

# 隐私政策

更新日期：2024 年 08 月 29 日

生效日期：2024 年 08 月 29 日

发布日期：2024 年 08 月 29 日

本政策将帮助您了解以下内容：

- 一、 我们如何收集和使用信息
- 二、 您如何管理您自己的信息
- 三、 我们如何使用 Cookie
- 四、 我们如何对外提供信息
- 五、 我们如何存储和保护信息
- 六、 我们如何保护未成年人的信息
- 七、 第三方责任说明
- 八、 本政策适用与修订
- 九、 如何联系我们

“TurboGo” 简称“本 APP” 由 I. FINE CONSULTING (HONGKONG) LIMITED

简称“我们”所有和运营。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隐私信息安全可靠。我们致力于维持您对我们的信任，保护您的个人信息，恪守权责一致原则、目的明确原则、选择同意原则、最少够用原则、确保安全原则、主体参与原则、公开透明原则等要求。同时，我们承诺，我们将遵守并落实《网络安全法》的各项规定，依照业界成熟的安全标准，采取相应的安全保护措施来保护您的个人信息。请您在使用我们的产品或服务前，仔细阅读本《隐私政策》，了解我们对您个人信息的处置原则和保护措施。阅读过程中，请与我们的客服联系咨询。如您不同意协议中的任何发布或修订的条款，您可选择注销本账户，同时您应知晓，我们将无法再为您提供相关服务。

本隐私政策中涉及的个人敏感信息，主要是为登录的用户鉴别与授权信息，以及在全类业务中收集、存储的，包括以下内容：

## 身份基本信息：

包括客户姓名、民族、性别、职业、联系方式、办公电话、办公传真、电子邮件、员工编号、年龄、办公地点、家庭电话。

## 网络身份标识信息：

包括系统账号、昵称、头像、IP 地址及与前述有关的密码

## 个人常用设备信息：

包括手机类型、系统设备版本、软件版本、硬件序列号。

**个人位置信息：**

包括定位信息。

**生物识别信息：**

语音信息。

**摄像头拍照信息：**

摄像头、拍照照片。

## 一、我们如何收集和使用信息

为了您可以正常使用我们的服务，下列情形下您需要向我们提供相关信息：

### 1. 使用服务过程中收集信息

#### (1) 设备信息

您需要同意即时通讯获取与您的设备相关的信息，包括手机类型、系统设备版本、软件版本、硬件序列号。这些信息能够使 App 应用系统适配相应设备并确保用户获得最新的版本功能，并且通过启用绑定设备功能来增强系统的安全性。

#### (2) 用户手机号码

即时通讯会根据受理用户的手机号码作为登录账号，用户手机号码能够使用户进行正常登录和接收短信。

#### (3) 用户基本信息

即时通讯的个人设置中心，向用户征集是否填写用户基本信息，这些信息由信息主体自愿提供，包括：姓名、用户性别、生日、登录别名、办公电话、办公传真、电子邮件、短号码、员工编号、头像。这些信息能够使相关的客户单位进行人员管理。

#### (4) 位置信息

当用户使用即时通讯应用时，向用户征集是否同意使用位置信息、WIFI mac 地址，即时通讯会在人员考勤中获取位置信息和 wifi 信息、外勤定位时获取地理位置信息地址并进行定位，这些信息能够使考勤、外勤功能正常进行位置信息更新。

#### (5) 语音信息

当用户使用视频会议时，用户可以选择开启手机的麦克风权限，如您不提供前述信息，可能无法为您提供相关服务，但不影响您使用我们提供的其他服务。

#### **(6) 日志信息**

当用户使用即时通讯应用时，即时通讯会自动收集用户对系统的详细使用情况，作为有关网络溯源信息存储在服务器日志中。此类信息包括：登录日志，操作日志。

**(7) 为您提供本应用的其他具体服务，本应用会在提供具体服务前通过弹窗方式另行取得您的授权：**

1. 为了您使用本 APP 拍照上传或本地图片上传功能场景，在邮件、公告、审批、会议、考勤功能，我们需要获取终端相机权限，我们会在这些场景通过弹窗的方式征求您的授权，如果您拒绝授权将无法使用拍照功能及上传附件功能。
2. 为了您使用拨打电话功能，在通讯录一个人详情拨打电话获取拨打电话权限，我们会通过弹窗方式征求您的授权，在您授权同意后获取本机拨打电话权限，如不授权该权限将不能使用该功能服务。
3. 为了能够便于您及时升级 APP 体验更新功能，我们会获取您的安装权限，用于方便您选择是否升级到最新版本。
4. 为了您能够使用本 APP 的考勤，我们会使用相关地图 SDK 在您授权同意后获取本机位置权限，如不授权该权限将不能使用所对应的功能服务。
5. 为了您能够使用本 APP 修改您的头像，在设置一个人资料中获取相机权限（拍照）、存储权限（相册），我们会通过弹窗方式征求您的授权，在您授权同意后获取本机摄像头及相册权限，如不授权该权限您将不能正常使用该服务。
6. 为了您能够使用本 APP 上传附件，在邮件、公告、审批、会议等功能，我们会通过弹窗方式征求您的授权，在您授权同意后获取文件存储权限，如不授权该权限您将不能正常使用该服务。

#### **(8) 后台运行时搜集信息与自启动或关联启动说明**

**后台运行：**当即时通讯应用在后台运行时，为了保障功能能正常后台使用，我们可能会结合下述 SDK 及相关的三方服务对您的一些基本信息进行搜集获取，信息如设备 Mac 地址、唯一设备识别码（如 IMEI/IDFA/OPENUDID/GUID、SIM 卡 IMSI 信息）、获取已安装应用等。详见下方：六、第三方责任说明

**推送相关：**为确保本应用处于关闭或后台运行状态下可正常接收到客户端推送的广播信息，本应用须使用（自启动）能力，将存在一定频率通过系统发送广播唤醒本应用自启动或关联启动行为，是因实现功能及服务所必要的；当您打开内容类

推送消息，在征得您的明确同意后，会跳转打开相关内容。在未征得您同意的情况下，则不会有关联启动。

如您作为企业组织管理员选择开通、管理即时通讯办公服务的，我们会收集您所在的企业组织用户在使用相关功能/应用的过程中提交或产生的信息和数据（下称“企业控制数据”），企业控制数据可能包括：

(1) 您所在企业组织分配给您的职位、隶属部门、办公电话信息，以及您为完成企业组织日常经营管理开通的考勤、审批、日志功能而要求提供或产生的地理位置个人信息以及考勤打卡信息、审批记录、发布日志信息。

(2) 您使用即时通讯服务或选购开通使用第三方应用服务时的订单交易信息，以便向您展示并便于您对订单进行管理。

(3) 如您所在企业组织管理员选择开通、管理和使用即时通讯通讯录服务，您需按照企业组织用户要求提供您的身份信息（姓名）、企业任职信息（部门、职位、职级）、企业及您个人的联系方式（手机、固定电话、邮箱）、企业及个人联系地址（办公地址）或您保存的个人通讯录信息企业组织用户提交或要求您提供的企业分配给您的信息或您的个人信息。

(4) 其他由企业组织用户提交的包含您个人信息的数据，即时通讯通讯录信息（包括企业组织用户的任职信息、联系方式信息）

您理解并同意，企业组织用户为上述企业控制数据的控制者，即时通讯仅根据企业组织用户管理员选择开通、管理和使用上述应用服务处理您的个人信息/数据。企业组织用户上传即时通讯企业组织通讯信息以及其他要求所在企业组织的即时通讯个人用户提交智能人事信息、外部业务联系人信息之前，应确保已经事先获得即时通讯个人用户的明确同意，并仅限收集实现企业运营及管理目的所必需最终用户信息，并已充分告知最终用户相关数据收集的目的、范围及使用方式。

随着本应用功能进一步丰富，后续新增功能如涉及获取用户授权权限时，我们将明确提示并在您授权同意后才会获取该功能所需权限。如未取得您的授权，我们将不会收集和使用相关信息。

## **2. 您充分知晓，以下情形中，我们收集、使用个人信息无需征得您的授权同意：**

(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)依照本法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。

## 二、您如何管理您自己的信息

1. 您可通过即时通讯手机客户端登录办公帐号点击【我的个人资料】，查阅与修改您的身份、账户信息，或修改您的个人资料，但出于安全性和身份识别的考虑或根据法律法规的强制规定，您可能无法修改注册时提供的初始认证信息。

2. 与您即时通讯的帐号中的个人信息相关的更多详细信息，您可以通过发送电子邮件或者通过您的设备登入帐号来访问、更改或删除。

3. 退出企业（注销账户），当你退出所在企业，我们将在合理期间内删除或匿名化处理你在该企业的相关个人信息。当你退出所有企业，即视为注销帐号，我们将停止为你提供服务，并在合理期限内删除或匿名化处理你的个人信息。您也可以发送电子邮件或通过本政策下方的其他方式与我们联系。

4. 如果您无法通过上述方式访问、更正或删除您的个人信息，或您需要访问、更正或删除您在使用我们产品与/或服务时所产生的其他个人信息，或您认为方是云（上海）技术有限公司存在任何违反法律法规或与您关于个人信息的收集或使用的约定，您均可以发送电子邮件或通过本政策下方的其他方式与我们联系。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，我们将在收到您反馈并验证您的身份后的 30 天内答复您的请求。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。

5. 在以下情形中，按照法律法规要求，我们将无法响应您的请求：

- 1) 与国家安全、国防安全有关的；
- 2) 与公共安全、公共卫生、重大公共利益有关的；
- 3) 与犯罪侦查、起诉和审判等有关的；
- 4) 有充分证据表明您存在主观恶意或滥用权利的；
- 5) 响应您的请求将导致您或其他个人、组织的合法权益受到严重损害的。

## 三、我们如何对外提供信息

### （一）共享

我们会按照法律法规及相关国家标准要求，以弹框提示、确认授权、电子协议形式征得您的同意，或确认第三方已征得您的同意，您可以选择停止共享您的信息。我们仅基于产品与/或服务的业务场景，与第三方共享您的信息，第三方包括关联公司、外部实名信息验证机构以及其他合作伙伴。对于我们与之共享信息的第三方，我们会在完成并通过针对第三方的信息安全风险评估后，与其签署必要的保密协定，要求他们严格遵守相关法律法规与监管要求，遵照我们的本隐私政策采取保密和安全措施来处理个人信息，未经您的授权严禁用于自身或第三方营销活动。

1. 我们提供的第三方产品与/或服务，可能由第三方提供或第三方联合我们提供，因此只有共享您的信息，才能实现我们的产品与/或服务的核心功能或提供您需要的服务；
2. 根据适用的法律法规、法律程序的要求、强制性的行政或司法要求所必须情况进行提供；
3. 在法律法规允许且不违背公序良俗的范围内，为维护方是云（上海）技术有限公司关联方、您或其他方是云（上海）技术有限公司用户或社会公共利益、财产或安全免遭损害而有必要提供，比如为防止欺诈违法活动和减少信用风险，而与其他公司和组织交换信息。不过这并不包括违反本隐私政策中所作的承诺而为获利目的出售、出租、共享或以其它方式披露的个人信息。我们的关联方无权将个人信息共享用于任何其他用途，我们的关联方如要改变个人信息的处理目的，将再次通过公告公示、弹框授权方式，征求您的授权同意；
4. 应您需求为您处理您与他人的纠纷或争议；
5. 基于研究而使用；

### （二）转让

我们不会将您的个人信息转让给任何公司、组织和个人，但以下情况除外：

1. 事先获得您明确的同意或授权；
2. 根据适用的法律法规、法律程序的要求、强制性的行政或司法要求所必须的情况进行提供；

3. 符合与您签署的相关协议（包括在线签署的电子协议以及相应的平台规则）或其他法律文件约定所提供。

### （三）公开披露

原则上我们不会将您的信息进行公开披露，但以下情形除外：

1. 根据您的需求，在您明确同意或授权的披露方式下披露您所指定的个人信息；
2. 根据法律法规的要求、强制性的行政执法或司法要求所必须提供您个人信息的情况下，我们可能会依据所要求的个人信息类型和披露方式，在法律法规许可的前提下，采取符合业界标准的安全防护措施的前提下公开披露您的个人信息。

## 四、我们如何存储和保护信息

1. 遵照《网络安全法》规定，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，即时通讯客户端未在境外提供任何产品及服务。我们将会按照国家相关法律规定的期限，保存您的身份资料、消费记录为期五年，超出期限后将您的个人信息进行匿名化处理或删除。

2. 我们已使用符合业界标准的安全防护措施保护您提供的个人信息，采取措施保护数据遭到未经授权访问、公开披露、使用、修改、损坏或丢失。我们会采取一切合理可行的措施，确保您个人信息的安全性、完整性、真实性、有效性，如下：

(1) 使用加密技术对个人信息数据进行存储，使用受信赖的保护机制防止数据遭到攻击；在涉及个人信息需要展示的应用界面，我们采用必要的掩码脱敏手段以确保不受非法窃取；即时通讯建立了 APP 消息通知渠道，当发生公众风险事件后，可通过上述渠道及时将影响分析和处置方式知会相关用户。

(2) 在您初次使用即时通讯时，我们会遵循最小化原则，结合具体业务场景及其所涉设备权限，按需阐明用途，征求您的充分授权，保障您的知情权和隐私权不受侵犯。

(3) 我们建立了数据安全管理制度，明确了数据分类分级方式和敏感信息管理要求，规范了信息存储准则。我们部署严格的访问控制、多重身份认证机制以及定期开展访问日志复核，确保只有授权人员才可访问个人信息，防止越权和违规操作；

(4) 我们建立了完备的安全事件处置措施和补救措施，每年针对个人信息保护进行应急预案的演练，及时定位风险，持续监控态势。同时定期举办敏感数据安全

和隐私保护培训课程，加深员工保护个人信息的安全意识，截止目前未发生任何个人信息泄露、毁损、丢失的风险事件。

3. 我们定期开展包括敏感信息内部审计、信息安全风险评估、代码安全检查、数据日志分析信息安全保护工作，从安全管理策略、安全技术保障多方面保护您的个人信息安全。

4. 我们推荐您安装升级方是云（上海）技术有限公司定期发布的最新版本 App，为您提供优化功能的稳定服务，防止泄露个人信息。

5. 对于所收集的信息，我们仅在本政策所述目的所必须且最短的时限内保存您的个人信息，超出保存期限后，我们将对所收集的信息进行匿名化处理。

6. 互联网并非绝对安全的环境，而且电子邮件并未严格受到强加密保护，为了您的个人信息安全，我们强烈建议您不要通过此类方式传输个人信息。尽可能最小化向第三方提供个人信息，防止非法窃取盗用和未经授权访问带来的信息泄露和资金损失。如您发现自己的个人信息泄密，尤其是您的账户信息及密码发生泄露，请您立即联络我们，以便我们尽快配合您采取相应措施。

## 五、我们如何保护未成年人信息

若您 18 周岁以下的未成年人，我们鼓励您在父母或监护人的指导下使用我们的服务，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，方是云（上海）技术有限公司根据国家相关法律法规的规定要求保护未成年人的个人信息我们重视未成年人的信息保护，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。

## 六、第三方责任说明

为保障即时通讯 App 业务场景的功能实现和应用平台的稳定运行，我们会嵌入由合作伙伴提供的第三方 SDK 或其他类似的应用程序为您提供相关服务，如您在我们平台上使用这类由第三方提供的服务时，您同意将由其直接收集和处理您的信息（如以嵌入代码、插件形式）。在这类第三方 SDK 服务嵌入即时通讯 APP 时，我们会进行严格的上线安全检测，确保最小化收集个人信息。目前我们产品中包含的第三方 SDK 服务如下：

**高德位置服务**

运营方：高德软件有限公司

功能：帮助用户在设置基于位置实现考勤打卡时的位置定位、对话框中发送或共享位置

收集个人信息类型：位置信息（包括 GNSS 信息、IP 地址、WLAN 热点、基站信息、蓝牙设备以及其他能够用于定位的传感器信息）、设备信息（包括终端设备唯一标识符（包含 IDFV、OAID、IMEI、MEID、IMSI）、mac 地址、Andriod ID、操作系统版本、设备品牌及型号、设备配置、运营商类型名称及代码、应用信息（应用名、应用版本号））、WiFi 信息、正在运行的应用列表、网络类型、BSSID、MEID、硬件序列号、手机存储权限

隐私权政策链接：

<https://lbs.amap.com/pages/privacy/>

#### 金山办公 WPS

运营方：珠海金山办公软件有限公司

功能：用于 APP 向用户提供文档预览及在线功能

收集个人信息类型：采集正在运行的应用信息、获取设备信息（IMEI、UDID、ANDROID\_ID）、读取外部存储权限、运营商名称、运营商代码、网络类型、网络 IP 信息

隐私权政策链接：

<https://www.wps.cn/privacy/privacyprotect>

#### 腾讯 TBS 浏览服务

运营方：深圳市腾讯计算机系统有限公司

功能：App 内打开网页

收集个人信息类型：粘贴板信息、运行中的应用列表信息

隐私权政策链接：

<https://x5.tencent.com/tbs/guide/develop.html#5>

## 腾讯 BugLy

运营方：深圳市腾讯计算机系统有限公司

功能：排查崩溃问题, 帮助 APP 提升稳定性

收集个人信息类型：设备信息（SSID、BSSID、IMEI、MEID、Android\_ID）、运营商信息、运行中的应用列表信息、外部存储权限、Wi-Fi 信息、网络 IP 信息

隐私权政策链接：

<https://privacy.qq.com/document/preview/fc748b3d96224fdb825ea79e132c1a56>

## 七、本政策适用与修订

未经您的同意，我们不会消减您按照隐私政策所应享有的权利。我们会以弹窗的形式发布对本政策所做的任何更改。对于修订或更新后的隐私政策，我们会再次征求您的同意。

本政策所指的重大变更包括以下内容：

1. 我们的服务模式发生重大变化。如处理个人信息的目的、类型及使用方式；
2. 个人信息共享、转让或公开披露的主要对象发生变化；
3. 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；
4. 我们负责处理个人信息安全的联络方式及投诉渠道发生变化时；
5. 个人信息安全影响评估报告以及敏感信息内部审计报告表明存在高风险时。

## 八、如何联系我们

1. 如您对本隐私政策或您个人信息的相关事宜有任何问题、意见、建议或申诉，可以通过如下方式与我们的个人信息保护团队联系：

电子邮箱: Paeanzhao@finecomn.com

2. 一般情况下, 我们将在 72 小时内回复, 特殊情形下, 不超过 15 个工作日。如果您对我们的回复不满意, 特别是我们的个人信息处理行为损害了您的合法权益, 您可以与我们再次沟通, 或向有权机关反映。