

人脸核身 相关协议



腾讯云

【 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 】



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

服务条款

安全合规说明

人脸核身数据安全与权限获取说明

合规与安全指南

SDK 人脸信息处理协议参考模板

慧眼 SDK 个人信息保护规则

人脸核身

意愿核身

实证 NFC

卡证 OCR

人机互动小程序端

相关协议

服务等级协议

最近更新时间：2023-06-28 11:07:17

详细信息请参见 [腾讯云慧眼人脸核身服务等级协议](#)。

服务条款

最近更新时间：2023-10-11 11:11:24

详细信息请参见 [腾讯云慧眼人脸核身服务条款](#)。

安全合规说明

人脸核身数据安全性与权限获取说明

最近更新时间：2025-04-02 16:42:41

腾讯云人脸核身基于腾讯自主研发的技术服务，本文档介绍了人脸核身服务智能终端权限的获取情况以及数据安全保障能力。

获取和使用智能终端权限说明

腾讯云人脸核身将获取智能终端的如下权限及个人信息：

1. 摄像头权限和网络权限（SaaS 服务需要），用于拍摄用户人脸信息并采集视频照片（以摄像头实际采集区域为准），进行活体检测和人脸比对，以核实是否为真实用户操作或用户的真实身份。
2. 设备信息权限（App SDK 服务需要），包括采集设备标识符（Android ID、IDFV 等标识符）、机型、操作系统版本、网络信息等（具体以腾讯云人脸核身个人信息授权书约定的为准），用于检测认证的实时风险，以便识别和排除用户恶意请求、维护服务安全，设备信息仅通过 SDK 临时调用，腾讯云不做存储。

说明

请您知悉，获取摄像头和网络权限是完成人脸核身服务的必要项，获取设备信息为可选项，可选项不影响人脸核身服务流程的进行。

数据传输安全性说明

腾讯云人脸核身将采用如下技术手段来保障数据传输的安全性：

1. **App SDK 和独立 H5 服务：**客户端请求报文会综合使用 RSA 非对称加密和 AES 对称加密（key 为动态生成）方式进行加密处理，同时会对人脸视频进行混淆处理；客户端与服务端之间的请求会通过 HTTPS 安全传输协议的机制来确保数据传输安全，确保数据在传输过程中不被泄露、篡改或替换。
2. **微信小程序、微信原生 H5 和 API 服务：**请求报文的敏感字段支持采用 AES 和 SM4 对称加密（key 为动态生成）方式进行加密传输，同时服务端传输会通过 HTTPS 安全传输协议的机制来确保数据传输安全，确保数据在传输过程中不被泄露、篡改或替换。

合规要求

在使用人脸核身服务之前，您务必知晓并遵循如下内容：

1. 确保终端用户首次启动应用时单独弹出《人脸信息处理协议》，在终端用户主动点击同意《人脸信息处理协议》后，再初始化腾讯云人脸核身 SDK。
2. 确保《人脸信息处理协议》的内容包含如下信息：
 - （1）使用的 SDK 名称为腾讯云人脸核身 SDK。
 - （2）服务功能为证件 OCR 识别、活体检测、人脸比对、识别和排除恶意请求，检测认证实时风险。

(3) 收集设备信息类型：设备标识符（Android ID、IDFV 等标识符）、机型、操作系统版本、网络信息等（具体以腾讯云人脸核身个人信息授权书约定的为准）。

合规与安全指南

最近更新时间：2023-06-14 10:01:27

前言

为帮助 App 开发运营者（以下简称“您”）作为腾讯云慧眼人脸核身产品和/或服务的使用者，在使用腾讯云慧眼人脸核身产品和/或服务（包括但不限于 SDK、API、H5 等形式，以下简称“本 SDK”）过程中更好地落实 App 用户个人信息保护相关事宜，避免违反相关法律法规及政策文件的规定，并对于本 SDK 的合规性和安全性有更加明确的了解，腾讯云（以下亦称“我们”）特编写《腾讯云慧眼人脸核身产品和/或合规与安全指南》（以下简称“《指南》”），供您参考。

请您注意，本《指南》参考现行的法律法规及政策文件的普适性要求以及部分法规对于 SDK 设置的安全指引要求所制定，相关要求及描述均应在合理前提下同样适用于慧眼人脸核身所有类型的产品和/或服务方案。

特别提示

本《指南》对本 SDK 的合规性和安全性描述与要求仅为我们向您提供的服务说明及使用建议，不构成也不应被视为我们对于任何法律法规及政策文件的及时的、完整的、全面的、甚至完全准确的分析，亦不构成我们对慧眼人脸核身产品和/或服务的承诺和保证。本《指南》不能作为判断您与您所开发、运营的 App 是否满足合规与安全要求的可依赖的标准，亦不构成我们对前述事宜作出的任何担保或保证，您应当自行、独立地对前述 App 承担合规与安全责任。

目录

本《指南》主要包括以下方面内容

- 定义
- 您应注意的用户个人信息保护合规要求
- 您在使用慧眼人脸核身时应遵守的合规事项
- 慧眼人脸核身具备的安全保护能力
- 联系我们

正文

一、定义

1. 本《指南》中的“您”是指：通过了腾讯云官网实名认证，在其开发和运营的 App 中接入和使用慧眼人脸核身服务依法用于其业务开展中对用户进行实人实名认证的主体，包括但不限于个人、团队、公司、组织等。
2. 本《指南》中“慧眼人脸核身服务”（以下也简称“服务”）指：腾讯云向您提供的实人实名认证产品，对用户身份信息真实性进行验证的服务，包含证件 OCR 识别、活体检测、人脸1:1对比等能力。具体服务内容详见 [腾讯云官网慧眼人脸核身产品介绍页](#)。
3. 本《指南》中的“用户”：提交本人个人信息给您或腾讯云，以供身份信息真实性核验的自然人。

二、用户个人信息保护合规要求

在使用本 SDK 产品和/或服务时，您应当遵守个人信息保护的相关合规要求及 App 开发运营者应当履行的合规要求，包括但不限于《民法典》、《网络安全法》、《个人信息保护法》、《数据安全法》、《消费者权益保护法》、《App 违法违规收集使用个人信息行为认定方法》、《App 违法违规收集使用个人信息自评估指南》、《移动互联网应用程序（App）收集使用个人信息自评估指南》、《关于开展纵深推进 App 侵害用户权益专项整治行动的通知》等所列举的相关内容，保护用户个人信息安全。

我们在此列举了您应当重点关注的个人信息保护合规事项，供您参考。

1. 用户个人信息处理规则的告知

您应当告知用户您所开发或运营的 App 对于个人信息的处理规则，以显著方式、清晰易懂的语言真实、准确、完整地告知用户下列事项，并在相关事项发生变化时，以适当方式通知用户：

- （1）App 涉及个人信息处理活动的个人信息处理者的名称或者姓名和联系方式。
- （2）App 涉及个人信息的处理目的、处理方式，处理的个人信息种类、保存期限，并应完整、清晰、区分说明各业务功能所收集的个人信息。每个业务功能在说明其所收集的个人信息类型时，应逐项列举，不应使用“等、例如”等方式概括说明；涉及处理敏感个人信息的，还应当向用户告知处理敏感个人信息的必要性以及对用户权益的影响。
- （3）针对嵌入的第三方代码、插件（如 SDK）收集个人信息，应当说明第三方代码、插件的类型或名称，及收集个人信息的目的、类型、方式以及 SDK 服务提供方的个人信息处理角色（注：例如可采用隐私政策、弹窗提示、文字备注、文本链接等方式说明，具体可参考我们在下文中的举例）。
- （4）App 用户作为个人信息主体行使适用法律规定权利的方式和程序。
- （5）法律、行政法规规定应当告知的其他事项。

特别地，针对接入和使用本 SDK 产品和/或服务前，您应当满足以下告知义务：

- （1）确保终端用户首次启动应用时单独弹出《[人脸信息处理协议](#)》（或类似文档，参考模板点此），在终端用户主动点击同意《人脸信息处理协议》后，再初始化本 SDK。
- （2）确保《人脸信息处理协议》的内容包含如下信息：
 - 使用的 SDK 名称为“腾讯云慧眼人脸核身 SDK”。
 - 处理目的为实人实名认证。
 - 处理方式为加密传输和必要处理：（1）对人脸视频进行活体检测，将用户姓名、身份证号、人脸图片与“互联网+可信身份认证平台”等核验机构存储的信息进行比对核验，得出一致或不一致的结果，并返回结果给您；（2）采集设备信息并进行去标识化处理，用于检测认证设备实时风险，得到风险等级用于判断认证结果。
 - 处理的个人信息类型：身份证照片或姓名和身份证件号码、人脸视频和照片、设备信息（不同版本收集的个人信息有所不同）：Android 版将收集内核版本、CPU 信息、机型、系统版本、设备制造商、运营商；iOS 版将收集 GUID、蜂窝网络 IP、WIFI IP。

2. 隐私政策的独立设置

您应当制定一份独立的隐私政策（而非作为任何其他文件的一部分）并进行单独展示，隐私政策中应包含有《收集个人信息明示清单》和《第三方个人信息共享清单》，用以说明您所开发或运营的 App 相关的个人信息收集和使用情

况。隐私政策的内容应当符合国家相关法律法规及政策文件，隐私政策的设置应当满足以下要求：

- （1）公开展示。隐私政策通过弹窗、文本链接、附件、常见问题等界面或形式展示，并包含个人信息处理规则。
- （2）主动提示。您应当在 App 首次运行或用户注册时主动提示用户阅读隐私政策（例如可采用通过弹窗、突出链接等主动方式提示用户阅读隐私政策）。
- （3）易于访问。用户进入主功能界面后，通过4次（含）以内的点击等操作，能够访问到隐私政策，且隐私政策链接位置突出、无遮挡；用户进入主功能界面后，通过2次（含）以内的点击等操作，能够访问到《收集个人信息明示清单》和《第三方个人信息共享清单》（含第三方 SDK 目录）。
- （4）易于阅读。隐私政策文本文字显示方式应当不会造成阅读困难（例如可采取与 App 其他界面等同的样式；例如文本字号过小、颜色与背景色相近、行间距过密、字迹模糊、列宽大于手机屏幕等易造成阅读困难）。
- （5）规则完整。隐私政策应当对 App 运营者基本情况描述，至少包括组织名称、注册地址或常用办公地址、个人信息保护工作机构或相关负责人联系方式。
- （6）自主同意。隐私政策应由 App 用户自主选择是否同意，不应以默认勾选同意的方式或是欺骗诱导的方式取得用户授权；
- （7）其他法律法规及政策文件对隐私政策提出的要求。

您的隐私政策应当添加特定文字表述，向 App 用户明示您在 App 中部署本 SDK、本 SDK 收集使用个人信息的目的、类型、方式和范围等，以及本 SDK 在个人信息处理活动中的角色和责任（例如接受您的委托处理个人信息），并提供符合法律法规要求、您与我们之间就本 SDK 约定的个人信息安全保护标准。

为了便于您参考描述，我们将本 SDK 适用的权限获取情况及对应目的说明如下，您应当在隐私政策中进行合理、完整、准确的披露：

权限	说明
相机	用于采集身份证照片以及人脸视频进行实人实名认证
麦克风	用于采集用户朗读文字的音频校验用户意愿
设备	用于采集设备信息检验认证实时风险
网络	用于连接网络，进行数据传输
存储	用于存储 SDK 配置文件和日志文件
网络状态	用于获取当前网络信息，进行传输优化

请您知悉，获取摄像头、网络权限是使用本 SDK 产品和/或服务的必要项，获取设备、麦克风、存储及网络状态权限为可选项，可选项不影响慧眼人脸核身服务流程的进行，但会影响设备实时风险检测、意愿核身、日志记录等业务功能的使用，您可根据该信息完善您在隐私政策中对于本 SDK 个人信息处理活动的披露。

您亦可参考下列表格形式向 App 用户说明本 SDK 产品和/或服务个人信息处理活动的相关信息：

S D K	SD K 服 务提 供方	处 理 目 的	处理方式	处理个人信息类型	申请的 权限	S D K 隐
-------------	-----------------------	------------------	------	----------	-----------	---------------

名称						私政策链接
腾讯云慧眼人脸核身SDK	腾讯云计算（北京）有限责任公司	用于实人实名认证	（1）对人脸视频进行活体检测，将姓名、身份证号、人脸图片与“互联网+可信身份认证平台”等核验机构存储的信息进行比对核验，得出一致或不一致的结果，并返回认证结果给开发者。 （2）采集设备信息并进行去标识化处理后，用于检测认证设备实时风险，得到风险等级用于认证结果的判断，增强版还会将认证结果返回开发者。	身份证照片或者姓名和身份证号码等身份信息、人脸视频和照片和设备信息（不同版本收集的设备信息有所不同）： Android 版将收集内核版本、CPU 信息、机型、系统版本、设备制造商、运营商。 IOS 版将收集 GUID、蜂窝网络 IP、WIFI IP。	摄像头、网络、读取存储权限、麦克风（仅 SDK、H5 需要，其中麦克风仅基础版需要）	腾讯云慧眼人脸核身 SDK 隐私保护指引

3. 用户个人信息权益响应机制安排

根据现行法律法规及政策文件，App 用户作为个人信息主体，享有的个人信息主体权益至少应当包括：

- （1）对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理。
- （2）有权查阅、复制其个人信息，或要求将个人信息转移至其指定的个人信息处理者。
- （3）发现其个人信息不准确或者不完整的，有权请求更正、补充。
- （4）在特定情况下，有权请求删除其个人信息。
- （5）有权要求对其个人信息处理规则进行解释说明。
- （6）有权拒绝自动化决策。
- （7）其他法律法规及政策文件规定的权利。

您应当告知 App 用户其行使上述个人信息权益的途径和方式（例如设置客服电话予以接收行权请求并履行内部响应程序），并在收到该等行权请求后，及时进行相应的处理。

特别地，您在使用本 SDK 产品和/或服务过程中，如果 App 用户根据您与我们的约定提出了个人信息相关的行权请求，并且您已确定该等行权请求涉及到了您向本 SDK 提供的个人信息时，请及时通过本《指南》中公示的联系方式告知我们，并附上必要的书面证明材料。我们将及时核验相关材料，并按照相关法律法规，以及我们在相关产品已对外公示的隐私政策等法律文本中明确的规则，在我们的能力范围内为您提供相应的支持与配合。请您注意，如该等行权请求经我们评估后确认为存在不合法、不合理、无端重复或需要过多技术手段、给他人合法权益带来风险或者其他不具备可行性的情形，我们可能会予以拒绝。

三、本 SDK 使用注意事项

1. 您使用本 SDK 产品和/或服务前的合规自查

您在使用本 SDK 产品和/或服务前，应当仔细阅读我们在官网公示的相关服务协议及隐私政策（或同样性质的类似法律文件），并依据您的 App 产品收集使用个人信息的情况进行合规自查。请您注意，我们向您提供本 SDK 产品和/或服务的前提是：

- （1）您已获得 App 用户充分必要的授权、同意和许可，尤其是涉及到人脸信息等生物识别特征时的明示、单独同意（若您的 App 是针对不满十四周岁的儿童设计和开发的，您应已采取必要的技术措施，保证已获得其监护人的授权、同意和许可），并确保该等授权在我们提供产品和服务期间的持续有效性。
- （2）遵守并将持续遵守适用的法律、法规和监管要求，包括但不限于制定和公布有关个人信息保护的相关政策。
- （3）向 App 用户提供便捷、可行、易于操作的行权途径和方式。

2. 我们对您的合规审查

我们作为本 SDK 产品和/或服务的提供者已在与您达成的服务协议中明确各方的责任和义务，并已通过官方网站公示自身产品与能力所适用的隐私政策，对于个人信息处理活动的相关细节进行了披露。您必须保证使用本 SDK 产品和/或服务过程中，委托我们处理的用户数据来源合法，并已合法合规地向该等用户履行告知义务，获得用户的有效、完整的授权同意。

为确保您满足上述使用条件，我们将可能视具体情况，在与您订立协议、开展合作前或合作过程中，对您进行必要的合规尽职调查与风险评估，包括但不限于：

- （1）要求您提供拟委托我们处理的个人信息的合法来源证明。
- （2）查阅您官网及其他公开渠道可获取的用户协议/服务条款与隐私政策等文本文件。
- （3）查看法律法规及政策文件要求的您应当履行的针对个人信息保护影响评估的结论文件。
- （4）试用您的 App 以审查同意授权与告知机制等。

如我们发现存在不合规情形，您可能被要求增加或补充相关合规措施，如您未按时增加或补充，我们有权拒绝您使用本 SDK 产品和/或服务。请您知悉，该等尽职调查与风险评估纯粹属于我们履行内部合规管理程序的手段和方式，不构成任何形式的承诺与保证，不具有对外部相对方的法律效力。

四、本 SDK 具备的安全保护能力

1. 安全保护措施

我们已使用符合业界标准的安全防护措施保护您和/或用户提供的个人信息，防止数据遭到未经授权访问、公开披露、使用、修改、损毁、泄露或丢失。

我们采用业界领先的技术保护措施。我们使用的技术手段包括但不限于防火墙、加密（例如 SSL）、去标识化处理、访问控制措施等。此外，我们还会不断加强将本 SDK 集成到第三方上的安全能力。

我们建立了专门保障个人信息安全的管理制度、流程和组织。我们也会审查该管理制度、流程和组织，以防未经授权的人员擅自访问、使用或披露用户的信息。

以下是我们关于主要环节数据安全措施的具体说明：

- （1）数据收集：我们将确保不会超授权范围处理用户个人信息，且所使用、存储的个人信息均是业务流程的实现所最小必要的，并采取适当的措施以保证在其授权下访问数据的员工仅在您书面指示的范围内处理个人信息。如因特殊原因我们未能按照要求处理个人信息，我们会及时告知您，并配合您进行信息安全影响评估，同时采取补救措施以保

护个人信息的安全，必要时您可以终止我们对个人信息的处理；

（2）数据传输：本 SDK 将采用如下技术手段确保个人信息在传输中的保密性、完整性和可用性：

- App SDK 和独立 H5 服务：客户端请求报文会综合使用 RSA 非对称加密和 AES 对称加密（key 为动态生成）方式进行加密处理，同时会对人脸视频进行混淆处理；客户端与服务端之间的请求会通过 HTTPS 安全传输协议的机制来确保数据传输安全，确保数据在传输过程中不被泄露、篡改或替换。
- 微信小程序、微信原生 H5 和 API 服务：请求报文的敏感字段支持采用腾讯云 KMS 进行加密传输，同时服务端传输会通过 HTTPS 安全传输协议的机制来确保数据传输安全，确保数据在传输过程中不被泄露、篡改或替换。

（3）数据存储：我们将根据您已获得的用户授权同意的范围，视您的独立决策而存储数据（例如您可使用删除接口定期清理数据），并根据不同的数据密级应用不同的安全存储机制，如加密存储、隔离存储。

（4）最小访问权限：我们将执行访问权限“最低权限”原则，包括但不限于将对数据的访问数量限制在最小数值，仅供确有需要，且经授权的员工访问，并留存个人信息访问审计日志和数据处理记录以追溯操作记录，以证明其数据处理活动符合本指南要求以及防止人为的个人信息泄露。

（5）数据安全保护措施：我们将在其所有网站/应用上维持合理的商用安全系统以及备份系统，并安装及维护防病毒和防恶意程序的防护软件，以保护数据免受可预见的威胁或危害，并防止未经授权的访问或使用。

2. 安全事件处置措施

若发生个人信息泄露、损毁、丢失等安全事件，我们会启动应急预案，阻止安全事件扩大。安全事件发生后，我们会及时以推送通知、邮件、短信等形式向您和/或用户告知安全事件的基本情况、我们即将或已经采取的处置措施和补救措施，以及我们对您和/或用户的应对建议。

五、联系方式

如您对本《指南》有任何问题，或根据本《指南》需要与我们联系：

- （1）通过 [腾讯客服](#) 或者 [腾讯云工单/客服](#) 与我们联系进行在线咨询。
- （2）发送邮件至：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）
- （4）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。

SDK 人脸信息处理协议参考模板

最近更新时间：2023-05-04 15:24:56

欢迎使用人脸核身服务！

根据相关法律法规的规定，您在使用【 】公司（简称“我们”）提供的【XX产品中的XX】功能服务前需完成实名认证，《人脸核身服务个人信息处理授权协议》（以下简称“本协议”）是我们与用户（简称“您”）所订立的有效合约。

我们在此善意的提醒您，在您使用我们的人脸核身服务（简称“本服务”）之前，请您务必审慎阅读、充分理解本协议各条款内容，本协议中与您的权益存在重大关系的条款，我们已采用加粗字体来特别提醒您，请您留意重点阅读。您应当仔细阅读、充分理解本协议的全部内容后再点击同意或勾选协议以使用本服务，一旦您主动点击同意按钮或勾选协议，将视为您同意接受本协议的全部内容。如果您未满18周岁，请在法定监护人的陪同下阅读本协议并做出是否接受本协议内容的决定。

一、我们提供的服务内容及个人信息处理规则

1. 您理解并同意，为了对您进行**实名认证**之目的，您同意我们将您的姓名、身份证号码或身份证照片传输给腾讯云计算（北京）有限责任公司及其合作服务商（简称“腾讯云”），并委托腾讯云通过摄像头、麦克风、网络、存储权限采集您的人脸信息和设备信息，对您的人脸信息进行活体检测并将您的上述身份信息向“互联网+可信身份认证平台”等核验机构传输，以实现身份信息的比对核验，从而验证您的身份。
2. 您理解并同意，为了对您进行**实名认证和意愿确认**之目的，您同意我们将您的姓名、身份证号码或身份证照片传输给腾讯云计算（北京）有限责任公司及其合作服务商（简称“腾讯云”），并委托腾讯云通过摄像头、麦克风、网络、存储权限采集您的人脸信息、朗读文字的音频和设备信息，对您的人脸信息进行活体检测并将您的上述身份信息向“互联网+可信身份认证平台”等核验机构传输，以实现身份信息的比对核验，从而验证您的身份。同时，我们还会对您朗读文字的音频进行核实，以核实您的认证意愿。
人脸信息、身份证属于敏感个人信息，且是我们为您提供本服务所必需。如您选择不提供或不同意我们处理以上敏感个人信息的，将导致您无法正常使用本服务，但不会影响您使用我们提供的其他身份验证服务（如有）。
3. 为了满足我们的实名认证服务需求以及提升本服务过程的安全性和准确性的必要，您同意我们对您的面部生物识别信息及相关视频图像、身份信息做必要的处理和保存，如您选择不提供或不同意我们处理以上敏感个人信息的，将导致您无法正常使用本服务。

二、我们如何保证您的个人信息安全

1. 我们只会符合法律法规规定的达成本协议所述目的所需最短期内保存您在本服务中提交的信息和认证结果。
为了保障您的个人信息安全，我们会在现有技术水平下采取合理必要的措施来保护您的个人信息，采取物理、技术和行政管理安全措施来降低丢失、误用、非授权访问、披露和更改的风险。如发生信息安全事件，我们有权根据法律规定及其应急管理制度处理您的个人信息，我们将及时告知您。
2. 除非您另行单独同意或者法律法规有明确要求，我们不会向任何第三方提供您在实名认证过程中向我们提供的信息。
3. 本服务收集和处理的个人信息将存储于中华人民共和国境内，未经您单独同意，我们不会向境外传输您的个人信息。

三、您如何管理您的个人信息

如您希望查阅、复制、更改、删除、撤回同意您的个人信息，您可以通过【 】向我们提出需求，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。

四、其他

1. 我们努力在现有技术基础上保障人脸核身服务有效、稳定运行，但是由于技术的限制、采集人脸信息过程中容易受到环境光线、表情、妆容等不特定因素的影响，且我们能用于认证的信息范围相对有限，技术水平和认证手段也在不断升级改进之中，**我们暂时无法保证每次人脸核身都能成功**。如果您发现实名认证不成功，您可以重新发起认证流程或者通过【 】联系我们，以便重新进行认证并提供认证服务水平。您也可以选择我们提供的其他认证方式（如有）完成身份真实性核验，但根据服务性质及风险控制等原因必须以人脸验证方式进行认证的除外。**为了保护您及他人的合法权益，我们有权在认为可能存在风险时暂停向您提供人脸核身相关服务。**
2. 为给您提供更好的服务或因国家法律法规、政策调整、技术条件、产品功能等变化需要，我们会适时对本协议进行更新并根据相关法律法规进行公示。**如您对更新后的内容有异议的，请立即停止使用本服务。若您知晓并继续使用本服务，即视为您认可并接受更新后的协议内容。**
3. 您已阅读并理解本授权书所有内容（特别是加粗字体内容）的意义以及由此产生的法律效力，自愿作出上述授权，本授权书是您真实的意思表示，您同意承担相关责任及后果。

慧眼 SDK 个人信息保护规则

人脸核身

最近更新时间：2025-01-07 16:12:53

您可以通过单击如下链接查看腾讯云慧眼人脸核身 SDK 个人信息保护规则：[单击此处 >>](#)

意愿核身

最近更新时间：2023-08-08 11:53:36

您可以通过单击如下链接查看腾讯云慧眼意愿核身 SDK 个人信息保护规则：[单击此处 >>](#)

实证 NFC

最近更新时间：2023-08-08 11:53:41

您可以通过单击如下链接查看腾讯云慧眼实证 NFC SDK 个人信息保护规则：[单击此处 >>](#)

卡证 OCR

最近更新时间：2023-08-08 11:54:48

您可以通过单击如下链接查看腾讯云慧眼卡证 OCR SDK 个人信息保护规则：[单击此处 >>](#)

人机互动小程序端

最近更新时间：2023-08-08 11:54:54

您可以通过单击如下链接查看腾讯云慧眼人机互动小程序端 SDK 个人信息保护规则：[单击此处 >>](#)