

人脸识别 相关协议



腾讯云

【 版权声明 】

©2013–2023 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 】



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

相关协议

服务等级协议

服务规则

腾讯云离线人脸识别 SDK 个人信息保护规则

相关协议

服务等级协议

最近更新时间：2023-06-28 11:03:51

详细信息请参见 [人脸识别服务等级协议](#)。

服务规则

最近更新时间：2023-07-21 14:24:01

详细信息请参见 [人脸识别服务规则](#)。

腾讯云离线人脸识别 SDK 个人信息保护规则

最近更新时间：2022-04-28 12:02:12

引言

腾讯云离线人脸识别 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。

《腾讯云离线人脸识别 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；同时，您应仅在征得终端用户的同意后集成 SDK 产品并处理终端用户的个人信息。

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. 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，并依法征得终端用户同意。
3. 在征得终端用户的同意前，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. 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	SDK 使用绑定设备的授权，一般按照设备数量计费。采集 Android ID 用于判定使用 SDK 的设备数量	<ol style="list-style-type: none">1. 本地化处理2. 当本 SDK 提供给移动端 App 使用时，本 SDK 不采集用户的 Android ID3. 本 SDK 仅在提供给机具设备使用（如刷脸支付一体机等），且系统版本为 Android 10及以上时，才收集 Android ID

硬件序列号	SDK 使用绑定设备的授权，一般按照设备数量计费。采集硬件序列号用于判定使用 SDK 的设备数量	<ol style="list-style-type: none"> 1. 本地化处理 2. 当本 SDK 提供给移动端APP使用时，本 SDK 不采集用户的硬件序列号本 SDK 仅在提供给机具设备使用（如刷脸支付一体机等），且系统版本为 Android 10以下（不含本数）时，才收集硬件序列号
设备型号	SDK 使用绑定设备的授权，一般按照设备数量计费。采集硬件序列号用于判定使用 SDK 的设备数量	<ol style="list-style-type: none"> 1. 本地化处理 2. 当本 SDK 提供给移动端 App 使用时，本 SDK 不采集用户的设备型号 3. 本 SDK 仅在提供给机具设备使用（如刷脸支付一体机等）时，才收集设备型号
操作系统	需要据此判断设备系统版本，做兼容处理，不采集可能导致使用异常	本地化处理
多媒体文件	用于使用图片注册人脸功能，以供本地人脸比对，如果不采集图片，注册人脸功能无法使用	本地化处理
人脸照片或视频流数据，以及分析出的人脸特征数据	用于人脸识别和注册功能，采集人脸数据，分析出人脸特征数据，回传给 App	本地化处理；加密处理；人脸特征信息加密为浮点数据存储和回传

人脸照片和视频属于敏感个人信息，且是我们为第三方开发者提供本服务所必需，如第三方开发者和终端用户选择不提供或不同意我们处理以上敏感个人信息的，将导致第三方开发者和终端用户无法正常使用本 SDK 产品提供的服务。

（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申请所需权限。

操作系统	权限名称	使用目的	是否可选
Android	相机	获取视频帧进行人脸识别和人脸注册，不授权则无法使用相应功能	必选
Android	存储	缓存人脸特征案例库到 sdcard。人脸比对功能需要使用本地人脸案例库，不获取权限无法使用该功能	必选
Android	电话	当本 SDK 在机具设备使用时，用于读取机器序列号，以便进行绑	可选；移动

roid		定设备的授权。SDK 一般按照设备数量计费，采集机器序列号用于判定使用的设备数量	App 使用时，无需申请
And roid	网络 访问	用于判断设备是否在提供服务的范围内，需要联网授权。不授权无法使用所有功能	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、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，具体请开发者调用以下接口（详情见接口文档）：

```

AIFaceSDKKitInterface.unregisterEvent(this);
FaceRetrieverHelper.getInstance().destroy();
AIFaceSDKKitInterface.destroy();
    
```

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。

三、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。

四、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。

我们建立严谨的管理制度、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。

五、未成年人保护

若您开发者，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、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，通过网站公告或电子邮件等方式进行告知。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 SDK 产品。**

七、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。