

## 社交云-IM SDK 隐私政策

本政策适用于平安科技（深圳）有限公司（以下简称“我们”或“社交云-IM SDK”）的社交云-IM SDK 的产品和服务。

发布日期：2025 年 6 月 11 日

更新日期：2025 年 6 月 11 日

生效日期：2025 年 6 月 11 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：[pub\\_kjdmtd@pingan.com.cn](mailto:pub_kjdmtd@pingan.com.cn)

### 提示条款：

社交云-IM SDK（在 iOS 系统为 PASocialCloudSDK，安卓及鸿蒙系统为 PAIMSDK，以下简称“社交云”或“我们”）非常尊重您的个人信息的保护，因此社交云将按照本隐私政策的规定收集、使用、共享、存储及保护您的个人信息。

在使用社交云各项服务前，请您务必仔细阅读并透彻理解本政策。

如对本政策或社交云其他协议及政策内容有任何疑问，您可通过本政策末尾（第 12 条）公布的联系方式向我们咨询或寻求帮助。**如果您不同意本政策或社交云其他协议及政策的内容的，您应暂停使用社交云服务，获得帮助或解答满意后方可继续使用。**

## 第一部分 定义

1、**平安科技**：指通过运营社交云向您提供服务的平安科技（深圳）有限公司。平安科技注册地址：深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼。

2、**个人信息**：指以电子或者其他方式记录的与已识别或可识别的自然人有关的各种信息，不包括你敏华处理后的信息。

3、**个人敏感信息**：是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，本政策中涉及的个人敏感信息包括（在具体收集的业务场景中使用加粗方式表明）：您的姓名及手机号码。删除个人信息：指在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

4、**关联公司**：是指中国平安保险（集团）股份有限公司及其通过股权、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中国平安保险（集团）股份有限公司投资的联营企业、合营企业；存在个人信息共享的关联公司范围包括：

【<http://www.pingan.cn/ir/financial-report.shtml>】。

5、**第三方**：是指集成社交云 IM SDK 的调用者，即通过 API 接口与社交云 IM SDK 进行数据交互的 App 或服务。

## 第二部分 隐私政策

## 第 1 条 适用范围

1.1 为您提供更专业、更优质、更个性化的服务是我们坚持不懈的追求，也希望通过社交云提供的服务可以更方便您的生活。本政策适用于社交云提供的所有服务，您使用社交云提供的服务，均适用本政策。

1.2 需要特别说明的是，本政策不适用于其他 SDK 向您提供的服务，例如：您通过金管家 APP、好车主 APP 等平台使用到的其他服务，您向对应平台提供的个人信息，应当遵守对应的隐私政策。

## 第 2 条 您须授权我们收集和使用您个人信息的情形

社交云收集您的个人信息是为了向您提供更专业、更优质、更个性化的服务，社交云收集信息的渠道如下：

2.1 为实现社交功能所必须：

1、为实现社交云 IM SDK 的相应功能所必需，我们将向终端用户或开发者收集终端用户在使用与社交云 IM SDK 相关的功能时产生的如下个人信息：

个人信息名称	处理目的	使用场景	处理方式	操作系统
Wi-Fi 状态	针对网络类型进行网络重连	在 IM 聊天场景中	去标识化、加密传输的安全处理方式	Android、iOS、Harmony
设备型号	Android/iOS/Harmony 的兼容问题、崩溃问题进行适配和分析	在 IM 聊天场景中	去标识化、加密传输的安全处理方式	Android、iOS、Harmony
程序版本号	Android/iOS/Harmony 的兼容问题、崩溃问题进行适配和分析	在 IM 聊天场景中	去标识化、加密传输的安全处理方式	Android、iOS、Harmony
操作系统	Android/iOS/Harmony 的兼容问题、崩溃问题进行适配和分析	在 IM 聊天场景中	去标识化、加密传输的安全处理方式	Android、iOS、Harmony
IP 地址	检测网络链连接质量	在 IM 聊天场景中	去标识化、加密传输的安全处理方式	Android、iOS、Harmony
CPU 信息	Android/iOS/Harmony 的兼容问题、崩溃问题进行适配和分析	在视频、语音通话场景中	去标识化、加密传输的安全处理方式	Android、iOS、Harmony

请理解，前述信息均为最终用户的设备信息，一般而言，前述设备信息无法与已识别或可识别的自然人建立关联，但我们仍将采取加密等信息安全措施对此部分信息进行保护。

2、为实现社交云 IM SDK 功能所需的权限

为实现社交云 IM SDK 的相应功能所必需，我们会通过开发者的应用在对应的功能场景下申请所需权限。如您是开发者，请您注意，您应按您的应用的具体功能场景，在

用户触发具体功能场景时调用 SDK 的相应功能、调用相应权限或处理终端用户的个人信息，未到具体业务或功能场景时不应调用相应权限。

请您注意，对于 社交云 IM SDK 相应功能的权限，我们不会强制获取，您可以关闭该权限，只影响相关的功能，不影响其他的功能使用，关闭权限后将同步停止收集您的信息。

操作系统	权限名称	使用功能	是否可以关闭
iOS、Android、HarmonyOS	网络	通过网络进行数据传输，与其他使用者进行聊天	是
	写入存储	存储聊天内容写入到数据库和存储日志文件	是
	读取存储	读取数据库中的历史聊天内容	是

## 2.2 社交云通过第三方便收集到的您信息：

为了给您提供更专业、更优质、更加个性化的服务，或为提高您查询的效率或速度，或共同为您提供服务，我们会向接入社交云的第三方 APP 运营主体获取您授权共享的您的姓名、手机号码、头像、所在地址及聊天记录，以便您可以及时查看您的聊天记录，并让您的好友或同事可以访问通讯录信息。

## 2.3 我们承诺不从非法渠道间接获取个人信息；不收集法律法规明令禁止收集的个人信息。

## 2.4 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) 与个人信息处理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、审判和判决执行等直接相关的；
- (5) 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；
- (6) 所涉及的个人信息是个人信息主体自行向社会公众公开的；
- (7) 根据个人信息主体要求签订和履行合同所必需的；注：隐私政策的主要功能为公开个人信息处理者收集、使用个人信息范围和规则，不应将其视为本条中的合同。
- (8) 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；
- (9) 维护所提供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；
- (10) 个人信息处理者为新闻单位，且其开展合法的新闻报道所必需的；个人信息处理者为学术研究机构，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。

## 第 3 条 您了解并同意，以下信息不适用本政策：

3.1 您违反法律规定或违反社交云规则行为及社交云已对您采取的措施；

3.2 应法律法规及监管要求需公示或提供的信息。

#### **第 4 条 您个人信息使用的规则**

4.1 我们会根据本隐私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。

4.2 收集您的个人信息后，我们将通过技术手段对数据进行去标识化处理，去标识化处理的信息在不借助额外信息的情况下，将无法识别特定自然人。请您了解并同意，在此情况下我们有权使用已经去标识化的信息；并在不透露您个人信息的前提下，我们有权对您数据库进行分析并予以商业化的利用。

4.3 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，除非您删除或通过系统设置拒绝我们收集，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。在您注销账号时，我们将停止使用并匿名化您的个人信息。

4.4 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。

4.5 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。

4.6 当我们要将您的个人信息用于本隐私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。如果您选择使用本隐私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、页面提示等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。

#### **第 5 条 我们如何使用 Cookies 和同类技术**

5.1 为实现您联机体验的个性化需求，使您获得更轻松的访问体验。我们会在您的计算机或移动设备上发送一个或多个名为 Cookies 的小数据文件，指定给您的 Cookies 是唯一的，它只能被将 Cookies 发布给您的域中的 Web 服务器读取。我们向您发送 Cookies 是为了简化您重复登录的步骤、存储您的购物偏好或您购物车中的商品等数据进而为您提供购物的偏好设置、帮助您优化对广告的选择与互动、帮助判断您的登录状态以及账户或数据安全。

5.2 我们不会将 Cookies 用于本隐私政策所述目的之外的任何用途。您可根据自己的偏好管理或删除 Cookies。您可以清除计算机上保存的所有 Cookies，大部分网络浏览器会自动接受 Cookies，但您通常可根据自己的需要来修改浏览器的设置以拒绝 Cookies；另外，您也可以清除软件内保存的所有 Cookies。但如果您这么做，您可能需要在每一

次访问平安科技网站时亲自更改您设置，而且您之前所记录的相应信息也均会被删除，并且可能会对您所使用服务的安全性有一定影响。

## **第 6 条 您个人信息的共享、提供和披露**

**第三方：**是指集成社交云 IM SDK 的调用者，即通过 API 接口与社交云 IM SDK 进行数据交互的 App 或服务。

6.1 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。我们共享、转让个人信息的目的、数据接收方的类型如下：

(1) 事先获得您的同意或授权，共享、转让经去标识化处理的个人信息，且确保数据接收方无法重新识别个人信息主体的除外；

(2) 共享、转让内容包含您的个人信息(您的姓名、手机号码、头像、所在地址)及通过社交云 IM SDK 及服务产生的聊天记录；

(3) 根据法律法规的规定或行政或司法机构的要求；

(4) 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，您的 IM 聊天消息可能会被共享给第三方。

(5) 如您出现违反中国有关法律、法规或者社交云相关协议或相关规则的情况，需要向包括但不限于权利人（包括社交云）、行政、司法机关等第三方披露等（包括进行公证、见证等证据保全）；

(6) 如您是适格的知识产权投诉人并已提起投诉，应被投诉人要求，向被投诉人披露您的姓名、联系方式信息，以便双方处理可能的权利纠纷；

(7) 在涉及合并、收购或破产清算时，如涉及到个人信息转让，我们会要求新的持有您个人信息的公司、组织继续受此隐私权政策的约束，否则我们会要求该公司、组织重新向您征求授权同意；

(8) 为维护我们及其关联公司或您的合法权益。

6.2 您同意并授权我们根据上述约定向相关第三方共享、转让您的个人信息。

6.3 我们向第三方共享、转让您个人敏感信息前，将在具体业务页面提示说明共享、转让的个人敏感信息类型、数据接收方的身份，并采取严格的审批和安全影响评估机制确保数据接收方的安全能力，要求其按照不低于社交云的标准采取个人信息保护措施。同时，在该提示说明项下另行获取您的明示同意。

6.4 个人信息共享、转让后，若您希望了解数据接收方对其个人信息的保存、使用等情况，要求实现个人信息主体的权利，例如，访问、更正、删除、注销账户等，您还可以随时通过本政策末尾（第 12 条）公示的联系方式联系我们，我们将在【15】天内通过邮箱回复您的请求。

6.5 但无论如何，我们不会将您的个人信息用于非法目的，也不会向任何用于非法目的的第三方分享您的个人信息。

6.6 以下情形中，我们共享、转让、公开披露个人信息无需事先征得您的授权同意：

(1) 与个人信息处理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、审判和判决执行等直接相关的；
- (5) 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；
- (6) 个人信息主体自行向社会公众公开的个人信息；
- (7) 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。

## 第7条 您个人信息的保护

### 7.1 我们保护您个人信息的技术与措施

我们非常重视个人信息安全，并采取一切合理可行的措施，保护您的个人信息：

#### (1) 数据安全保护措施

- 我们会采用符合业界标准的安全防护措施，包括建立合理的制度规范、安全技术来防止您的个人信息遭到未经授权的访问使用、修改，避免数据的损坏或丢失。
- 平安科技的网络服务采取了传输层安全协议等加密技术，通过 https 等方式提供浏览服务，确保您数据在传输过程中的安全。
- 平安科技采取加密技术对您个人信息进行加密保存，并通过隔离技术进行隔离。
- 在个人信息使用时，例如个人信息展示、个人信息关联计算，我们会采用包括内容替换、SHA256 在内多种数据脱敏技术增强个人信息在使用中安全性。
- 平安科技采用严格的数据访问权限控制和多重身份认证技术保护个人信息，避免数据被违规使用。
- 平安科技采用代码安全自动检查、数据访问日志分析技术进行个人信息安全审计。

#### (2) 平安科技为保护个人信息采取的其他安全措施

- 平安科技通过建立数据分类分级制度、数据安全管理制度、数据安全开发规范来管理规范个人信息的存储和使用。
- 平安科技通过信息接触者保密协议、监控和审计机制来对数据进行全面安全控制。
- 平安科技建立数据安全委员会并下设信息保护专职部门、数据安全应急响应组织来推进和保障个人信息安全。
- 安全认证和服务。我们存储您个人信息的底层云技术取得了数据中心联盟颁发的“可信云”认证三级认证、通过了公安部安全等级保护三级认证，同时还获得了 ISO27000 认证。
- 加强安全意识。我们还会举办安全和隐私保护培训课程，加强员工对于保护个人信息重要性的认识。

- (3) 我们仅允许有必要知晓这些信息的平安科技及平安科技关联公司的员工、合作伙伴访问个人信息，并为此设置了严格的访问权限控制和监控机制。我们同时要求可能接触到您个人信息的所有人员履行相应的保密义务。如果未能履行这些义务，可能会被追究法律责任或被中止与平安科技的合作关系。我们会采取一切合理可行的措施，确保未收集无关的个人信息。

(4) 我们还在您数据保护上做了一些创造性工作在配送体系，采用了独特的“微笑面单”，避免您敏感信息在配送环节的暴露，同时,大力强化对平安科技物流员工的数据安全培训和要求，提高物流员工保护您敏感信息的意识。

(5) 互联网并非绝对安全的环境，而且电子邮件、即时通讯、社交软件等与其他您的交流方式无法确定是否完全加密，我们建议您使用此类工具时请使用复杂密码，并注意保护您的个人信息安全。在通过平安科技与第三方进行网上产品与/或服务的交易时，您不可避免的要向交易对方或潜在的交易对方披露自己的个人信息，如联络方式或者邮政地址等。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。

#### (6) 安全事件处置

- 为应对个人信息泄露、损毁和丢失等可能出现的风险，平安科技制定了多项制度，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。平安科技也为安全事件建立了专门的应急响应团队，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。

- 一旦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、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。

- 互联网环境并非百分之百安全，我们将尽力确保或担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。如果您对我们的个人信息保护有任何疑问，可通过本隐私政策中约定的联系方式联系我们。如您发现自己的个人信息泄密，尤其是您的账户及密码发生泄露，请您立即通过本隐私政策第 12 条中约定的联系方式联络我们，以便我们采取相应措施。

## 7.2 您个人信息的保存

您的个人信息储存于中华人民共和国境内。除非获得您的特别同意，或者满足法律规定的评估及许可程序，我们不会跨境转移您的个人信息。

除非法律法规另有规定，我们将按如下期间保存您的信息：

- (1) 您使用我们的平台服务期间，我们将根据业务需要在法律许可的最长时间范围内持续为您保存个人信息，除非您自主取消授权、删除这些信息或者注销账户；

- (2) 当您取消授权、删除个人信息或注销账户后，我们将按照法律规定删除您的个人信息，或者在法律许可的情况作匿名化处理。

## 第 8 条 您如何管理您的信息

平安科技非常重视您对个人信息的关注，并尽全力保护您对于您个人信息访问、更正、删除以及撤回同意的权利，以使您拥有充分的能力保障您的隐私和安全。

**8.1 访问和更正您的个人信息除法律法规规定外，您有权随时访问和更正您的个人信息，具体包括：**

(1) 对于您在使用我们的产品与/或服务过程中产生的其他个人信息需要访问或更正，请随时联系我们。我们会根据本隐私政策所列明的方式和期限响应您的请求。

(2) 您无法访问和更正的个人信息：除上述列明的信息外，您的部分个人信息我们无法为您提供访问和更正的服务，这些信息主要是为了提升您的您体验和保证交易安全所收集的您的设备信息、您使用扩展功能时产生的个人信息。上述信息我们会在您的授权范围内进行使用，您无法访问和更正，但您可联系我们进行删除或做匿名化处理。

## 8.2 删除您的个人信息

您在我们的产品与/或服务页面中可以直接清除或删除的信息，包括订单信息、浏览信息、收货地址信息。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，或您注销了平安科技账号；
- (5) 如果我们终止服务及运营。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。若我们响应您的删除请求，我们不能保证立即从备份系统中删除相应的信息，但会在备份系统更新时删除这些信息。

## 8.3 改变您授权同意的范围或撤回您的授权

您可以通过删除信息、关闭设备功能、在平安科技网站或软件中进行隐私设置等方式改变您授权我们继续收集个人信息的范围或撤回您的授权。您也可以通过注销账户的方式，撤回我们继续收集您个人信息的全部授权。

请您理解，每个业务功能需要一些基本的个人信息才能得以完成，当您撤回同意或授权后，我们无法继续为您提供撤回同意或授权所对应的服务，也不再处理您相应的个人信息。但您撤回同意或授权的决定，不会影响此前基于您的授权而开展的个人信息处理。

## 8.4 获取您的个人信息副本

您有权获取您的个人信息副本。如您需要获取我们收集的您的个人信息副本，您随时联系我们。在符合相关法律规定且技术可行的前提下，我们将根据您的要求向您提供您的个人信息副本。

## 8.5 响应您的请求

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者获取个人信息副本，或您认为平安科技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联系我们。为了保障安全，我们可能需要您提供书面请求，或提供您的身份证明文件，我们将在收到您反馈并验证您的身份后的 15 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的请求，我们可能会予以拒绝。

## 8.6 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) 与个人信息处理者履行法律法规规定的义务相关的；
- (2) 与国家安全、国防安全有关的；
- (3) 与公共安全、公共卫生、重大公共利益有关的；
- (4) 与犯罪侦查、起诉和审判和执行判决等有关的；
- (5) 有充分证据表明您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；
- (8) 涉及商业秘密的。

## **第 9 条 未成年人保护**

9.1 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（不满 14 周岁）不得使用。

9.2 对于经父母同意而收集儿童个人信息的情况，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儿童所必要的情况下使用或公开披露此信息。

9.3 如果我们发现在未事先获得可证实的父母同意的情况下收集了儿童的个人信息，则会设法尽快删除相关数据。

## **第 10 条 免责声明（非常重要）**

10.1 请您理解，由于计算机及互联网技术的飞速发展及同步速度的限制，可能存在或出现各种恶意或非恶意的攻击手段。虽然我们持续致力于提升和加强安全措施，以保护您的个人信息免遭意外或破坏，但仍无法始终保证您的个人信息的百分之百安全。

10.2 请您理解，您使用产品或服务时所用的系统和通讯网络，或硬件设备等我们均无法控制，请您了解并注意保护您的个人信息安全。

10.3 例如所有的企业都可能面临的问题一样，考虑到信息技术、网络空间本身的特点，在某些特殊情况下（例如黑客攻击、电信故障等），尽管我们采取了法律、法规等规定的必要的措施，但仍然存在个人信息泄露的风险。除非本隐私政策有其他规定，为了保护您的人身及财产安全，我们特别提醒您不要通过公共网络，向我们或任何以我们名义为您提供服务的第三方，提供您的账户密码、验证码、通信内容等信息。

## **第 11 条 本政策如何更新**

11.1 本隐私政策在页首载明生效日更新。

11.2 当适用的法律政策发生变更，或者我们的产品或服务功能发生重大变化的，我们的隐私政策可能变更。但是，未经您明确同意，我们不会削减您按照本隐私政策所应享有的权利。

## **第 12 条 您如何联系我们**

12.1 如您对本隐私政策的内容，或对我们如何处理您的个人信息，有任何疑问、意见、建议、担忧、投诉或举报，请按照如下方式联系我们：

联系地址：【深圳市南山区科技南十二路 20 号嘉联支付大厦】

我们会在 15 日内响应您的请求，并依据本隐私政策及法律法规处理您的请求。

12.2 在经与我们沟通后，如您对我们的答复不满意，您可以联系负责个人信息保护相关投诉的有关行业协会、主管部门，或者依据适用的法律向具有管辖权的法院提起诉讼。