即时通信 IM

协议与认证

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

协议与认证
- 服务等级协议
- IM SDK 个人信息保护规则
- IM SDK 合规使用指南
- 安全合规认证
- 数据委托处理协议
- 苹果隐私策略：PrivacyInfo.xcprivacy

版权所有：腾讯云计算（北京）有限责任公司

协议与认证
服务等级协议

最近更新时间：2023-06-06 15:02:32

详细信息，请参见 腾讯云即时通信 IM 服务等级协议 。

版权所有：腾讯云计算（北京）有限责任公司

IM SDK 个人信息保护规则

最近更新时间：2025-06-25 16:10:43

更新说明

IM SDK 隐私保护指引内容更新。
2025年3月31日更新内容：
增加了 HarmonyOS 相关权限说明，完善了 SDK 对个人信息处理的具体内容。
2023年12月27日更新内容：
1. 增加了个人信息、系统权限是否必选的说明。
2. 增加了对扩展功能的描述。

2023年7月11日更新内容：
1. 更新了对 SDK 收集终端用户个人信息的要求。
2. 删除了 Cookie 使用情况表述，本 SDK 不涉及 Cookie 的使用。
3. 完善了 SDK 对个人信息处理的具体内容。

引言

腾讯云即时通信 IM SDK 是一款由腾讯云计算（北京）有限责任公司（以下简称“我们”）提供服务的公有云产品，公司注册地为北京市海淀区知春路49号3层西部309。腾讯云即时通信 IM SDK 产品对接方式包含 SDK、API 能力，由于目前相关法律法规、政策及标准中主要对 SDK 产品的应用提供相关指引，以下将统一以 SDK 视角描述相关内容，如果您是集成、调用 API 能力的第三方开发者，本指引中的内容同样适用于您。
《IM SDK 个人信息保护规则》（以下简称“本规则”）主要向开发者及其终端用户(“终端用户”)告知，为了实现 SDK 产品的相关功能，SDK 产品需收集、使用和处理终端用户个人信息的情况。
请开发者及终端用户认真阅读本规则。如您是开发者，请您确认充分了解并同意本规则后再集成SDK产品，如果您不同意本规则及按照本规则履行对应的用户个人信息保护义务，应立即停止接入及使用 SDK 产品。
特别说明：
如您是开发者，您应当：
1. 遵守法律、法规收集、使用和处理终端用户的个人信息，包括但不限于制定和公布有关个人信息保护的隐私政策等；
2. 告知终端用户 SDK 产品收集、使用和处理终端用户个人信息的情况，并依法征得终端用户同意，在征得终端用户同意后初始化 SDK 产品；
3. 在征得终端用户的同意前、以及在用户触发相应功能场景前，除非法律法规另有规定，不应收集任何终端用户的个人信息；
4. 应按您的应用的具体功能场景，在用户触发具体功能场景时调用 SDK 的相应功能、调用相应权限或处理终端用户的个人信息，未到具体功能场景时不应调用相应的 SDK 功能、调用相应权限或处理终端用户的个人信息。
5. 向终端用户提供易于操作且满足法律法规要求的用户权利实现机制，并告知终端用户如何查阅、复制、修改、删除个人信息，撤回同意，以及限制个人信息处理、转移个人信息、获取个人信息副本和注销账号；

版权所有：腾讯云计算（北京）有限责任公司

6. 遵守本规则的要求，并详细阅读 IM SDK 合规使用指南 查看详细操作指引。如开发者和终端用户对本规则内容有任何疑问或建议，可随时通过本规则第八条提供的方式与我们联系。

一、我们收集的信息及我们如何使用信息

（一）为实现 SDK 产品功能所需收集的个人信息

为实现 SDK 产品的相应功能所必须，我们将向终端用户或开发者收集终端用户在使用与SDK产品相关的功能时产生的如下个人信息：

基本功能：本 SDK 的基本功能是为开发者提供稳定的即时通信服务，包括登录、会话、聊天、关系链、群组等基础服务。

扩展功能：在基本功能的基础上，本 SDK 还提供了额外的扩展功能，例如推送服务、文本消息翻译、客服、语音转文字插件等功能，各插件接入请参见 插件开通指引；推送服务涉及可选信息收集，可参考下文进行接入。

必选信息

为实现基本功能和扩展功能都必须收集的个人信息如下：

服务方案	个人信息类型	处理目的	处理方式	申请的权限	接入方式	敏感个人信息处理的必要性说明
IM SDK	网络连接状态	用于连网优化	调用系统API，获取网络连接状态（WiFi状态及4G\5G状态），进行逻辑判断	网络访问权限	SDK	当网络连接状态（WiFi 状态及4G\5G状态）发生切换时，需要根据当前连接的网络连接状态（WiFi 状态及4G\5G状态），重新连接后台服务器
IM SDK	设备型号	用于离线推送和SDK内部逻辑优化	调用系统API，获取设备型号，进行逻辑判断	无	SDK	1. Android 、iOS 和 Harmony的 IM SDK 需要根据手机类型来判断走哪一个厂商的离线推送通道 2. Web、小程序、Windows 和 macOS 的 IM SDK 根据用户使用设备型号做逻辑优化

IM SDK	系统版本	用于SDK内部逻辑优化	调用系统API，获取系统版本，进行逻辑判断	无	SDK	根据用户使用设备系统版本做逻辑优化

可选信息

基本功能和扩展功能（除推送服务外）不再收集其他可选信息。

为实现推送服务，我们会在 SDK 产品中嵌入第三方 SDK，第三方 SDK 的信息如下：

第三方公司名称	第三方SDK名称	处理的个人信息类型	使用目的	使用功能场景	自启动、关联启动说明	第三方SDK个人信息保护规则
广东欢太科技有限公司	OPPO推送SDK	设备相关信息（例如IMEI 号、Serial Number、IMSI、User ID、Android ID、Google Advertising ID、手机Region 设置、设备型号、手机电量、手机操作系统版本及语言等）、使用推送服务的应用信息、推送 SDK 版本号、网络相关信息、消息发送结果	用于实现消息推送	推送通知消息	基于消息推送的目的，OPPO推送SDK 可能存在自启动行为	https://open.oppomobile.com/wiki/doc#id=10288
华为软件技术有限公司	华为推送SDK	设备相关信息（HMS Core openId）、应用Token、Topic 订阅关系、缓存消息、消息下发记录、PushToken、AAID（应用匿名标识）、Token 申请记录、显示/点击/关闭打点上报记录、应用 ID、应用包名、服务器公网IP地址	用于实现消息推送	推送通知消息	基于消息推送的目的，华为推送SDK 可能存在自启动行为	https://developer.huawei.com/consumer/cn/doc/development/HMSCore-Guides/sdk-data-security-0000001050042177 https://developer.huawei.com/consumer/cn/devservice/term

维沃移动通信有限公司	vivo推送SDK	设备标识信息（如IMEI号）、手机型号、系统类型、系统版本	用于实现消息推送	推送通知消息	基于消息推送的目的，vivo 推送 SDK 可能存在自启动行为	https://www.vivo.com.cn/about-vivo/privacy-policy
小米移动软件有限公司	小米推送SDK	设备相关信息（包括IMEI、OAID（适用于Android Q以上系统）、IMEI MD5、MEIDMD5、Android ID、VAID、AAID，以及用户 MID（适用于MIUI 系统）、设备型号等）	用于实现消息推送	推送通知消息	基于消息推送的目的，小米推送 SDK 可能存在自启动行为	https://dev.mi.com/console/doc/detail?pId=1822
珠海市魅族通讯设备有限公司	魅族推送SDK	位置信息、设备标识信息（WIFI 信息、正在运行的应用列表、手机 ID 信息、运营商信息、MAC地址）	用于实现消息推送	推送通知消息	基于消息推送的目的，魅族推送 SDK 可能存在自启动行为	https://www.meizu.com/legal.html
荣耀终端有限公司	荣耀推送SDK	设备标识符（AAID、PushToken、OAID）、推送消息内容	用于实现消息推送	推送通知消息	基于消息推送的目的，荣耀推送 SDK 可能存在自启动行为	https://developer.hihonor.com/cn/kitdoc?category=%E5%9F%BA%E7%A1%80%E6%9C%8D%E5%8A%A1&kitId=11002&navigation=guides&docId=sdk-data-security.md

Google	Google FCM 推送 SDK	设备唯一标识符、设备类型和设置、操作系统、移动网络信息以及应用版本号、 IP 地址、崩溃报告、系统活动以及相应请求的日期、时间和引荐来源网址、运营商名称、崩溃报告、您已安装的应用，以及关于您如何使用 Android 设备的其他信息（具体取决于您的设备设置）	用于实现消息推送	推送通知消息	基于消息推送的目的，Google FCM 推送 SDK 可能存在自启动行为	https://policies.google.com/privacy https://support.google.com/policies/answer/9581826
Apple（仅 iOS）	Apple Push Notification service	设备令牌（例如device token ）、手机型号、系统版本	用于实现消息推送	推送通知消息	无	https://www.apple.com/legal/privacy/szh/

推送服务集成了 8 家手机厂商的消息推送 SDK，用户使用推送服务时，手机厂商收集和处理用户个人信息的方式，详见手机厂商相关隐私政策。请您查阅以下文档理解每个推送厂商收集的信息类型，根据需求选择具体的厂商进行接入，调用对应平台的集成接口进行相应配置：

Android 平台消息推送 SDK 集成对应厂商指引：Android集成 TIMPush

iOS 平台消息推送 SDK 集成对应厂商指引：iOS集成 TIMPush

（二）为实现 SDK 产品功能所需的权限

为实现 SDK 产品的相应功能所必须，我们会通过开发者的应用在对应的功能场景下申请所需权限。如您是开发者，请您注意，您应按您的应用的具体功能场景，在用户触发具体功能场景时调用 SDK 的相应功能、调用相应权限或处理终端用户的个人信息，未到具体业务或功能场景时不应调用相应权限，点击 IM SDK 合规使用指南 可查看相关操作指引。

操作系统	权限名称	使用目的	功能场景（申请时机）	是否可选
Android	android.permission.INTERNET	用于长连接连网优化	初始化 SDK 时。	否

HarmonyOS	ohos.permission.INTERNET	用于长连接连网优化	初始化 SDK 时。	否

请注意，在不同设备和系统中，权限显示方式及关闭方式可能有所不同，请终端用户参考其使用的设备及操作系统开发方的说明或指引。当终端用户关闭权限即代表其取消了相应的授权，我们和第三方开发者将无法继续收集和使用对应的个人信息，也无法为终端用户提供上述与该等授权所对应的功能。

（三）根据法律法规的规定，以下是征得用户同意的例外情形

1. 为订立、履行与终端用户的合同所必需。
2. 为履行我们的法定义务所必需。
3. 为应对突发公共卫生事件，或者紧急情况下为保护终端用户的生命健康和财产安全所必需。
4. 为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理终端用户的个人信息。
5. 依照本法规定在合理的范围内处理终端用户自行公开或者其他已经合法公开的个人信息。
6. 法律行政法规规定的其他情形。

特别提示: 如我们收集的信息无法单独或结合其他信息识别到终端用户的个人身份，其不属于法律意义上的个人信息。

二、第三方数据处理及信息的公开披露

我们不会与我们的关联公司、合作伙伴及第三方共享（“接收方”）终端用户的个人信息。
我们与第三方合作过程中，将遵守法律规定，按照最小必要原则，安全审慎地处理相关数据。
我们将按照法律法规的规定，对数据处理涉及的第三方进行严格的限制，要求其严格遵守我们关于个人信息保护的措施与要求。
我们不会将终端用户的个人信息转移给任何公司、组织和个人, 但以下情况除外：

1. 事先告知终端用户转移个人信息的种类、目的、方式和范围,并征得终端用户的单独同意;
2. 如涉及合并、分立、解散、被宣告破产等原因需要转移个人信息的, 我们会向终端用户告知接收方的名称或者姓名和联系方式, 并要求接收方继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的, 我们会要求接收方重新取得终端用户的同意。

我们不会公开披露终端用户的个人信息, 但以下情况除外：

1. 告知终端用户公开披露的个人信息的种类、目的、方式和范围并征得终端用户的单独同意后;
2. 在法律法规、法律程序、诉讼或政府主管部门强制要求的情况下。

三、终端用户如何管理自己的信息

我们非常重视终端用户对其个人信息管理的权利，并尽全力帮助终端用户管理其个人信息，包括个人信息查阅、复制、修改、删除、撤回同意、限制个人信息处理、获取个人信息副本、注销账号以及设置隐私功能等，以使终端用户有能力保障自身的隐私和信息安全。
如您是开发者，您应当为终端用户提供并明确其查阅、复制、修改、删除个人信息、撤回同意、转移个人信息、限制个人信息处理、获取个人信息副本和注销账号的方式。

如您是终端用户，由于您不是我们的直接用户，与我们无直接的交互对话界面，为保障您的权利实现，我们已要求开发者提供便于操作的用户权利实现方式。您也可通过本规则 第八条 中的方式与我们取得联系。请您理解，特定的业务功能和服务将需要您的信息才能得以完成，当您撤回同意或授权后，我们无法继续为您提供对应的功能和服务，也不再处理您相应的个人信息。但您撤回同意或授权的决定，不会影响我们此前基于您的授权而开展的个人信息处理。

四、信息的存储

（一）存储信息的地点

我们遵守法律法规的规定，将在中华人民共和国境内收集和产生的个人信息存储在境内。

（二）存储信息的期限

一般而言，我们仅在为实现目的所必需的最短时间内保留终端用户的个人信息，但下列情况除外：

- 为遵守适用的法律法规等有关规定。
- 为遵守法院判决、裁定或其他法律程序的规定。
- 为遵守相关政府机关执法的要求。

五、信息安全

我们为终端用户的个人信息提供相应的安全保障，以防止信息的丢失、不当使用、未经授权访问或披露。
我们严格遵守法律法规保护终端用户的个人信息。
我们将在合理的安全水平内使用各种安全保护措施以保障信息的安全。例如，我们使用加密技术、匿名化处理等手段来保护终端用户的个人信息。
我们建立专门的管理制度、流程和组织确保信息安全。例如，我们严格限制访问信息的人员范围，要求他们遵守保密义务，并进行审查。
若发生个人信息泄露等安全事件，我们会启动应急预案，阻止安全事件扩大，并以推送通知、公告等形式告知开发者。

六、未成年人保护

本 SDK 产品主要面向成年人。
若您是开发者，如果终端用户是未满14周岁的未成年人（“儿童”），您应当向儿童的父母或其他监护人告知本规则，并在征得儿童儿童的父母或其他监护人同意的前提下处理儿童个人信息。如果我们发现开发者未征得儿童监护人同意向我们提供儿童个人信息的，我们将会采取措施尽快删除。
若您是儿童监护人，当您对您所监护儿童个人信息保护有相关疑问或权利请求时，您可以联系开发者，或通过本规则第八条提供的方式与我们联系。

七、变更

我们可能适时修订本规则的内容。
如该等变更会导致终端用户在本规则项下权利的实质减损，我们将在变更生效前，通过网站公告等方式进行提示。如您是开发者，当更新后的本规则对处理终端用户的个人信息情况有重大变化的，您应当适时更新隐私政策，并以弹框形式通知终端用户并且获得其同意，如果终端用户不同意接受本规则，请停止集成 SDK 产品。

八、联系我们

我们设立了专门的个人信息保护团队和个人信息保护负责人，如果开发者和/或终端用户对本规则或个人信息保护相关事宜有任何疑问或投诉、建议时，可以通过以下方式与我们联系：

通过 https://kf.qq.com/ 与我们联系。

将问题发送至 Dataprivacy@tencent.com。

邮寄信件至：中国广东省深圳市南山区海天二路33号腾讯滨海大厦 数据隐私保护部（收）邮编：518054。

我们将尽快审核所涉问题，并在15个工作日或法律法规规定的期限内予以反馈。

IM SDK 合规使用指南

最近更新时间：2025-06-06 14:23:23

为帮助使用腾讯云即时通信 IM SDK 的开发运营者（以下简称“您”）在符合个人信息保护相关法律法规、政策及标准的规定下合规接入、使用第三方 SDK，腾讯云计算（北京）有限责任公司（以下简称"我们"）特制定《腾讯云即时通信 IM SDK 接入使用说明文档》（以下简称“文档”），便于您使用腾讯云即时通信 IM SDK 过程中符合相应的合规要求。请您在接入、使用腾讯云即时通信 IM SDK 前，充分阅读和了解本文档内容。

一、接入/升级至满足监管新规的最新SDK版本

我们高度重视 SDK 的功能优化、个人信息安全和保护，将适时升级迭代 SDK 版本以提升产品的安全性和稳定性，确保符合相关法律法规及、监管及标准的最新合规要求。强烈建议您升级使用最新版本 SDK，以便保障您正常使用 SDK 最新功能、避免因您更新不及时产生的不利影响（例如 App 被通报或下架等）。
SDK 更新后，我们会及时通过官网公告通知或其他适当的方式提醒您更新的内容，以便您及时了解 SDK 最新版本信息。同时，您可以访问SDK最新版本下载链接：
https://cloud.tencent.com/document/product/269/1606 。

二、App 隐私政策中应披露第三方 SDK 相关情况

请您确保您开发或运营的 App 配备了符合监管要求的《隐私政策》文本。请您务必明确告知终端用户您的 App集成了第三方 SDK 服务。您应在《隐私政策》中添加关于本 SDK 收集使用个人信息的目的、方式和范围等，并显示本 SDK 的开发运营者名称及隐私政策链接。您应在 APP 登录注册页面及 APP 首次运行时，通过弹窗、文本链接及附件等简洁明显且易于访问的方式，应当以清晰易懂的语言告知用户《隐私政策》，由用户在充分知情的前提下，作出自愿明确的意思表示。
我们提供以下告知文案示例供您参考，您可以通过文字或表格方式向用户告知。请您理解 SDK 不同版本提供的功能服务及所需的字段信息可能会因开发者的选择或配置不同而存在差异，因此请您参考 SDK 隐私政策及您实际接入使用的 SDK 运行情况向用户进行充分告知并获得用户的同意。

第三方 SDK 名称：腾讯云即时通信 IM SDK
第三方 SDK 提供方的公司名称：腾讯云计算（北京）有限责任公司
使用目的及功能场景：为用户提供单聊、群聊、关系链、资料管理功能服务
处理的个人信息类型：用户标识信息、网络类型、系统语言类型
实现 SDK 产品功能所必需的权限：android.permission.INTERNET(Android)、ohos.permission.INTERNET(HarmonyOS)
第三方 SDK 隐私政策链接：https://cloud.tencent.com/document/product/269/58094
第三方 SDK 官网链接（可选披露）：https://cloud.tencent.com/product/im
处理方式（可选披露）：1.采用 SSL 协议加密及 HTTPS 传输加密技术保障安全；2.采取加密、去标识化等安全措施脱敏处理

三、获得用户同意后再初始化 SDK

为满足法律法规及监管要求，您应确保在获得用户的同意后再初始化 SDK，并在用户触发 SDK 具体功能服务后通过配置 SDK 的相关参数完成发送请求的调用，此时 SDK 才会按照您设置的配置方式采集功能所需的个人信息或申请功能所需的权限。为了避免您在获取用户同意前，提前启动 SDK 收集使用用户个人信息，SDK 提供了 SDK 初始化调用的 API 接口、合规初始化技术配置方案，单击 此处 查看详细操作指引。
1、确保在用户阅读 App 隐私政策并取得用户授权之后，按 App 功能需要在合适时机调用正式初始化函数 initSDK 初始化 SDK。
反之，如果用户不同意《隐私政策》授权，则不能调用初始化接口。该接口仅进行初始化，不会获取个人信息。
2、请勿在用户同意隐私政策之前动态申请涉及用户个人信息的敏感设备权限；请勿在用户同意隐私政策前私自采集和上报个人信息（尤其注意Android_ID、OAID、IMEI、MAC地址、硬件序列号、应用安装列表等用户信息）。
请勿在App处于未激活状态时（例如App在后台运行），请求SDK相关服务。

四、可选信息配置开关

SDK 向您提供了可选个人信息及权限的控制开关，您可以根据 APP 所需的 SDK 功能服务自行配置打开或关闭隐私信息请求开关。

1、配置可选权限

请您注意，SDK 不强制获取可选权限，即使没有获取可选权限，SDK 提供的基本功能也能正常运行。您可以配置可选权限，以便使用SDK提供的其他可选功能。建议调用请求前在合适的时机调用 SDK 提供的方法，在用户授权的情况下获取声明中的权限。

操作系统	权限名称	使用目的	功能场景（申请时机）	是否可选
Android	android.permission.INTERNET	用于长连接连网优化	初始化 SDK 时。	否
HarmonyOS	ohos.permission.INTERNET	用于长连接连网优化	初始化 SDK 时。	否

请注意，在不同设备和系统中，权限显示方式及关闭方式可能有所不同，请终端用户参考其使用的设备及操作系统开发方的说明或指引。当终端用户关闭权限即代表其取消了相应的授权，我们和开发者将无法继续收集和使用对应的个人信息，也无法为终端用户提供上述与该等授权所对应的功能。

2、配置可选个人信息

请您注意，SDK 不强制获取可选参数，即使没有获取可选参数，SDK 提供的基本功能也能正常运行。您可以配置可选参数，以便使用 SDK 提供的其他可选功能。建议调用请求前在合适的时机调用 SDK 提供的方法，在用户授权的情况下获取声明中的参数信息。点击 IM SDK 隐私保护指引 查看详细操作指引。

3、配置可按照不同频次、精度收集个人信息

SDK 的数据采集仅在 App 调用/最终用户触发相关功能时触发，不涉及定时逻辑等频次控制选项。

4、指导建议

请您重点关注，在 App 安装、运行和使用相关功能时，您应遵从国家相关法律法规、监管政策及标准的要求，收集用户个人信息或申请敏感权限，不得存在以下违规行为：
（1）未经用户同意不得收集任何个人信息。
（2）非服务所必需或无合理应用场景下，用户拒绝相关授权申请后，应用不得自动退出或关闭。
（3）在用户明确拒绝权限申请后，APP 不应向用户频繁弹窗或反复申请开启与当前服务场景无关的权限、影响用户正常使用，建议掌握合适时机申请敏感权限，不得影响其他功能可用。
（4）不得未明确告知用户索取权限的目的和用途。
（5）App 首次打开或运行中，未见使用权限对应的相关功能或服务时，不应提前向用户弹窗申请开启敏感权限。
（6）不得超出业务功能实际需要过度收集个人信息。

五、SDK扩展业务功能配置方式

基本业务功能：本 SDK 的基本功能是为开发者提供稳定的即时通信服务，包括登录、会话、聊天、关系链、群组等基础服务。
扩展业务功能：在基本功能的基础上，本 SDK 还提供了额外的扩展功能，比如推送服务、文本消息翻译、客服插件、语音转文字插件等功能。
点击 IM SDK 隐私保护指引 查看详细操作指引。

六、用户权利保障机制

如果您需要我们协助来实现您最终用户的其他个人信息主体权利请求，您可以通过“联系方式”来申请协助。

七、Demo 的使用说明

为了帮助您快速了解、体验SDK功能，我们向您提供 SDK Demo，仅供您参考，不做为正式产品。请您理解，由于 Demo 运行方式与正式 App 运行方式有所差异，为实现 Demo 正常运行以便向您提供尽可能全面的 SDK 功能体验，我们在 Demo 中引用了部分依赖库，且仅限于在 Demo 场景下使用。当您接入正式 SDK 产品时请按照 SDK 正式集成文档进行操作。

八、联系方式

我们设立了专门的个人信息保护团队和个人信息保护负责人, 如果您和/或终端用户对本规则或个人信息保护相关事宜有任何疑问或投诉、建议时, 可以通过以下方式与我们联系：
(i) 通过 腾讯客服（ https://kf.qq.com/ ）或 填写工单 与我们联系。
(ii) 将问题发送至 Dataprivacy@tencent.com。
(iii) 邮寄信件至: 中国广东省深圳市南山区海天二路33号腾讯滨海大厦 数据隐私保护部(收)邮编: 518054。
我们将尽快审核所涉问题, 并在15个工作日或法律法规规定的期限内予以反馈。

九、注意事项

1. 您接入腾讯云即时通信 IM SDK 前的合规自查

为确保您就本 SDK 的使用获得终端用户的授权，且遵守个人信息保护要求和合规流程，我们建议您在接入腾讯云即时通信 IM SDK 前进行合规自查。

1.1 请仔细阅读并按本说明文档提示对您 App 的《隐私政策》进行合规自查。

1.2 请务必做延迟初始化配置，确保获得用户同意后再初始化 SDK。

1.3 当腾讯云即时通信 IM SDK 基于最新的法律法规或监管要求进行更新后，请您在收到版本更新通知时及时将您 App 集成的腾讯云即时通信 IM SDK 升级到最新版本。

1.4 其他国家相关法律法规、监管政策及标准的要求。

2. 以下合规文件供开发者参考：

（1）《个人信息保护法》
（2）《工业和信息化部关于进一步提升移动互联网应用服务能力的通知》
（3）《工业和信息化部关于开展信息通信服务感知提升行动的通知》
（4）《工业和信息化部关于开展纵深推进APP侵害用户权益专项整治行动的通知》
（5）《工业和信息化部关于开展APP侵害用户权益专项整治工作的通知》
（6）《App违法违规收集使用个人信息行为认定方法》
（7）《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》
（8）《常见类型移动互联网应用程序必要个人信息范围规定》
（9）《GB/T 35273-2020信息安全技术 个人信息安全规范》
（10）《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》
（11）《网络安全标准实践指南—移动互联网应用程序（App）系统权限申请使用指南》《网络安全标准实践指南—移动互联网应用程序（App）系统权限申请使用指南》

安全合规认证

最近更新时间：2022-04-19 16:58:19

合规性是腾讯云即时通信 IM 发展的基础，腾讯云即时通信 IM 遵从不同国家和行业的合规性要求，除了保证所提供服务的安全性、合规性、可用性、保密性和隐私性之外，还可以为使用即时通信 IM 的客户提供相关支持，满足企业及其客户的多项合规监管需求，降低公司及客户在审计工作上的重复投入，提高审计与管理效率。
即时通信 IM 已通过 SOC 系列审计报告（包括 SOC 1、SOC 2、SOC 3）、网络安全等级保护2.0（三级）、ISO系列认证（包括 ISO 9001、ISO 20000、ISO 27001、ISO 27017、ISO 27018、ISO 27701、ISO 29151）、CSA STAR、NIST CSF、BS10012 和 KISMS 等认证。

SOC 1 Type II报告

参照 AICPA 审计准则 SSAE No. 18 中的 AT-C section 320 针对腾讯云云服务体系的控制环境出具的报告

SOC 2 Type II报告

参照 AICPA 审计准则 SSAE No. 18 中的 AT-C section 205 以及 TSP section 100 2017版，针对云服务体系的安全性、可用性、机密性出具的报告

SOC 3 Type II报告

参照 AICPA 审计准则 SSAE No. 18 中的 AT-C section 205 以及 TSP section 100 2017版，针对云服务体系的安全性、可用性、机密性报告出具的一般控制报告

网络安全等级保护2.0

腾讯金融云通过了等级保护四级备案和测评，公有云通过了等级保护三级备案和测评

ISO 9001 质量管理体系认证

腾讯云是国内首家在云计算领域获得 ISO 9001 CNAS 和 ANAB 双认可的云计算服务商，实施有效的质量控制流程交付优质的云服务

版权所有：腾讯云计算（北京）有限责任公司

ISO 20000 IT 服务管理体系认证

腾讯云是国内首家通过 ISO 20000-1:2018 新版标准认证的云计算服务商，建立并严格执行标准的 IT 服务管理流程

ISO 27001 信息安全管理体系认证

ISO/IEC 27001:2015 是 ISO/IEC 27002:2013 的补充，腾讯云通过 ISO 27001指导证书，证明腾讯云实施了有效设计和实施云计算信息安全控制

ISO 27017 云服务信息安全控制实施指引

ISO/IEC 27017:2015 是 ISO/IEC 27002:2013 的补充，腾讯云通过 ISO 27017指导证书，证明腾讯云实施了有效设计和实施云计算信息安全控制

版权所有：腾讯云计算（北京）有限责任公司

ISO 27018 公有云个人信息保护认证

腾讯云致力于保护每个客户的个人信息，构建完善的个人信息管理体系，采用各种技术手段保护用户个人信息

ISO 27701 个人信息管理体系国际标准

腾讯云是全球首家通过 ISO/IEC 27701认证的云服务提供商，建立和实施了隐私信息管理体系，并具备持续改进的能力

ISO 29151 个人身份信息保护实践指南

腾讯云提供了恰当的信息安全风险管理环境用于个人身份信息的保护，同时满足行业最佳实践，具备持续改进的能力

CSA STAR 云安全管理体系认证

CSA STAR 是针对云安全特性的一项国际性认证，腾讯云以金牌等级通过了 STAR 认证，强化云安全技术管控

NIST 网络安全框架

NIST CSF 是美国国家标准技术研究所根据行政命令(E0) 13636“改进关键基础设施网络安全”开发，该框架侧重于使用业务驱动因素来指导网络安全活动

KISMS 认证

腾讯云是中国首家通过 KISMS 认证的云计算服务商，证明腾讯云建立的信息安全管理体系和能力满足相关韩国法律和标准合规性要求

BS 10012

英国标准协会发布的个人信息管理体系标准

数据委托处理协议

最近更新时间：2025-02-11 11:30:43

本数据处理协议是腾讯云计算（北京）有限责任公司（简称“腾讯云”）与您之间就您使用腾讯云即时通信 IM 服务时，您委托腾讯云处理您的数据所签订的协议。您应当充分阅读、理解本协议，其中限制、免责条款或者其他涉及您重大权益的条款将会以加粗、加下划线等形式提示您重点注意。
您通过勾选、点击确认或以其他方式表示接受本协议，或您以任何方式使用腾讯云即时通信 IM 服务的，即视为您已阅读并同意接受本协议的约束，本协议即在您与腾讯云之间产生法律效力。

1. 定义与解释

除本协议上下文另有说明外，本协议中所涉及的术语具有如下含义：
1.1 个人信息，是指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。
1.2 非个人信息，是指以电子或其他方式记录的除个人信息外的各种信息，包括但不限于非属于个人信息的运营数据信息、用于大数据分析的聚合匿名数据集等。如技术发展能够将匿名数据转换成个人信息，那么这些信息将被视为个人信息，适用本协议以及适用法律法规中对于个人信息的相关规定。
1.3 敏感个人信息，是指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，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。
1.4 个人信息主体，是指个人信息所标识或者关联的自然人。
1.5 数据处理者，是指在数据处理活动中自主决定处理目的、处理方式，应依法履行数据处理相关义务并对数据处理活动负责的组织和个人，为免疑义，在本协议约定的委托处理关系项下，委托方为数据处理者。
1.6 数据处理，是指数据处理者对数据所采取的包括但不限于收集、存储、使用、加工、传输、提供、公开、删除等处理活动。
1.7 个人信息保护影响评估，是指针对个人信息处理活动，检验其处理目的、处理方式是否合法正当必要，对个人权益的影响和安全风险，所采取的保护措施是否合法有效并与风险程度相适应的评估活动。
1.8 数据出境，是指数据处理者向境外提供其在中华人民共和国（为本协议之目的，不包括香港、澳门、台湾地区）境内运营中收集和产生的数据。
1.9 适用的数据保护法，是指数据处理活动涉及国家或地区的适用的关于网络安全与数据保护的法律、法规、规章、规范性文件及其他具有强制约束力的规范或指令及其不断修订、更新的版本；为本协议之目的，适用法律包括但不限于《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等。
1.10 本协议中其他未定义术语的含义，如无特殊约定的应与相关法律法规规定的含义保持一致。

2. 委托处理数据的范围及目的

2.1 双方确认并同意，由您委托腾讯云进行数据处理活动，其中您为数据处理者，腾讯云为接受您委托根据您指令进行数据处理活动的受托方。在本协议项下，您作为数据处理者，享有并承担适用的数据保护法及本协议规定的作为数据处理者的所有权利和义务，对个人信息处理活动负责。腾讯云将严格遵守适用的数据保护法及本协议规定的所有义务，按照您的指示进行数据处理活动。

版权所有：腾讯云计算（北京）有限责任公司

2.2 您委托腾讯云对您所有、收集或控制的数据进行委托处理活动，委托处理数据的数据范围、处理目的、处理方式、委托处理期限具体如下：

业务场景	数据清单	处理目的	处理方式	处理期限
使用即时通信 IM 服务	用户信息：本功能相关用户的昵称、头像 URL、个性签名等（视用户设置 而定） 消息内容：文字、照片、音频、视频	提供即时通信服务，实现在终端用户之间通讯消息传输	您或您的终端用户上传。 您可选择是否存储在腾讯云的服务器，如存储在腾讯云服务器，数据将存储在您选择的数据中心，根据您设置的时长存储，默认存储时长为7天。 如不存储在腾讯云的服务器，此类数据只会在腾讯云服务器处理，用于消息传输，不存储。	具体以双方业务合作所必须的处理期限为准。
	公网出口 IP、接口请求日志（包括请求的接口名称和时间）、接口异常信息（包括发生异常的原因）	确保功能正常运行，并用于故障排除	您或您的终端用户在使用即时通信 IM 服务时，向腾讯云即时通信 IM 后台发送请求产生的日志数据。存储在您选择的数据中心，数据产生后7天自动删除。	具体以双方业务合作所必须的处理期限为准。
	应用程序维度接口的成功率和平均延迟	服务质量统计分析、优化服务体验	终端上报实时监控数据，存储在您选择的数据中心，数据产生后2天自动删除。 聚合实时数据生成统计数据，存储在您选择的数据中心，数据产生后2个月自动删除。	具体以双方业务合作所必须的处理期限为准。
	应用程序配置信息，包括：您的套餐/包月信息、管理员账户、应用程序详细信息（如应用程序名称、SDKAPPI	维护应用程序的相关配置，确保功能正常运行，并用于计费	您在即时通信 IM 控制台创建应用后，配置的应用数据，存储在您选择的数据中心。 其中应用程序信息为实现腾讯云计费将传输到中国大陆（不包括香港、澳门和台湾地区）。	具体以双方业务合作所必须的处理期限为准。

	D、简介、应用程序类型、应用程序密钥、应用 ID、应用程序描述、应用程序状态、应用程序创建时间、应用程序更新时间）、自定义好友字段、自定义用户字段、自定义组成员字段、自定义组字段等			
使用音视频通话能力（在视频、语音通话场景中）	Wi-Fi 状态	针对网络类型进行网络优化	您或您的终端用户在使用音视频通话能力时，向腾讯云实时音视频 TRTC 后台发送请求产生的日志数据。存储在您选择的站点，数据产生后15天自动删除。	具体以双方业务合作所必须的处理期限为准。
	系统属性	针对 Android 兼容性问题进行适配	您或您的终端用户在使用音视频通话能力时，向腾讯云实时音视频 TRTC 后台发送请求产生的日志数据。存储在您选择的站点，数据产生后15天自动删除。	具体以双方业务合作所必须的处理期限为准。
	设备型号	Android/iOS 的兼容问题、崩溃问题进行适配和分析	您或您的终端用户在使用音视频通话能力时，向腾讯云实时音视频 TRTC 后台发送请求产生的日志数据。存储在您选择的站点，数据产生后15天自动删除。	具体以双方业务合作所必须的处理期限为准。
	操作系统	Android/iOS 的兼容问题、崩溃问题进行适配和分析	您或您的终端用户在使用音视频通话能力时，向腾讯云实时音视频 TRT后台发送请求产生的日志数据。存储在您选择的站点，数据产生后15天自动删除。	具体以双方业务合作所必须的处理期限为准。
	IP 地址	检测网络链连接质量	您或您的终端用户在使用音视频通话能力时，向腾讯云实时音视频 TRTC 后台发	具体以双方业务合

			送请求产生的日志数据。存储在您选择的站点，数据产生后15天自动删除。	作所必须的处理期限为准。
	相机	视频通话时采集视频画面	您或您的终端用户上传。 采用去标识化、加密传输的安全处理方式，此类数据只会在腾讯云服务器处理，用于数据传输，不存储。	具体以双方业务合作所必须的处理期限为准。
	录音	视频、音频通话时采集声音	您或您的终端用户上传。 采用去标识化、加密传输的安全处理方式，此类数据只会在腾讯云服务器处理，用于数据传输，不存储。	具体以双方业务合作所必须的处理期限为准。
	传感器信息	获取手机横竖屏状态来适配采集画面的方向	仅做本地处理、不传输不上报。	具体以双方业务合作所必须的处理期限为准。
使用音视频通话能力（合唱、K歌中需要听到自己的声音等场景）	音频数据	在华为设备上开启/关闭硬件耳返功能	由音视频通话能力服务集成华为技术有限公司“硬件耳返”SDK 处理相关数据。 采集华为设备终端的音频信息并在本终端上进行实时播放（仅限连接有耳机时）。	具体以双方业务合作所必须的处理期限为准。
使用音视频通话能力（在视频、语音通话场景中）	信令数据	处理 IM 信令信息	由音视频通话能力服务“com.google.gson”SDK 处理相关数据。 转换通话中信令消息的格式。	具体以双方业务合作所必须的处理期限为准。
使用通话记录功能	userId	用于在通话记录看板上展示 userId 信息	通话结束后终端进行上报，存储在您选择的数据中心，如果您未开通通话记录功能，我们不会存储，如果您开通了通话记	具体以双方业务合作所必须

			录功能，我们按照您选择的存储期限进行存储。	的处理期限为准。
	platform（Andriod、iOS）	用于在通话记录看板上展示platform（Andriod、iOS）信息	通话结束后终端进行上报，存储在您选择的数据中心，如果您未开通通话记录功能，我们不会存储，如果您开通了通话记录功能，我们按照您选择的存储期限进行存储。	具体以双方业务合作所必须的处理期限为准。
	通话时长	用于在通话记录看板上展示通话时长信息	通话结束后终端进行上报，存储在您选择的数据中心，如果您未开通通话记录功能，我们不会存储，如果您开通了通话记录功能，我们按照您选择的存储期限进行存储。	具体以双方业务合作所必须的处理期限为准。

2.3 双方同意，在本协议有效期内，如双方需要对委托处理活动的数据范围、处理目的、处理方式等进行变更或者修改的，应当在经双方协商一致后，通过签订书面补充协议的方式进行补充约定或者替代约定。

3. 双方的数据处理义务

3.1 数据处理原则

3.1.3 腾讯云将遵循合法、正当、必要和诚信原则，基于您的委托、指令和需求并以向您提供本服务为目的处理包括个人信息在内的相关数据，腾讯云开展的数据处理活动不能超出您指示以及本协议约定的目的、方式和范围。
3.1.2 腾讯云认为您的指示违反适用法律时，有权立即通知您，停止提供本服务，并不承担违约责任。

3.2 数据出境

3.2.1 您充分理解并同意：使用该服务时将会对您的数据传输至境外服务器，以实现服务目的；数据出境行为是根据您的指示执行，腾讯云仅受您的委托提供技术服务。您应当承担数据处理者有关数据出境的责任和义务，包括但不限于：告知个人信息主体并获得个人信息主体的同意、按照境内法律法规和监管要求进行数据出境安全评估和申报等。
3.2.2 如因您未按照要求履行数据出境相关义务，由此导致的全部后果由您自行承担，与腾讯云无关。

3.3 数据安全

3.3.1 腾讯云将根据适用法律的要求，确保数据安全，并采取符合行业标准的数据安全保护措施，保护处理的数据免受意外、非法或未经授权的破坏、丢失、更改、访问、披露或使用，以及其他形式的非法处理。发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施。
3.3.2 如您对数据安全措施有特殊要求的，应当以书面形式向腾讯云提出，腾讯云将在适用法律允许的范围内，结合届时的技术水平，对您的合理要求予以响应。

3.4 数据合规

您承诺已就本协议项下所涉的数据委托处理行为履行法定义务，有权开展该等数据委托处理行为。特别地，如委托处理数据包括个人信息的，您应履行包括但不限于如下合规要求：

（a）您承诺其已经就可能委托第三方开展个人信息的委托处理向个人信息主体履行适当的告知义务，如适用法律要求的，还应当取得符合要求的个人信息主体授权同意。对于本协议及本项目中所述的数据和目的，您保证其拥有所有必要的数据主体的授权并应留存相关的日志或记录；
（b）您承诺向个人信息主体提供易于操作的查阅、复制、更正、删除其个人信息，撤销或更改其授权同意、注销其个人账号等用户权利响应的实现机制，并依法及时响应个人信息主体的权利请求；
（c）若您未能适当履行本条约定的合规义务或存在其他违反法律法规的情形，腾讯云有权单方终止服务，您应自行承担前述行为造成的法律责任；如前述行为给腾讯云造成损失的，您还应向腾讯云全额赔偿。

3.5 转委托

腾讯云在征得您的书面同意后可提供上述信息并委托子处理者进行数据处理；腾讯云将以书面或电子形式与子处理者签订协议，并体现本协议项下的数据保护条款。

3.6 个人信息权利的响应

3.6.1 腾讯云理解本协议项下数据包括个人信息，并确认将在合理必要范围内协助您响应个人信息主体的权利，如访问、修改、删除、携带等。如果任何个人信息主体联系您，提出个人信息主体权利，包括但不限于访问、更正、限制处理、删除、携带、拒绝和不受自动化决策的要求以及所有类似的要求，且响应该等要求需要腾讯云配合的，**您将及时书面告知腾讯云并作出明确的指示，并与腾讯云开展合作提供合理的协助；如因您迟延通知、指示错误、怠于协助导致腾讯云未能协助完成响应个人信息主体权利请求的，腾讯云不承担任何责任。**
3.6.2 除非双方另有约定，腾讯云不实际承担响应个人信息主体权利请求或承担相关责任。您应当自行响应并处理个人信息主体的权利请求或投诉、司法或行政机关的调查，并开展必要的个人信息保护影响评估。腾讯云将根据适用的数据保护法给予必要的协助，在向您提供任何网络安全和数据保护方面的协助时，您应当保证相关协助不会对腾讯云正常业务经营造成不利影响，且相关的费用支出均由您承担。

3.7 数据安全事故处置

当腾讯云或者接受转委托的主体在处理数据过程中发生了包括数据泄露、篡改、丢失在内的数据安全事故，均将保留任何与已知或可疑的数据泄露、篡改、丢失有关的记录，腾讯云将按照本协议约定的通知方式及时向您发送通知，并根据您的合理要求，在合理期限内补充提供其他有关数据安全事故的材料。

3.8 数据删除

本协议终止、被认定无效或者被撤销的，您有权要求腾讯云返还或彻底删除数据，除非法律法规另有规定除外。如果适用的数据保护法或其他法律法规、监管要求不允许腾讯云删除此类数据，则腾讯云不会将这些数据用于除业务合作之外的任何其他用途，并且始终遵守业务合作协议以及本协议的规定。若删除数据从技术上难以实现的，腾讯云将停止除存储和采取必要的安全保护措施之外的处理。

3.9 其他

如任一方适用法律、行政法规对其数据处理活动有其他规定的，该方应确保其数据处理活动已满足适用法律、行政法规的要求。

4. 陈述与保证

4.1 您陈述和保证如下：

（a）您已采取必要的行动，获得必要的授权以签署、交付和履行本协议；您对本协议的签署、交付和履行不违反适用法律的明确规定；

（b）本协议构成对您合法、有效、有约束力且可强制执行的义务，您将根据本协议的约定及适用法律的要求履行本协议；

（c）您承诺对本协议、与本协议有关的内容以及基于本协议接收的任何资料予以保密。

4.2 腾讯云陈述和保证如下：

（a）腾讯云已采取必要的公司行动，获得必要的授权以签署、交付和履行本协议；腾讯云对本协议的签署、交付和履行不违反适用法律的明确规定；

（b）本协议构成对腾讯云合法、有效、有约束力且可强制执行的义务，腾讯云将根据本协议的约定及适用法律的要求履行本协议；

（c）腾讯云承诺对本协议、与本协议有关的内容以及基于本协议接收的任何资料予以保密。

5. 违约责任

5.1 任一方违反本协议或适用法律相关规定的，或造成数据丢失、泄露、损坏或销毁的，应当承担相应的法律责任；一方的前述行为给另一方造成损失的，应当赔偿受到损失的一方所遭受的损失。

5.2 非因腾讯云过错导致数据的丢失、泄露、损坏或销毁等，腾讯云不承担责任。

5.3 如因您未履行适用法律要求的义务(包括但不限于向个人信息主体履行告知义务并获得授权同意(如适用)等)，导致腾讯云遭受任何损失的，您应当赔偿腾讯云的损失。

6. 法律适用及争议解决

6.1 本协议的订立、效力、执行和解释均应适用中华人民共和国法律。

6.2 本协议签订地为中华人民共和国广东省深圳市南山区。

6.3 凡因本协议引起的或与本协议项下的受委托处理的数据或者数据处理活动有关的任何争议，双方应首先协商解决；双方未能协商解决的，任何乙方均可向广东省深圳市南山区人民法院提起诉讼。

7. 其他

7.1 本协议的任何变更均应以双方同意的形式做出，否则无效。

7.2 如由于政策法规的变更或发生其他不可抗力事件导致本协议项下事项的履行存在客观现实困难的，双方应友好协商并确定解决方案。特别地，如果由于政策法规的变更或监管机关的进一步要求导致本协议中的约定内容需要做进一步调整的，双方均同意在尽可能维持原合作模式的前提下，对本协议做适当的变更和修订。

7.3 本协议的标题仅为阅读而设，不应被用来解释、说明或在其他方面影响本协议各项规定的含义。

7.4 如本协议有任何一条或多条规定根据任何法律或法规在任何方面被裁定为无效、不合法或不可执行，本协议其余规定的有效性、合法性或可执行性不应因此在任何方面受到影响或损害。

7.5 本协议是《 腾讯云服务协议 》的补充，本协议内容与《 腾讯云服务协议 》内容冲突的，以本协议内容为准；如本协议没有约定的内容，以《 腾讯云服务协议 》内容为准。

版权所有：腾讯云计算（北京）有限责任公司

苹果隐私策略：PrivacyInfo.xcprivacy

最近更新时间：2024-04-22 14:29:31

根据苹果公司发布的 App Store 提交的隐私更新，自2024年春季开始，上架 App Store 的应用需要同时提供一份 App 的**隐私清单文件**。
当您准备分发 App 时，Xcode 会将 App 使用的所有第三方 SDK 的隐私清单合并为一个简单易用的报告。
这个报告内容全面，总结了 App 中的所有第三方 SDK，让您能够更轻松地创建更准确的隐私标签。
因此嵌入 App 的 SDK 和三方库都需要包含 **PrivacyInfo.xcprivacy** 。

即时通信 IM 的适配

在 **7.8.5505** 及以上版本的 IM SDK 会默认包含 **PrivacyInfo.xcprivacy** 文件。
在 **7.9.5666** 及以上版本的 TUIKit 组件 会默认包含 **PrivacyInfo.xcprivacy** 文件。
在 **2.3.0.920** 及以上版本的 TUICallKit 会默认包含 **PrivacyInfo.xcprivacy** 文件。
在 **2.3.0** 及以上版本的 TUIRoomKit 会默认包含 **PrivacyInfo.xcprivacy** 文件。

- 当您使用 CocoaPod 集成时，我们会通过 Pod 为您添加 **PrivacyInfo.xcprivacy** 到工程内，**您无需为此做额外工作**。
- 当您手动集成时，请注意需要将源代码目录下的 **PrivacyInfo.xcprivacy 拷贝进您的代码工程里。**

IM 相关的 PrivacyInfo.xcprivacy

IM SDK 及 TUIKit组件

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>NSPrivacyTracking</key>
    <false/>
    <key>NSPrivacyCollectedDataTypes</key>
    <array/>
    <key>NSPrivacyTrackingDomains</key>
    <array/>
    <key>NSPrivacyAccessedAPITypes</key>
    <array>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>

<string>NSPrivacyAccessedAPICategorySystemBootTime</string>
```

```
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
                <string>35F9.1</string>
            </array>
        </dict>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>
            <string>NSPrivacyAccessedAPICategoryDiskSpace</string>
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
                <string>E174.1</string>
            </array>
        </dict>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>

<string>NSPrivacyAccessedAPICategoryFileTimestamp</string>
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
                <string>C617.1</string>
            </array>
        </dict>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>

<string>NSPrivacyAccessedAPICategoryUserDefaults</string>
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
                <string>CA92.1</string>
            </array>
        </dict>
    </array>
</dict>
</plist>
```

TUICallKit

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>NSPrivacyTracking</key>
    <false/>
    <key>NSPrivacyTrackingDomains</key>
    <array/>
    <key>NSPrivacyCollectedDataTypes</key>
    <array>
        <dict>
            <key>NSPrivacyCollectedDataType</key>
            <string>NSPrivacyCollectedDataTypeUserID</string>
            <key>NSPrivacyCollectedDataTypeLinked</key>
            <false/>
            <key>NSPrivacyCollectedDataTypeTracking</key>
            <false/>
            <key>NSPrivacyCollectedDataTypePurposes</key>
            <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
            </array>
        </dict>
    </array>
    <key>NSPrivacyAccessedAPITypes</key>
    <array>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>
            <string>NSPrivacyAccessedAPICategoryDiskSpace</string>
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
                <string>E174.1</string>
            </array>
        </dict>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>

<string>NSPrivacyAccessedAPICategoryUserDefaults</string>
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
                <string>CA92.1</string>
            </array>
        </dict>
```

```
    </array>
</dict>
</plist>
```

TUIRoomKit

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>NSPrivacyTracking</key>
    <false/>
    <key>NSPrivacyTrackingDomains</key>
    <array/>
    <key>NSPrivacyCollectedDataTypes</key>
    <array>
        <dict>
            <key>NSPrivacyCollectedDataType</key>
            <string>NSPrivacyCollectedDataTypeUserID</string>
            <key>NSPrivacyCollectedDataTypeLinked</key>
            <false/>
            <key>NSPrivacyCollectedDataTypeTracking</key>
            <false/>
            <key>NSPrivacyCollectedDataTypePurposes</key>
            <array>

<string>NSPrivacyCollectedDataTypePurposeAppFunctionality</string>
            </array>
        </dict>
    </array>
    <key>NSPrivacyAccessedAPITypes</key>
    <array>
        <dict>
            <key>NSPrivacyAccessedAPIType</key>

<string>NSPrivacyAccessedAPICategorySystemBootTime</string>
            <key>NSPrivacyAccessedAPITypeReasons</key>
            <array>
```

```
                <string>35F9.1</string>
            </array>
        </dict>
    </array>
</dict>
</plist>
```

手动导入自身 App

除了通过 CocoaPod 自动导入 PrivacyInfo 外，开发者还可以直接将 IM SDK的 **PrivacyInfo.xcprivacy** 中的条款补全到自身 App 的**PrivacyInfo.xcprivacy** 中。具体补全方式可以参见以下内容：

- 使用 Source Code 方式添加

  Xcode 中使用 Source Code方式打开 app 项目下的 **PrivacyInfo.xcprivacy** 。复制腾讯云 **PrivacyInfo.xcprivacy** 中的条目，注意不要重复添加或错行。
- 使用 Property List 的方式添加

  在 Xcode 中双击打开 **PrivacyInfo.xcprivacy** 文件，在其中点击+，Xcode会提示可选的条款和可设置项，按照需求进行增补即可。

版权所有：腾讯云计算（北京）有限责任公司