

平安人 SDK 隐私政策

概述

本政策仅适用于由平安科技（深圳）有限公司（注册地址：中国广东省深圳市益田路 5033 号 23 楼；联系电话：4001635888；以下简称“我们”或“平安科技”）运营的、专供平安集团及其关联公司的所有员工使用的移动办公应用程序（简称“SDK”），名称为平安人，同时包含该 SDK 的中后台管理系统所提供的平台服务（包括平安人网站、客户端在内的各种服务形态，也包括未来技术发展出现的其他新服务形态）。平安集团及其关联公司使用平安人产品或服务，对正式员工进行人力资源管理及相关活动。

最新版本生效日期：2025 年 5 月 26 日

最近版本更新日期：2025 年 5 月 26 日

如果您有任何疑问、意见或建议，请通过以下联系方式与我们联系：

电子邮件：DEPT_PASJKJHRYGFWYX@PINGAN.COM

电话：4001635888

本政策将帮助您了解以下内容：

[一、 个人信息的收集与使用](#)

[二、 个人信息的共享、转让、公开披露](#)

[三、 个人信息的安全保障](#)

[四、 个人信息的存储期限与地点](#)

[五、 您对个人信息的权利与选择](#)

[六、 未成年人的保护](#)

[七、 隐私政策的更新](#)

[八、 联系我们](#)

[附录 1、平安人设备权限列表](#)

[附录 2、第三方 SDK 列表](#)

[附录 3、个人信息收集清单](#)

[附录 4、相关定义](#)

我们深知个人信息对您的重要性，并会尽全力保护您的个人信息安全可靠。我们致力于维持您对我们的信任，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、最小必要原则、确保安全原则、主体参与原则、公开透明原则。同时，我们承诺，我们将按业界成熟的安全标准，采取相应的安全措施来保护您的个人信息。

请在使用我们的产品或服务前，仔细阅读并了解本《平安人隐私政策》，我们将详细地介绍在人力资源管理中如何收集、存储、使用、保护及对关联方共享您的信息，并说明您享有的权利。

摘要如下：

1. 为了便于您了解您在使用我们的服务时，我们需要收集的信息类型与用途，我们将结合具体服务向您逐一说明。

2. 为了向您提供服务所需，我们会按照合法、正当、必需的原则收集您的信息。我们只会在您使用特定业务功能时，仅收集为了正常运行该业务功能所必需的信息，在您停止该业务功能的使用后，我们将会停止您的个人信息收集的行为。

3. 如果为了向您提供服务而需要将您的信息共享至第三方，我们将评估该第三方收集信息的合法性、正当性、必要性。我们将要求第三方对您的信息采取保护措施并且严格遵守相关法律法规与监管要求。另外，我们会按照法律法规及国家标准的要求以确认协议、具体场景下的文案确认、弹窗提示形式征得您的同意或确认第三方已经征得您的同意。

4. 您可以通过本政策介绍的方式访问和管理您的信息、设置个人信息功能、注销相关阶段的账户或进行投诉举报。

在开始使用我们的产品或服务前，请您务必仔细阅读并充分理解本政策，**特别是以粗体标识的条款**，并决定是否同意我们据此处理您的个人信息。**请您注意，如果您不同意本政策，将会影响您使用我们的产品或服务。在法律允许的情况下，我们可以不基于您的同意而收集、使用您的个人信息。在法律要求的情况下，我们将会就处理个人信息的特定情形征求您的单独同意。**

请您注意，本政策仅适用于平安科技在平安人 SDK 及其他网页或客户端形态中提供的产品或服务（以下简称“平安人”）。对于我们提供的**平安人**之外的任何产品或服务，或对于与**平安人**存在接入、业务合作、广告展示关系的任何第三方的产品或服务，本政策并不适用，**请您阅读相应的产品、服务、及第三方的隐私政策，我们不对第三方的个人信息处理活动承担任何法律责任。**

请您注意，您所受聘或服务的可能为实施人力资源管理而收集、使用、共享或以其他方式处理您的个人信息。平安科技受平安集团及其关联公司的委托，通过**平安人**收集公司员工及相关外部服务人员的个人信息，并对该等个人信息进行存储、使用、共享或其他处理。**请您阅读您所受聘或服务的公司的劳动规章制度，了解公司处理员工个人信息的相关规则。**

如果您对本政策有任何疑问或建议，您可以通过本政策 [“联系我们”](#) 中所提供的方式与我们联系。

一、 个人信息的收集与使用

在您使用我们的产品或服务时，我们可能收集、使用的您的个人信息。

具体而言，我们为您提供如下功能，各个功能涉及的处理目的、个人信息类型（其中的敏感个人信息已加粗显示，请您特别注意）如下所示。

（一） 注册登录

如您为平安员工或实习生，您所服务的公司将自动为您生成员工账号，您可以使用您的员工账号、手机号或个人电子邮箱进行登录。

（二） 重要操作验证

1. 测评与离职办理

您在参加测评、离职办理时，为了保障前述业务的安全性，我们需要加强对您的身份的真实性、有效性的验证，为此您可能需开启您的设备的摄像头权限，向我们提供**脸部图像或视频，如您不同意提供相关个人信息，请勿开启摄像头权限**。如您不提供相关信息，您可能无法使用测评、离职办理相关服务，但不影响您使用我们提供的其他服务。

2. 重要操作行为验证

为了保障您的账户和信息安全，在您进行找回密码、个人薪酬查询、合同签署及变更、办证、离职、团队薪酬功能相关重要操作时，我们需要加强对您的身份的真实性、有效性的验证，为此您可能需向我们提供**指纹、面容 ID 或手势密码的身份认证验证结果，前述身份信息将存储于您用于登录的本地终端（手机），我们仅接收验证结果，并不收集您的指纹信息或面容 ID 信息**；如您不同意提供前述信息，您将无法完成特定操作、使用相应的服务功能，但不影响您使用我们提供的其他服务；

当您在平安人使用**实习生转正、服务、请假、我的档案、薪酬**时，您可以通过**OCR 影像识别、照片上传或手动输入方式**提供办理前述手续所必须的有效信息以供我们核对并留存；如您不提供或不同意我们留存，可能无法使用与证明办理、个人信息修改相关的部分服务。

（三） 用户意见管理

为了保障用户的意见反馈获得更有效处理和解决，以及预防安全风险，我们需要记录您使用的**设备型号、设备软件版本信息、移动电话、固定电话、岗位信息、公司邮箱地址、姓名、员工账号**。如您不同意我们记录前述信息，可能无法更高效处理您的意见反馈。

（四）为保障系统安全所必须的功能。

为提高您使用**平安人**产品和服务时系统的安全性，更准确地预防钓鱼网站欺诈和保护账户安全，我们需要通过了解您的**设备信息、日志信息**来判断您的账号风险。

1. 设备信息

我们会根据您在软件安装及使用中授予的具体权限，自动接收并记录您所使用的**设备相关信息（设备型号、终端制造厂商、操作系统版本、设备设置、IMEI、IMSI、Android ID、MAC 地址、SIM 卡运营商、SIM 卡序列号、时区和软硬件特征信息、WiFi 状态、SSID、BSSID、IDFV，涉及 SDK 的设备信息具体类型详见本政策**平安人第三方 SDK 列表**指引的相应隐私政策）、剪贴板、软件安装列表、设备所在位置相关信息（IP 地址、GPS/北斗位置信息以及能够提供相关信息的 Wi-Fi 接入点、蓝牙和基站传感器信息）**，包括等于后台运行时我们仍存在收集前述设备相关信息的情形以便于您使用移动打卡、消息推送功能及 **SDK** 进行安全风控，如您不提供前述信息，我们将无法为您提供前述服务，但不影响您使用我们提供的其他服务。

在您同意本政策后，我们基于正常数据统计、安全风控、保障软件服务及您的账号安全的目的，通过集成的 **SDK** 收集您的 **MAC 地址、IMEI、Android ID、IMSI** 和应用安装列表。

2. 日志信息

当您使用**平安人**产品或服务时，我们会自动收集您对我们服务的详细使用情况，作为有关网络日志保存。您的**搜索查询记录、浏览记录、IP 地址、浏览器的类型、电信运营商、使用的语言、访问日期和时间、您访问的网页记录、审批日志信息、考勤日志信息、办公信息操作日志信息**。

3. 相册存储空间

您可以开启手机的存储空间权限，用于 **SDK** 运行过程中日志信息、应用缓存的读写，以便您在使用“请假申请、识别二维码、证件夹、人脸采集、个人信息修改”功能时从相册中获取**图片**，如您不提供前述权限，您将无法使用与此权限相关的特定功能，但不影响您使用我们提供的其他服务。

（五）基于位置信息的服务

您可以选择开启手机的定位权限，用于提供您的**位置信息**，以便您基于所在地点位置接受移动打卡、外出签到、打卡地址变更的服务；如您不提供前述权限，我们将无法为您提供前述服务，但不影响您使用我们提供的其他服务。

（六）基于摄像头（相机）和/或相册的服务

您可以选择开启手机的相册权限，用于读取您的相册信息，以便于您在使用“上传照片、更换头像、团队相册、请假申请、识别二维码、**OCR** 识别、证件夹、人脸采集、个人信息修改”功能时从相册中上传**图片**；如您不提供前述权限，我们将无法为您提供前述服务，但不影响您使用我们提供的其他服务。

（七）基于麦克风的服务

您可以选择开启手机的麦克风权限，使用麦克风设备来进行语音输入，在视频面试的使用过程中，我们需要收集您的语音内容并进行必要的处理；如您不提供前述权限，我们将无法为您提供语音相关服务，但不影响您使用我们提供的其他服务。

（八） 基于日历的服务

您可以开启手机的日历权限，用于写入和读取您的日历信息，以便于您使用“移动打卡、异常考勤”功能，如您不提供前述权限，我们将无法为您提供前述服务，但不影响您使用我们提供的其他服务。

（九） 基于电话权限的服务

您可以开启手机的电话权限，以便于您使用“服务”功能模块时可进行电话呼出，如您不提供前述权限，我们将无法为您提供电话呼出的服务，但不影响您使用我们提供的其他服务。

（十）基于在职人员的服务

如果您作为正式员工使用平安人信息修改时，我们将按如下目的、方式去收集您的信息以便更新您的信息。如您不提供相关必需信息，将无法更新个人信息。

信息类型	目的	方式	范围
教育经历	记录您的个人信息，形成个人档案	用户自行输入	必需：毕业院校、地址、专业、入学时间、毕业时间、学位、学历、学习形式、毕业形式、学历证与学位证
工作经历	记录您的个人信息，形成个人档案	用户自行输入	必需：开始时间、结束时间、工作单位、最后职务、工作证明
工资卡	用于工资发放	用户自行输入	必需：开户行 1、分行、卡号
证件信息	归档个人证件	用户自行输入	必需：证件名称、证件附件

（十一） 基于监听应用安装的服务

用于写入和读取您是否存在虚拟定位之类的应用，以便于您使用“移动打卡、异常考勤”功能，如您不提供前述权限，我们将无法为您提供前述服务，但不影响您使用我们提供的其他服务。

（十二） 身份安全核验

我们可能会将您的身份信息与风险名单核对，以履行我们在反洗钱、反恐怖主义、协助通缉调查、监管报送相关方面的法定义务、特殊行业从业人员背景调查等相关方面的法定义务。

（十三） 个人信息使用的规则

1. 我们会根据本政策的约定并为实现我们的产品与/或服务功能对所收集的个人信息进行使用。
2. 请您了解并同意，您在使用我们的产品与/或服务时所提供的所有个人信息，除非您撤回授权拒绝我们收集，否则将在您使用我们的产品与/或服务期间持续授权我们使用。

3. 我们会对我们的产品与/或服务使用情况进行统计，并可能会与公众或第三方共享这些统计信息，以展示我们的产品与/服务的整体使用趋势。但这些统计信息不包含您的任何身份识别信息。

4. 当我们展示您的个人信息时，我们会采用包括内容替换、匿名处理方式对您的信息进行脱敏，以保护您的信息安全。

5. 当我们要将您的个人信息用于本政策未载明的其它用途时，或基于特定目的收集而来的信息用于其他目的时，会实现征求您的明示同意。请您理解，我们向您提供的产品与/或服务将不断更新变化。如果您选择使用本政策中尚未列明的其他产品与/或服务时，我们会在收集您的个人信息前通过协议、页面提示方式向您详细说明信息收集的目的、方式、范围并征求您的同意。若您不同意提供前述信息，您可能无法使用该项产品与/或服务，但不影响您使用现有产品与/或服务。

您可点击查看[平安人设备权限列表](#)，进一步了解各个权限的名称、使用目的、调用情况说明。

（十四）Cookie 和同类技术的使用

1. Cookie 的使用

Cookie 是互联网中普遍使用的技术，在您使用我们的产品或服务时，为优化您的访问体验并保障产品或服务正常高效运转，我们可能会在您的设备上存储一个或多个名为 **Cookie** 的小型文件。我们可能使用 **Cookie** 简化您的登录流程、判断您的使用环境安全状态、帮助您优化对广告的选择与互动、保护您的数据安全。您可以自行管理或删除计算机或移动设备上所储存的 **Cookie**。大多数浏览器会自动接收 **Cookie**，但您通常可以根据自己的需要更改浏览器的 **Cookie** 设置。

2. Proxy 技术的使用

当您通过我们的网站或 **SDK** 使用第三方的服务时，为保障您的账户安全，我们可能会使用专用的网络协议及代理技术（简称“**Proxy** 技术”）。**Proxy** 技术能够帮助您识别我们已知的高风险站点，避免恶意攻击者篡改您和您希望访问的第三方之间的通信内容。在此过程中，我们可能收集、保存您的 **IP** 地址、设备信息以及您所希望访问的页面位置。

（十五）无需您同意的收集、使用、处理

请您注意，根据法律法规的规定，在以下情形中，我们无需取得您的同意即可收集、使用或以其他方式处理您的个人信息：

1. 为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需。
2. 为履行法定职责或者法定义务所必需。
3. 为应对突发公共卫生事件，或者紧急情况下为保护自然人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个人信息。
5. 依照法律规定在合理的范围内处理个人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。

匿名化处理后的信息不再属于个人信息，因此不受本政策的约束和保护。

二、 个人信息的共享、转让、公开披露

我们高度重视保护您的个人信息，仅在取得您的同意或法律法规允许的情况下，才会共享、转让、公开披露您的个人信息。

（一） 共享

1. 与您所就职公司共享

请您理解，**您所就职的公司基于人力管理需要通过平安人对您的员工信息进行管理**，为了向您和您所就职的公司提供员工账户服务，**我们会向您所就职的公司提供您在平安人上的各项个人信息。**

提供您的个人信息系为向您提供员工信息查询、企业员工管理所必需，或是为防范风险、保障安全、实现合规所必要。请您授权我们进行该等共享，否则我们难以为您提供安全的、统一的服务。

2. 与平安集团旗下关联公司共享

为了更好地为您提供产品与服务，履行我们的社会责任与法定义务，同时实现我们的商业价值，**我们将在平安集团内部与关联公司共享您的个人信息。**

关联公司是指中国平安保险（集团）股份有限公司（简称“平安集团”）及其通过股权、协议或其他方式直接或间接控制、共同控制或施加重大影响的公司，或其投资的联营企业、合营企业，详见年报（<http://www.pingan.cn/ir/financial-report.shtml>）。关联公司所涉行业包括：保险、银行、信托、证券、资产管理、财富管理、基金管理、融资租赁、普惠金融、健康医疗、科技业务等。

基本业务功能系为向您提供产品与服务所必需，或是为防范风险、保障安全、实现合规所必要。请您授权我们进行该等共享，否则我们难以为您提供安全的、统一的服务。具体而言，我们的基本业务功能包括：

- 1）人力资源管理：**我们可能使用您在在职、离职各阶段与工作相关的信息，通过系统同步、人工数据采集或数据查看权限申请的方式进行统计，以便实施集团层面的人力资源管理以及相应的数据分析。共享的方式经过严格的业务流程评估和权限管控。
- 2）统一用户服务：**我们可能共享您必要的个人信息，从而为您提供告知、信息查询、投诉、电话热线相关客服功能，妥善处理您的意见与反馈。
- 3）风险防控与安全保障：**我们可能共享您必要的个人信息，实现我们在风险防控、防范欺诈、合规内控相关方面的要求，从而在安全的前提下为您提供产品与服务。
- 4）为您提供产品与服务：**我们可能共享您必要的个人信息，以便联合向您提供您所要求的产品或服务。例如，当您使用工资理财查询的功能时，由业务合作伙伴平安银行股份有限公司提供服务。
- 5）改善产品与提升服务：**为了持续改善您的用户体验，我们可能共享您主动提供、业务中产生、系统自动采集的相关信息，用于相关产品的持续优化与改善。例如，对平安集团旗下员工开展群体分析，作为开发新产品、下架旧产品、调整服务方式的参考。
- 6）员工调研：**我们可能对平安集团旗下的产品或服务、人力资源管理、公司文化建设等内容进行调研并共享相关信息，从而了解您对我们及平安集团的想法与建议。例如，我们可能向您发送调研问卷，邀请您参与反馈。

3. 与第三方合作伙伴共享

为了更好地为您提供产品或服务，我们与第三方合作伙伴进行业务合作，并在实现业务合作的必要合理范围内共享您的个人信息。

1) 供应商和其他合作伙伴：我们将信息委托给我们业务的供应商或其他合作伙伴处理，这些支持包含实施人力资源管理所必须的环节。我们可能共享您必要的个人信息，以便联合向您提供您所要求的产品或服务。当您使用测评、背调功能时，我们可能向委托的供应商同步测评、背调所需的信息。

2) 交易与物流：SDK 中的商品及送货由第三方商家提供，我们可能与相应的供应商共享您的订单信息、姓名、手机号码、收货地址，从而向您提供商品、售后等服务。

3) 广告推送与统计分析：我们可能与广告服务提供商提供您**脱敏后的信息**，以实现广告投放、优化广告体验、分析广告投放有效性，请您理解，**相关信息仅会用于广告统计处理**。

4) 保障运行安全：我们可能与安全服务提供商共享您的设备信息、网络信息、**日志信息**，以综合判断您的账号风险、预防安全事件、保障我们产品或服务的安全运行。

5) 统计、优化服务：我们可能与运营服务提供商共享您的设备信息、**日志信息**、网络信息，以快速发现并解决异常、分析故障的产生原因、改善产品或服务的使用体验、掌握产品运营动态、及时跟进用户反馈。

4. 通过 SDK 共享

为了更好地向您提供产品与服务，我们会通过软件开发工具包（SDK）、应用程序接口（API）的方式进行必要的数据共享。我们会对接入的 SDK、API 进行安全监测，并要求其采取数据保护措施。

您可点击查看[平安人第三方 SDK 列表](#)，进一步了解 SDK 的名称、运营方、使用目的、个人信息使用的具体情况。

（二）转让

如果我们因合并、分立、解散、被宣告破产等原因需要转移您的个人信息，我们会向您告知接收方的名称或者姓名和联系方式，并要求接收方**继续受本政策的约束**。接受方如果变更原先的处理目的、处理方式，将依法重新征求您的同意，除非法律法规另有规定。在破产清算且无接收方的情形下，我们将删除您的个人信息，除非法律法规另有规定。

（三）公开披露

我们一般不会公开披露您的信息，除非取得您的单独同意，或依据法律法规的相关要求。

请注意，您在使用我们的产品或服务的过程中可能会自行公开的一些信息，其中可能涉及您的个人信息甚至敏感个人信息，请您谨慎考虑是否公开上述信息。如果涉及他人的个人信息，您可能需要征得他人的同意（如适用）。

（四）无需您同意的共享、转让、公开披露

请您注意，根据法律法规的规定，在以下情形中，我们无需取得您的同意即可共享、转让、公开披露您的个人信息：

1. 为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需。
2. 为履行法定职责或者法定义务所必需。

3. 为应对突发公共卫生事件，或者紧急情况下为保护自然人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个人信息。
5. 依照法律规定在合理的范围内处理个人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。

匿名化处理后的信息不再属于个人信息，因此不受本政策的约束和保护。

三、 个人信息的安全保障

我们高度重视您的个人信息安全，并采取符合法律法规、业界标准、合理可行的各类安全措施，保护您的个人信息，防止发生个人信息的泄露、损毁、丢失、篡改等安全事件。

1. **管理措施：**我们建立了个人信息安全相关的公司制度、组织机构与管理人员。我们严格限制有权访问个人信息的人员范围，要求他们遵守保密义务。我们还会举办个人信息保护与安全的培训课程，加强员工对个人信息保护的意识与能力。
2. **技术措施：**我们会使用加密技术提高个人信息的安全性，您的 **SDK** 与服务器之间的数据交换可能受 **SSL** 协议加密保护。我们使用受信赖的保护机制防止个人信息遭到恶意攻击。为了保障您的聊天信息安全，我们对消息采用端到端加密技术，数据从源点到终点的传输过程中始终以密文形式存在，在整个系统中，只有参与通信的双方用户可以读取数据，第三方无法获取，保证信息安全。为进一步加强信息安全，我们还设置了消息定期销毁机制，本地及服务端均不留存。我们还为内外网之间的数据传输建立了 **VPN**、**https** 请求安全传输通道，极大地保障了您的通信数据安全。
3. **安全事件应对：**我们制定了个人信息安全事件应急预案，并注意风险的监测与预防。若不幸发生或可能发生个人信息泄露、篡改、丢失等安全事件，我们会立即启动应急预案、采取补救措施，尽力降低安全事件的影响。我们将通过邮件、推送、公告等合理、有效的方式，依法告知您安全事件的原因、危害、个人信息的类型、补救措施等事项。我们还将依法向有关监管机构上报安全事件的相关情况。
4. **请您共同防范安全风险：**我们将尽力确保您在使用我们的产品或服务过程中的信息安全，但请您理解，互联网环境并非绝对安全的环境。请您妥善保管您的账号及密码，并尽量使用复杂密码，共同维护您的账户及个人信息的安全。

目前，我们在信息安全方面已经达到了 **ISO27001** 国际信息安全管理体系标准，并已获得认证。

四、 个人信息的存储期限与地点

（一） 存储期限

一般而言，我们只会在实现处理目的所必需的期限内保留您的个人信息，除非法律法规另有规定。我们判断个人信息的存储期限主要依据以下标准，

1. 您在履行劳动合同、参与公司人力资源管理活动时提供的个人信息：我们将保存您的个人信息直至您离职后的合理期限。
 - 我们将在短期内尽快清理您的个人生物识别信息。
 - 我们将较长时间内保留您的个人信息，包含且不限于：基础个人信息、任职记录、个人绩效数据、考勤、培训、薪酬、权限记录、劳动合同及相关协议信息。用于人力资源管理需要，如员工用工信息溯源查询、用工档案存档、相关诉讼举证等。

- 我们将长期保留您的个人信息，包含且不限于：基础个人信息、任职记录、薪酬、劳动合同及相关协议等信息，或相关重要岗位人员的信息。主要出于企业合规运营和履行企业合规义务，如在相关监管要求下履行监管义务进行员工信息定期报送、配合社保稽查或税务稽查等需要。

2. 对于您创建的信息：我们将保存您创建的个人信息，直至您离职后的合理期限。您在公共平台的发帖、留言等信息不属于个人信息，不在本政策范围内约定。

3 对于您报名参与的活动：我们将保存与活动相关的个人信息至活动结束后的合理期限。

4. 在法律另有规定的情况下，员工信息的保留期限将遵守其特别规定，我们有必要以符合法律法规的方式进行员工个人信息存储。或者我们和您另有约定，则以该等规定或约定的存储期限为准。

在超出存储期限后，我们会依法删除或匿名化处理您的个人信息。如果删除从技术上难以实现的，我们会停止除存储和采取必要的安全保护措施之外的处理活动。

如我们停止运营**平安人**，我们将提前 **30** 天通知您，停止相关的个人信息收集活动，并在合理的期限内删除或匿名化处理您的个人信息。

如果您想了解我们存储的具体信息，或对部分信息有疑问，您可以通过本政策的 [“联系我们”](#) 提出您的问题和要求，我们将协助解答。

（二） 存储地点

我们将在中华人民共和国（简称“中国”）境内收集和产生的个人信息存储在中国境内。

如果今后涉及个人信息的出境（存储地点从中国境内转移到中国境外），届时我们将严格依照法律法规的规定，落实个人信息出境的要求与条件。

五、 您对个人信息的权利

您对您的个人信息依法享有如下的权利与选择，我们充分尊重您对个人信息的权利和选择，并保障该等权利的行使。

（一） 知情、决定

您对我们如何处理您的个人信息享有知情权、决定权，您可以限制、拒绝我们处理您的个人信息，除非法律法规另有规定。

我们特此制定本政策，向您介绍我们的个人信息处理规则。在开始使用我们的产品或服务前，请您务必仔细阅读并充分理解本政策，**特别是以粗体标识的条款**，并决定是否同意我们据此处理您的个人信息。**请您注意，如果您不同意本政策，将会影响您使用我们的产品或服务。在法律允许的情况下，我们可以不基于您的同意而收集、使用您的个人信息。在法律要求的情况下，我们将会就处理个人信息的特定情形征求您的单独同意。**

如果您对我们的个人信息处理规则或本政策有任何疑问，可以通过本政策 [“联系我们”](#) 中所提供的方式请求我们进行**解释说明**。

（二） 查阅

您有权查阅您的个人信息，请通过以下方式行使：

1. 您在职期间，登录**平安人 SDK** 查阅您的部分个人信息，操作路径为：“我的”-“我的档案”-“我的画像”-“个人信息”“职务信息”“工作经历”“教育信息”“综合绩效”“奖惩信息”“劳动合同”。

2. 通过本政策“[联系我们](#)”中所提供的方式向我们提出请求，查阅您的其他个人信息。

（三） 更正、补充

如果您发现您的个人信息不准确或不完整，您有权更正、补充您的个人信息，请通过以下方式行使：

1. 通过平安人更正、补充您的部分个人信息，该等修改将在 24 小时内同步更新至平安人 。
2. 通过本政策“[联系我们](#)”中所提供的方式向我们提出请求，更正、补充您的其他个人信息。

（四） 复制、转移

您有权复制我们所存储的您的个人信息，请通过本政策“[联系我们](#)”中所提供的方式向我们提出请求。

在符合法律法规的条件下，您还可以请求我们将您的个人信息转移至您指定的个人信息处理者，我们会依法为您提供转移的路径，请通过本政策“[联系我们](#)”中所提供的方式向我们提出请求。

（五） 约束自动化决策

自动化决策是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。对于自动化决策，我们将保证决策的透明度和结果的公平、公正。通过自动化决策方式的信息推送、商业营销，我们将同时提供不针对您个人特征的选项，或向您提供便捷的拒绝方式。通过自动化决策方式作出对您个人权益有重大影响的决定，您有权要求我们予以说明，并有权拒绝我们仅通过自动化决策的方式作出决定。

（六） 改变授权范围

您可以改变或者撤回您授权我们收集、处理您的个人信息的范围。

您使用平安人参与公司内部人力资源管理时，您授权并提供的个人数据服务于正常的人力资源管理活动。您在撤回授权之前提供的人力资源管理所需要的数据，平安人会继续保留以便您重新进行授权时直接使用。该部分数据如果删除，将可能影响正常合同履行期间和个人信息有关的工作活动，也可能影响个人和公司进行正常的合同履行。

改变或撤回授权，请通过以下方式行使：

1. 通过您手机或其他设备的系统权限管理页面，修改与 SDK 相关的设备权限。撤销路径：我的-》设置-》隐私政策-》撤回
2. 通过本政策“[联系我们](#)”中所提供的方式向我们提出变更请求。请您注意，当您执行上述操作后，我们将无法继续为您提供与授权所对应的服务，但这不会影响此前基于您的授权而进行的个人信息处理活动。

（七） 删除

您有权请求我们删除您的个人信息，请通过以下方式行使：

1. 通过本政策“[联系我们](#)”中所提供的方式向我们提出请求，删除您的个人信息；
2. 申请注销账户，从而删除您的个人信息。

请您注意，删除权的行使并非绝对的，仅在法定情形下，您有权请求我们删除您的个人信息。此外，出于保存期限的法定要求或技术上的限制，我们可能难以删除您的个人信息，但我们会停止除存储和采取必要的安全保护措施之外的处理活动。

请您注意，您选择删除个人信息或注销账号后，我们可能将无法再为您提供简历查询、工作证明查阅及其他与您个人信息相关的服务。

（八） 注销账户

您入职后正式员工账号开始生效，同时用于登录平安人，在您离职后，系统将自动锁定您的登录账号。后续该账号无法再进行登录，也不会被其他用户使用。该账号有效期间关联的您的个人数据，我们会严格保密，并在合理期限内对您的个人信息进行删除处理（除非法律法规另有规定）。在账号锁定之后，我们将停止为您提供平安人产品和服务。关于账号锁定后，个人信息处理方式可参考本政策[存储期限](#)内容。

（九） 已故用户的个人信息保护

如果我们的用户不幸逝世，您作为近亲属，为了自身的合法、正当利益，您可以依法对逝者的相关个人信息行使查阅、复制、更正、删除等权利，除非逝者生前另有安排。请通过本政策[“联系我们”](#)中所提供的方式向我们提出请求。为了保护逝者的个人信息，我们需要您协助提交相应的证明文件。

（十） 响应您的请求

我们充分尊重您的个人信息权利，并全力响应您的行权请求。

请您注意，对于您的合理请求，我们原则上不收取费用。对于多次、重复、超出合理限度的请求，我们可能酌情收取一定费用。如果您的请求包含不属于您的个人信息、超出合理限度、需要过多技术手段（如需要开发新系统或从根本上改变现行惯例）、可能侵害他人合法权益、不切实际，或者我们存在合法、正当的其他理由，我们可能拒绝响应您的请求，并向您说明理由。

我们将尽快处理您的请求，并在验证您的身份后的 15 个工作日内予以回复。

如果您对我们的回复不满意，特别是您认为我们的个人信息处理活动损害了您的合法权益，您可以依法向监管机构投诉或向法院提起诉讼。

六、 未成年人的保护

平安人主要面向成年人。我们高度重视对未成年人个人信息的保护。如果您为 14 周岁以下的未成年人，请勿使用平安人，如您发现我们收集了不满 14 周岁的未成年人的个人信息，请您与我们联系，我们将在获悉后及时删除相关信息。若您未成年人的监护人，当您对您所监护的未成年人的个人信息有相关疑问时，请通过本政策的[“联系我们”](#)协助解答您的疑问、解决您的问题。

七、 隐私政策的更新

随着我们的业务、产品与服务的完善与变化，本政策也可能随之变更。我们将在 SDK 中发布本政策的更新版本，**对于本政策的重大变更，我们将会以更显著的方式通知您**，例如，弹窗、推送、公告、邮件、或其他符合法律要求的适当形式。**未经您的知情和同意（如适用），我们不会削减您按照本政策所享有的权利。**

本政策所指的重大变更包括但不限于：

1. 我们的业务、产品或服务的模式发生重大变化，影响到个人信息的处理目的、处理方式、处理的个人信息种类。
2. 我们在所有权结构、组织架构等方面发生重大变化，导致处理个人信息的主体发生变化。

3. 个人信息共享、转让、公开披露的主要对象发生变化。

4. 您行使个人信息权利的方式和程序发生重大变化。

5. 我们的个人信息保护团队、个人信息保护负责人的联系方式发生变化。

6. 我们的个人信息保护影响评估提示存在高风险。

7. 其他可能对您的人格权益有重大影响的情形。

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，如您对本隐私政策或您的个人信息的相关事宜或投诉、举报、有任何问题、意见或建议，您可以通过以下方式与我们联系：

1. 您可以发邮件至【DEPT_PASJKJHRYGFWYX@PINGAN.COM】

2. 您可以拨打电话【4001635888】

3. 我们的注册地址：广东省深圳市福田区益田路 5033 号平安金融中心 23 楼

4. 我们的办公地址：深圳市福田区平安金融中心

一般情况下，我们会在收到您消息后 15 个工作日回复。

附录 1、平安人设备权限列表

您可查看平安人设备权限列表，进一步了解各个权限的名称、使用目的、调用情况说明。

1. iOS 系统

设备权限	使用目的	是否询问	可否关闭
定位	移动考勤（招聘服务不涉及）	是	是
设备 IDFA	移动考勤（招聘服务不涉及）、推送	是	是
麦克风	语音录入、视频面试	是	是

摄像头	拍照、视频面试、扫一扫	是	是
日历	考勤异常统计（招聘服务不涉及）	是	是
安装应用	SDK 升级	是	是
通知栏提醒	消息推送提醒	是	是
相册	写入和读取用户相册信息	是	是
电话	快捷拨号（招聘服务不涉及）	是	是
流量	获取隐私政策内容	否	是
NSUserTrackingUsageDescription	方便您使用平安消息推送	是	是
NSRemindersUsageDescription	打卡提醒功能	是	是
NSFaceIDUsageDescription	方便您面容识别打开薪酬等二次校验密码的页面	是	是

2. Android 系统

设备权限	使用目的	是否询问	可否关闭
定位	移动考勤（招聘服务不涉及）	是	是
设备 IMEI	移动考勤（招聘服务不涉及）、推送	是	是
麦克风	语音录入、视频面试	是	是
摄像头	拍照、视频面试、扫一扫	是	是

日历	考勤异常统计（招聘服务不涉及）	是	是
安装应用	SDK 升级	是	是
通知栏提醒	消息推送提醒	是	是
相册	写入和读取用户相册信息	是	是
显示在其他应用的上层	应用悬浮窗	是	是
悬浮窗	应用悬浮窗	是	是
电话	快捷拨号、登录/消息推送/移动打卡时获取设备信息	是	是
GET TASKS	用于判断应用是否在后台，便于后台节电优化	否	否
蓝牙设备	获取设备蓝牙标识，便于提供更准确的统计分析服务	是	是
读取手机状态和身份	记录“网络状态”，便于判断出现打卡失败情况时排查异常问题	是	是

附录 2、平安人第三方 SDK 列表

为向您提供更好的服务体验，我们会接入第三方提供的软件工具开发包（即 SDK）。在接入前，为保障您个人数据的安全，我们会对合作伙伴提供的 SDK 进行严格的安全检测。

随着产品功能的更新迭代，我们可能会对接入的第三方 SDK 进行调整，并及时在本列表中向您公开接入的最新情况。此外，第三方 SDK 可能会因为版本升级、策略调整等原因导致获取的数据类型存在变化，请以其公示的官方说明为准。

目前平安人接入并涉及个人数据处理的第三方 SDK 如下：

1.第三方 SDK 名称：OCR（文字识别），含 IDCardOCR、paBankCardSDK

- 业务场景（收集目的）：身份证、银行卡识别，用于实习生转正、服务、请假、我的档案
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**摄像头信息**
- 收集方式：SDK 获取
- SDK 供应商：平安科技（深圳）有限公司
- 官网链接：<https://tech.pingan.com>

• 隐私政策链接：暂无

2.第三方 SDK 名称：社交云直播，含 PALive、HappyDNS

- 业务场景（收集目的）：面试（音视频通话）
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**终端设备信息（包括设备摄像头、麦克风、网络、蓝牙、动态加载 SO 文件、闪光灯权限）以及获取您的网络信息（WIFI/4G/5G）、设备型号、iOS 系统版本、流量类型、时区**

- 收集方式：SDK 获取
- SDK 供应商：平安科技（深圳）有限公司
- 官网链接：<https://tech.pingan.com>
- 隐私政策链接：暂无

3.第三方 SDK 名称：看云

- 业务场景（收集目的）：应用性能监控
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**唯一设备识别码（IMEI、Android ID）、硬件序列号、手机型号、系统类型、系统版本、网络类型、**

设备信息

- 收集方式：SDK 获取
- SDK 供应商：平安科技（深圳）有限公司
- 官网链接：<https://tech.pingan.com>
- 隐私政策链接：<https://wizard.paic.com.cn/portal-docs#/post/38109908>

4.第三方 SDK 名称：人脸识别

- 业务场景（收集目的）：生物特征识别
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**唯一设备识别码（IMEI、Android ID）、SIM 卡 IMSI 信息、摄像头信息**

- 收集方式：SDK 获取
- SDK 供应商：平安科技（深圳）有限公司
- 官网链接：<https://tech.pingan.com>
- 隐私政策链接：暂无

5.第三方 SDK 名称：平安推送 PAPush

- 业务场景（收集目的）：推送服务
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**设备标识 OAID 和加密的 Android ID、IMEI、IDFA、IDFV，应用包名、版本号、运行状态、设备厂商、设备型号、设备内存、操作系统版本、平安推送 SDK 版本、设备归属地（国家或地区）、SIM 卡运营商名称、当前网络类型。收集通知栏设置信息、设备厂商、设备型号、设备内存、操作系统版本、平安推送 SDK 版本、设备归属地（国家或地区）、SIM 卡运营商名称、当前网络类型、获取应用列表信息**

- 收集方式：SDK 获取
- SDK 供应商：平安科技（深圳）有限公司
- 官网链接：<https://tech.pingan.com>
- 隐私政策链接：<http://td-bmms.pingan.com.cn/td-bmms/privacyAgreement.html>

6.第三方 SDK 名称：天眼

- 业务场景（收集目的）：应用统计分析
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**应用版本名、版本号、设备型号、操作系统 sdk 版本、cpu 型号、国家、运营商、语言、时区、手机操作系统版本、是否有网络连接、网络类型、设备操作系统、cpu 个数及频率、总内存、空闲内存、显示屏宽度、显示屏高度、显示屏密度、设备显示信息、设备位置信息、广告 ID（安卓系统为 OAID，苹果系统为 IDFA）、获取 AndroidID 信息、查询媒体库信息（图片）**

- 收集方式：SDK 获取
- SDK 供应商：平安科技（深圳）有限公司
- 官网链接：<https://tech.pingan.com>
- 隐私政策链接：<https://eits-web.paic.com.cn/Sdk#quickstart>

7.第三方 SDK 名称：Sparta

- 业务场景（收集目的）：设备安全标识

- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：

Android: Android 设备串号、经纬度信息、网络类型、基站定位、移动国家码、移动网络号、SIM 卡串号、IMSI、IMEI、手机 MAC 地址、手机蓝牙地址、存储总空间（Internal）、存储剩余空间（Internal）、网络代理信息、卡 2 的 IMESI、卡 2 的 SIM 串号、卡 2 的手机号码、扫描到的 Wi-Fi 列表、传感器、ICCID、IP、SSID、BSSID、运营商；

iOS: 经纬度信息、连接 Wi-Fi 的名称、连接的 Wi-Fi MAC 地址、是否安装了阿里小号、是否安装了 v8 插件

- 收集方式：SDK 获取
- SDK 供应商：平安科技（深圳）有限公司
- 官网链接：<https://tech.pingan.com>
- 隐私政策链接：http://isec.paic.com.cn/homePage/documentDetails/KNK7YHAB37tidkR2Hdl_?type_id=f&title_id=b

8.第三方 SDK 名称：平安语音识别

- 业务场景（收集目的）：面试语音输入
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**网络状态、麦克风录音权限、手机外部存储；查看 WLAN 连接；获取粗略位置；获取精确位置；读取手机状态和身份；检索正在运行的应用**

- 收集方式：SDK 获取
- SDK 供应商：平安科技（深圳）有限公司
- 官网链接：<https://tech.pingan.com>
- 隐私政策链接：暂无

9.第三方 SDK 名称：微博分享

- 业务场景（收集目的）：微博分享
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**硬件序列号、设备 Mac 地址、软件列表、唯一设备标识码（IMEI、Android ID）、SIM 卡 IMSI 信息**

- 收集方式：SDK 获取
- SDK 供应商：北京微梦创科网络技术有限公司
- 官网链接：www.sina.com.cn
- 隐私政策链接：<https://m.weibo.cn/c/privacy>

10.第三方 SDK 名称：微信分享

- 业务场景（收集目的）：微信分享
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**设备信息、应用安装列表**
- 收集方式：SDK 获取
- SDK 供应商：深圳市腾讯计算机系统有限公司
- 官网链接：<https://weixin.qq.com>
- 隐私政策链接：https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy

11.第三方 SDK 名称：QQ 分享

- 业务场景（收集目的）：基于位置的服务，实现定位功能
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**唯一设备识别码（IMEI、Android ID）、设备屏幕信息、网络信息、设备品牌及型号、系统版本**
- 收集方式：SDK 获取
- SDK 供应商：深圳市腾讯计算机系统有限公司
- 官网链接：<https://docs.qq.com>
- 隐私政策链接：<https://docs.qq.com/doc/DQVFLeGd4Ym1oTm5P?pub=1&dver=2.1.27013722>

12.第三方 SDK 名称：百度定位

- 业务场景（收集目的）：考勤打卡定位，天气定位
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**唯一设备识别码（Android ID）、设备 Mac 地址、软件列表、经纬度信息、传感器、BSSID、读写文件**

文件

- 收集方式：SDK 获取
- SDK 供应商：百度在线网络技术公司
- 官网链接：<https://map.baidu.com>
- 隐私政策链接：<https://map.baidu.com/zt/client/privacy/index.html>

13.第三方 SDK 名称：腾讯 Bugly

- 业务场景（收集目的）：异常上报，监测 SDK 异常卡顿闪退信息，获取 IMSI 信息
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**唯一设备识别码（IMEI、Android ID）、设备屏幕信息、网络信息、设备品牌及型号、系统版本、ICCID 、**

MAC

- 收集方式：SDK 获取
- SDK 供应商：深圳市腾讯计算机系统有限公司
- 官网链接：<https://bugly.qq.com/v2/>
- 隐私政策链接：<https://privacy.qq.com/document/preview/fc748b3d96224fdb825ea79e132c1a56>

14.第三方 SDK 名称：腾讯灯塔

- 业务场景（收集目的）：数据上报服务
- 应用客户端：Android
- SDK 收集的信息或申请的权限：**SDK 或 API 版本、平台、时间戳、应用标识符、应用程序版本、终端制造厂商、终端设备操作系统版本、当地语言、时区、网络状态、网络日志信息，以及使用灯塔 SDK 服务的频率、崩溃数据及使用情况、IP 地址**

- 收集方式：SDK 获取
- SDK 供应商：深圳市腾讯计算机系统有限公司
- 官网链接：<https://beacom.qq.com>
- 隐私政策链接：<https://privacy.qq.com/document/preview/a19a8cf4f2354306b137a7db39d32024>

15.第三方 SDK 名称：Zxing

- 业务场景（收集目的）：扫一扫
- 应用客户端：Android
- SDK 收集的信息或申请的权限：**摄像头信息**
- 收集方式：SDK 获取
- SDK 供应商：zxing
- 官网链接：（github 链接见下）
- 隐私政策链接：<https://github.com/zxing/zxing>

16.第三方 SDK 名称：AndPermission

- 业务场景（收集目的）：权限申请组件
- 应用客户端：Android
- SDK 收集的信息或申请的权限：**获取粗略位置；获取精确位置；摄像头；读取通话记录；读取联系人；读取外置存储卡；读取手机状态和身份；读取短信；录音；拨打/接听 SIP 电话；新建/修改/删除通话记录；写入外部存储卡；添加语音邮件；获取 IMEI 信息**
- 收集方式：SDK 获取
- SDK 供应商：yanzhenjie
- 官网链接：（github 链接见下）
- 隐私政策链接：<https://github.com/yanzhenjie/AndPermission>

17.第三方 SDK 名称：Glide

- 业务场景（收集目的）：图片加载和缓存
- 应用客户端：Android
- SDK 收集的信息或申请的权限：**网络、设备分辨率；读取外置存储卡；写入外部存储卡**
- 收集方式：SDK 获取
- SDK 供应商：bumptech
- 官网链接：（github 链接见下）
- 隐私政策链接：<https://github.com/bumptech/glide>

18.第三方 SDK 名称：LzyImagepicker

- 业务场景（收集目的）：选择图片
- 应用客户端：Android
- SDK 收集的信息或申请的权限：**读取外置存储卡；写入外部存储卡**
- 收集方式：SDK 获取
- SDK 供应商：bumptech
- 官网链接：（github 链接见下）
- 隐私政策链接：<https://github.com/yechaoa/UploadImage>

19.第三方 SDK 名称：Lottie

- 业务场景（收集目的）：动画组件
- 应用客户端：Android
- SDK 收集的信息或申请的权限：**设备型号、读取外置存储卡；写入外部存储卡**
- 收集方式：SDK 获取
- SDK 供应商：爱彼迎
- 官网链接：（github 链接见下）
- 隐私政策链接：<https://github.com/airbnb/lottie-android>

20.第三方 SDK 名称：七牛 SDK

- 业务场景（收集目的）：我的公益
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**读取文件、写入文件**
- 收集方式：SDK 获取
- SDK 供应商：上海七牛信息技术有限公司
- 官网链接：无
- 隐私政策链接：无

21.第三方 SDK 名称：深圳众海城 SDK

- 业务场景（收集目的）：我的公益
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：无
- 收集方式：SDK 获取
- SDK 供应商：深圳众海诚信息咨询有限公司
- 官网链接：无
- 隐私政策链接：无

22.第三方 SDK 名称：腾讯 tbs SDK（腾讯浏览服务）

- 业务场景（收集目的）：我的档案页面进行 html 页面访问，进行页面状态上传，以提供更好的网页访问体验
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**设备 id、网络状态、页面异常、写入文件**

- 收集方式：SDK 获取
- SDK 供应商：深圳市腾讯计算机系统有限公司
- 官网链接：<https://www.tencent.com/>
- 隐私政策链接：<https://x5.tencent.com/tbs/guide/develop.html>

23.第三方 SDK 名称：百度统计 SDK

- 业务场景（收集目的）：平安大学
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**获取运行列表、读取/写入外部存储卡、查看 WLAN 链接、读取手机状态和身份、使用蓝牙、广告标**

识符 IDFA

- 收集方式：SDK 获取
- SDK 供应商：百度在线网络技术公司
- 官网链接：<https://tongji.baidu.com/web/help/article?id=330&type=0>
- 隐私政策链接：无

24.第三方 SDK 名称：知鸟 SDK

- 业务场景（收集目的）：平安大学
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**软件列表、唯一设备识别码、设备信息、手机外部存储、蓝牙信息、地理位置**
- 收集方式：SDK 获取
- SDK 供应商：平安国际智慧城市科技股份有限公司
- 官网链接：无
- 隐私政策链接：无

25.第三方 SDK 名称：chromium

- 业务场景（收集目的）：用于收集设备、网络信息，用于埋点上报用户状态，进行数据
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**ssid、监听剪切板、获取传感器**
- 收集方式：SDK 获取
- SDK 供应商：谷歌开源 SDK
- 官网链接：<https://policies.google.com/privacy>
- 隐私政策链接：无

26.第三方 SDK 名称：com.paic.com.cn

- 业务场景（收集目的）：语音转文字
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**麦克风**
- 收集方式：SDK 获取
- SDK 供应商：平安科技（深圳）有限公司
- 官网链接：<https://policies.google.com/privacy>
- 隐私政策链接：暂无

27.第三方 SDK 名称：腾讯云通信 IM

- 业务场景（收集目的）：连网优化，离线推送和 SDK 内部逻辑优化
- 应用客户端：iOS、Android
- SDK 收集的信息或申请的权限：**网络连接状态,设备型号,系统版本**
- 收集方式：SDK 获取
- SDK 供应商：深圳市腾讯计算机系统有限公司
- 官网链接：<https://cloud.tencent.com>

- 隐私政策链接: <https://cloud.tencent.com/document/product/269/58094>

28.第三方 SDK 名称: Vivo 推送

- 业务场景（收集目的）: Vivo 推送 SDK 主要用于推送消息和通知服务。
- 应用客户端: 暂未提供明确的应用客户端信息。
- SDK 收集的信息或申请的权限: **根据提供的隐私政策, Vivo 推送 SDK 可能收集设备及应用信息, 包括操作系统版本号、应用程序信息（包括应用安装列表）、设备标识符（如 IMEI、ICCID、EMMCID/UFSID、oaid/vaid/aaid、SN 码、IMSI、android id、移动国家码和 vivo Android 设备的移动网号等）、MAC 地址、移动运营商、使用语言、系统设置等系统、设备和应用程序数据, 以及日志信息, 包括登录日志、网络请求、访问时间、访问次数、访问 IP、应用操作信息（包括下载、安装、切换、更新、卸载）、错误崩溃等信息。**
- 收集方式: SDK 获取
- SDK 供应商: 暂未提供明确的 SDK 供应商信息。
- 官网链接: <https://www.vivo.com.cn>
- 隐私政策链接: <https://www.vivo.com.cn/about-vivo/privacy-policy>

29.第三方 SDK 名称: 科大讯飞 SDK

- 业务场景（收集目的）: 语音输入、用户将语音信息转换为文字
- 应用客户端: iOS、Android
- SDK 收集的信息或申请的权限: **语音信息、IMEI、IMSI、IP 地址、Android ID、DEVICEID、中国移动 UAID、OAID、文本信息、日志信息**
- 收集方式: SDK 获取
- SDK 供应商: 科大讯飞股份有限公司
- 官网链接: <https://www.xfyun.cn>
- 隐私政策链接: https://www.xfyun.cn/doc/asr/lfasr/lfasr_sdkprivacy.html

30.第三方 SDK 名称: 腾讯地图 SDK

- 业务场景（收集目的）: 地图展示
- 应用客户端: iOS、Android
- SDK 收集的信息或申请的权限: **网络类型、手机终端标识信息（IMEI）、设备设备型号、设备传感器信息、手机屏幕密度、尺寸、操作系统及版本、OAID、IP 地址申请设备权限: 网络权限、存储权限**
- 收集方式: SDK 获取
- SDK 供应商: 深圳市腾讯计算机系统有限公司
- 官网链接: <https://privacy.qq.com>
- 隐私政策链接: <https://privacy.qq.com/document/preview/dbd484ce652c486cb6d7e43ef12cefb0>

31.第三方 SDK 名称: 移动解析 HTTPDNS SDK

- 业务场景（收集目的）: 用于移动互联网服务中域名解析
- 应用客户端: iOS、Android
- SDK 收集的信息或申请的权限: **网络状态信息、设备信息（IMEI）**
- 收集方式: SDK 获取
- SDK 供应商: 深圳市腾讯计算机系统有限公司
- 官网链接: <https://cloud.tencent.com>
- 隐私政策链接: <https://cloud.tencent.com/document/product/379>

32.第三方 SDK 名称: 小米推送 SDK

- 业务场景（收集目的）: 用于实现对小米品牌的手机进行消息推送
- 应用客户端: iOS、Android
- SDK 收集的信息或申请的权限: **设备标识符**
- 收集方式: SDK 获取
- SDK 供应商: 小米科技有限责任公司

- 官网链接: <https://dev.mi.com>
- 隐私政策链接: <https://dev.mi.com/console/doc/detail?pId=1822>

33.第三方 SDK 名称: 即构语音 SDK

- 业务场景 (收集目的): 提供音频服务, 帮助用户语音互动聊天
- 应用客户端: iOS、Android
- SDK 收集的信息或申请的权限: **网络访问, 读取网络状态, 获取 WIFI 状态、录音、更改声音设置, 读取电话状态, 蓝牙、写入外部**

存储、相机

- 收集方式: SDK 获取
- SDK 供应商: 深圳市即构科技有限公司
- 官网链接: <https://www.zego.im>
- 隐私政策链接: <https://www.zego.im/privacy>

34.第三方 SDK 名称: Okhttp3(okhttp3)

- 业务场景 (收集目的): 网络请求
- 应用客户端: iOS、Android
- SDK 收集的信息或申请的权限: **写入文件、创建文件夹、获取 IP 地址、获取 IMSI 信息**
- 收集方式: SDK 获取
- SDK 供应商: Square
- 官网链接: <https://square.github.io>
- 隐私政策链接: 暂无

35.第三方 SDK 名称: 阿里 ARouter

- 业务场景 (收集目的): ARouter 是阿里巴巴开源的 Android 平台中对页面、服务提供路由功能的中间件, 提倡的是简单且够用。
- 应用客户端: Android
- SDK 收集的信息或申请的权限: 无
- 收集方式: SDK 获取
- SDK 供应商: 阿里巴巴集团
- 官网链接: (github 链接见下)
- 隐私政策链接: <https://github.com/alibaba/ARouter>

36.第三方 SDK 名称: OPPO 推送

- 业务场景 (收集目的): OPPO PUSH 是 ColorOS 上的系统级通道, 为开发者提供稳定, 高效的消息推送服务。
- 应用客户端: Android
- SDK 收集的信息或申请的权限: 无
- 收集方式: SDK 获取
- SDK 供应商: 广东欢太科技有限公司
- 官网链接: <https://open.oppomobile.com>
- 隐私政策链接: <https://open.oppomobile.com/new/developmentDoc/info?id=11221>

37.第三方 SDK 名称: AskBob 3.0, 含天眼、闻舒

- 业务场景 (收集目的): 智能问答、语音搜索
- 应用客户端: iOS、Android
- SDK 收集的信息或权限: **麦克风权限、存储权限、网络和网络状态权限、定位权限**
- 收集方式: SDK 获取
- SDK 供应商: 平安科技 (深圳) 有限公司
- 官网链接: 无
- 隐私政策链接: 无

第三方 SDK 名称: ButterKnife

- 业务场景（收集目的）：用于简化 Android 视图的绑定操作，减少冗余代码，提升开发效率
- 应用客户端：Android
- SDK 收集的信息或申请的权限：**创建文件夹、写入文件、关联唤醒**
- 收集方式：不收集信息
- SDK 供应商：Jake Wharton（开源社区）
- 官网链接：<https://jakewharton.github.io/butterknife/>
- 隐私政策链接：无第三方 SDK 名称：RxJava-2
- 业务场景（收集目的）：用于处理异步任务和事件驱动编程，提高应用的性能与响应速度。
- 应用客户端：Android
- SDK 收集的信息或申请的权限：**读取文件**
- 收集方式：不直接收集信息
- SDK 供应商：RxJava 是由开源社区维护
- 官网链接：<https://github.com/ReactiveX/RxJava>
- 隐私政策链接：无第三方 SDK 名称：Okio
- 业务场景（收集目的）：用于高效处理文件、网络流和字节数据的读写操作，提高应用的存储和网络性能。
- 应用客户端：Android
- SDK 收集的信息或申请的权限：**读取文件**
- 收集方式：不直接收集信息
- SDK 供应商：Square, Inc.
- 官网链接：<https://square.github.io/okio/>
- 隐私政策链接：无第三方 SDK 名称：EventBus
- 业务场景（收集目的）：用于在应用中实现组件间的事件发布与订阅机制，提高模块间的通信效率。
- 应用客户端：Android
- SDK 收集的信息或申请的权限：**获取当前已连接上的 wifi 的信息、获取 IP 地址**
- 收集方式：不直接收集信息
- SDK 供应商：GreenRobot
- 官网链接：<https://greenrobot.org/eventbus/>
- **隐私政策链接：无附录 3、个人信息收集清单**

我们会收集您在使用服务时主动提供的、以及在您的授权下收集您在使用功能或接受服务过程中产生的下述信息。您可以通过《平安人隐私政策》中的联系方式联系我们对下列部分信息的具体内容进行咨询和管理。

您在职、离职各阶段工作中会使用不同的服务在不同阶段提供与工作相关的个人信息，主要包含：

- 1)在办理个人信息修改时提供的信息。
- 2) 您使用平安人参与人力资源管理工作时主动提供的信息。

信息清单具体包含：

一、实名制管理所需

二、身份验证所需

三、用户意见管理所需

四、系统安全保障所需

五、基于位置的服务所需

六、基于摄像头或相册的服务所需

七、基于麦克风的服务所需

八、基于日历的服务所需

九、基于电话权限的服务所需

十、其他服务所需

一、 实名制管理所需

1. 账户

采集频率：仅登录发生时

使用目的：登录时匹配用户及权限

使用场景：正式员工登录系统

收集信息：正式员工服务所需的手机号码、员工账号

2. 有效证件信息

场景 1

采集频率：仅用户主动使用 OCR 影像识别、照片上传、手动输入时

使用目的：完成实名认证、证明办理、个人信息修改相关服务

使用场景：实习生转正、服务、请假、我的档案、长期激励时

收集信息：身份证件

场景 2

采集频率：仅用户主动办理服务时

使用目的：完成证明办理、个人信息修改相关服务

使用场景：请假、我的档案信息修改

收集信息：结婚证件

二、 身份验证所需

1. 登录验证

采集频率：仅用户主动使用时

使用目的：账号安全保障

使用场景：移动面试、测评、离职办理时

收集信息：手机号码、电子邮箱、员工账号、密码、短信验证码、脸部图像或视频以及相关结果

2. 重要操作行为验证

采集频率：仅用户主动使用时

使用目的：账号安全保障、个人信息安全保障

使用场景：找回密码、个人薪酬查询、合同签署及变更、办证、离职、团队薪酬功能、签订长服或持股授予协议重要操作

收集信息：指纹、面容 ID、手势密码以及相关验证结果

三、 用户意见管理所需

采集频率：仅用户主动使用系统时

使用目的：安全保障、兼容性保障

使用场景：保障用户的意见反馈获得有效处理和解决、预防其他兼容性或安全风险

收集信息：设备型号、设备软件版本信息、移动电话、固定电话、岗位信息、公司邮箱地址、姓名、员工账号

四、 系统安全保证所需

1. 设备信息

采集频率：仅用户使用系统过程中，包括前台、后台运行时

使用目的：用于识别设备，进行信息推送和安全保障、兼容性判断相关功能

使用场景：用户安全使用系统

收集信息：设备信息，包含设备型号和名称、终端制造厂商、操作系统版本、设备设置、IMEI、IMSI、Android ID、应用安装列表、MAC 地址、SIM 卡运营商、SIM 卡序列号、时区和软硬件特征信息、WiFi 状态、SSID、BSSID、IDFV、IP 地址

2. 日志信息

采集频率：仅用户主动使用时

使用目的：安全管理及生产问题定位，提高使用系统的安全性，更准确地预防钓鱼网站欺诈、保护账户安全

使用场景：用户使用过程及遇到问题时

收集信息：日志信息

3. 存储空间

采集频率：仅用户主动使用时

使用目的：安全保障

使用场景：用户使用过程及遇到问题时

收集信息：存储空间信息

4. 正在运行的软件

采集频率：仅用户主动使用时

使用目的：安全保障

使用场景：用户使用过程及遇到问题时

收集信息：存储空间信息

五、 基于位置的服务所需

1. 位置信息

采集频率：仅用户主动使用时

使用目的：便于基于位置信息的体验服务

使用场景：考勤打卡、外出签到、打卡地址变更

收集信息：位置信息

六、 基于摄像头或相册的服务所需

1. 相册信息

采集频率：仅用户主动使用时

使用目的：便于基于相册信息的体验服务

使用场景：上传照片、更换头像、团队相册、请假申请、识别二维码、视频面试、OCR 识别、意见反馈、人工客服、证件夹、人脸采集、个人信息修改功能需从相册上传图片

收集信息：相册信息

2. 摄像头信息

采集频率：仅用户主动使用时

使用目的：便于基于摄像头信息的体验服务

使用场景：上述提到的相册信息进入相册可通过摄像头入口进入摄像头；识别二维码、视频面试、OCR 识别、意见反馈、人工客服、证件夹、人脸采集、个人信息修改功能需使用摄像头

收集信息：相册信息

七、 基于麦克风的服务所需

1. 语音信息

采集频率：仅用户主动使用时

使用目的：便于基于语音的体验服务

使用场景：视频面试使用过程

收集信息：语音信息

八、 基于日历的服务所需

1. 日历信息

采集频率：仅用户主动使用时

使用目的：便于基于日历信息的体验服务

使用场景：移动打卡、异常考勤

收集信息：日历信息

九、 基于电话权限的服务所需

1. 设备信息

采集频率：仅用户主动使用时

使用目的：便于基于电话权限的体验服务

使用场景：服务电话呼出

收集信息：设备信息

十、 其他服务所需

1. 头像

采集频率：仅用户主动上传、修改时

使用目的：个人形象展示

使用场景：中后台管理系统个人形象展示

收集信息：员工头像（可选）

2. 银行卡号

采集频率：仅用户主动修改时

使用目的：发放工资

使用场景：工资发放

收集信息：银行卡号

3. 民族信息

采集频率：仅用户主动修改时

使用目的：人事管理及申请民族假相关考勤需要

使用场景：用户个人档案信息修改时
收集信息：民族（提供“其他”选项）

4. 婚姻状况

采集频率：仅用户主动修改时
使用目的：人事管理及婚育假相关考勤申请
使用场景：个人信息补充、婚育假申请
收集信息：婚姻状况（提供“其他”“未知”选项）、结婚日期（可选）

5. 家庭成员信息

采集频率：仅用户主动修改时
使用目的：向员工提供家庭福利所需，申请婚假
使用场景：用户个人信息补充、婚育假申请
收集信息：家庭成员姓名、与员工关系、手机号（加密、可选）、出生日期（可选）、工作单位（可选）、家庭地址（可选）

6. 地址信息

采集频率：仅用户主动修改时
使用目的：人事管理及物品派送
使用场景：用户个人信息补充、邮寄事项办理
收集信息：地址信息（可选）

7. 紧急联系人信息

采集频率：仅用户主动修改时
使用目的：员工紧急事项通知
使用场景：用户个人信息补充、紧急事项通知
收集信息：紧急联系人姓名（可选）、联系方式（加密、可选）、地址（可选）、与员工关系（可选）

我们将严格遵循《平安人隐私政策》中个人信息使用的规则进行个人信息收集。您也可在隐私政策查看[平安人设备权限列表](#)，进一步了解各个权限的名称、使用目的、调用情况说明。

附录 4、相关定义

为了帮助您更好地理解本政策，我们在附录中向您介绍以下专有名词的定义与示例。

1. **个人信息**：指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

信息类型	具体内容
个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、 个人电话号码、电子邮件地址
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保

	卡、居住证
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征
网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单
个人财产信息	银行账户、鉴别信息（口令）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人通信信息	通信记录和内容、短信、彩信、电子邮件、以及描述个人通信的数据（通常称为元数据）
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表
个人常用设备信息	指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息）在内的描述个人常用设备基本情况的信

	息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录

2. 敏感个人信息：指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。敏感个人信息包括，生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹信息，以及不满十四周岁未成年人的个人信息。

3. 设备信息：包括设备标识符（IMEI、IDFA、Android ID、MAC、OAID、IMSI 及其他设备相关信息）、应用信息（应用崩溃信息、通知开关状态、应用安装列表及其他应用相关信息）、设备参数及系统信息（设备类型、设备型号、操作系统及硬件相关信息）、设备网络环境信息（IP 地址、Wi-Fi 信息、基站信息及其他网络相关信息）。具体以产品或服务的实际情况为准。

4. 日志信息：包括浏览记录、点击查看记录、搜索查询记录、收藏记录、添加至购物车记录、关注分享信息、发布信息、IP 地址、浏览器的类型、使用的语言、操作系统的版本、访问的日期和时间、电信运营商。具体以产品或服务的实际情况为准。

5. 去标识化：指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。去标识化处理后的信息仍属于个人信息。

6. 匿名化：指个人信息经过处理无法识别特定自然人且不能复原的过程。匿名化处理后的信息不再属于个人信息。

7. 处理：包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除。