

个人信息保护政策

深圳摘星录科技有限公司（以下简称“摘星录”）非常重视保护用户的隐私和个人信息，摘星录亦将本个人信息保护政策（以下也称“本政策”）中的内容以高度审慎的义务对待和处理。

本政策与您所使用的我们的产品与/或服务息息相关，您在下载、安装、启动、浏览、注册、登录、使用我们的产品与/或服务（以下统称“使用我们的产品或服务”）时，我们将按照本政策的约定处理和保护您的个人信息，因此我们希望您能够仔细阅读、充分理解本政策的全文，并在需要时，按照本政策的指引，作出您认为适当的选择。本政策之中涉及的相关技术词汇，我们尽量以简明扼要的表述向您解释，以便于您理解。我们在此善意的提醒您，本政策中与您的权益可能存在重大关系的条款，我们已采用加粗字体来特别提醒您，请您留意重点查阅。

您应当在仔细阅读、充分理解本政策后使用我们的产品或服务，如果您不同意本政策的内容，将可能导致我们的产品或服务无法正常运行，或者无法达到我们拟达到的服务效果，您应立即停止访问或使用我们的产品或服务。您使用或继续使用我们提供的产品或服务的行为，都表示您充分理解和同意本政策的全部内容。

如您在阅读本政策过程中有任何疑惑或其他相关事宜的，我们为您提供了多种反馈渠道，公司情况说明以及反馈渠道具体请见本政策结尾处的联系方式，我们会尽快为您解答。

如您想更详细的了解我们的公司、平台，您可以通过本政策文末提供的联系方式与我们联系。

一、本政策内容

本政策为我们的所有产品或服务统一适用的通用内容,当您使用我们的任何产品或服务时,本政策即适用,无论该产品或服务是否单独设置了隐私条款,也无论您是浏览用户(访客)还是注册登录用户。若我们的产品或服务可能会包含或链接至第三方提供的信息或第三方服务(包括任何第三方应用、网站、产品、服务等),这些信息或服务由第三方负责运营,您使用该等信息或服务与我们无关。我们在此善意的提醒您,您在使用第三方信息或服务时,应留意和仔细阅读第三方向您展示的相关用户协议和个人信息保护政策,并妥善保管和谨慎提供您的个人信息。

本政策将帮助您了解以下内容:

- **我们如何收集并使用您的个人信息**
- **您对个人信息享有的控制权**
- **我们如何存储和保护您的个人信息**
- **我们如何处理儿童的个人信息**
- **本政策如何更新**
- **如何联系我们**
- **其他**

二、我们如何收集并使用您的个人信息

1、收集信息的类型

您在使用我们的产品或服务时，我们可能需要收集和使用您的一些个人信息，我们收集和使用的您的个人信息类型分为两种：

一种为基本业务功能所必需的信息：此类信息为产品或服务正常运行的必要信息，您须授权我们收集。如您拒绝提供，您将无法正常使用我们的产品或服务；

另一种为附加业务功能可能需要收集的信息：此信息为非基本业务功能所需的信息，您可以选择是否授权我们收集。如您拒绝提供，将导致附加业务功能无法实现或无法达到我们拟达到的效果，但不影响您对基本业务功能的正常使用。

我们需要特别提醒您的是：由于我们的产品和服务较多，为您提供的内容也不同，因此基本业务功能包括其收集的您的个人信息类型也会因产品服务的内容不同而有所区别，具体以产品/服务实际提供为准。除此之外，您理解并同意，我们可能会经常推出新的业务功能，可能需要收集新的个人信息或变更个人信息使用目的或方式。如果某一需要收集您的个人信息的功能或产品/服务未能在本政策中予以说明的，我们会通过更新本政策、页面提示、弹窗、网站公告等方式另行向您说明该信息收集的目的、内容、使用方式和范围，并为您提供自主选择同意的方式，且在征得您明示同意后收集。

在此过程中，如果您对相关事宜有任何疑问的，可以通过文末提供的方式联系我们，我们会尽快为您作出解答。

2、具体业务功能场景包括：

（一）注册及会员功能

使用摘星录 App 首先需要注册成为我们的注册用户。当您使用注册功能时，您需要按照我们的指引完成一系列注册的程序，在您成为注册用户后，我们将为您提供专属于注册用户的产品与/或服务。在此过程中，您需要提供给我们一些单独或者结合识别您的用户身份的信息，包括：手机号码、验证码匹配结果，并创建账号 UID、密码。我们收集这些信息是用以完成注册程序、为您持续稳定提供注册服务，并保护您注册账号的安全。您应知悉，手机号码和验证码匹配结果属于您的个人敏感信息，我们收集该类信息是为了满足相关法律法规的要求，如您拒绝提供可能导致您无法使用我们的此功能，请您谨慎考虑后再提供。同时，您也可以注册时或后续使用过程中填写或补充您的昵称、头像、介绍信息，如您未填写或后续删除、变更此类信息的，不会影响注册及会员功能的正常使用。

需要说明的是，我们的一些平台支持您使用第三方平台的账号（例如微信账号）进行登录，如您使用第三方平台的账号登录的，我们将根据您的授权获取该第三方账号下的相关信息（包括：用户名、昵称、头像，具体以您的授权内容为准）以及手机号验证信息。我们收集这些信息是用于为您提供账号登录服务以及保障您的账号安全，防范安全风险。如您拒绝授权此类信息的，您将无法使用第三方平台的账号登录我们平台，但不影响我们为您提供的其他产品和服务的正常使用。

如果您的账号遗失，我们将提供三种方式验证您的身份，身份验证后可重置密码，如手机身份验证后重置密码，或通过客服方式重置密码，在此过程中需您提供一些信息以验证您的身份。在找回密码时，我方可能需要您提供经常登录地点、经常登录设备、经常收听内容、注册时间和城市信息。

（二）更换/上传头像功能

当您使用更换/上传头像功能时，我们将收集您主动提供的上述图文内容信息，同时我们还将为便于您更换/上传头像功能而经过您的同意后访问您的手机相册权限。同时，您也可以随时通过相关手机功能设置开启/取消该权限。

您开启该权限即视为您授权我们可以访问、获取、收集、使用您的该等个人信息；当您取消该授权后，我们将不再收集该信息，也无法再为您提供上述与之对应的服务；但除非您依照法律的规定删除了您的个人信息，否则您的取消行为不会影响我们基于您之前的授权进行的个人信息的处理、存储。

（三）上传或发布评论等信息

您可以通过我们的服务建立联系和相互分享。在发表评论时，您公开分享的任何信息，如您发表的评论/跟评，您的头像、昵称、用户名称均会向他人披露。也可能会涉及披露您自己的个人信息。请您妥善保护自己的个人信息，仅在必要的情形下向他人提供、展示自己的信息。如您发现自己的个人信息泄露，尤其是您的账户或密码发生泄露，请您立即联系我方客服，采取相应措施。

（七）其他附加功能

获取网络状态以及电话/通话状态：

获取电话状态适用于不同通话状态下浏览服务的调整，通话时中断音频播放；通话中断后恢复音频播放。获取网络状态是基于 App 激活根据获取的网络状态提供服务选项，在无网络状态下会提示无法提供服务。

基于相机/摄像头的扫码功能：

您可在开启相机/摄像头权限后使用该功能。我们访问您的相机是为了使您可以使用摄像头扫码二维码和 AR 识别用图像，用于激活或 AR 展示等核心功能，以及其他您明确知悉的场景。如果您不授权，将会导致我们无法提供该业务功能。除上述权限之外，您可自主选择是否额外授予我们其他的系统权限。

读写存储卡：

保存、更新景区、景点信息。

获取应用列表：

我们接入的第三方推送服务要求获取该权限。

安全保障功能：

我们可能使用您的个人信息以预防、发现、调查欺诈、危害安全、非法或违反与我们或其关联方协议、政策或规则的行为，如会员账号活动异常、多端登录、流量异常等，从而保护您、其他用户，或我方或关联方的合法权益。

如上文所述，如果某一需要收集您的个人信息的功能或产品/服务未能在本个人信息保护政策中予以说明的，或者我们超出了与收集您的个人信息时所声称的目

的及具有直接或合理关联范围的，我们将在收集和使用你的个人信息前，通过页面提示、弹窗、消息通知、网站公告或其他便于您获知的方式另行向您说明，并为您提供自主选择同意的方式，且在征得您明示同意后收集和使用。

例外情形

另外，您充分理解并同意，我们在以下情况下收集、使用您的个人信息无需您的授权同意：

- 1) 与国家安全、国防安全有关的；与公共安全、公共卫生、重大公共利益有关的；
- 2) 与犯罪侦查、起诉、审判和判决执行等直接相关的；
- 3) 出于维护您或其他个人的生命、财产等重大合法权益但又很难得到您本人同意的；
- 4) 所收集的信息是您自行向社会公开的或者是从合法公开的渠道（如合法的新闻报道、政府信息公开等渠道）中收集到的；
- 5) 根据与您签订和履行相关协议或其他书面文件所必需的；
- 6) 用于维护我们的产品与/或服务的安全稳定运行所必需的，例如发现、处置产品与/或服务的故障；
- 7) 有权机关的要求、法律法规规定的其他情形。

3、我们如何使用 Cookie 和同类技术

在您使用我们的产品或服务时，我们可能会使用 Cookie 和同类技术收集您的一些个人信息，包括：上次内容进度、您的登录信息，Cookie 和同类技术收集该类信息是为了您使用我们的产品与/或服务的必要、简化您重复操作的步骤(如注册、登录)、便于您查看使用历史。我们承诺仅在本政策所述目的范围内使用 Cookie 和同类技术。

如果您的设置允许，您可以通过您的手机的设置以管理、（部分/全部）拒绝 Cookie 与/或同类技术；或删除已经储存在您的计算机、移动设备或其他装置内的 Cookie 与/或同类技术，从而实现我们无法全部或部分追踪您的个人信息。

4、我们如何共享、转让、公开披露您的个人信息

（一）共享

我们会重视对您的个人信息的保护，您的个人信息是我们为您提供产品与/或服务的重要依据和组成部分，对于您的个人信息，我们仅在本个人信息保护政策所述目的和范围内或根据法律法规的要求收集和使用，并严格保密，我们不会与第三方公司、组织和个人共享您的个人信息，除非存在以下一种或多种情形：您自行提出要求的；事先已征得您的明确授权同意。

目前，我们在以下情形中征求您对共享个人信息的授权同意，我们涉及嵌入第三方从而传输信息的情形逐项列举如下：

1.sdk 名称：AlipaySDK

应用场景描述：应用于支付宝登录

支付宝如何收集和使用个人信息：第三方应用集成 App 支付宝客户端 SDK 并提供服务的过程中，为了保障您的账户和资金安全以及支付服务的安全稳定运行，同时为了履行反洗钱、反恐怖融资、反电信网络诈骗等法定义务，我们需要收集和使用您的下列个人信息：可变更设备唯一标识、基本设备信息、软件安装列表以及 网络信息。为实现网络链路的选择和优化，以提升用户体验，我们需要收集和使用网络信息。

使用 App 支付宝客户端 SDK 的服务将涉及以下权限的申请，开发者应根据实际需求向您进行权限获取请求：

平台	权限	是否必选	申请目的
安卓平台	设备状态权限	必选	为了保障您的账户和资金安全以及支付服务的安全稳定运行。 为履行反洗钱、反恐怖融资、反电信网络诈骗等法定义务。
	网络连接权限	必选	允许程序使用网络连接，进行数据传输。 允许程序获取当前网络信息。
iOS 平台	网络连接权限	必选	允许程序使用网络连接，进行数据传输。 允许程序获取当前网络信息。
鸿蒙平台	设备状态权限	必选	为了保障您的账户和资金安全以及支付服务的安全稳定运行。 为履行反洗钱、反恐怖融资、反电信网络诈骗等法定义务。
	网络连接权限	必选	允许程序使用网络连接，进行数据传输。 允许程序获取当前网络信息。

我们如何存储和保护个人信息

- 我们在中华人民共和国境内收集和产生的个人信息将存储在中华人民共和国境内。我们仅在本说明所述目的所必需期间和法律法规及监管规定的时限内保存您的个人信息。如涉及前述信息向境外提供的，我们将严格遵守相关法律法规及监管要求，包括但不限于：向您说明个人信息出境的目的以及涉及的个人信息类型，按照国家网信部门会同国务院有关部门制定的办法和相关标准进行安全评估，并符合其要求。
- 为了保障您的信息安全，我们在收集您的信息后，将采取各种合理必要的措施保护您的信息。例如，在技术开发环境当中，我们仅使用经去标识化处理的信息进行统计分析；对外提供研究报告时，我们将对报告中所包含的信息进行去标识化处理。我们会将去标识化后的信息与可用于恢复识别个人的信息分开存储，确保在针对去标识化信息的后续处理中不重新识别个人。

3. 我们承诺我们将使信息安全保护达到业界领先的安全水平。为保障您的信息安全，我们致力于使用各种安全技术及配套的管理体系来尽量降低您的信息被泄露、毁损、误用、非授权访问、非授权披露和更改的风险。例如：通过网络安全层软件（SSL）进行加密传输、信息加密存储、严格限制数据中心的访问。传输和存储个人敏感信息（含个人生物识别信息）时，我们将采用加密、权限控制、去标识化/匿名化等安全措施。
4. 我们设立了个人信息保护责任部门，针对个人信息处理开展个人信息安全影响评估。同时，我们建立了相关内控制度，对可能接触到您的信息的工作人员采取最小够用授权的原则；对工作人员处理您的信息的行为进行系统监控，不断对工作人员培训相关法律法规及隐私安全准则，并进行安全意识强化宣导，每年组织全体工作人员参加安全考试。另外，我们的相应网络/系统通过了国家网络安全等级保护的测评。我们每年还会聘请外部独立第三方对我们的信息安全管理体进行评估。
5. 我们已制定个人信息安全事件应急预案，定期组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程。在不幸发生个人信息安全事件后，我们将按照法律法规的要求，及时向您告知：安全事件的基本情况和可能的影响、我们已采取或将要采取的处置措施、您可自主防范和降低风险的建议、对您的补救措施等。
6. 如开发者去除其应用中集成的本 SDK，我们将停止通过前述开发者应用向您提供本服务。

当您停止使用我们提供的服务时，我们将按照法律要求删除您的服务信息，但如有相关个人信息按照法律法规规定的保存期限未届满或者其他依法不适宜删除的情形，我们将停止除存储和采取必要的安全保护措施之外的处理。

您如何访问和管理个人信息

1. 我们非常重视您对个人信息的管理，并尽全力保护您对于个人信息依法享有的各项权利，以确保您有能力保障自身的隐私和信息安全。为了使您可以更加便捷地访问和管理个人信息，我们通过支付宝官方网站和支付宝客户端为您提供了相应的操作设置，请参考[《支付宝隐私权政策》](#)中的相关指引进行操作。
2. 如您需要进一步行使访问、更正、删除等个人信息权利，您可以通过[《支付宝隐私权政策》](#)中列明的联系方式与我们取得联系，联系渠道包括：
 - 客服热线 4007585858（应用开发者服务电话）、95188（用户服务电话）。
 - 在线客服“我的客服”。
 - 个人信息保护负责人邮箱：privacy-protection-officer@service.alipay.com。
 - 邮寄地址：杭州市西湖区西溪路 569 号蚂蚁 A 空间 隐私保护办公室。

客服部门将会同隐私保护办公室及时答复您。为了及时进行服务响应，我们推荐您使用前述客服热线或线上服务方式与我们联系。我们将在核验您的身份和凭证资料后十五个工作日或法律法规规定期限内作出答复。

我们如何保护未成年人的信息

1. 我们非常重视对未成年人个人信息的保护。我们期望父母或监护人指导未成年人使用我们的服务。我们将根据国家相关法律法规的规定保护未成年人的信息的保密性及安全性。

2. 如您为未成年人，建议请您的父母或监护人阅读本政策，并在征得您父母或监护人同意的前提下使用我们的服务或向我们提供您的信息。对于经父母或监护人同意而收集您的信息的情况，我们只会在受到法律允许、父母或监护人明确同意或者保护您的权益所必要的情况下使用或公开披露此信息。如您的监护人不同意您按照本政策使用我们的服务或向我们提供信息，请您立即终止使用我们的服务并及时通知我们，以便我们采取相应的措施。
3. 如您为未成年人的父母或监护人，当您对您所监护的未成年人的信息处理存在疑问时，请通过上文中的联系方式联系我们。
4. 特别提示：14 周岁以下的儿童及其监护人在为儿童注册支付宝账户前，敬请仔细阅读专门为儿童制定的《儿童个人信息保护规则》。在儿童使用我们的服务之前，应当确保已取得其监护人对《儿童个人信息保护规则》的同意。更多详情，敬请查阅[《儿童个人信息保护规则》](#)。

特别说明

由于 App 支付宝客户端 SDK 与用户无直接的交互对话界面，开发者应当根据适用的法律、法规和监管要求，保证我们可以合法地处理最终用户的相关个人信息。建议开发者在集成该 SDK，使用或者计划使用本 SDK 的服务时，应当在应用的显著位置或以其他可触达最终用户的方式告知最终用户（包括但不限于：SDK 提供方名称、收集的个人信息类型、使用目的、最终用户可浏览本隐私说明的链接），确保最终用户可以阅读并理解本 SDK 服务的信息收集状况，便于最终用户作出适当的选择。开发者可以参考如下方式提供条款内容：

- 第三方 SDK 名称：App 支付宝客户端 SDK
- 第三方名称：支付宝（中国）网络技术有限公司
- 收集的个人信息类型：Android ID、OAID、AAID、SSID、BSSID；系统设置、系统属性、设备型号、设备品牌、操作系统；IP 地址、网络类型、运营商信息、Wi-Fi 状态、Wi-Fi 参数、Wi-Fi 列表。
- 使用目的：
 - a. 保障用户账户和资金安全以及支付服务的安全稳定运行。
 - b. 履行反洗钱、反恐怖融资、反电信网络诈骗等法定义务。
 - c. 实现网络链路的选择和优化，以提升用户体验。

SDK 隐私说明链接：[App 支付宝客户端 SDK 隐私说明](#)

附录

1. 重点概念说明
 - a. 可变更的唯一设备识别码：是指用户可重置、变更或关闭追踪的唯一设备识别码，如 Android ID、OAID、AAID、SSID、BSSID。
 - b. 基本设备信息：设备机型相关信息，通常用于功能适配、稳定性等功能，如系统设置、系统属性、设备型号、设备品牌、操作系统。
 - c. 网络信息：如 IP 地址、网络类型、运营商信息、Wi-Fi 状态、Wi-Fi 参数、Wi-Fi 列表。

1. 如本政策发生更新,我们将通过支付宝官方网站发布公告或其他推送方式进行通知。如您在本政策更新生效后继续使用本服务,即表示您已充分阅读、理解并接受更新后的政策并愿意受更新后的政策约束。
2. 本说明未明确约定的部分以[《支付宝隐私权政策》](#)为准。

第三方机构名称: 蚂蚁金融服务集团

2.sdk 名称 : 微信登录 SDK

应用场景描述: 1. 用途概述

微信登录 SDK 为用户提供了一种便捷的登录方式,允许用户通过微信账号快速注册和登录第三方应用或网站。通过集成微信登录 SDK,用户无需额外创建账号,只需授权即可使用微信账号登录,简化了注册流程,提升了用户体验。

2. 权限与数据访问

为了确保微信登录功能的正常运行,微信登录 SDK 需要访问以下用户数据和设备权限:

微信账号信息

用途: 获取用户的基本信息(如昵称、头像),用于在第三方应用中显示用户身份。

数据范围: 用户的微信昵称、头像、OpenID(唯一标识符)。

设备权限

网络访问权限: 用于与微信服务器通信,完成登录授权和数据同步。

存储权限：用于缓存登录状态和用户信息，提升登录效率。

授权范围

静默授权：无需用户确认，获取用户的 OpenID。

用户确认授权：需要用户确认，获取用户的昵称、头像等公开信息。

3. 数据安全与隐私保护

数据加密

所有数据传输均通过 HTTPS 加密，确保用户信息在传输过程中的安全性。

数据存储

用户信息仅在用户授权的情况下存储，且存储过程符合相关隐私保护法规。

数据共享

用户信息仅用于登录和身份验证，不会与第三方共享或用于其他用途。

4. 用户控制与选择

授权控制

用户可以在登录时选择授权范围，决定是否分享昵称、头像等信息。

撤销授权

用户可以通过微信设置随时撤销对第三方应用的授权，停止数据共享。

隐私政策

第三方应用需提供明确的隐私政策，告知用户数据使用方式和保护措施。

5. 法律责任与合规性

合规性

微信登录 SDK 的使用需遵守《中华人民共和国网络安全法》和《个人信息保护法》等相关法律法规。

责任声明

第三方应用需对用户数据的收集、存储和使用负责，确保数据安全和隐私保护。

第三方机构名称：腾讯科技（深圳）有限公司

3.sdk 名称：Vuforia SDK

应用场景描述：1. 用途概述 获取相关传感器权限，具体信息如下。

Vuforia SDK 是一款增强现实（AR）开发工具包，旨在帮助开发者创建基于图像识别、物体识别和空间定位的 AR 应用。通过集成 Vuforia SDK，开发者可以为用户提供沉浸式的 AR 体验，例如虚拟物体叠加、交互式 3D 内容展示等。

2. 权限与数据访问

为了确保 AR 功能的正常运行，Vuforia SDK 需要访问以下用户数据和设备权限：

摄像头权限

用途：访问设备的摄像头，用于捕捉现实世界的图像或视频，以实现 AR 内容的叠加和交互。

数据范围：实时摄像头画面（仅用于 AR 处理，不会存储或上传）。

存储权限

用途：读取或存储 AR 应用所需的资源文件（如识别图、3D 模型）。

数据范围：应用本地文件，不涉及用户个人数据。

网络访问权限

用途：下载 AR 资源或与 Vuforia 服务器通信，用于识别图管理或云识别功能。

数据范围：仅限于 Vuforia 服务相关的数据传输。

设备信息

用途：获取设备型号、操作系统版本等信息，用于优化 AR 应用的性能和兼容性。

数据范围：匿名设备信息，不涉及用户个人身份信息。

3. 数据安全与隐私保护

数据加密

所有数据传输均通过 HTTPS 加密，确保数据在传输过程中的安全性。

数据存储

摄像头画面仅用于实时 AR 处理，不会存储或上传至服务器。

用户本地存储的 AR 资源文件仅用于应用功能，不会共享或上传。

数据共享

Vuforia SDK 不会主动收集或共享用户个人数据。

如果使用 Vuforia 的云识别服务，识别图数据可能会上传至 Vuforia 服务器，但不会与第三方共享。

4. 用户控制与选择

权限控制

用户可以在设备设置中随时关闭摄像头或存储权限，但可能会影响 AR 功能的正常使用。

隐私政策

开发者需在应用中提供明确的隐私政策，告知用户 Vuforia SDK 的数据使用方式和保护措施。

透明度

开发者应确保用户了解 AR 功能的运行机制，特别是摄像头和网络权限的使用目的。

5. 法律责任与合规性

合规性

Vuforia SDK 的使用需遵守《中华人民共和国网络安全法》和《个人信息保护法》等相关法律法规。

责任声明

开发者需对 AR 应用中的数据收集、存储和使用负责，确保用户隐私得到充分保护。

第三方机构名称：PTC Inc

4.sdk 名称：Vuplex WebView

应用场景描述：1. 用途概述

Vuplex WebView 是一款用于 Unity 的插件，允许开发者在 3D 应用中嵌入网页内容。通过集成 Vuplex WebView，开发者可以在 VR、AR 或桌面应用

中显示网页、运行 Web 应用程序或与 Web 服务交互，从而为用户提供丰富的互联网内容体验。

2. 权限与数据访问

为了确保网页内容的正常显示和交互，Vuplex WebView 需要访问以下用户数据和设备权限：

网络访问权限

用途：加载网页内容、与 Web 服务通信，确保网页的正常显示和功能运行。

数据范围：仅限于用户访问的网页内容和相关资源（如图片、脚本）。

存储权限

用途：缓存网页内容（如 Cookies、本地存储数据），以提升加载速度和用户体验。

数据范围：仅限于网页缓存数据，不涉及用户个人文件。

设备信息

用途：获取设备型号、操作系统版本等信息，用于优化网页渲染性能和兼容性。

数据范围：匿名设备信息，不涉及用户个人身份信息。

摄像头与麦克风权限（可选）

用途：如果网页内容涉及视频通话或音频录制，可能需要访问摄像头和麦克风。

数据范围：仅限于网页功能所需，不会存储或上传用户音视频数据。

3. 数据安全和隐私保护

数据加密

所有网络请求均通过 HTTPS 加密，确保数据传输的安全性。

数据存储

网页缓存数据仅存储在设备本地，不会上传至服务器。

用户可以通过清除缓存功能删除本地存储的网页数据。

数据共享

Vuplex WebView 不会主动收集或共享用户个人数据。

网页内容的数据使用和共享由网页提供方负责，开发者需确保网页内容的隐私合规性。

4. 用户控制与选择

权限控制

用户可以在设备设置中随时关闭网络、存储、摄像头或麦克风权限，但可能会影响网页功能的正常使用。

隐私政策

开发者需在应用中提供明确的隐私政策,告知用户 Vuplex WebView 的数据使用方式和保护措施。

透明度

开发者应确保用户了解网页内容的来源和数据使用方式,特别是涉及摄像头和麦克风权限的功能。

5. 法律责任与合规性

合规性

Vuplex WebView 的使用需遵守《中华人民共和国网络安全法》和《个人信息保护法》等相关法律法规。

责任声明

开发者需对应用中网页内容的数据收集、存储和使用负责,确保用户隐私得到充分保护。 第三方机构名称: Vuplex

使用插件

Dotween UI 动画

VolumetricLights 灯光效果

Unity-Logs-Viewer 问题跟踪、测试

5.sdk 名称 : Addressable

应用场景描述: 1. 用途概述

Addressable 是 Unity 提供的一种资源管理系统,旨在帮助开发者更高效地管理和加载游戏或应用中的资源(如场景、模型、纹理、音频等)。通过使用 Addressable,开发者可以实现资源的动态加载、卸载和更新,从而优化应用性能并减少初始安装包大小。

2. 权限与数据访问

为了确保 Addressable 系统的正常运行,可能需要访问以下用户数据和设备权限:

存储权限

用途: 读取或写入资源文件(如 AssetBundles), 用于动态加载和更新资源。

数据范围: 仅限于应用本地存储的资源文件, 不涉及用户个人数据。

网络访问权限

用途: 从远程服务器下载资源文件(如 AssetBundles), 用于资源的热更新。

数据范围: 仅限于资源文件的下载和更新, 不涉及用户个人数据。

设备信息

用途: 获取设备型号、操作系统版本等信息, 用于优化资源加载性能和兼容性。

数据范围：匿名设备信息，不涉及用户个人身份信息。

3. 数据安全和隐私保护

数据加密

所有网络请求均通过 HTTPS 加密，确保资源文件在传输过程中的安全性。

数据存储

资源文件仅存储在设备本地，不会上传至服务器。

用户可以通过清除缓存功能删除本地存储的资源文件。

数据共享

Addressable 不会主动收集或共享用户个人数据。

资源文件的使用和共享由开发者负责，需确保其隐私合规性。

4. 用户控制与选择

权限控制

用户可以在设备设置中随时关闭存储或网络权限，但可能会影响资源加载和更新功能。

隐私政策

开发者需在应用中提供明确的隐私政策,告知用户 Addressable 的数据使用方式和保护措施。

透明度

开发者应确保用户了解资源加载和更新的机制,特别是存储和网络权限的使用目的。

5. 法律责任与合规性

合规性

Addressable 的使用需遵守《中华人民共和国网络安全法》和《个人信息保护法》等相关法律法规。

责任声明

开发者需对应用中资源文件的数据收集、存储和使用负责,确保用户隐私得到充分保护。

6.sdk 名称 : dotween

应用场景描述: 1. 用途概述

DOTween 是一款用于 Unity 的动画插件,旨在帮助开发者快速实现平滑的动画效果(如移动、旋转、缩放、颜色变化等)。通过集成 DOTween,开发者可以简化动画代码的编写,提升开发效率,并为用户提供流畅的视觉体验。

2. 权限与数据访问

DOTween 作为一款纯代码库，主要用于处理动画逻辑，通常 不需要访问用户数据或设备权限。以下是其可能涉及的权限说明：

无直接权限需求

DOTween 本身不涉及用户数据的收集、存储或传输，因此不需要访问摄像头、麦克风、存储或网络权限。

间接权限依赖

如果开发者使用 DOTween 实现的功能涉及权限（如动画中需要访问摄像头或位置信息），则需在应用中单独声明相关权限。

例如：

如果 DOTween 用于控制摄像头的移动动画，则需要声明摄像头权限。

如果 DOTween 用于基于位置信息的动画效果，则需要声明位置权限。

3. 数据安全与隐私保护

无数据收集

DOTween 不会主动收集、存储或传输任何用户数据。

开发者责任

开发者需确保使用 DOTween 实现的功能符合隐私政策和相关法律法规。

如果动画功能涉及用户数据（如位置、摄像头画面），开发者需明确告知用户并获取授权。

4. 用户控制与选择

权限控制

如果 DOTween 实现的功能涉及权限（如摄像头、位置），用户可以在设备设置中随时关闭相关权限。

隐私政策

开发者需在应用中提供明确的隐私政策，告知用户相关功能的数据使用方式和保护措施。

5. 法律责任与合规性

合规性

DOTween 的使用需遵守《中华人民共和国网络安全法》和《个人信息保护法》等相关法律法规。

责任声明

开发者需对应用中动画功能的数据使用负责，确保用户隐私得到充分保护。

7.sdk 名称：Localization

应用场景描述：1. 用途概述

Localization（本地化）是一种技术或工具，用于将应用程序或游戏的内容（如文本、图片、音频等）适配到不同语言和地区，以提升全球用户的体验。通过集成 Localization 工具，开发者可以为用户提供多语言支持、文化适配的内容展示，从而满足不同地区用户的需求。

2. 权限与数据访问

Localization 工具通常 不需要直接访问用户数据或设备权限，但在某些场景下可能会涉及以下权限：

设备语言与区域设置

用途：获取设备的语言和区域设置，以自动适配用户的首选语言和格式（如日期、货币）。

数据范围：仅限于设备的语言和区域设置信息，不涉及用户个人数据。

网络访问权限（可选）

用途：如果本地化资源需要从远程服务器动态加载（如多语言文本、图片），则需要访问网络权限。

数据范围：仅限于本地化资源的下载，不涉及用户个人数据。

存储权限（可选）

用途：如果本地化资源需要存储在设备本地（如多语言文本文件、音频文件），则需要访问存储权限。

数据范围：仅限于本地化资源文件，不涉及用户个人数据。

3. 数据安全和隐私保护

无数据收集

Localization 工具本身不会主动收集、存储或传输任何用户个人数据。

开发者责任

开发者需确保本地化资源的使用符合隐私政策和相关法律法规。

如果本地化资源涉及用户数据（如用户生成内容），开发者需明确告知用户并获取授权。

4. 用户控制与选择

语言与区域设置

用户可以在设备设置中随时更改语言和区域设置，以切换应用的语言和格式。

权限控制

如果本地化功能涉及网络或存储权限，用户可以在设备设置中随时关闭相关权限。

隐私政策

开发者需在应用中提供明确的隐私政策,告知用户本地化功能的数据使用方式和保护措施。

5. 法律责任与合规性

合规性

Localization 的使用需遵守《中华人民共和国网络安全法》和《个人信息保护法》等相关法律法规。

责任声明

开发者需对应用中本地化功能的数据使用负责,确保用户隐私得到充分保护。

8.sdk 名称 : pathsystem

应用场景描述: 1. 用途概述

PathSystem 是一种用于 Unity 的工具或插件,旨在帮助开发者实现路径规划、导航和移动控制功能。通过集成 PathSystem,开发者可以为游戏或应用中的角色、车辆或其他对象提供智能的路径计算和移动逻辑,从而提升用户体验。

2. 权限与数据访问

PathSystem 作为一款路径规划和导航工具,通常 不需要直接访问用户数据或设备权限。但在某些场景下可能会涉及以下权限:

位置权限 (可选)

用途：如果 PathSystem 用于基于真实地理位置的路径规划（如地图导航），则需要访问设备的位置信息。

数据范围：仅限于设备的 GPS 或网络定位数据，用于路径计算。

存储权限（可选）

用途：如果 PathSystem 需要读取或存储路径数据（如地图文件、路径缓存），则需要访问存储权限。

数据范围：仅限于路径相关文件，不涉及用户个人数据。

网络访问权限（可选）

用途：如果 PathSystem 需要从远程服务器获取路径数据（如实时交通信息、地图更新），则需要访问网络权限。

数据范围：仅限于路径数据的下载和更新，不涉及用户个人数据。

3. 数据安全和隐私保护

无数据收集

PathSystem 本身不会主动收集、存储或传输任何用户个人数据。

开发者责任

开发者需确保路径规划功能的使用符合隐私政策和相关法律法规。

如果路径规划涉及用户数据 (如位置信息), 开发者需明确告知用户并获取授权。

4. 用户控制与选择

权限控制

如果 PathSystem 涉及位置、存储或网络权限, 用户可以在设备设置中随时关闭相关权限。

隐私政策

开发者需在应用中提供明确的隐私政策, 告知用户路径规划功能的数据使用方式和保护措施。

5. 法律责任与合规性

合规性

PathSystem 的使用需遵守《中华人民共和国网络安全法》和《个人信息保护法》等相关法律法规。

责任声明

开发者需对应用中路径规划功能的数据使用负责, 确保用户隐私得到充分保护。

8.sdk 名称 : pathsystem

应用场景描述: 1. 用途概述

阿里云 SDK 提供了 支付宝登录 和 手机号一键登录 功能，旨在为用户提供便捷、安全的登录方式。通过集成这些功能，用户可以使用支付宝账号或手机号快速注册和登录第三方应用，简化登录流程，提升用户体验。

2. 权限与数据访问

为了确保登录功能的正常运行，阿里云 SDK 需要访问以下用户数据和设备权限：

支付宝登录

用途：通过支付宝账号快速登录第三方应用。

数据范围：

用户的支付宝账号信息（如昵称、头像）。

用户的唯一标识符（OpenID）。

权限需求：

网络访问权限：用于与支付宝服务器通信，完成登录授权。

存储权限：用于缓存登录状态和用户信息。

手机号一键登录

用途：通过手机号快速登录第三方应用，无需输入验证码。

数据范围：

用户的手机号码。

设备的唯一标识符（如 IMEI）。

权限需求：

网络访问权限：用于与运营商服务器通信，完成手机号验证。

读取手机状态权限：用于获取设备信息，确保登录安全。

3. 数据安全和隐私保护

数据加密

所有数据传输均通过 HTTPS 加密，确保用户信息在传输过程中的安全性。

数据存储

用户信息仅在用户授权的情况下存储，且存储过程符合相关隐私保护法规。

数据共享

用户信息仅用于登录和身份验证，不会与第三方共享或用于其他用途。

4. 用户控制与选择

授权控制

用户可以在登录时选择授权范围，决定是否分享昵称、头像等信息。

撤销授权

用户可以通过支付宝设置或运营商服务随时撤销对第三方应用的授权, 停止数据共享。

隐私政策

第三方应用需提供明确的隐私政策, 告知用户数据使用方式和保护措施。

5. 法律责任与合规性

合规性

阿里云 SDK 的使用需遵守《中华人民共和国网络安全法》和《个人信息保护法》等相关法律法规。

责任声明

第三方应用需对用户数据的收集、存储和使用负责, 确保数据安全和隐私保护。

(二) 转让

转让是指将个人信息控制权向其他公司、组织或个人转移的过程。原则上我们不会将您的个人信息转让, 但以下情况除外: 您自行提出要求的; 事先已征得您的明确授权同意; 如我们进行兼并、收购、重组、分立、破产、资产转让或类似的交易, 而您的个人信息有可能作为此类交易的一部分而被转移, 我们将要求其重新获取您的明示授权同意; 并且要求新持有人继续遵守和履行该个人信息保护政策的全部内容 (包括使用目的、使用规则、安全保护措施等), 法律法规等规定

的其他情形。如具备上述事由确需转让的，我们会在转让前向您告知转让的信息的目的、类型（如涉及您的个人敏感信息的，我们还会向您告知涉及的敏感信息的内容），并在征得您的授权同意后再转让，但法律法规另有规定的或本政策另有约定的除外。

（三）公开披露

公开披露是指向社会或不特定人群发布信息的行为。除了因需要对违规账号、欺诈行为等进行处罚公告、公布中奖/获胜者等名单时脱敏展示相关信息等必要事宜而进行的必要披露外，我们不会对您的个人信息进行公开披露，如具备合理事由确需公开披露的，我们会在公开披露前向您告知公开披露的信息的目的、类型（如涉及您的个人敏感信息的，我们还会向您告知涉及的敏感信息的内容），并在征得您的授权同意后再公开披露，但法律法规另有规定的或本政策另有约定的除外。

对于公开披露的您的个人信息，我们会充分重视风险，在收到公开披露申请后第一时间且审慎审查其正当性、合理性、合法性，并在公开披露时和公开披露后采取不低于本政策约定的个人信息安全保护措施和手段的程度对其进行保护。

请您知悉，即使已经取得您的授权同意，我们也仅会出于合法、正当、必要、特定、明确的目的公开披露您的个人信息，并尽量对公开披露内容中的个人信息进行去标识化处理。您理解并知悉，去标识化或匿名化处理后的信息无法指向与识别您，已不属于您的个人信息，其公开披露无需征得您的授权同意。

我们将严格按照本政策的约定及相关法律法规的要求执行对个人信息的共享、转让、公开披露的操作，如因我们的过错原因导致您的合法权益遭受损害的，我们愿意就我们的过错在法律规定的范围内向您承担相应的损害赔偿责任。

二、您对个人信息享有的控制权

您对我们产品与/或服务中的您的个人信息享有多种方式的控制权，包括：您可以访问、更正/修改、删除您的个人信息，也可以撤回之前作出的对您个人信息的同意，同时您也可以注销您的摘星录 APP 的账号，获取您的个人信息副本。为便于您行使您的上述控制权，我们在产品的相关功能页面为您提供了操作指引和操作设置，您可以自行进行操作，如您在操作过程中有疑惑或困难的可以通过文末的方式联系我们来进行控制，我们会及时为您处理。

我们为您提供账号注销权限，您可以通过在线申请注销或联系我们的客服或通过其他我们公示的方式注销您的账号（但法律法规另有规定的或本政策另有约定的除外），一旦您注销账号，将无法使用我们提供的全线用户产品的服务且自动放弃已有的权益，因此请您谨慎操作。除法律法规另有规定外，注销账号之后，我们将停止为您提供我们所有的产品和服务，您曾通过该账号使用的我们的产品与服务下的所有内容、信息、数据、记录将会被删除或匿名化处理。

为保障安全，您可能需要提供书面请求，或以其他方式证明您的身份。我们可能会先要求您验证自己的身份，然后再处理您的请求。我们将在 30 天内作出答复。对于您合理的请求，我们原则上不收取费用，但对多次重复、超出合理限度的请求，我们将视情收取一定成本费用。对于那些无端重复、需要过多技术手段(例

如，需要开发新系统或从根本上改变现行惯例)、给他人合法权益带来风险或者非常不切实际(例如，涉及备份磁带上存放的信息)的请求，我们可能会予以拒绝。

在以下情形中，我们将无法响应您的请求：1、与个人信息控制者履行法律法规规定的义务相关的；2、与国家安全、国防安全直接相关的；3、与公共安全、公共卫生、重大公共利益直接相关的；4、与刑事侦查、起诉、审判和执行判决等直接相关的；5、个人信息控制者有充分证据表明个人信息主体存在主观恶意或滥用权利的；6、出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的；7、响应个人信息主体的请求将导致个人信息主体或其他个人、组织的合法权益受到严重损害的；涉及商业秘密的。

三、我们如何存储和保护您的个人信息

(一) 个人信息的存储

存储地点：我们依照法律法规的规定，将您的个人信息存储于中华人民共和国境内。目前我们暂时不存在跨境存储您的个人信息或向境外提供个人信息的场景。如需跨境存储或向境外提供个人信息的，我们会单独向您明确告知（包括出境的目的、接收方、使用方式与范围、使用内容、安全保障措施、安全风险等）并再次征得您的授权同意，并严格要求接收方按照本政策以及其他相关要求来处理您的个人信息；

存储期限：我们在为提供我们的产品和服务之目的所必需且最短的期间内保留您的个人信息，例如：当您使用我们的注册及会员功能时，我们需要收集您的手机号码，且在您提供后并在您使用该功能期间，我们需要持续为您保持您的手机号

码,以向您正常提供该功能、保障您的账号和系统安全。在超出上述存储期限后,我们会对您的个人信息进行删除或匿名化处理。但您行使删除权、注销账户的或法律法规另有规定的除外(例如:《电子商务法》规定:商品和服务信息、交易信息保存时间自交易完成之日起不少于三年)。

说明:如您申请注销账号且已成功向我们提交注销申请的,该账号将被永久注销,该账号下的相关信息我们会作删除或匿名化处理。

(二) 个人信息的保护措施

我们一直都极为重视保护用户的个人信息安全,为此我们采用了符合行业标准的安全技术措施及配套的组织架构和管理体系等多层面保护措施以最大程度降低您的信息被泄露、毁损、误用、非授权访问、非授权披露和更改的风险。包括:

数据安全技术措施

(1) 数据安全传输方面防止传输链路被嗅探、窃听截取风险,建立安全的隐私数据采集环境,保证数据采集的私密性和完整性;

(2) 数据安全存储方面对用户个人敏感信息采取独立、加密存储等额外的安全保护措施;

(3) 数据访问和使用的安全控制方面,实施严格的数据权限控制机制,采取多重身份认证技术,并对能够处理您的信息的行为进行监控,避免数据被违规访问和未授权使用;

(4) 建立完整的审计机制，对数据生命周期的全流程进行监控与审计，防止您的个人信息遭遇未经授权的访问、公开披露、使用、修改、人为或意外的损坏或丢失；

(5) 其他实现数据安全保护的措施。

(三) 数据安全组织和管理措施

(1) 对可能接触到您的信息的工作人员采取最小化权限原则；

(2) 建立数据分类分级制度、业务数据安全使用规范、数据合作规范等管理体系，保障您的信息在收集、传输、使用、存储、转移、销毁等环节的处置满足法律法规相关规范和安全要求；

(3) 定期组织员工参加安全与隐私保护相关培训并要求完成规定的考核，加强员工对于保护个人信息重要性的认知；

(4) 其他可行的安全组织和管理措施。

四、我们如何处理未成年人/儿童的个人信息

我们的产品、网站和服务主要面向成人。如果没有父母或监护人的同意，儿童不应创建自己的个人信息主体账户。未成年人使用我们的产品与/或服务之前应首先取得其监护人的同意。如您为未成年人，在使用我们的产品与/或服务前，应在监护人监护、指导下共同阅读本个人信息保护政策，且应在监护人明确同意和指导下使用我们的产品与/或服务、提交个人信息。我们根据国家相关法律法规

的规定保护未成年人的个人信息，只会在法律法规允许、监护人明确同意或保护您的权益所必要的情况下收集、使用或公开披露未成年人的个人信息；若您是未成年人的监护人，当您对您所监护的未成年人的个人信息有相关疑问时，请通过如何联系我们章节末的联系方式与我们联系。如果我们发现在未事先获得可证实的监护人同意的情况下收集了未成年人的个人信息，则会设法尽快删除相关数据。

五、本政策如何更新

我们鼓励您在每次使用我们的产品或服务时都查阅我们的个人信息保护政策。为了给您提供更好的服务，我们会根据产品的更新情况及法律法规的相关要求更新本政策的条款，该等更新构成本政策的一部分。如该等更新造成您在本政策下权利的实质减少或重大变更，我们将在本政策生效前通过在显著位置提示或向您发送推送消息或以其他方式通知您，若您继续使用我们的服务，即表示您充分阅读、理解并同意受经修订的个人信息保护政策的约束。为保障您的合法权益，我们建议您定期在我们平台的设置页面中查看本政策。

本政策所指的重大变更包括但不限于：

- 1、我们的服务模式发生重大变化。如处理个人信息的目的、处理的个人信息类型、个人信息的使用方式等；
- 2、我们在所有权结构、组织架构等方面发生重大变化。如业务调整、破产并购等引起的所有者变更等；
- 3、个人信息共享、转让或公开披露的主要对象发生变化；

4、您参与个人信息处理方面的权利及其行使方式发生重大变化;

5、我们负责处理个人信息安全的责任部门、联络方式及投诉渠道发生变化时。

六、如何联系我们

(一)如您对本政策的执行或使用我们的服务时遇到的与隐私保护相关的事宜有任何问题咨询、投诉等,我们专门为您提供了多种反馈通道,您可与我们平台上产品功能页面上在线提交意见反馈;或者通过邮件反馈:

zhaixinglu@szzxl.work

关于深圳摘星录科技有限公司:

公司基本情况如下:

(1) 公司名称: 深圳摘星录科技有限公司

(2) 注册地址: 深圳市龙岗区坂田街道象角塘社区佳兆业中央广场二期 3 栋
1912

(3) 注册时间: 2024-8-29

(二)我们会在收到您的意见及建议后,并在验证您后用户身份后的 30 日内尽快向您回复。

七、其他

(一) 本政策的解释及争议解决均应适用中华人民共和国大陆地区法律。与本政策相关的任何纠纷，双方应协商友好解决；若不能协商解决，您同意将争议提交至北京市西城区人民法院诉讼解决。

(二) 本政策的标题仅为方便及阅读而设，并不影响正文其中任何规定的含义或解释。

本版更新时间：2024 年 12 月 29 日

本版生效时间：2024 年 12 月 29 日

深圳摘星录科技有限公司