

东吴人寿“掌上东吴 app”隐私政策

更新日期：2024 年 9 月 4 日

生效日期：2024 年 9 月 4 日

注册名称：东吴人寿保险股份有限公司

注册地址：江苏省苏州市虎丘区高新区狮山路 28 号高新广场 31-34 楼

东吴人寿保险股份有限公司（以下简称“我司”）深知个人信息对您的重要性，会尽力保护您的个人信息安全。我司致力于维护您对我行的信任，恪守以下原则保护您的个人信息：权责一致原则、目的明确原则、选择同意原则、必要性原则、确保安全原则、公开透明原则等。同时，我司承诺依法采取相应的安全保护措施来保护您的个人信息。

“掌上东吴 app”是一款为东吴人寿客户提供线上业务办理服务的移动应用，我们将通过本政策向您说明东吴人寿如何收集、存储和使用你的个人信息及你享有的权利，其中要点如下：

- 1、我们将说明我们收集的你的个人信息类型及其对应的用途，以便你了解我们能所收集的个人信息类别、使用理由及收集方式。
- 2、当你使用一些功能和服务时，除了按照相关法律法规要求必须收集的，我们都会在获得你的同意后收集你的个人信息。
- 3、我们不会主动向东吴人寿旗下产品以外的第三方共享或转让你的个人信息，如果发生我们需要向你提供特定服务或因你个人原因需要我们将你的个人信息共享或转让至东吴人寿以外的第三方情形时，我们会按照法律法规及国家标准的要求确认相关协议，并直接或确认第三方征得你对上述行为的明示同意。
- 4、我们不会主动从东吴人寿以外的第三方获取你的个人信息。如未来需要从第三方间接获取你的个人信息，我们会严格遵守相关法律法规的规定。我们会在评估和确认第三方保障其提供的信息的合法性之后、获取相应信息前向你明示信息的来源、类型及使用范围，并征得你的明示同意。
- 5、你可以通过本政策介绍的方式管理你的个人信息，包括设置隐私功能、注销帐号和投诉举报。

如你想了解详尽信息，请根据以下索引阅读具体内容：

1. 我们收集的信息
2. 设备权限使用
3. 信息的存储和使用
4. 信息的对外提供
5. 你的权利
6. 本政策的适用及更新
7. 对未成年人的保护
8. 联系我们

1.我们收集的信息

我们的产品基于 DCloud uni-app(5+ App/Wap2App)开发，应用运行期间需要收集您的设备唯一识别码（IMEI/android ID/DEVICE_ID/IDFA、SIM 卡 IMSI 信息）以提供统计分析服务，并通过应用启动数据及异常错误日志分析改进性能和用户体验，为用户提供更好的服务。详情内容请访问[《DCloud 用户服务条款》](#)。

当您通过掌上东吴 app 查看选购我们的产品或接受我们的服务，并投保具体保险产品时，我们可能需要获得您的如下信息：

1.1 基于保险产品选购、投保、保全、保单查询等基本功能需要收集的相关信息

- 1) **登录信息：**手机号码、姓名、身份证号。如您选择通过微信或者指纹登录，我们还需要获得您的微信地区、性别、昵称、头像信息、指纹信息。如果您拒绝提供这些信息，您可能无法正常使用我们的服务。
- 2) **投保信息：**投保人和被保险人的姓名、身份证件、出生日期、性别、民族、国籍、地址、邮箱、工作信息、健康生理信息、收入、人脸信息、投保人与被保险人、受益人之间的关系；受益人的姓名、身份证件、联系方式，以及保险订单信息及投保所需的必要信息。如果您拒绝提供这些信息，我们将无法为您提供相关服务以完成投保手续。
- 3) **支付信息：**第三方支付信息、银行账户信息、以及其它支付和财务信息。如果您拒绝提供这些信息，我们将无法为您提供相关服务以完成投保手续。
- 4) 当您通过我们的平台申请保险合同保全时，我们可能收集您申请保全时所需要的相关信息，包括：**保单信息、联系方式、被保险人姓名、被保险人身份证号码、保全申请事由**。如果您拒绝提供这些信息，我们将无法为您提供相关服务以完成投保手续。

5) 当您通过我们的平台申请使用投保、保全、保单查询等功能时, 您同意授权我们, 收集您合法留存在保险公司的投保、保全、以及保单等相关信息。

1.2 为了账户安全需要收集的信息

为了保障您的账号安全、交易安全、系统运行安全, 满足法律法规和我们协议规则的相关要求, 以及不断地改进我们的产品, 在您使用我们的产品和服务时, 我们需要收集相关的日志信息与设备信息。日志信息包括 IP 地址、访问的浏览器信息、点击和浏览我们产品和服务功能或页面的 URL 地址及其使用情况与频率、应用崩溃情况、总体安装使用情况、性能数据、应用来源;

1) **个人常用设备信息:** 包括与您使用设备的软硬件特征和设备环境信息相关的信息, 例如 IDFV、设备标识 Oaid、Android ID、设备型号、操作系统、唯一设备标识符、登陆 IP 地址、App 版本号、接入网络的方式、类型和状态、网络质量数据、设备加速器 (如重力感应设备)、位置信息、IMEI、MAC、软件安装列表、操作日志。对于从您的各种设备上收集到的信息, 我们可能会将它们进行关联, 以便我们能在这些设备上为您提供一致的服务。我们可能会将您的设备信息或电话号码与您的掌上东吴账号相关联。

1.3 根据相关法律法规及国家标准, 以下情形中, 我们可能会收集、使用你的相关个人信息无需征求你的授权同意:

- 1) 与国家安全、国防安全等国家利益直接相关的;
- 2) 与公共安全、公共卫生、公众知情等重大公共利益直接相关的;
- 3) 与犯罪侦查、起诉、审判和判决执行等直接相关的;
- 4) 出于维护你或其他个人的生命、财产、声誉等重大合法权益但又很难得到本人同意的;
- 5) 所收集的个人信息是你自行向社会公众公开的;
- 6) 从合法公开披露的信息中收集个人信息的, 如合法的新闻报道、政府信息公开等渠道;
- 7) 根据你要求签订和履行合同所必需的;
- 8) 用于维护所提供的产品或服务的安全稳定运行所必需的, 例如发现、处置产品或服务的故障;
- 9) 为开展合法的新闻报道所必需的;
- 10) 出于公共利益开展统计或学术研究所必要, 且其对外提供学术研究或描述的结果时, 对结果中所包含的个人信息进行去标识化处理的;
- 11) 法律法规规定的其他情形。

请你理解, 我们向你提供的功能和服务是不断更新和发展的, 如果发生功能或服务未在前述说明中且需要收集你的信息, 我们会通过页面提示、交互流程、网站公告等方式另行向你说明信息收集的内容、范围和目的, 并征得你的同意。目前掌上东吴 App 不会主动从东吴人寿以外的第三方获取你的个人信息。如因业务发展需要从第三方获取你的个人信息时, 我们会在获取前向你明示你个人信息的来源、类型及使用范围, 我们将在处理你的个人信息前, 征得你的明示同意; 我们会严格遵守相关法律法规的规定, 要求第三方保障其提供的信息的合法性。

2.设备权限使用

为您提供优质、便捷的服务, 您知悉并同意我们使用您设备的一些权限, 我们现将可能设备权限使用列表及对应目的说明:

2.1 位置 您需要授权我们使用位置权限, 以便我们提供考勤功能。禁用后可能会影响相关服务的使用。

2.2 相机 您需要授权我们使用相机权限, 以便我们的核心业务功能的使用: 拍照上传资料、人脸识别和证件卡片扫描。禁用后可能会影响相关服务的使用。

2.3 存储 您需要授权我们使用存储权限, 以便我们的移动客户端可以写入、存储用户信息和日志等。禁用后可能会影响相关服务的使用。

2.4 相册 您需要授权我们使用访问相册权限, 以便我们提供从相册中选择图片进行上传的服务。禁用后可能会影响相关服务的使用。

2.5 拨打电话 您需要授权我们使用拨打电话的权限, 以便我们提供快速呼叫客户的功能。禁用后可能会影响相关服务的使用。

2.6 网络 您需要授权我们申请网络连接的权限, 以便我们的服务能在网络环境下正常运行。禁用后可能会影响相关服务的使用。

2.7 手机信息 您需要授权我们申请获取手机信息(唯一设备标识符/MAC 地址/AndroidId/IDFA/IMEI)权限, 以便我们能够收集信息更好的进行产品优化及错误分析。禁用后可能会影响相关服务的使用。

2.8 指纹 您需要授权我们获取指纹的权限, 以便我们提供指纹登录的功能。禁用后可能会影响相关服务的使用。

以上权限如您拒绝授权, 可能无法正常使用移动客户端

当我们要将信息用于本策略未载明的其它用途时, 会事先征求您的同意。当我们要将基于特定目的收集而来的信息用于其他目的时, 会事先征求您的同意。

3.信息的存储和使用

3.1 信息存储的地点

我们会按照法律法规规定, 将境内收集的用户个人信息存储于中国境内。

3.2 信息存储的期限

我们仅为实现目的所必需的时间保留你的个人信息。当我们的产品或服务发生停止运营的情形时，我们将以推送通知、公告等形式通知你，并在相关法律法规要求期限内删除你的个人信息或进行匿名化处理。

3.3 信息的使用

一般情况下，我们从相应功能下收集的你的个人信息是应用在该功能与服务的提供与支持。特定情况下，我们也可能需要将通过某些功能所收集的信息用于我们的其他服务，还可能为了提供更稳定安全的服务而记录应用程序崩溃数据、使用情况、性能数据的信息。如我们在使用你的个人信息，超出了与收集时所声称的目的及具有直接或合理关联的范围，我们将在使用你的个人信息前，再次向你告知并征得你的明示同意。

3.4 掌上东吴涉及用户信息使用的 SDK 相关情况列举，详见本政策[附件](#)。

3.5 安全事件处置

1) 互联网环境并非百分之百安全，我们将尽力确保您发送给我们的任何信息的安全性。如果我们的物理、技术、或管理防护设施遭到破坏，导致信息被非授权访问、公开披露、篡改、或毁坏，导致您的合法权益受损，我们将承担相应的法律责任

2) 为应对个人信息泄露、损毁和丢失等可能出现的风险，我们制定了多项制度，明确安全事件、安全漏洞的分类分级标准及相应的处理流程。我们将按照安全事件处置规范要求，针对不同安全事件启动安全预案，进行止损、分析、定位、制定补救措施、联合相关部门进行溯源和打击。

3) 一旦发生个人信息安全事件，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 and 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。我们同时将及时将事件相关情况以邮件、信函、电话、推送通知等方式告知您，难以逐一告知个人信息主体时，我们会采取合理、有效的方式发布公告。同时，我们还将按照监管部门要求，主动上报个人信息安全事件的处置情况。

4) 如您发现自己的个人信息泄密，尤其是您的账号及密码发生泄露，请您立即通过本政策约定的联系方式联络我们，以便我们采取相应措施。

4. 信息的对外提供

4.1 我们不会主动共享或转让你的个人信息至东吴人寿外的第三方，如发生确实需要共享或转让你的个人信息或你需要我们将你的个人信息共享或转让至东吴人寿以外的第三方情形时，我们会直确认第三方征得你对上述行为的明示同意。

4.2 我们不会对外公开披露你的个人信息，如必须公开披露时，我们会向你告知此次公开披露的目的、披露信息的类型和内容，并征得你的明示同意。

4.3 随着我们业务的持续发展，如果我们需要进行合并、重组、收购、资产转让时，我们将告知你相关情况，我们会按照法律法规及不低于本指引所要求的标准继续保护或要求新的个人信息保管者继续保护你的个人信息。

4.4 根据相关法律法规及国家标准，以下情形中，我们可能会共享、转让、公开披露个人信息无需事先征得你的授权同意：

- 1) 与国家安全、国防安全等国家利益直接相关的；
- 2) 与公共安全、公共卫生、公众知情等重大公共利益直接相关的；
- 3) 与犯罪侦查、起诉、审判和判决执行等直接相关的；
- 4) 出于维护你或其他个人的生命、财产、声誉等重大合法权益但又很难得到本人同意的；
- 5) 所收集的个人信息是你自行向社会公众公开的；
- 6) 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；

5. 你的权利

按照中国相关的法律法规与标准，我们保障你对你的个人信息行使以下权利：

5.1 删除个人信息

在以下情形中，您可以向我们提出删除个人信息的请求：

- 1) 如果我们处理个人信息的行为违反法律法规；
- 2) 如果我们收集、使用您的个人信息，却未征得您的同意；
- 3) 如果我们处理个人信息的行为违反了与您的约定；
- 4) 如果您不再使用我们的产品或服务，或您注销了账号；
- 5) 如果我们不再为您提供产品或服务。

若我们决定响应您的删除请求，我们还将同时通知从我们获得您的个人信息的实体，要求其及时删除，除非法律法规另有规定，或这些实体获得您的独立授权。

5.2 注销你的帐号

您随时可注销此前注册的账户，您可以通过以下方式自行操作：

- 1) 进入掌上东吴后，点击“个人中心->设置”；
- 2) 点击“永久注销工号”；

在注销账户之后，我们将停止为您提供产品或服务，并依据您的要求，删除您的个人信息，法律法规另有规定的除外。

5.3 撤回个人信息

- 1) 进入掌上东吴后，点击“个人中心->设置”；
- 2) 点击“永久注销工号”可以撤回同意收集个人信息；

5.4 更正个人信息

可以通过 <http://www.soochowlife.net> 更正个人信息

可以通过客服电话 95354 更正个人信息

5.6 响应您的上述请求

如果您无法通过上述方式访问、更正、删除（含备份数据）您的用户信息或注销账户，或您需要访问、更正或删除您在使用我们服务或功能时所产生的其他用户信息，或您认为我们存在任何违反法律法规或与您关于用户信息的收集或使用的约定，您均可通过客服电话 95354 与我们联系。为了保障安全，我们可能需要您提供书面请求，或以其他方式证明您的身份，我们将在十五天内完成核查和处理。如您不满意，还可以通过以下途径投诉：

通过 <http://www.soochowlife.net>

客服电话 95354

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。

另外，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) 与犯罪侦查、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；
- 8) 涉及商业秘密的。

6. 本政策的适用及更新

- 1) 我们的基本情况发生变化，例如：兼并、收购、重组引起的所有者变更
- 2) 收集、存储、使用个人信息的范围、目的、规则发生变化
- 3) 对外提供个人信息的对象、范围、目的发生变化
- 4) 您访问和管理个人信息的方式发生变化
- 5) 数据安全能力、信息安全风险发生变化
- 6) 用户询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式发生变化
- 7) 其他可能对您的个人信息权益产生重大影响的变化

7. 对未成年人的保护

我们非常重视对未成年人个人信息的保护。本平台提供的服务主要面向成人。根据相关法律法规的规定，若您 18 周岁以下的未成年人（特别是未满十四周岁的儿童），在使用本平台的服务前，您需要在您的监护人的陪同下阅读本政策，我们已使用加粗字体标注未成年人（特别是未满十四周岁的儿童）个人信息的相关条款，请您和您的监护人务必仔细阅读；请您在取得您的监护人对本政策全部条款的同意之后使用本平台提供的各项产品和服务。如果没有监护人同意，儿童不应创建自己的个人信息主体账户。

监护人特别说明：

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的保密性及安全性。若您未成年人的监护人，请帮助我们保护您监护的未成年人的个人信息和隐私安全，要求他们在您的监护下共同阅读并接受本协议，且应在您的同意和指导下提交个人信息、使用平台提供的服务。若您不同意本政策内容，您应要求您监护的未成年人立即停止访问/使用本平台服务，并及时通知我们，以便我们采取相应的措施。若您监护的未成年人使用/继续使用我们的服务，即表示您和您监护的未成年人同意接受本政策的约束。

儿童特别说明：

我们建议任何儿童参加网上活动都应事先取得监护人的同意。对于可能涉及的不满 14 周岁的儿童个人信息，我们将进一步采取措施，除遵守本政策关于个人信息的约定外，严格遵循《儿童个人信息网络保护规定》等法律法规的要求，且不会超过实现收集、使用目的所必须的期限，到期后我们会对儿童个人信息进行删除或匿名化处理。

如果您是儿童，请通知您的监护人共同阅读本政策，并在您提交个人信息、使用本平台服务之前，寻求并取得您的监护人的同意和指导。您点击同意本政策，或您使用/继续使用本平台服务、提交个人信息，即表示您已获得您的监护人的许可，且您的监护人亦同意受本政策的约束。

8. 联系我们

1、当你有其他关于个人信息保护的问题时，请通过 <http://www.soochowlife.net>、客户服务平台 APP、在线客服、东吴人寿-在线客服，客服电话 95354 与我们联系。你也可以将你的问题发送至 services@soochowlife.net 或寄到如下地址：中国江苏省苏州市高新区狮山路 28 号高新广场 31 楼 运营部（收）邮编：215000

2、一般情况下，我行将在 15 个工作日内给予答复。如果您对我们的答复不满意，特别是如果您认为我们的个人信息处理行为损害了您的合法权益，您还可以向网信、电信、公安及市场监管等监管部门进行投诉或举报，您还可以通过向被告住所地有管辖权的法院提起诉讼来寻求解决。

东吴人寿保险股份有限公司

2024 年 9 月 4 日

用户服务条款

服务条款确认与接纳

DCloud 拥有 dcloud.io、dcloud.net.cn 其涉及到的产品、相关软件的所有权和运作权，DCloud 享有对其产品的上一切活动的监督、提示、检查、纠正及处罚等权利。用户通过注册程序阅读本服务条款并点击“注册”按钮完成注册，即表示用户与 DCloud 已达成协议，自愿接受本服务条款的所有内容。如果用户不同意服务条款的条件，则不能获得使用 DCloud 服务以及注册成为 DCloud 用户的权利。

使用规则

1.

用户注册成功后，DCloud 将给予每个用户一个用户账号及相应的密码，该用户账号和密码由用户负责保管；用户应当对以其用户账号进行的所有活动和事件负法律责任。

2.

用户须对在 DCloud 的注册信息的真实性、合法性、有效性承担全部责任，用户不得冒充他人；不得利用他人的名义发布任何信息；不得恶意使用注册帐户导致其他用户误认；否则 DCloud 有权立即停止提供服务，收回其账号并由用户独自承担由此而产生的一切法律责任。

3.

用户不得使用 DCloud 服务发送或传播敏感信息和违反国家法律制度的信息，包括但不限于下列信息：

- 反对宪法所确定的基本原则的；
- 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- 损害国家荣誉和利益的；
- 煽动民族仇恨、民族歧视，破坏民族团结的；
- 破坏国家宗教政策，宣扬邪教和封建迷信的；
- 散布谣言，扰乱社会秩序，破坏社会稳定的；
- 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
- 侮辱或者诽谤他人，侵害他人合法权益的；
- 含有法律、行政法规禁止的其他内容的。

4.

DCloud 有权对用户使用 DCloud 产品的情况进行审查和监督，如用户在使用 DCloud 产品时违反任何上述规定，DCloud 或其授权的人有权要求用户改正或直接采取一切必要的措施以减轻用户不当行为造成的影响。

5.

盗取他人用户账号或利用网络通讯骚扰他人，均属于非法行为。用户不得采用测试、欺骗等任何非法手段，盗取其他用户的账号和对他人进行骚扰。

免责声明

1.

DCloud 不能对用户在本社区回答问题的答案或评论的准确性及合理性进行保证。

2.

若 DCloud 产品已经明示其网络服务提供方式发生变更并提醒用户应当注意事项，用户未按要求操作所产生的一切后果由用户自行承担。

3.

用户明确同意其使用 DCloud 产品网络服务所存在的风险将完全由其自己承担；因其使用 DCloud 服务而产生的一切后果也由其自己承担，DCloud 对用户不承担任何责任。

4.

DCloud 不保证网络服务一定能满足用户的要求，也不保证网络服务不会中断，对网络服务的及时性、安全性、准确性也都不作保证。

5.

对于因不可抗力或 DCloud 不能控制的原因造成的网络服务中断或其它缺陷，DCloud 不承担任何责任，但将尽力减少因此而给用户造成的损失和影响。

5.

用户同意保障和维护 DCloud 及其他用户的利益，用户在 DCloud 发表的内容仅表明其个人的立场和观点，并不代表 DCloud 的立场或观点。由于用户发表内容违法、不真实、不正当、侵犯第三方合法权益，或用户违反本协议项下的任何条款而给 DCloud 或任何其他第三人造成损失，用户同意承担由此造成的损害赔偿赔偿责任。

服务条款的修改

DCloud 会在必要时修改服务条款，服务条款一旦发生变动，DCloud 将会为用户进入下一步使用前的页面提示修改内容。如果您同意改动，请再一次激活"我同意"按钮。如果您不接受，请及时取消您的帐户。用户要继续使用 DCloud 各项服务需要两方面的确认：

1.
首先确认 DCloud 服务条款及其变动。
2.
同意接受所有的服务条款限制。

隐私政策

DCloud 非常重视对用户隐私权的保护，承诺不会在未获得用户许可的情况下擅自将用户的个人资料信息出租或出售给任何第三方，但以下情况除外：

- 您同意让第三方共享资料；
- 您同意公开你的个人资料，享受为您提供的产品和服务；
- 本站需要听从法庭传票、法律命令或遵循法律程序；
- 本站发现您违反了本站服务条款或本站其它使用规定。

如果您对此条款有任何疑问或建议，欢迎通过邮件联系我们：service@dcloud.io

掌上东吴 SDK 情况表

“掌上东吴 app”是一款为东吴人寿客户提供线上业务办理服务的移动应用，我们将通过本政策向您说明东吴人寿如何收集、存储和使用你的个人信息及你享有的权利，其中要点如下：

1.友盟

公司全称：友盟同欣(北京)科技有限公司

SDK 类型：工具

SDK 使用目的：友盟提供了数据统计，分享服务。

SDK 使用场景：统计各渠道用户 app 使用情况，分享功能。

SDK 所需用户信息：独立设备标识符、iOS 广告标识符 (IDFA)、安卓广告主标识符、网卡 (MAC) 地址、国际移动设备识别码 (IMEI)、设备型号、终端制造厂商、终端设备操作系统版本 [隐私权政策链接](#)

使用目的：统计数据更好的优化产品。

关联引用 sdk：阿里 UC 崩溃 SDK、UC 浏览器服务 SDK、啄木鸟 SDK。

2.百度地图

公司全称：北京百度网讯科技有限公司

SDK 类型：定位

SDK 使用目的：百度地图提供地图，定位，导航等功能。

SDK 使用场景：考勤和查找客户等功能。

SDK 所需用户信息：硬件型号、操作系统版本、设备配置、唯一设备标识符、网络设备硬件地址 MAC、广告标识符 IDFA 信息、设备连接信息以及设备状态信息、网络身份标识信息、国际移动设备身份码 IMEI。

使用目的：进行位置的定位和访问。

3.微信开放平台

公司全称：深圳市腾讯计算机系统有限公司

SDK 类型：社交

SDK 使用目的：微信分享、登录、收藏等功能

SDK 使用场景：微信分享，绑定微信登录。

SDK 所需用户信息：独立设备标识符、iOS 广告标识符 (IDFA)、安卓广告主标识符、网卡 (MAC) 地址、国际移动设备识别码 (IMEI)、设备型号、终端制造厂商、终端设备操作系统版本

使用目的：实现微信分享和快捷登录功能。

4.腾讯 OCR

公司全称：腾讯云计算（北京）有限责任公司

SDK 类型：工具

SDK 使用目的：腾讯云提供丰富的 OCR 识别服务，覆盖不同场景下文字识别需求。

SDK 使用场景：证件，银行卡，文字快速识别。

SDK 所需用户信息：设备型号，系统版本，手机型号

使用目的：通过文字识别，便捷地录入身份证，银行卡号信息。

5.个推·消息推送

公司全称：每日互动股份有限公司

SDK 类型：消息推送

SDK 使用目的：Dcloud 集成的包括多家手机厂商系统推送和个推的独立推送。

SDK 使用场景：获取关键节点业务的推送消息。

SDK 所需用户信息：由每日互动股份有限公司提供推送技术服务，我们可能会将您的设备平台、设备厂商、设备品牌、设备识别码等设备信息，应用列表信息、网络信息以及位置相关信息提供给每日互动股份有限公司，用于为您提供消息推送技术服务。我们在向您推送消息时，我们可能会授权每日互动股份有限公司进行链路调节，相互促活被关闭的 SDK 推送进程，保障您可以及时接收到我们向您推送的消息。详细内容请访问 [《个推用户隐私政策》](#)

使用目的：获取推送消息。

6.小米·消息推送

公司全称：北京小米移动软件有限公司

SDK 类型：消息推送

SDK 使用目的：Dcloud 集成的手机厂商系统推送。

SDK 使用场景：在小米手机终端推送消息时使用获取关键节点业务的推送消息。

SDK 所需用户信息：如您接入的是安卓版，在您注册使用小米推送服务时，我们会收集您的设备标识 OAID 和加密的 Android ID，以及使用推送服务的应用信息如应用包名、版本号和运行状态；如您接入的

是 iOS 版，我们会收集 IDFA（当收集不到 IDFA 时则不收集）、应用包名、版本号。详细内容请访问[《小米推送隐私政策》](#)

使用目的：获取推送消息。

关联引用 sdk：米聊。

7.OPPO·消息推送

公司全称：广东欢太科技有限公司

SDK 类型：消息推送

SDK 使用目的：Dcloud 集成的手机厂商系统推送。

SDK 使用场景：在 OPPO 手机终端推送消息时使用获取关键节点业务的推送消息。

SDK 所需用户信息：为您提供推送服务，发送关于软件更新或新品发布等通知（包括但不限于我们及相关第三方产品或服务的营销信息），您同意我们暂存从开发者处获取的消息内容，并收集您的设备相关信息（如 IMEI 或 OAID，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）、使用推送服务的应用信息（如 APP 包名及版本号，运行状态）、推送 SDK 版本号、网络相关信息（如 IP 或域名连接结果，当前网络类型）、消息发送结果、通知栏状态（如通知栏权限、用户点击行为），锁屏状态（如是否锁屏，是否允许锁屏通知）。详细内容请访问[《OPPO 推送隐私政策》](#)

使用目的：获取推送消息。

8.华为·消息推送

公司全称：华为技术有限公司

SDK 类型：消息推送

SDK 使用目的：Dcloud 集成的手机厂商系统推送。

SDK 使用场景：华为手机厂商推送获取关键节点业务的推送消息。

SDK 所需用户信息：为了向开发者提供便捷、安全的信息推送服务，确保您可以收到开发者应用的通知消息，SDK 会直接收集开发者应用调用 SDK 接口的信息。处理的个人信息包括应用信息（应用基本信息），设备信息（AAID、设备标识符、设备硬件信息、系统基本信息、系统设置）。以上信息将会通过安全传输通道上传至华为服务器处理。详细内容请访问[《华为推送隐私政策》](#)

使用目的：获取推送消息。

9.腾讯 X5WebView

公司全称：深圳市腾讯计算机系统有限公司

SDK 类型：浏览服务

SDK 使用目的：腾讯浏览服务致力于优化移动端 webview 体验。

SDK 使用场景：兼容各系统 webview 浏览体验。

SDK 所需用户信息：无

使用目的：提升浏览网页体验。

10.博睿性能采集

SDK 类型：工具

SDK 使用目的：提供问题定位，性能监测功能。

SDK 使用场景：应用性能监测，快速发现问题及影响范围。

SDK 所需用户信息：设备 ID、设备品牌、设备型号、设备类型、设备内存、设备储存空间、设备电量、设备出口 IP、设备网络制式

使用目的：提供全业务链的性能监控，方便定位，快速发现性能问题及影响范围，降低故障恢复时间，降低业务损失。

11.腾讯云慧眼人脸核身

公司全称：腾讯云计算（北京）有限责任公司

SDK 类型：工具

SDK 使用目的：腾讯云慧眼人脸核身是一组对用户身份信息真实性进行验证审核的服务套件。

SDK 使用场景：安全认证

SDK 所需用户信息：姓名、身份证、摄像头权限、网络权限、设备信息权限。详细内容请访问[《腾讯云慧眼人脸核身 SDK 隐私保护指引》](#)

使用目的：验证用户身份信息提供安全性。

关联引用 sdk：腾讯图灵盾风险识别 SDK

12.okhttp/retrofit2.0/okio

公司全称：Square

SDK 类型：工具

SDK 使用场景：网络请求

SDK 所需用户信息：无

13.移动安全联盟 SDK(OAID SDK)

SDK 类型：工具

SDK 使用场景：应用性能监测，快速发现问题及影响范围。

SDK 所需用户信息：设备信息、唯一设备识别码式。详细内容请访问[《隐私权政策链接/官网》](#)

使用目的：获取 oaid（用于 MSA 移动安全联盟推送设备 OAID 生成）

关联引用 sdk：Samsung Mobile SDKs

14.ButterKnife

SDK 类型：工具

SDK 使用场景：安卓绑定页面控件。

SDK 所需用户信息：无

官网：[《官网》](#)

15.阿里 fastjson

SDK 类型：工具

SDK 使用场景：JSON 解析。

SDK 所需用户信息：无

官网：[《官网》](#)

16.百度身份识别(OCR)

公司全称：北京百度网讯科技有限公司

SDK 类型：工具

SDK 使用目的：百度提供丰富的 OCR 识别服务，覆盖不同场景下文字识别需求。

SDK 使用场景：证件，银行卡，文字快速识别。

SDK 所需用户信息：身份证信息、银行卡信息、访问相册、打开相机/摄像头、读取/写入外部存储卡

[《隐私权政策链接/官网》](#)

使用目的：通过文字识别，便捷地录入身份证，银行卡号信息。

17.Bugly

公司全称：深圳市腾讯计算机系统有限公司

SDK 类型：工具

SDK 使用目的：将如何处理终端用户的个人信息,“处理”包括收集、存储、使用、加工、传输、提供、公开个人信息等行为。

SDK 使用场景：数据收集

SDK 所需用户信息 android：手机型号、手机品牌、Android 系统版本、厂商系统版本、cpu 架构类型、设备是否 root、磁盘空间占用大小、sdcard 空间占用大小、内存空间占用大小、网络类型、应用当前正在运行的进程名和 PID

SDK 所需用户信息 ios：设备型号、操作系统版本、操作系统内部版本号、wifi 状态、cpu 属性、内存剩余空间、磁盘空间/磁盘剩余空间、运行时手机状态、idfv、是否越狱、地区编码 [隐私权政策链接](#)