更改个人信息处理规则；
b) 不应擅自变更 SDK 使用者各项业务功能及个人信息配置状态；
c) 因主管部门、监管机构要求整改或个人信息处理规则发生重大变更的 SDK 版本更新，应通过邮件、电话等方式告知 SDK 使用者，SDK 使用者 3 个月未更新的，宜采用强制方式要求 SDK 使用者更新；
d) 发生或可能发生个人信息泄露、篡改、丢失的，应通过邮件、电话等方式告知 SDK 使用者，并采取补救措施，需要更新 SDK 版本的，宜采用强制方式要求 SDK 使用者更新；
e) 停止集成某 SDK 时，应及时移除该 SDK 相关代码，并告知该 SDK 提供者，要求删除相关个人信息或匿名化处理（法律法规要求留存的除外）；
f) 版本更新后，宜采用便捷方式兼容 SDK 使用者已有的配置选项；
g) 提供互联网弹窗信息服务的，不应出现欺骗、误导、强迫最终用户跳转、下载、浏览等行为；
h) 应建立最终用户诉求和投诉响应管理机制，并在接到诉求和投诉后 15 个工作日内进行响应；
i) 宜定期对 SDK 个人信息保护能力进行评估（自评估或第三方检测机构评估）。

6 SDK 停止提供服务后的保障要求

SDK停止提供服务后应满足以下要求：
a) 停止对外提供服务后，应删除该 SDK 全部处理的个人信息，或进行匿名化处理（法律法规要求留存的除外）；
注：在仍有部分SDK使用者逐步退出阶段，不宜再留存相关个人信息，具体按照双方协议完成后续处理行为。
b) 停止对外提供服务前，应告知相关 SDK 使用者对已处理个人信息的处理方式。

7 SDK 与 SDK 使用者双方的权利义务

SDK应与SDK使用者明确各方权利和义务，要求如下：
a) 应通过合同等形式明确约定以下内容（包括但不限于）：
1) SDK 个人信息处理规则；
2) SDK 响应最终用户诉求、投诉的方式、程序；
3) 各方处理关系变更或解除后的个人信息处理方式；
4) 个人信息安全责任、保护措施及应对突发事件的联动机制。
b) SDK 应对自身业务功能、个人信息处理活动、保障措施负责：
1) 应根据相关法律法规、主管部门或监管机构相关要求设计开发 SDK 产品；
2) 应按照约定内容向 SDK 使用者提供相关文件资料及功能服务；
3) 应满足本文件规定的各项保障基本要求；

4） 不应欺骗、隐瞒个人信息处理相关事项。

c） SDK 使用者承担使用 SDK 的相应个人信息保护责任，要求如下：

1） 应对集成使用的 SDK 进行来源确认和完整性校验；

2） 使用 SDK 应按照相关法律法规、主管部门或监管机构相关要求对 SDK 进行个人信息保护能力评估，不应使用存在违法违规问题的 SDK；

3） 应按照自身业务场景，合规使用、配置 SDK 产品；

4） 应向最终用户告知 SDK 名称、主体名称、处理个人信息种类及目的、个人信息处理规则等内容，以同意为合法性基础的，应在取得最终用户同意后方可使用 SDK 开展相关业务功能；

5） 应关注SDK版本变更，及时更新使用对最终用户权益和个人信息保护影响较小的SDK版本；

6） 停止使用 SDK 功能服务后，应及时告知 SDK 提供者，并按照约定内容履行双方个人信息删除或匿名化责任义务。

电信终端产业协会团体标准

软件开发工具包（SDK）用户权益保障基本要求

T/TAF 189—2023

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn