人脸支付

腾讯云人脸支付 SDK 个人信息保护规则

腾讯云

【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。

腾讯云人脸支付 SDK 个人信息保护规则

最近更新时间：2022-10-13 10:39:58

引言

腾讯云人脸支付 SDK（以下简称“SDK 产品”）由腾讯云计算（北京）有限责任公司（以下简称“我们”）开发，公司注册地为北京市海淀区知春路49号3层西部309。
《腾讯云人脸支付 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

本规则旨在说明本 SDK 产品常规处理个人信息的目的、方式和范围等。如开发者需要额外处理个人信息或数据的，需要开发者在处理前根据其产品功能以及选择开启的本 SDK 功能更新其隐私政策。本 SDK 采用私有化部署方式，即 SDK 是部署在开发者自有或自主控制的服务器，除 AndroidID 及硬件序列号外，本 SDK 产品使用过程中产生和收集的其他信息和数据均由开发者收集、控制和处理，相关的安全措施和权限限制也均由开发者掌握，对于开发者服务器的数据我们不接触且开发者无授权时我们无法获取。开发者应当遵守本规则，并仅可将本SDK用于合法用途，确保使用行为符合相关法律法规的规定和监管要求，不侵犯任何主体及终端用户的合法权益。
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. **在集成 SDK 产品前，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，依法征得终端用户同意，并在征得终端用户同意后方可初始化 SDK 产品。如果开发者需要变更 SDK 产品收集、处理终端用户的个人信息，或者通过 SDK 产品收集、处理终端用户的个人信息超出了收集时所称目的和范围的，开发者应告知终端用户并获得其同意。**
3. **在征得终端用户的同意、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或提前获取相应权限。**
4. **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。**
5. **遵守本规则的要求。**

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：

个人信息类型	处理目的	处理方式
AndroidID（Android 10及以上版本）	首次激活设备时需对设备进行鉴权并作为计费判断依据	1. 加密处理 2. 仅在首次激活设备且设备 Android 系统版本在10及以上时，SDK 需要联网将收集的 AndroidID 上报到我们的服务器，生成 license 文件到设备本地存储后，在 license 文件有效期内均不会再联网且不会再收集、上报 AndroidID 信息
硬件序列号（Android 10以下（不含本数）版本）	首次激活设备时需对设备进行鉴权并作为计费判断依据	1. 加密处理 2. 仅在首次激活设备且设备 Android 系统版本在10以下（不含本数）时，SDK 需要联网将收集的硬件序列号上报到我们的服务器，生成 license 文件到设备本地存储后，在 license 文件有效期内均不会再联网且不会再收集、上报硬件序列号信息
人脸照片或人脸视频	用于人脸识别支付功能	1. 私有化部署，加密本地化处理 2. 采集人脸视频，截取最佳帧人脸照片，并提取出人脸特征数据，在设备本地将每次收集提取的人脸特征数据与已存储的底图人脸特征数据进行比对，得出是否一致的结果用于支付业务功能的判断 3. 底图的人脸特征数据会回传到开发者服务器，每次收集提取的人脸特征数据仅在设备本地处理，不会回传到开发者服务 4. 退出设备后所有人脸数据均会删除，下次登录需要重新收集

（二）为实现 SDK 产品功能所需的权限

为确保支持开发者收集信息和数据的正常开展，以实现本 SDK 产品的相应功能所必需，本 SDK 产品会通过开发者应用在对应的功能场景下申请所需权限。开发者应根据其应用的具体功能场景，在终端用户触发下表所示的具体功能场景时调用 SDK 的相应功能、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实施前述行为。

操作系统	权限名称	使用目的	功能场景	是否可选
Android	相机	获取人脸视频进行人脸识别，不授权则无法使用相应功能	打开摄像头	必选
An	存储	从本地上传人脸照片作为比对底图，同时需要将鉴权文件和提取的人脸特征数据存储到设备本地。不获取则无	从设备本地上传人脸底	必选

droid		法使用相应功能	图或存储人脸数据时	
Android	电话	首次激活设备时需要获取本权限以读取硬件序列号，用于对设备进行鉴权并作为计费判断依据。不授权则Android10以下（不含本数）设备无法使用相应功能	首次激活设备时	可选，Android 10及以上设备无需获取本权限
Android	网络访问	首次激活设备时需要联网将 AndroidID 或硬件序列号回传到我们的服务器，以便生成鉴权文件。不授权则无法使用相应功能	首次激活设备时	必选

请注意，在不同设备和系统中，权限显示方式及关闭方式会有所不同，需同时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，我们和开发者将不会继续收集和使用相关权限所对应的个人信息，也无法为终端用户提供需要终端用户开启权限才能提供的对应的功能。

（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

我们不会通过本 SDK 产品与第三方共享终端用户的个人信息。
开发者不应将终端用户的个人信息转移（包括共享）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、接收方的名称或者姓名、联系方式,并征得终端用户的单独同意。 同时，应与接收方签署协议并按照法律法规的规定，对接收方数据处理进行严格的限制，确保接收方在终端用户同意的处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应要求接收方重新取得终端用户的同意。
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，开发者应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，开发者应要求接收方重新取得终端用户的同意。

开发者不应公开披露终端用户的个人信息，除非开发者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，法律法规另有规定的除外。

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，并竭力帮助终端用户管理个人信息，包括个人信息查阅、复制、删除、注销账号以及设置隐私功能等，以保障终端用户的权利。如您是开发者，您应当为终端用户提供实现查阅、复制、修改、删除个人信息、撤回同意和注销账号的方式。

基于终端用户的同意而进行的个人信息处理活动，终端用户有权撤回该同意。我们已向开发者提供关闭本 SDK 产品的能力，开发者可以通过发起对 YTSDKKitInterface.globalRelease() 的调用来停止收集和处理终端用户的个人信息。由于我们与终端用户无直接的交互对话界面，终端用户可以直接联系开发者停止使用本 SDK 产品，也可通过本规则第八条提供的方式与我们联系。如您是终端用户，请您理解，特定的业务功能或服务需要您提供服务所需的信息才能得以完成，当您撤回同意后，我们无法继续为您提供对应的功能或服务，也不再处理您相应的个人信息。您撤回同意的决定，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、AndroidID 及硬件序列号信息的存储

（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：

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

五、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，或通过本规则提供的方式与我们联系。

六、免责声明

如果开发者使用本 SDK 产品进行数据收集，应当保证数据来源合法合规，或者已经取得相关方和终端用户的授权，开发者违反前述规定的相应责任由开发者承担。开发者对终端用户的信息处理应当合法合规，否则我们有权要

求开发者停止使用本 SDK 产品，并保留追究责任的权利，且不视为我们违约。在面向终端用户时，已私有化部署的 SDK 产品部署在开发者自有系统中，由于我们无法获取开发者收集和控制的数据，因此开发者的隐私政策中，我们不被视为是共享、接收、转授、获取（或可能的其他接触途径）相关信息和数据的第三方。为了符合《个人信息保护法》关于“收集个人信息前应取得个人信息主体同意”的要求，开发者如使用本 SDK 产品进行个人信息收集时，需要在其隐私政策内披露第三方 SDK 并提及我们的本 SDK 产品。示例参考如下（示例仅供参考，具体请依照法律和监管要求进行调整）：

- SDK 名称：腾讯云人脸支付 SDK。
- 第三方公司名称：腾讯云计算（北京）有限责任公司。
- 使用目的：人脸支付。
- 收集个人信息范围： AndroidID 或硬件序列号；私有化部署，由开发者收集个人信息**人脸照片或人脸视频**。
- 隐私政策链接： 腾讯云人脸支付 SDK 个人信息保护规则 。

七、变更

我们会适时修订本规则的内容。
如本规则的修订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告知。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变动的，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征得其同意，**如果终端用户不同意接受本规则，请停止集成本 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：

1. 通过 https://kf.qq.com/ 与我们联系。
2. 将问题发送至 Dataprivacy@tencent.com。
3. 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。