
• 奕丰金融平台

隐私政策

本版本最新修改日期：2023 年 12 月 07 日

本版本生效日期：2023 年 12 月 07 日

引言

奕丰基金销售有限公司（以下简称“我们”）是经中国证券监督管理委员会核准的独立基金销售机构，受中国证券监督管理委员会的监督管理。奕丰基金销售有限公司主营业务是销售公募基金及其他金融理财产品，是中国证券投资基金业协会的联席会员及深圳市投资基金同业公会的会员。

公司名称：奕丰基金销售有限公司

统一社会信用代码：91440300310541398Q

中国证券监督管理委员会基金销售业务许可批准文号：深证局许可字[2015]123 号

中国证券监督管理委员会基金销售业务许可证书编号：000000381

中国人民银行金融机构编码：E2025144000018

我们深知个人信息对您的重要性，并非常重视您的隐私权利和个人信息保护，以及采取必要安全保护措施保护您的个人信息。感谢您的信任。

在您浏览我们的网站、奕丰 App、奕丰理财师 APP、财可夫斯基 APP 等互联网服务平台（合称“奕丰金融平台”），或使用我们的产品和服务时，我们将通过《奕丰金融平台隐私政策》（“本政策”）向您说明我们在您使用我们的服务时如何收集、使用、保存、共享和转让这些信息，以及我们为您提供的访问、更新、删除和保护这些信息的方式。

我们遵守法律法规和遵循以下隐私保护原则，向您收集和处理个人信息，并为您提供安全可靠的服务：

- 1、合法合理与必要原则；
- 2、用户自主选择原则；
- 3、安全与保护原则；
- 4、诚信、公开与透明原则。

本政策主要向您说明：

第一条、 释义

第二条、 目的、适用范围

第三条、 我们如何收集您的个人信息

第四条、 我们如何使用您的个人信息

第五条、 我们如何使用 Cookie 和同类技术

第六条、 我们如何共享、公开披露、转让披露您的个人信息

第七条、 我们可能向您发送的信息

第八条、 我们如何保存和保护您的个人信息

第九条、 您的权利

第十一条、我们如何保护未成年人的信息

第十一条、适用法律与争议解决

第十二条、修订变更

第十三条、您如何联系我们

请您在使用我们的服务前认真阅读并确认充分理解本政策，以便您做出您认为适当的选择。您使用或继续使用我们的服务，即意味着您已阅读本政策所有条款，对本政策条款的含义及相应的法律后果已全部通晓并充分理解，并且同意我们按照本政策收集、使用并保护您的个人信息。如果您不同意本政策的部分或全部内容、或对本政策内容有任何疑问，您应立即停止使用我们的服务。

本政策对与您的权益具有或可能具有重大关系的条款，及对我们的服务具有或可能具有免责或限制责任的条款用粗体字予以标注，请您注意。

您可以通过 App “我的-设置-《隐私政策》” 访问本政策文本。

第一条、释义

信息或个人信息：个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。请详见“我们如何收集您的个人信息”栏目。

个人敏感信息：个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健

康受到损害或歧视性待遇等的个人信息，因此个人信息中包含了个人敏感信息。

奕丰或“我们”：指奕丰基金销售有限公司。注册于深圳市前海深港合作区前湾一路1号A栋201室（入驻深圳市前海商务秘书有限公司），常用办公地点为深圳市南山区海德三道航天科技广场A座17楼1703-04室。

奕丰金融平台：指奕丰基金销售有限公司的官方网站、移动应用程序客户端、官方微信号，以及通过第三方服务机构访问等方式（包括但不限于H5链接跳转等方式），为个人用户直接或间接提供信息管理以及基金交易的基金销售服务平台。

第三方服务机构：指与奕丰基金销售有限公司签署相关合作或服务协议，同意根据协议约定并基于奕丰基金销售有限公司的基金销售服务，为客户提供账户开立、产品推介与销售、在线交易、信息中介与信息管理等服务的金融机构，以及或其他具备相关业务许可或完成必要备案流程的从业机构，以及为您使用我们的服务提供技术支持以及必要服务的其他第三方服务机构，包括但不限于我们的关联公司、持有相关业务资质的基金管理公司、基金销售公司、商业银行、证券公司、资产管理公司、基金支付结算机构、信息技术服务机构、信息发布平台、传播媒介等其他第三方服务机构。

未成年人：是根据《中华人民共和国未成年人保护法》规定的未满十八周岁的公民

第二条、 目的、适用范围

1、我们收集、存储、使用、加工、传输、提供、公开、删除您的信息是出于遵守《中华人民共和国网络安全法》、《中华人民共和国证券投资基金法》、《中华人民共和国反洗钱法》、《证券期货投资者适当性管理办法》、《非居民金融账户涉税信息尽职调查管理办法》及其他相关法律法规及监管部门要求，以及向您提供产品和服务及提升产品和服务质量的目的（包括支持我们开发新产品或完善已有产品功能，为您和其他客户提供更为优质或适合的产品和服务，向有权机关依法提供信息，与第三方服务机构合作为您和其他客户提供服务）。

2、本政策属于《奕丰金融平台服务协议》不可分割的一部分，未尽事宜遵照《奕丰金融平台服务协议》相关条款执行。本政策中涉及的相关术语，我们尽量以简明扼要的表述，除另有约定外，所用术语与《奕丰金融平台服务协议》中的术语释义具有相同的涵义。如您对本政策或相关事宜有任何问题，请联系我们。

3、本政策适用于我们通过奕丰金融平台向您提供的所有服务。但某些服务有其特定的隐私指引/声明，该特定隐私指引/声明更具体地说明我们在该服务中如何处理您的信息。如本政策与特定服务的隐私指引/声明有不一致之处，请以该特定隐私指引/声明为准。如本政策的条款与个人信息相关的法律法规或监管部门要求存在不一致或冲突之处，应当以相关的法律法规或监管部门要求为准。

4、需要特别说明的是，本政策不适用于部分第三方服务机构提供的服务。奕丰金融平台也可能含有到其他第三方服务

机构的网站的链接，我们对该等链接网站的信息保护措施不负责任。我们会依据法律法规的要求采取必要措施对相关网站进行审查，但我们无法保证该等链接网站的运营方会按照我们的要求采取保护措施。我们建议您查看该等网站的隐私政策，了解他们如何处理您的信息，以便审慎决策。

5、我们依据基金及反洗钱相关基金法律法规要求开展基金销售业务，仅面向年满十八周岁且具有完全民事行为能力的个人投资者提供基金销售服务。

第三条、我们如何收集您的个人信息

我们是一家从事基金销售服务的持牌机构，出于履行基金服务过程中法律法规和监管规定的法定义务（如客户身份识别及反洗钱职责、投资者适当性管理职责、风险防护措施），及向您提供各类产品和服务，以及提高产品和服务质量之需要，或为了与您进行联络、沟通，了解您的需求，建立、维护、发展与您的关系，我们会在您访问、浏览、使用我们移动应用程序、申请使用我们的服务、沟通联络的过程中，接收或留取您或相关方主动提供的个人信息，或依据法律法规、监管规定或您的授权或同意，通过适当方式向我们或其他第三方（包括但不限于合作金融机构、相关权力机关等）收集、查询、核实您及相关方的个人信息，我们收集的个人信息将在相应的用户服务协议当中向您充分说明。此外，您在使用服务的持续过程中，您有可能通过更新身份信息、更新调查问卷等信息等主动形式向我们提供个人信息。如果您不使用我们的服务，我们将停止收集相关个人信息。

1、我们对个人信息的收集范围

1.1、根据《信息安全技术个人信息安全规范》（GB/35273-2020）附录A(资料性附录)个人信息示例中表A.1个人信息举例，本政策涉及的个人信息包括：

- 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：有效身份证件的证件类型、证件号码、证件签发机关、证件有效期限
- 个人生物识别信息：面部识别特征、指纹
- 网络身份标识信息：个人信息主体账号、IP地址
- 个人教育信息：个人职业、学历、学位、教育经历、工作经历
- 个人财产信息：银行账户、鉴别信息（口令）、存款信息、信贷记录、交易和消费记录、流水记录
- 个人通信信息：电子邮件
- 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（如IMEI/Android ID/IDFA/OpenUDID/GUID/SIM卡IMSI信息等）等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

1.2、根据《个人金融信息保护技术规范》（JR/T0171-2020）“个人金融信息概述”，按照个人金融信息内容分类，本政策涉及的个人信息包括：

- 账户信息：账户开立时间、开户机构、账户余额以及基于上述信息产生的信息
- 鉴别信息：验证主体是否具有访问或使用权限的信息，包括登录密码、账户查询密码、交易密码、短信验证码

-
- 金融交易信息：在交易过程中产生的各类信息，包括但不限于交易金额、交易记录、交易日志、资产持仓信息
 - 个人身份基本信息：名称、性别、国籍、民族、职业、婚姻状况、家庭状况、收入情况、身份证件、手机号码、固定电话号码、电子邮箱、地址
 - 个人生物识别信息：指纹、人脸
 - 财产信息：指我们提供基金销售服务过程中，收集或生成的个人金融信息主体财产信息，包括但不限于个人收入状况、资产情况。

1.3、《个人金融信息保护技术规范》（JR/T0171-2020）还根据信息遭到未经授权的查看或未经授权的变更后所产生的影响和危害，将个人金融信息按敏感程度从高到低分为 C3、C2、C1 三个类别，其中本政策涉及的个人信息包括：

- C3 类别的用户鉴别信息：登录密码、交易密码、用于用户鉴别的个人生物识别信息
- C2 类别的可识别特定个人金融信息主体身份与金融状况的个人金融信息以及用于金融产品与服务的关键信息：证件类识别标识与证件信息、手机号码、账户登录的用户名、用户鉴别辅助信息、个人财产信息、交易信息、满足监管需要的影像信息及其他能够识别出特定主体的信息
- C1 类别的供金机构内部使用的个人金融信息：账户开立时间、开户机构、基于账户信息产生的支付标记信息、C2 和 C3 类别信息中未包含的其他个人金融信息

1.4、根据《信息安全技术个人信息安全规范》（GB/35273-2020）附录 B（资料性附录）-个人敏感信息判定-表 B.1，本政策涉及的个人敏感信息包括：

- 个人身份信息：有效身份证件的证件类型、证件号码、证件签发机关、证件有效期限
- 个人生物识别信息：面部识别特征、指纹
- 个人财产信息：银行账户、鉴别信息（口令）、存款信息、信贷记录、交易和消费记录、流水记录
- 其他信息：精准定位信息

2、我们在基础业务功能场景、拓展业务功能场景收集的个人信息和设备权限

《信息安全技术个人信息安全规范》（GB/ 35273-2020）附录 C（资料性附录）将物品，我们所提供的产品服务分为基础业务和拓展业务。

2.1、为实现我们提供的基础业务功能，我们必须向您收集个人信息的场景

向您提供基金销售服务是我们服务的基本业务功能，如果您不同意我们收集基本业务功能所必要收集的个人信息，我们将无法向您提供基金销售服务。为了您可以正常使用我们的基金销售服务，我们会在下列情形及业务场景下收集您的相关个人信息，同时也可能从合法存储您相关信息的第三方处收集您的个人信息：

2.1.1、注册平台账户

当您注册我们平台账户时，您需要提供手机号码及手机验证码。如果您拒绝提供这部分信息，您可能无法完成注册

或无法正常使用我们服务。若您选择跳过绑定银行卡步骤，您将停留在平台账户注册阶段，无法使用我们提供的基金销售服务。

根据《中华人民共和国网络安全法》、《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》收集您在使用平台账户时的设备型号**浏览器类型**、**访问日期和时间**、**登录 IP 地址**作为日志内容进行保存，根据《中华人民共和国网络安全法》规定，我们将保留日志不少于 6 个月。

2.1.2、注册基金交易账户

平台账户是开通基金交易账户的基础。当您通过手机号码注册平台账户成功后，您可以进一步通过绑定银行卡完成实名认证以开立基金交易账户，使用我们的基金销售服务。

在注册过程中，我们会根据《中华人民共和国网络安全法》、《移动互联网应用程序信息服务管理规定》、《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》，需要您提供**姓名、性别、国籍、身份证明文件的类型、号码和有效期限、银行卡卡号、银行预留手机号、联络手机号码、电子邮箱、联络地址、个人职业**，**填报税收居民身份信息、实际受益人信息、实际控制人信息和不良诚信记录**，同时您授权我们前述信息与相应商业银行或基金支付结算机构进行身份验证，我们会收集您在使用我们服务时设置的**交易密码**，作为每次提供交易指令或开通功能的授权指令。

我们还会根据《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》中“第三条 客户交易终端信息是指客户通过证券期货经营机构下达交易指令的交易终端特征代码。客户交易终端信息是客户委托记录、交易记录的重要组

成部分，包括但不限于以下内容：电话号码、互联网通讯协议地址（IP 地址）、媒介访问控制地址（MAC 地址）以及其他能识别客户交易终端的特征代码。”的要求收集您的如上信息。并根据中国人民银行及基金管理公司的要求，将您填写的身份信息报送至上述机构。

- 风险承受能力调查服务

为履行投资者适当性管理义务，在您开通使用基金销售服务前，当您注册基金交易账户后，开始基金交易前，我们会依据《证券期货投资者适当性管理办法》，通过《风险承受能力调查评估问卷》对您向您收集**收入来源和数额、资产与债务的财务状况、投资相关的学习工作经历、投资经验、投资期限、投资品种、期望收益、投资目标、市场波动反应**。如您拒绝提供前述个人信息，则可能无法使用我们提供的基金交易服务，但不影响您使用我们提供的其他服务。

2.1.3、基金销售服务

当您通过账户认申购基金产品或服务时，需要您提供**选定投资标的、下单金额、确认风险匹配信息（如有）、选定订单支付方式**，输入您设置的**交易密码**完成交易申请。当您通过账户赎回基金产品或服务时，需要您提供**选定投资标的、下单份额数量/金额、选定赎回资金到账路径**，输入您设置的**交易密码**完成交易申请。为了保障交易安全，加强数据记录和留痕，在您申请每一次认申购、赎回等交易时，我们会同步收集您发出申请的个人常用设备信息，包括设备 **MAC 地址、软件列表、唯一设备识别码（如IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等）**

2.1.4、银行账户（卡）变更服务

当您申请变更已绑定在账户的银行卡时，我们按照《中华人民共和国反洗钱法》等有关法律

法规要求，需要对您的银行账户（卡）信息进行真实性核验，我们可能需要您以面对面视频形式向我们展示您的本人人像照片及凭证材料，或通过邮寄的方式提供银行卡注销证明原件。为了更进一步保证大额交易用户的资金安全，我们也会要求上传其他相应的凭证。

2.1.5、忘记密码功能

当您忘记密码使用找回密码功能时，如果手机号码没有变化可以正常接受我们的验证短信，您需填写身份证号码、姓名，凭手机短信验证码即可在线完成重置密码。

2.1.6、基于产品业务功能收集使用您的信息，我们逐项列举如下表所示：

分类：风控安全

面部解锁：收集个人信息类型为网络身份标识信息、个人生物识别信息。具体个人信息字段为个人主体账号信息、面部 ID、。

发送日志：收集个人信息类型为个人常用设备信息、个人通信信息、个人基本资料，具体个人信息字段为设备信息、唯一设备识别码、运营商信息、电话号码。

用户同意本《隐私政策》后，应用程序将在后台状态下获取用户的 ANDROID ID, MAC 地址，用于 SDK-Sentry 库上报用户使用应用程序过程中发生的崩溃日志。未获得用户同意前将不会在后台状态收集用户上述个人常用设备信息。

分类：常用功能

信息推送：收集个人信息类型为个人上网记录。具体个人信息字段为**设备信息、交易记录**。

基金搜索：收集个人信息类型为个人上网记录。具体个人信息字段为**搜索记录、浏览记录、点击记录**。

关注、收藏、自选基金：收集个人信息类型为个人上网记录、网络身份标识信息。具体个人信息字段为**关注记录、个人主体账号信息**。

分类：登录和个人信息管理

登录：收集个人信息类型为个人基本资料、网络身份标识信息、个人生物识别信息。具体个人信息字段为**手机号（手机号登录时所需）、身份证号（身份证号登录时所需）、个人主体账号信息及**相关数字口令信息、登录密码、手机号、验证码、指纹（指纹登录时所需）****。

银行卡管理：收集个人信息类型为个人基本资料、个人身份信息、个人财产信息、个人上网记录。具体个人信息字段为**姓名、证件号码、银行卡号、银行卡预留手机号、操作记录**。

合格投资者申请：收集个人信息类型为个人基本信息、个人财产信息。具体个人信息字段为**身份证明文件的类型、号码和有效期限，收入或资产证明、婚姻证明**。

个人信息更改：收集个人信息类型为个人基本资料、个人身份信息、个人财产信息、个人教育工作信息、个人上网记录。具体个人信息字段为**姓名、性别、国籍、身份证明文件的类型、号码和有效期限、银行卡卡号、银行预留手机**

号、联络手机号码、电子邮箱、联络地址、个人职业，填报税收居民身份信息、实际受益人信息、实际控制人信息和不良诚信记录。

分类：交易管理

重新进行风险承受能力调查：收集个人信息类型为个人教育工作信息、个人财产信息、个人上网记录。具体个人信息字段为收入来源和数额、资产与债务的财务状况，投资相关的学习工作经历、投资经验，投资期限、投资品种、期望收益、投资目标，市场波动反应。

交易与撤单：收集个人信息类型为个人财产信息、网络身份标识信息。具体个人信息字段为选定投资标的、下单份额数量/金额、确认风险匹配信息（如有）、选定订单支付方式、选定赎回资金到账路径、交易密码。

2.2、为实现我们提供的拓展业务功能，您可选择授权我们收集个人信息的场景

基于使用便利和安全的角度，您在使用我们 App 时需要按需授权以下功能：

2.2.1、您在苹果客户端中，涉及拓展业务功能的授权情况

通知：允许 App 向您提供交易信息提醒通知。若您停止授权该权限，您可以通过您终端设备上的设置菜单中的通知，找到 App，关闭“允许通知”，这将会影响向您提供交易信息提醒通知，但并不影响您使用我们的其他服务。涉及个人信息：设备信息

无线网络：允许 App 使用 WLAN 与蜂窝移动网。若您停止授权该权限，您可以在您的终端设备上的设置菜单中的无线局

域网内关闭“WLAN 与蜂窝移动网”或仅关闭“WLAN”，若您选择同时关闭“WLAN 与蜂窝移动网”将会影响您使用我们的服务。涉及个人信息：网络信息

相机权限：在您使用身份认证、扫码支付、银行卡识别、身份证识别以及人脸识别登录等服务时，允许 App 获取您的相机权限。若您停止授权该权限，您可以在您的终端设备上的设置菜单中的隐私-相机，找 App，关闭“允许相机”，这将会影响您使用扫描识别功能及拍摄上传材料的功能，但并不影响您使用我们的其他服务。涉及个人信息：设备信息

相册权限：在您进行身份认证等图像上传功能并选择上传相册中的图片时，允许 App 获取您的相册权限。若您停止授权该权限，您可以在您的终端设备上的设置菜单中的隐私-相册，找到 App，关闭“允许相册”，这将会影响身份认证功能的正常使用，但是不影响您使用我们 APP 的其他功能。涉及个人信息：相册文件

地理位置权限：在您进行地址信息填报时，允许 App 获取您的地理位置权限。若您停止授权该权限，您可以在您的终端设备上的设置菜单中的隐私-位置服务，找到 App，关闭“允许使用位置服务”，这将会影响您在使用地址自动填写功能，但并不影响您使用我们的其他服务。涉及个人信息：位置信息

指纹权限：允许 App 调用您设备的指纹验证系统，帮助我们完成您个人身份识别、登录、鉴权等指令操作。若您停止授权该权限，您可以在您的终端设备上的“设置”找到 App，关闭指纹权限，这将会影响您在使用了指纹相关功能，但并不影响您使用我们的其他服务。涉及个人信息：指纹信息

传感器权限：在您使用拍照录像相关功能时，允许 APP 获取您的陀螺仪传感器, 加速度传感器, 重力传感器信息，用于获取拍摄手机角度。若您停止授权该权限，您可以在您的终端设备上的“设置”找到 App，关闭传感器权限，这将会影响您正在使用的拍照录像相关功能，但并不影响您使用我们的其他服务。涉及个人信息：**设备信息**

您可以通过“我的-设置-权限管理”修改对我们的授权。

2.2.2、您在安卓客户端中，涉及拓展业务功能的授权情况

存储权限：允许 APP 缓存图片基金自选数据，以及读取设备上的照片、媒体内容及文件。若您停止授权该权限，您可以在您的终端设备上的“设置”找到 App，关闭存储权限。涉及个人信息：**设备信息**

电话权限：允许您在 App 中唤起电话拨打功能和致电奕丰客服中心，以及允许获取设备 MAC 地址、IMEI、IMSI、MEID 和 Android_id 等设备信息用于校验设备信息，供账号安全及反洗钱审查使用。若您停止授权该权限，您可以在您的终端设备上的“设置”找到 App，关闭电话权限，关闭后不会影响您使用我们的其他服务。涉及个人信息：**设备信息**

访问网络：允许 App 使用网络。若您停止授权该权限，您可以在您的终端设备上的“设置”找到 App，关闭网络，关闭后您将无法使用我们的服务。涉及个人信息：**网络信息**

相机权限：在您使用身份认证、扫码支付、银行卡识别、身份证识别以及人脸识别登录等服务时，允许 App 获取您的相机权限。若您停止授权该权限，您可以在您的终端设备上的

“设置”找到 App，关闭相机权限，这将会影响您使用扫描识别功能及拍摄上传材料的功能，但并不影响您使用我们的其他服务。涉及个人信息：设备信息

相册权限：在您进行身份认证等图像上传功能并选择上传相册中的图片时，允许 App 获取您的相册权限。若您停止授权该权限，您可以在您的终端设备上的“设置”找到 App，关闭相册权限，这将会影响身份认证功能的正常使用，但是不影响您使用我们 APP 的其他功能。涉及个人信息：相册文件

地理位置权限 在您进行地址信息填报时，允许 App 获取您的地理位置权限。若您停止授权该权限，您可以在您的终端设备上的“设置”找到 App，关闭位置权限，这将会影响您在使用地址自动填写功能，但并不影响您使用我们的其他服务。涉及个人信息：位置信息

指纹权限：允许 App 调用您设备的指纹验证系统，帮助我们完成您个人身份识别、登录、鉴权等指令操作。若您停止授权该权限，您可以在您的终端设备上的“设置”找到 App，关闭指纹权限，这将会影响您在使用的指纹相关功能，但并不影响您使用我们的其他服务。涉及个人信息：**指纹信息**

传感器权限：在您使用拍照录像相关功能时，允许 APP 获取您的陀螺仪传感器,加速度传感器,重力传感器信息，用于获取拍摄手机角度。若您停止授权该权限，您可以在您的终端设备上的“设置”找到 App，关闭传感器权限，这将会影响您在使用的拍照录像相关功能，但并不影响您使用我们的其他服务。涉及个人信息：**设备信息**

您可以通过“我的-设置-权限管理”修改对我们的授权。

2.2.3、您在使用 App 的拓展业务功能中，可能开启您的设备访问权限的情况

联系客服：为方便客户联系客服，可直接在 APP 中唤起电话；为了能在使用在线客服时直接给客服发送语音。访问和使用的权限：电话权限

身份认证：拍照上传。访问和使用的权限：相机权限、相册权限

保存图片：保存图片到本地。访问和使用的权限：写外部存储权限

缓存图片：为了让客户的浏览更顺畅，适当缓存图片。访问和使用的权限：存储权限

信息推送：向您提供重要事项的通知，包括交易状态通知等。访问和使用的权限：通知权限、悬浮窗权限

面部解锁：登录（IOS）。访问和使用的权限：面部 ID

指纹解锁：登录解锁、支付解锁。访问和使用的权限：指纹

社交分享：使用微信分享功能时，判断是否安装相应应用。访问和使用的权限：获取应用安装列表

微信登录：使用微信登录功能时，判断是否安装微信。访问和使用的权限：获取应用安装列表

3、我们从第三方服务机构获取的个人信息

3.1、您通过奕丰金融平台触发、申请、使用第三方服务机构服务时，我们将会获得您的个人信息。为履行基金销售服务的法定义务，我们将在取得您同意授权下，依法将您的个人信息发送给商业银行、基金支付结算机构、基金管理公司

等第三方服务机构，由第三方服务机构依法完成对您的实名认证服务、银行账户归属认证、提供基金支付结算服务等服务，并向我们依次反馈服务结果和您的相关个人信息。

3.2、我们可能会获得您在使用已授权第三方服务机构服务时所产生或共享的信息。当您基于我们的服务与第三方服务机构进行互动，或使用第三方服务机构提供的相关产品或服务时，为我们与第三方服务机构共同向您提供服务、开展信息交叉验证及提高服务质量和用户体验的需要，您同意并授权我们在法律法规的允许范畴内，收集您在使用第三方服务机构提供的产品或服务的过程中，在该等第三方服务机构留存或形成的、与我们的服务相关的个人信息。除法律法规另有规定外，第三方服务机构会在征得您同意、授权的前提下，向我们提供由第三方服务机构收集或者储存的您的信息。如果您想取消该等同意、授权，您可以遵循第三方服务机构提供的联系方式或隐私政策规定向其提出相应的要求。请您仔细阅读第三方服务机构的用户协议及隐私政策。

4、您需充分知晓，在以下根据《信息安全技术 个人信息安全规范》（GB/T 35273—2020）5.6 章

节的例外情形及其他例外情形中，我们可能收集、使用您的个人信息无需征得您的授权同意：

- 4.1、与国家安全、国防安全直接相关的；
- 4.2、与公共安全、公共卫生、重大公共利益直接相关的；
- 4.3、与公检法等执法部门法律程序直接相关的，如刑事侦查、起诉、审判和判决执行等；

-
- 4.4、与履行国家法律法规及监管部门有关规定的义务相关的；
 - 4.5、所收集的个人信息是您自行向社会公众公开披露的；
 - 4.6、从合法公开披露的信息中收集的您的个人信息的，如合法的新闻报道、政府信息公开等渠道；
 - 4.7、根据您的要求签订和履行合同所必需的；
 - 4.8、履行法律法规规定的义务相关，以及用于维护我们所提供的产品与/或服务的安全稳定运行所必需的，例如识别、处置金融产品与/或服务的故障、欺诈或被盗用等；
 - 4.9、出于维护您或其他个人的财产等重大合法权益但又很难得到您本人同意的。

第四条、 我们如何使用您的个人信息

1、为了遵守国家法律法规及监管要求，以及向您提供服务及提升服务质量，或保障您的账户和资金安全，我们可能会在以下情形中使用您的个人信息，并在使用中采取合理必要的措施保障安全：

1.1、实现本政策中“我们如何收集个人信息”所述目的及向您提供相关服务。

1.2、为了确保我们向您提供的服务或产品的安全性，在您使用我们提供的服务时，我们将您的信息用于身份验证、客户服务、安全防范、诈骗检测、预防或禁止非法活动、存档和备份用途。

1.3、为履行法律法规规定义务、配合有权部门组织实施的统计、档案管理活动，履行监管协查义务，我们会在前述领

域继续使用此前收集的您的相关个人信息，但我们会采取严格的保护措施。

1.4、为提升您的产品或服务体验，或为防范风险，我们会采取脱敏、匿名化方式对您的身份信息、交易信息及联系方式等信息进行综合统计、分析或加工等处理，以改善我们现有产品或服务。但这些信息不会包含您的任何身份识别信息。

1.5、为了维护您或其他第三方商业主体或我们的权益，或者为了解决与您相关的争议。

1.6、经您授权同意的，以及于法律法规允许的其他用途。

2、当我们要将信息用于本政策未载明的其他用途时，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动作等形式再次征求您的同意。

第五条、 我们如何使用 Cookie 和同类技术

您访问和使用我们的服务时，我们或奕丰合作伙伴可能通过放置安全的 Cookie 及相关技术（包括但不限于 Cookie，移动客户端本地存储、Flash Cookie，或您的浏览器或关联应用程序提供的其他本地存储）收集您的信息并识别您的身份，以帮助您省去重复输入注册信息的步骤，或者帮助判断您的账户安全状态。

我们会严格要求奕丰合作伙伴遵守本政策的相关要求。您可以通过计算机浏览器或移动设备设置管理 Cookie。但请注意，如果停用 Cookie，您可能无法享受最佳的服务体验，某些服务也可能无法正常使用。

我们不会将 Cookie 用于本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 Cookie。您可以清除计算机浏览器或移动设备上保存的所有 Cookie，大部分计算机浏览器或移动设备都设有阻止 Cookie 的功能。

第六条、 我们如何共享、公开披露、转让您的个人信息

1、共享

我们承诺会根据相关法律法规及监管部门要求对您的信息承担保密义务，但为了向您提供服务之目的，我们可能会将您的信息与第三方服务机构共享。我们只会共享必要的个人信息，且受本政策中所声明目的的约束。第三方服务机构如要改变信息的处理目的，将再次征求您的授权同意。在共享信息前，我们会对合作机构或其他相关第三方进行商业上合理的审查，评估其收集信息的合法性、正当性、安全性以及必要性，并督促他们按照法律法规及监管部门要求来处理您的信息，一旦发现其违反约定将采取有效措施甚至终止合作。

1.1、在符合法律法规及监管部门的前提下和经您事先明确授权同意的情况下，为了您与我们以及第三方服务机构建立服务关系、完成交易程序、实现交易目的，我们需要向第三方服务机构提供您的身份信息、银行账户信息、账号信息和其他满足本政策目的所需收集的个人信息，法律法规及监管部门禁止提供的个人信息除外。我们共享您的信息用于以下用途：

1.1.1、为了完成您的交易，履行相应合同的需要，或为落实反洗钱、涉税信息尽职调查等法律法规要求、行政监管要

求和司法机关要求的情况下向有权机关或第三方服务机构提供；

1.1.2、某些情况下，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，或为了维护您或我们或第三方的合法权益所采取的措施；

1.1.3、履行我们在《奕丰金融平台服务协议》或本政策中的义务和行使我们的权利而提供。

1.1.4、为满足内部审计的需要，向我们的审计机构提供必须信息。

1.2、仅为实现增值服务的目的和经过您的事先明确授权同意的情况下，我们可能会与第三方服务机构（包括但不限于关联公司、基金管理公司、商业银行、基金支付结算机构、第三方服务供应商、承包商、合作伙伴、应用开发者等，例如，代表我们发出电子邮件或推送通知的通讯服务提供商）共享您的个人信息，让第三方服务机构按照我们的说明、本政策以及其他相关的保密和安全措施来为我们处理上述信息，并用于以下用途：

1.2.1、向您提供增值服务；例如您选择参与我们和第三方服务机构联合展开的活动，包括但不限于抽奖、竞赛等活动，我们可能与其共享活动过程中产生的、为了完成活动所必要的信息，以便第三方服务机构能及时向您发放奖品或提供服务；例如法律法规允许的范围内，授权已取得您明确同意的第三方商业主体向我们查询、采集您在我们的个人信息。

1.2.2、实现“我们如何使用您的个人信息”部分所述目的；

1.2.3、理解、维护和改善我们的服务。

如我们与上述第三方服务机构共享您的信息，我们将会采用加密、匿名化处理等手段保障您的信息安全。共享前，我们将开展个人信息安全影响评估，对第三方服务机构的个人信息安全防护能力水平提出要求，确认其采集个人信息行为的合法性、正当性、安全性、必要性，与其签订保密协议，对其查询行为进行监控，督促其遵守国家法律法规及协议中约定的安全防护措施和保密条例，一旦发现其违反协议约定将会采取有效措施甚至终止合作：

1.3、移动应用程序的软件开发工具包 SDK 说明

为了您能使用我们的移动应用程序功能，我们会在移动应用程序中嵌入授权合作伙伴的软件开发工具包 SDK（简称 SDK）或其他类似程序。我们按照合法合理与必要原则对相关第三方 SDK 进行信息安全影响评估。在您同意本政策之前，第三方 SDK 不会收集您的个人信息。

当前 App 中存在的第三方 SDK 的使用目的、权限获取情况逐项列举：

1.3.1、高德地图 SDK

使用目的：用于定位服务获取地理位置

官网链接：<https://lbs.amap.com>

隐私政策链接：<https://lbs.amap.com/pages/privacy>

请求权限情况：获取大概的位置、获取精确位置、查看 WLAN 连接、获取 wifi 状态、改变 wifi 状态、读取手机状态和身份、读取外部存储卡、写入外部存储卡、申请调用 A-GPS 模块、蓝牙权限

收集个人信息类型：位置信息、设备信息、网络信息

使用场景：用户填写地址信息业务场景

1.3.2、微信分享 SDK

使用目的：用于微信登录及分享服务

官网链接：<https://open.weixin.qq.com>

隐私政策链接：https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy

请求权限情况：查看 WLAN 连接、读取手机状态和身份、读取外部存储卡、写入外部存储卡、读取 MAC 地址、软件安装列表权限

收集个人信息类型：设备信息、网络信息、MAC 地址、软件安装列表

使用场景：用户点击微信登录或分享文章等资讯业务场景

1.3.3、极光推送 SDK (cn.jpusth.android)

使用目的：用于向手机客户端推送消息通知服务

官网链接：<https://www.jiguang.cn>

隐私政策链接：<https://www.jiguang.cn/license/privacy>

请求权限情况：设备参数及系统信息、设备标识符、网络信息、应用列表信息

收集个人信息类型：

设备参数及系统信息(设备类型、设备型号、系统版本、及相关硬件信息)：用于识别用户的设备类型、设备型号、系统版本等，确保消息准确下发；

设备标识符 (IMEI、IDFA、Android ID、GAID、MAC、OAID、VAID、AAID、IMSI、MEID、UAID、硬件序列号信息、ICCID、

SIM 信息)：用于识别唯一用户，保证推送的精准送达及推送信息的准确统计；

网络信息(IP 地址、WiFi 信息、基站信息、DNS 地址、DHCP 地址、SSID、BSSID)与位置信息(经纬度)：用于优化 SDK 与极光服务器的网络连接请求，保证服务的稳定性和连续性，同时实现区域推送功能；

应用列表信息(应用崩溃信息、通知开关状态、APP 应用列表及活跃状态、APP 应用页面信息、APP 功能事件相关信息)：当一个设备有多个 APP 的推送链路同时活跃时，我们采用合并链路技术，随机合并成一条链路，以达到为用户节省电省流量的目的。

数据处理方式：通过去标识化、加密传输及其他安全方式

使用场景：用户向客户端发送消息通知业务场景

自启动和关联启动说明：为确保本应用处于关闭或者后台运行状态下可以正常接收客户端推送的重要的交易类消息通知，本应用须开启自启动能力，将存在一定频率通过收集系统发送广播唤醒本应用的自启动行为，此为实现本应用功能及服务所必要的。

本应用在后台时应用获取 BSSID, IP 地址, SSID 个人信息说明：为保证本应用处于关闭或者后台运行状态下可以接收客户端推送的重要交易栏消息通知，本应用须获取 BSSID, IP 地址, SSID 信息，用于优化 SDK 与极光服务器的网络连接请求，保证服务的稳定性和连续性，同时实现区域推送功能。

1.3.4、北京腾云天下 SDK (Talking Data 库、TalkingData 移到应用分析统计)

使用目的：用于应用软件数据统计和分析

官网链接：<https://www.talkingdata.com>

隐私政策链接：
https://www.talkingdata.com/privacy.jsp?languagetype=zh_cn

请求权限情况：访问网络、获取网络状态、读取手机设备 MAC 地址及唯一设备标识码 IMEI 码、Android_ID、写入外部存储卡、设备位置信息权限、接收短信权限、读取短信权限、获取运行中进程信息、获取已安装的应用、获取设备传感器、监听传感器

收集个人信息类型：设备信息、网络信息、地理位置信息、应用信息

使用场景：用户进行交易时收集用户操作流程业务场景，收集频率由用户交易次数决定，用于数据统计分析

1.3.5、io.sentry SDK (Sentry 库、React Native, sentry-android, io.sentry.react)

使用目的：用于上报应用使用过程中发生的崩溃信息

官网链接：<https://github.com/joshdholtz/Sentry-Android>

隐私政策链接：<https://sentry.io/privacy/>

请求权限情况：获取运行中进程信息、获取设备传感器、监听传感器

收集个人信息类型：应用信息、设备信息。用户同意本《隐私政策》后，应用程序将在后台状态下获取用户的 ANDROID ID, MAC 地址，用于 SDK-Sentry 库上报用户使用应

用程序过程中发生的崩溃日志。未获得用户同意前将不会在后台状态收集用户上述个人常用设备信息。

使用场景：用户使用客户端时发生异常或者崩溃时发送错误日志业务场景，便于开发工程师排查问题，收集频率由客户端崩溃次数决定

1.3.6、asyncstorage SDK

使用目的：用于应用本地存储数据的开源工具类

官网链接：<https://github.com/react-native-community/async-storage>

请求权限情况：获取粘贴板信息

收集个人信息类型：应用信息

使用场景：用户获取转账银行卡卡号点击复制业务场景，收集频率由用户点击次数决定

1.3.7、react SDK

使用目的：用于构建用户界面的 JavaScript 库

官网链接：<https://github.com/facebook/react>

请求权限情况：获取粘贴板信息

收集个人信息类型：应用信息

使用场景：用户获取转账银行卡卡号点击复制业务场景，收集频率由用户点击次数决定

1.3.8、小米推送 SDK

使用目的：推送消息

官网链接：<https://dev.mi.com/console/appservice/push.html>

隐私政策链接：

<https://dev.mi.com/console/doc/detail?pId=1822>

请求权限情况：设备标识符（Android ID、OAID、GAID）

收集个人信息类型：设备信息

使用场景：在小米手机终端推送消息时使用

1.3.9、华为 HMS SDK

使用目的：推送消息

官网链接：<https://developer.huawei.com/consumer/cn/>

隐私政策链接：

<https://developer.huawei.com/consumer/cn/doc/development/HMSCore-Guides/sdk-data-security-0000001050042177>

请求权限情况：应用基本信息、应用内设备标识符、设备的硬件信息、系统基本信息和系统设置信息

收集个人信息类型：应用信息、设备信息

使用场景：在华为手机终端推送消息时使用

1.3.10、OPPO 推送 SDK

使用目的：推送消息

官网链接：https://open.oppomobile.com/new/introduction?page_name=oppopush

隐私政策链接：

<https://open.oppomobile.com/wiki/doc#id=10288>

请求权限情况：IMEI、ICCID、IMSI、Android ID、GAID、应用包名、版本号和运行状态、IP 或域名连接结果，当前网络类型

收集个人信息类型：设备信息、网络信息、应用信息

使用场景：在 OPPO 手机终端推送消息时使用

1.3.11、vivo 推送 SDK

使用目的：推送消息

官网链接：<https://dev.vivo.com.cn/promote/pushNews>

隐私政策链接：<https://www.vivo.com.cn/about-vivo/privacy-policy>

请求权限情况：设备标识符（Android ID、OAID、GAID）

收集个人信息类型：设备信息

使用场景：在 vivo 手机终端推送消息时使用

1.4、共享信息的特别情形：

1.4.1、根据法律法规及合理商业习惯，在我们与其他公司合并或被其收购或进行其他资本市场活动（包括但不限于IPO，债券发行）时，以及其他情形下我们接受来自审计、法律等其他主体的尽职调查时，我们可能需要把您的信息提供（共享）给必要的第三方商业主体，但我们会通过和这些主体签署保密协议等方式要求其对该等信息采取合理的保密措施，要求其按照相关法律法规及监管部门要求处理您的信息，且完成必要工作后在合理的期限内删除您的信息。

1.4.2、当您与他人因使用我们的服务发生争议时，为了保护您及他人的合法权益，我们可能会将您的姓名及有效证件号码、联系方式和与争议相关的信息提供（共享）给监管部门或您与他人协议约定的其他争议解决机构，以便及时解决纠纷，但法律法规明确禁止提供的除外。例如，为了处理您的交易纠纷或争议，我们可能需要向银行或交易对手方提供（共享）交易信息或您的个人信息。

1.4.3、我们有理由确信需要遵守法律法规及监管部门要求所采取的措施。例如为执行相关服务协议或本政策、维护社会公共利益，为保护我们的客户、我们或我们的关联公司、

其他用户或雇员的人身财产安全或其他合法权益合理且必要的用途。

1.4.4、在法律法规及监管部门允许的范围内，已取得您明确授权同意的第三方商业主体（包括但不限于第三方服务机构）根据您的授权范围向我们查询、采集您在我们的个人信息。

2、公开披露

2.1、原则上我们不会公开披露您的个人信息，但以下情况除外：

2.1.1、事先获得您的明确授权同意。

2.1.2、为遵守适用的法律法规、诉讼目的或者监管部门、行政机关、司法机构或其他法定授权组织的要求依法提出的要求而公开披露您的个人信息。如果我们确定您出现违反适用的法律法规的情况，或为保护我们及我们关联方或其他用户或公众的权利、财产或安全免遭损害，我们也可能公开披露关于您的信息，包括相关违规行为以及我们已对您采取的措施。

2.1.3、因您参与活动获益、按照活动规则予以公开披露。例如在中奖活动名单需要公示的中奖用户登录名以及脱敏后的其他信息。

2.1.4、公开披露前，我们将向您告知公开披露的目的、类别。我们将开展信息安全影响评估，根据评估结果采取有效措施保护您的权益，并准确记录和保存公开披露的情况，包括日期、规模、目的、内容、公开范围等。

2.1.5、我们通过技术手段对数据进行去标识化处理后，去标识化处理的信息将无法识别主体。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；在不透露您个人信息的前提下，我们有权对用户数据库进行分析并予以商业化的利用。例如，我们将收集到的信息用于分析形成不包含任何个人信息的分析报告。我们可能对外公开并与我们的合作伙伴共享经统计加工后不含身份识别内容的信息，用于了解用户如何使用我们服务或让公众了解我们服务的总体使用趋势。除法律另有规定外，为了提升信息处理效率，降低信息处理成本，或提高信息处理准确性，我们可能会委托有能力的数据服务机构代表我们，在遵循本政策以及授权范围的情况下对您的信息进行加工、分析、处理。

3、转让

我们不会将您的个人信息转让给任何公司、组织或个人，但以下情况除外：

- 3.1、事先获得您的明确授权同意。
- 3.2、根据法律法规或强制性的行政要求、司法要求。
- 3.3、在涉及资产转让、收购、合并兼并、分立、重组、解散或破产清算时，涉及到的个人信息转让。

我们将在转让前向您告知转让的目的、内容，并开展信息安全影响评估，根据评估结果采取有效措施保护您的权益。我们将要求新的持有您个人信息的公司、组织继续受法律法规及本政策的约束，签署数据保护责任承诺。如变更个人信息使用目的时，我们将要求该公司、组织重新取得您的明确授权同意。

4、共享、公开披露、转让的例外情形

根据相关法律法规，在以下情形中，我们可能会依法共享、公开披露、转让您的个人信息而无需征得您的授权同意：

- 4.1、与国家安全、国防安全直接相关的；
- 4.2、与公共安全、公共卫生、重大公共利益直接相关的；
- 4.3、与公检法等执法部门法律程序直接相关的，如犯罪侦查、起诉、审判和判决执行等；
- 4.4、与履行国家法律法规及监管部门有关规定的义务相关的
- 4.5、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及时得到您本人授权同意的；
- 4.6、您自行向社会公众公开披露的个人信息；
- 4.7、从合法公开披露的信息中收集的您的个人信息的，如合法的新闻报道、政府信息公开等渠道。

第七条、 我们可能向您发送的信息

作为基金销售服务机构，我们仅在法定情形和必要情况下发送电子邮件、短信或推送通知等方式向您发送与基金服务相关的通知或公告，例如您的交易申请出现份额确认失败，您持份的基金产品出现法定重大事项，身份验证或安全验证等情形。

如您不愿接受这些信息，您可以通过信息中提供的退订方式予以退订，或通过 App “我的-设置-消息通知” 按您需要分别关闭 App 通知、短信通知、邮件通知。

第八条、 我们如何存储和保护您的个人信息

请您务必妥善保管好您的个人信息。在您使用各项服务时，我们会通过涉及身份要素的个人信息识别您的身份，如您泄露了前述信息将可能蒙受损失；互联网并非绝对安全的环境，电子邮件、即时通讯、及与一些在线交流方式并未加密，我们强烈建议您不要通过此类方式发送个人信息；请您使用复杂密码，协助我们保证您的账号安全。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。

我们承诺为您的信息提供相应的安全保障，以防止信息的丢失、不当使用、未经授权访问或披露。

1、存储

1.1、我们根据法律法规及监管部门要求，将中华人民共和国境内收集和产生的个人信息存储于中华人民共和国的境内，并依法对这些信息进行严格保密。

我们根据《证券期货投资者适当性管理办法》、《基金募集机构投资者适当性管理实施指引(试行)》的规定，投资者适当性相关信息内容应至少保存 20 年，同时根据《证券投资基金销售业务信息管理平台管理规定》基金投资人信息和交易备份应当在不可修改的介质上保存 15 年的要求，我们将按监管机构要求额最高年限妥善保管本指引内所述的您的个人信息，并将对其至少保存 20 年，超过上述个人信息保存期限后，我们会对个人信息进行匿名化或删除处理。

在您终止我们所提供的所有服务后，我们会停止对您的信息的收集和使用，法律法规或监管部门另有规定的除外。

2、去标识化处理

2.1、我们承诺收集您的个人信息后，采取合理必要的保护措施来保护您的个人信息。当需要通过脱敏处理您的个人信息时，我们将通过技术手段对数据进行去标识化处理，去标识化后的数据为不可逆或可用于可逆恢复识别的数据分开存储，确保去标识化处理的信息无法重新识别个人主体。如果我们出现停止运营的情况，我们将立即停止收集您个人信息的行为，对所存储的所有个人信息进行删除或匿名化处理，并以逐一送达或公告的形式将停止运营的消息向您发布。

2.2、您的个人信息经去标识化处理后将形成可以使用及流通的数据，我们对此类数据的保存及处理无需另行通知并征得您的授权同意。

3、信息技术措施

我们承诺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，防止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信息技术措施，保护您的个人信息，包括但不限于：

3.1、通过 SSL (Secure Sockets Layer 安全套接层) 加密技术保护，例如您的浏览器与“服务”之间交换数据。

3.2、通过 https 方式进行信息加密传输和存储。例如您的浏览器访问我们官方网站或 H5 链接时的安全浏览方式。

3.3、在服务器层面使用 Secure Shell 网络传输协议。

3.4、在数据层面使用 Oracle 透明数据加密 (TDE)，以确保数据的保密性。

3.5、使用受信赖的保护机制防止数据遭到恶意攻击。

3.6、部署数据访问控制机制，确保只有授权人员才可访问个人信息。

3.7、使用专用网络通道及网络代理。

4、安全事件应对机制

我们严格遵守法律法规保护用户的通信秘密，若发生个人信息泄露等安全事件，我们会启动应急预案，阻止安全事件扩大，并以推送通知、公告等形式告知您。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。

4.1、如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理措施、您可自主防范和降低风险的建议、对您的补救措施等。我们会及时将事件相关情况以站内通知、短信通知、电话、邮件等您预留的联系方式告知您，因特殊情况难以逐一告知用户时，我们会采取合理、有效的方式发布公告。

4.2、我们会及时处置系统漏洞、网络攻击、病毒侵袭及网络侵入等安全风险。在发生危害网络安全的事件时，我们会按照网络安全事件应急预案，及时采取相应的补救措施，并按照规定向有关主管部门报告。

4.3、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、篡改或损毁以致您的合法权益受损，我们将严格依照法律法规承担相应的责任。

5、个人信息保护管理机制

我们建立针对个人信息保护的管理制度、流程和组织确保信息安全，包括但不限于以下措施：

5.1、建立内控管理制度，以合规与风险管理部为个人信息保护专责部门，以法定代表人为个人信息保护负责人。

5.2、严格限制访问信息的内部人员范围，以最小授权原则，严格限制能访问您个人信息的人员范围，以及要求该等内部人员遵守保密义务，并进行定期审查访问权限。

5.3、监控及定期审查内部人员处理个人信息的行为。

5.4、举办相关法律法规、隐私安全和隐私保护的培训课程及考核机制，加强员工对于保护个人信息重要性的认识。

6、个人信息保护申诉机制

我们针对个人信息收集、使用、共享、授权等事宜设立了专门个人信息保护申诉反馈机制，您可以通过本政策“第十二条、您如何联系我们”的联系方式与我们联系，客服会将相关事项转交给个人信息保护专责部门处理，我们将在验证您的个人身份后的两个工作日内予以回复您的请求。

第九条、您的权利

我们非常尊重您对个人信息的关注，并为您提供了管理个人信息的方法。您有权利访问、更正、删除、撤销、管理自己的信息并保护自己的隐私和安全：

1、访问您的个人信息

如果您想行使数据访问权，可以通过我们官方网站或我们移动应用程序登陆账户，编辑个人信息、风险调查问卷、更改密码等操作。App 访问路径为“我的-个人信息”。为了您的信息安全，您的手机号码、身份证号码、银行卡号码等信息会进行脱敏展示。

2、更正您的个人信息

当您的个人信息出现错误或发生变更，您有权要求我们做出更正，您可以通过“我的-个人信息”自行更正，或按照我们官方网站帮助中心的业务指南与要求，递交相关资料申请变更。详情您可进一步联系我们的客服热线。

3、删除您的个人信息

在以下情形中，您可以向我们提出删除个人信息的请求，您可进一步联系我们的客服热线：

- 3.1、如果我们处理个人信息的行为违反法律法规；
- 3.2、如果我们收集、使用您的个人信息，却未征得您的同意；
- 3.3、如果我们处理个人信息的行为违反了与您的约定；
- 3.4、如果您不再使用我们的产品或服务，且您申请注销了基金交易账号、基金账户；
- 3.5、如果我们不再为您提供产品或服务。

您可以访问 App “我的-帮助中心-注销账户指引”了解注销账户的指引，或通过 App “我的-我的账户-注销账户”申请注销账户。

您的基金交易账户受相关法律法规要求保护和约束。您在发出删除个人信息（注销账户）前，您需确保满足我们明示的业务规则条件后，再向我们提出请求。例如，您申请注销账户时，须确保您基金交易账户属于正常状态、资产余额为零、没有在途资金和没有赎回出款失败资金等条件。我们还将按程序验证您个人身份。对符合受理条件的申请，我们将于 1 个工作日后完成注销。当您从我们的服务中删除个人信息后，

我们可能不会立即备份系统中删除相应的个人信息，但会在备份更新时删除这些个人信息。

4、撤回您已同意的授权

您可以通过卸载 App 的方式撤回全部授权，您也可以通过访问“我的-设置-权限管理”改变部分您授权我们继续收集个人信息的范围或撤销您的授权。

5、约束信息系统自动决策

在某些业务功能中，我们可能仅依据信息系统、算法等在内的非人工自动决策机制做出决定。如果这些决定显著影响您的合法权益，您有权要求我们做出解释，我们也将提供适当的救济方式。

6、响应您的上述请求

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。我们将尽合理商业努力，满足您对于个人信息的访问、更正、删除、撤销、管理的要求。

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。

6、尽管有上述约定，但在以下情形中，我们可能将无法响应您的请求：

-
- 6.1、与履行国家法律法规及监管部门有关规定的义务相关的；
 - 6.2、与国家安全、国防安全直接相关的；
 - 6.3、与公共安全、公共卫生、重大公共利益直接相关的；
 - 6.4、与公检法等执法部门法律程序直接相关的，如犯罪侦查、起诉、审判和判决执行等；
 - 6.5、我们有充分证据表明您存在主观恶意或滥用权利的；
 - 6.6、出于维护您或其他主体的生命、财产等重大合法权益但又很难得到您本人同意的；
 - 6.7、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；
 - 6.8、涉及商业秘密的。

第十条、 我们如何保护未成年人的信息

我们提供的基金销售服务产品，以及配套网站、App 等服务平台主要面向成年人，仅面向年满十八周岁且具有完全民事行为能力个人投资者提供基金销售服务。如果您是未成年人，您仅能通过手机号码及验证码注册我们的平台账户（非实名制），以及浏览我们服务平台的信息，我们暂不支持向您提供注册基金交易账户服务。

如果您是未成年人，建议您请监护人阅读本指引或在监护人的指导下阅读本政策，并在取得您的监护人同意的前提下向我们提供您的相关个人信息以便访问和浏览我们服务平台的信息，我们将根据相关法律法规规定对您的个人信息保密性及安全性进行特别保护。如您的监护人不同意您按照本指引

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。

如您是未成年人的监护人，若您对该未成年人的个人信息处理存有疑问，请通过本政策“第十二条、您如何联系我们”的联系方式与我们联系。

第十一条、 适用法律与争议解决

1、本政策的执行、解释及争议的解决均适用中华人民共和国法律（为本政策之目的，不包括香港特别行政区、澳门特别行政区和台湾地区法律）管辖。如本政策条款与相关法律法规相抵触的，以法律法规为准。本政策为可分割的，被判决或裁定为无效的条款，不影响其他条款的有效性。

2、您和我们就本政策内容或其执行发生任何争议的，双方应友好协商解决。如双方无法协商解决争议时，任一方可以向深圳证券期货业纠纷调解中心、中国证券投资者保护网、中国证券投资基金业协会等有权部门申请调解。如经协商或调解不能解决争议的，双方同意应将争议提交至深圳国际仲裁院按照届时有效的仲裁规则仲裁，仲裁地点为深圳，仲裁语言为中文，仲裁费用由败诉方承担。仲裁裁决具有终局性，对双方均具有法律约束力。

第十二条、 修订变更

1、为更好地提供服务，我们可能适时修订变更本政策内容。如该等变更导致您在本政策项下权利的实质减损，我们将在变更生效前，通过在页面显著位置提示、向您发送电子邮件、站内信或公告等方式通知您，说明具体变更的内容。在

该种情况下，若您继续使用我们的服务，即表示已经充分阅读、理解并同意接受经修订的政策，并受其约束。

2、我们会将本政策的旧版本存档。

第十三条、 您如何联系我们

如您对本政策或您个人信息的相关事宜有任何问题、意见或建议，请通过访问以下多种方式与我们联系。部分情况下，为保障您个人信息的安全，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。我们将尽快审核所涉问题、意见或建议，并在验证您的用户身份后的两个工作日内予以回复。

1、登陆我们官方网站 www.ifastps.com.cn 并点击在线客服系统。

2、发送邮件至客服邮箱：cs@ifastfinancial.com.cn。

3、拨打客服热线：400-684-0500。

4、寄信至深圳市南山区海德三道航天科技广场 A 座 17 楼 1703-04 室（客服部收），邮编：518054。