ICS 03.060
CCS A 11

团　　体　　标　　准

T/TSAC 001—2025

证券公司投资者个人信息保护技术规范

Technical specification on investors' personal information protection of securities companies

2025-09-25 发布　　2025-09-25 实施

中 国 证 券 业 协 会　　发 布

目 次

前　言

本文件按照GB/T1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中泰证券股份有限公司提出。

本文件由中国证券业协会归口。

本文件起草单位：中泰证券股份有限公司、财信证券股份有限公司、中国信息通信研究院、万联证券股份有限公司、国泰海通证券股份有限公司、腾讯科技（北京）有限公司、东北证券股份有限公司、国联民生证券股份有限公司、招商证券股份有限公司。

本文件主要起草人：张勇、张佳佳、李赛男、杨玲玲、王恩潭、孙文渊、陈杨、宁文卓、刘洋、熊嘉、黄志程、王健、秦维华、李奕、董延敏、马国文、张秀敏、马原、钟雪玲、杨曦、邓韬、杜楚逸、齐欢、梁叶、夏曼、郭恋、陶茜、马书原、李姣、韩冰。

引　言

证券公司因业务需要收集、使用投资者个人信息，给证券公司和客户业务办理带来便利的同时，也可能出现投资者个人信息的非法收集、篡改、滥用、泄露、丢失等问题，投资者个人信息安全面临一定风险。投资者个人信息一旦泄露，不仅会直接侵害投资者的合法权益、影响证券公司的正常运营，甚至可能会带来行业系统性金融风险。为加强证券公司投资者个人信息保护管理，指导证券公司规范处理投资者个人信息，最大程度保障投资者合法权益，维护金融市场稳定，编制本文件。

证券公司投资者个人信息保护技术规范

1 范围

本文件规定了证券公司投资者个人信息的保护要求，包含基本原则、投资者个人信息分类分级、投资者个人信息保护体系、投资者个人信息全生命周期保护要求、特定场景中的投资者个人信息保护、个人信息保护政策模板等。

本文件适用于证券公司以及其开展证券、期货、基金等业务的子公司在提供相关产品和服务的过程中开展投资者个人信息保护工作参考使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

GB/T 25069—2022 信息安全技术 术语

GB/T 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

GB/T 42574—2023 信息安全技术 个人信息处理中告知和同意的实施指南

GB/T 42775—2023 证券期货业数据安全风险防控 数据分类分级指引

GB/T 43697—2024 数据安全技术 数据分类分级规则

JR/T 0158—2018 证券期货业数据分类分级指引

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0250—2022 证券期货业数据安全管理与保护指引

3 术语和定义

GB/T 35273—2020 和 JR/T 0171—2020 界定的以及下列术语和定义适用于本文件。

3.1

投资者 investor

开展证券交易的自然人、法人、非法人组织，以及依法设立的金融产品。

3.2

个人信息 personal information

个人信息是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。

3.3

投资者个人信息 investors'personal information

投资者（3.1）所涉及的自然人的个人信息，不包括匿名化处理后的信息。

3.4

敏感个人信息 sensitive personal information

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，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

注：具体参见附录A“敏感”标识为“是”的数据类别。

3.5

公开/公开披露 public disclosure

向社会或不特定群体发布信息的行为。

[来源：GB/T 35273—2020,3.11]

3.6

明示同意 explicit consent

投资者（3.1）通过书面声明或主动作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。

肯定性动作包括投资者主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

[来源：JR/T 0171—2020,3.22,有修改]

3.7

匿名化 anonymization

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。

3.8

去标识化 de—identification

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。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

3.9

鉴别 authentication

验证某一种实体所声称身份的过程。

[来源：GB/T 25069—2022,3.296]

3.10

单独同意 separate consent

个人针对其个人信息进行特定处理而专门作出具体、明确授权的行为，不包括一次性针对多种目的或方式的个人信息处理活动作出的同意。

注：单独同意的告知内容与取得同意的方式需与其他处理活动予以区分。

[来源：GB/T 42574—2023,3.7]

3.11

自动化决策 automated decision making

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。

3.12

用户画像 user profile

通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，形成其个人特征模型的过程。

注：直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

[来源：GB/T 35273—2020,3.8]

3.13

可识别 identifiable

仅凭某个信息本身无法识别出特定的自然人,但是只要将该等信息进行结合就可以识别出特定的自然人。即采用可能使用的手段、考虑所有客观因素，通过要素结合分析能识别到特定身份的可能。

3.14

汇聚融合 convergence

集成多个数据源以产生比任何单独数据源更有价值的过程,包括个人信息处理者内部不同业务线的数据“打通”实现共享、融合，以及集团内不同关联企业之间的数据融合。

3.15

提供 provide

个人信息处理者通过共享、转移等方式将个人信息传输或披露给其他个人信息处理者的行为。

注：委托第三方处理个人信息的，不属于向其他个人信息处理者提供个人信息的行为。

[来源：GB/T 42574—2023,3.8]

3.16

转让 transfer of control

将投资者个人信息控制权由一个控制者向另一个控制者转移的过程。

[来源：GB/T 42574—2023,3.12,有修改]

3.17

删除 delete

本指引所称“删除”是指在实现日常业务功能所涉及的系统或档案中除去个人信息的行为，使其保持不可被检索、访问的状态。删除所要实现的目的为保持个人信息不可通过任何形式被检索、访问，不包括删除前端数据但存于后端做访问限制的形式。

3.18

使用 use

个人信息的使用有广义和狭义之分，狭义的个人信息的使用不包括个人信息的存储、加工、传输、提供以及公开，仅指个人信息处理者对个人信息进行的分析和利用。

4 缩略语

IP：互联网协议（Internet Protocol）
SDK：软件开发工具包（Software Development Kit）

5 基本原则

证券公司在落实投资者个人信息保护有关要求时，应遵守有关法律法规和中国证监会的规定。

证券公司应以“权责一致、目的明确、告知同意、最小必要、分级保护、公开透明、确保安全、主体参与、确保质量”为原则，制定并实施覆盖投资者个人信息全生命周期的安全保护策略，具体包括：

a) 权责一致：采取技术和其他必要的措施保障投资者个人信息的安全，对其个人信息处理活动对投资者合法权益造成的损害承担责任；
b) 目的明确：具有正当、明确、清晰、具体的投资者个人信息处理目的；
c) 告知同意：向投资者明示投资者个人信息处理目的、方式、范围等规则，取得其授权同意或具备处理投资者个人信息的其他合法性基础；
d) 最小必要：只处理满足投资者授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时按照相关法律法规相关规定处理投资者个人信息。建议证券公司遵循具体业务规则，根据具体业务需要，严格执行最小必要原则处理投资者个人信息；
e) 分级保护：结合证券公司自身数据管理需要，依据投资者个人信息的数据类型、敏感程度等差异，划分不同的数据安全层级，采取针对性的安全保护措施。应当按照投资者个人信息的不同安全级别进行分级别安全防护，安全层级越高的数据应当采用更严格的防护措施；
f) 公开透明：以明确、易懂和合理的方式公开处理投资者个人信息的范围、目的、规则等，并接受外部监督；
g) 确保安全：具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性；
h) 主体参与：向投资者提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法；
i) 确保质量：保证所处理的个人信息的质量，避免因为个人信息的不准确、不完整对

个人权益造成不利影响。

6 投资者个人信息分类分级

6.1 概述

证券公司应遵循 JR/T 0158—2018 的要求，根据证券公司各自情况对投资者个人信息进行分类分级，可参考附录 A。

6.2 证券公司投资者个人信息内容及分类

证券公司应遵循系统性、规范性、稳定性、明确性、扩展性原则对投资者个人信息进行分类。

证券公司投资者个人信息包括投资者个人基本信息、身份信息、鉴别信息、账户信息、交易信息、财产信息、信用信息、合约信息、行为信息、衍生信息、设备信息、位置信息和其他反映特定投资者个人信息主体某些情况的信息，具体如下：

a) 投资者个人基本信息指参与证券期货市场业务活动的自然人、法人、非法人组织、依法设立的金融产品涉及的自然人的个人基本信息，包含姓名、性别、民族、出生日期、年龄、联系地址、移动电话、电子邮件、国籍等信息；

b) 投资者个人身份信息是指参与证券期货市场业务活动的自然人、法人、非法人组织、依法设立的金融产品涉及的自然人身份信息，包含个人身份证件信息、个人特定身份信息，个人身份证件信息包括投资者个人证件类型、证件号码、证件地址、证件有效期、签发机关等；个人特定身份信息指残障人士身份信息、犯罪人员身份信息、特定工作信息（如军人、警察）等；

c) 投资者个人鉴别信息指投资者的账户认证信息和个人生物识别信息，账户认证信息包含账户密码、数字证书、动态口令、口令保护答案、短信验证码等信息，个人生物识别信息包括指纹认证信息、人脸认证信息等；

d) 投资者个人账户信息包括开户/账户信息、投资者编码信息。开户/账户信息指投资者与业务活动相关的识别信息，包含账户名称、投资者标识、账户类别、证券账户编码、账户用途、账户状态代码等信息，投资者编码指投资者在证券公司的内部统一编码；

e) 投资者个人交易信息指投资者在参与证券期货市场交易活动中产生的各类信息，包括但不限于成交信息、委托信息、银证转账、交易业务参数信息、交易日志信息以及有关规定要求的反映交易真实情况的合同、业务凭证、单据、业务函件和其他资料；

f) 投资者个人财产信息指证券公司在提供金融产品和服务过程中，收集或生成的投资者个人财产信息，包括但不限于持仓信息、银行账务信息、资金状况信息、资金账户金额、个人收入状况等；

g) 投资者个人信用信息指投资者的信用相关信息，包含账户编码、信用等级、信用额度、融资融券偿还情况以及投资者在交易活动中形成的，能够反映其信用状况的其他信息；

h) 投资者个人合约信息指参与交易活动所产生的契约信息。包含账户编码、流水号、合同号、市场代码、证券代码、证券数量、发生金额、归还日期等；

i) 投资者个人行为信息指在开展业务或参与交易等活动中记录下来的投资者行为过程数据，包含投资者在 App、网站中的行为信息，操作日志等；

j) 投资者衍生信息指对投资者交易及行为数据进行处理、分析所形成的反映特定投资

者某些情况的信息，包含:投资者分类、投资能力、投资意愿、行为习惯、兴趣偏好等；

k) 投资者个人设备信息指投资者个人在证券公司提供产品或服务过程中使用的设备信息，包括但不限于硬件序列号、设备 MAC 地址、唯一设备设别码（如 IMEI/Android ID/IDFA/Open UDID/GUID/SIM 卡 IMSI 信息等）、机型、系统版本、存储位置、应用软件列表等在内的描述个人常用设备基本情况的信息；

l) 投资者个人位置信息指投资者个人粗略位置信息、精准定位信息、经纬度等。

6.3 证券公司投资者个人信息的分级

证券公司应依据依从性、可执行性、时效性、自主性、合理性、客观性原则对投资者个人信息进行分级。

证券公司应根据个人信息的安全性（保密性、完整性、可用性等）遭受破坏后的影响和危害大小，将投资者个人信息从高到低分为4级、3级、2级、1级四个级别：

a) 4 级主要指用于大型或特大型行业机构中的重要业务，一般针对特定人员公开，且仅为必要知悉的对象访问或使用的投资者个人信息。主要包括投资者鉴别信息。该类信息一旦遭到未经授权的查看、变更或者破坏，会对投资者个人信息安全与财产安全造成特别严重危害；

b) 3 级主要指用于重要业务，针对特定人员公开，且仅为必要知悉的对象访问或使用的投资者个人信息。主要包括投资者个人身份信息与财产信息，以及用于相关产品与服务的关键信息。该类信息一旦遭到未经授权的查看、变更或者破坏，会对投资者的信息安全与财产安全造成严重危害；

c) 2 级主要指用于一般业务，针对受限对象公开且不宜广泛公开的投资者个人信息。该类信息一旦遭到未经授权的查看、变更或者破坏，会对投资者的信息安全与财产安全造成一般危害；

d) 1 级主要指可被公开或可被公众获知、使用的投资者个人信息。该类信息一旦遭到未经授权的查看、变更或者破坏，不会对投资者的信息安全与财产安全造成实质危害。

投资者敏感个人信息一般定义为3级及以上。上述两种或两种以上的低敏感程度信息经过组合、关联和分析后可能产生高敏感程度的信息，宜参照高敏感程度信息进行安全防护。同一信息在不同的服务场景中可能处于不同的级别，可依据服务场景以及该信息在其中的作用对信息的类别进行识别和定级，并实施针对性的保护措施。

7 证券公司投资者个人信息保护体系

证券公司处理投资者个人信息，应当建立健全投资者个人信息保护体系，明确相关岗位及职责要求，建立健全投资者个人信息处理、安全防护、应急处置、审计监督等管理机制，加强投资者个人信息保护。

7.1 建立健全内控制度体系

证券公司应建立投资者个人信息保护制度体系，明确工作职责，规范工作流程。制度体系的管理范畴需要涵盖本机构、外包服务机构与外部合作机构，确保相关制度发布、传达给本机构员工，并确保可落地执行。相关制度包括但不限于投资者个人信息保护管理规定、日常管理及操作流程、外包服务机构与外部合作机构管理、内外部检查及监督机制、应急处理流程和预案。具体要求如下：

a) 制定覆盖投资者个人信息保护全过程的管理制度，提出本机构投资者个人信息保护工作方针、目标和原则；
b) 开展投资者个人信息分类分级管理，针对不同类别、级别的投资者个人信息，实施相应的安全策略和保障措施；
c) 建立日常管理及操作流程，对投资者个人信息的收集、存储、使用、加工、传输、提供、公开、删除等环节提出具体保护要求，制定投资者个人信息时效性管理规程，确保符合所在国家或地区法律法规有关规定；
d) 建立投资者个人信息脱敏管理规范和制度，明确不同类别、级别的投资者个人信息脱敏规则、脱敏方法和脱敏数据的使用限制；
e) 制定并公开投资者个人信息处理规则，明确告知投资者个人信息处理目的、处理方式、处理投资者个人信息种类、保存期限等内容；
f) 制定外包服务机构与外部合作机构管理制度，内容包括但不限于：
   1) 应自行对外包服务机构与外部合作机构的个人信息保护能力进行审查，或要求对方提供第三方评估认证机构证明其个人信息保护能力符合相关标准的评估证书，以评估其个人信息的保护能力是否达到国家个人信息保护主管监管部门、证券期货行业主管部门以及金融监督管理部门的要求；
   2) 对外包服务机构与外部合作机构明确其在投资者个人信息安全保护能力、定期审查、留存信息、保密责任等方面的要求，根据要求落实控制措施，并将资料留档备查；
   3) 对可能访问投资者个人信息的外包服务机构、外部合作机构及其人员，证券公司应要求外包服务机构与外部合作机构向有关人员传达投资者个人信息保护要求，与其签署保密协议；
   4) 为防范因外包人员因素导致的信息泄露风险，原则上对于外包人员接触投资者敏感个人信息的情况，要求其在现场办公，并明确规定不得复制敏感信息或将敏感信息带离现场；对于非现场办公的情形，应加强对外包人员的操作监督，定期对外包人员查询、复制、导出、下载敏感个人信息等操作行为进行审计；
   5) 应定期对外包服务机构、外部合作机构的投资者个人信息保护措施落实情况进行确认，确认的方式包括但不限于外部信息安全评估、现场检查等。
g) 建立投资者个人信息安全检查及监督机制，包括投资者个人信息安全日常检查机制和工作流程等，必要时可将个人信息相关合规及安全事件纳入公司内部的奖惩管理办法和要求中；
h) 将投资者个人信息泄露等相关事件处理纳入机构网络安全事件应急处置工作机制，明确应急处置流程和预案，定期评估应急处理流程和预案的有效性，及时保障、有效应对投资者个人信息网络安全事件，降低网络安全事件造成的损失和不利影响；
i) 建立健全内部检查问责机制，根据检查结果，及时组织调查，完成问题整改，追究问题责任；
j) 建立投资者个人信息投诉与申诉处理程序，明确投诉与申诉受理部门、处理程序，对投资者要求更正或删除证券公司收集其个人信息的情况，及时受理、核实，并依据法律或证券期货行业主管部门的要求予以处理；
k) 建立投资者个人信息保护意见反馈机制，意见反馈渠道可参照投诉与申诉处理程序；
l) 根据公司实际情况，在管理制度或投资者个人信息处理规则中细化投资者个人信息共享、存储、使用和销毁的期限，具备投资者个人信息存储时效性的控制能力；
m) 对投资者个人信息保护相关管理制度进行定期的评审与修订，确保可以应对最新的安全威胁与风险。

7.2 组织架构及岗位设置

组织架构及岗位设置具体要求如下：

a) 建立健全投资者个人信息保护组织架构，明确机构各层级内设部门与相关岗位投资者个人信息总体要求与保护职责，形成相互监督相互制约的管理机制；

b) 应指定投资者个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施进行监督。除法律法规和中国证监会另有规定外，可由合规总监、首席风险官等兼任投资者个人信息保护负责人；

c) 明确机构内部投资者个人信息保护的牵头组织机构，并组织或监督内部相关责任机构根据职责分工履行以下工作职责：

1) 制定、修订投资者个人信息保护管理制度；

2) 开展投资者个人信息分类分级管理，针对不同级别和敏感程度的投资者个人信息，制定相应的安全策略和保障措施；

3) 建立投资者个人信息脱敏管理规范或制度，明确投资者个人信息脱敏规则、脱敏方法等；

4) 组织 App 客户端等金融产品或服务上线或重大变更前的安全检测，避免未知的不当行为，包括与国家法律法规、证券行业监管要求不符，或存在潜在威胁等，并对发现的风险及时进行整改加固；

5) 建立投资者个人信息安全检查及监督机制，定期评估个人信息管理方面存在的不足，并及时调整检查机制和工作流程；

6) 监督本机构内部，以及本机构与外部合作方投资者个人信息保护安全管理；

7) 开展投资者个人信息保护影响评估，处置发现的安全风险，提出投资者个人信息保护的对策；

8) 将投资者个人信息安全事件纳入数据安全事件应急处置工作机制，制定有关应急预案；

9) 投资者个人信息安全事件相关的分析、处置及内外部报告等工作，提出投资者个人信息保护的对策建议；

10) 开展投资者个人信息保护培训与意识教育活动，并保留相关记录；

11) 与监管、管理部门保持沟通，通报或报告个人信息保护和事件处置等情况。

d) 明确在提供金融产品和服务的相关过程中知悉投资者个人信息的岗位，并针对相关岗位明确其投资者个人信息安全管理责任与保密责任。

7.3 人员管理

对涉及投资者个人信息相关人员的安全管理，具体要求如下：

a) 录用员工前，应进行必要的背景调查，如除了常规的背调外，可进一步核查是否发生过个人信息违法违规事件，并与所有可访问投资者个人信息的员工签署保密协议，或者在劳动合同中设置保密条款；

b) 在发生人员调离岗位或终止劳动合同时，立即调整和完成相关人员的投资者个人信息访问、使用等权限的配置，并明确有关人员后续的投资者个人信息保护管理权限和保密责任；若有关人员调整后的岗位不涉及投资者个人信息的访问与处理的，明确其继续履行有关信息的保密义务要求；

c) 在个人信息保护政策、个人信息保护相关法律法规、行业规范发生重大变化时，对投资者个人信息处理岗位上的相关人员开展投资者个人信息安全专业化培训和考核，确保相关人员熟练掌握个人信息保护政策和相关规程。

7.4 安全防护技术要求和措施

证券公司应根据国家与证券期货行业主管部门的要求，加强投资者个人信息安全技术能力建设，落实必要的管理和技术措施，防止投资者个人信息的泄露、损毁、丢失及篡改。可采取包括但不限于以下安全技术要求和措施：

a) 信息管理流程：完善投资者信息收集、存储、使用、加工、传输、提供、公开、删除等全生命周期管理流程；
b) 数据分类分级管理：开展投资者个人信息分类分级管理，针对不同级别和敏感程度的投资者个人信息，实施相应的安全策略和保障措施；
c) 信息技术系统建设：可采取网络隔离、用户鉴别、数据加密、数据备份、数据销毁、病毒防范、非法入侵检测等安全技术措施，确保信息技术系统的安全性。并采取异常流量监测、用户行为分析等技术措施对投资者个人信息进行风险识别和监测；
d) 数据传输控制措施：可采取传输途径和存储介质的安全管理，系统权限分级授权，数据加密等安全控制措施；
e) 数据存储控制措施：可采取数据库加密、数据库防火墙、数据库运维管理、数据审计、数据库脱敏等安全控制措施；
f) 数据展示控制措施：可通过增加桌面水印的方式，控制操作人员通过截屏/拍照的方式获取投资者敏感个人信息。

7.5 访问控制

为避免发生投资者个人信息泄露和未经授权的访问，控制投资者个人信息使用过程中的各项风险，证券公司应加强投资者个人信息的访问控制管理，具体要求如下：

a) 对于可访问和处理投资者个人信息的系统，根据“最小必要”原则，设置访问控制策略，严格控制和分配访问、使用投资者个人信息，且仅具备完成职责所需的最少数据操作权限，权限申请经审批后方可进行分配；禁止账户共用；
b) 传输、处理、存储投资者个人信息的系统默认用户权限应为“拒绝所有访问”；
c) 对投资者个人信息使用的权限管理应设置权限指派、回收、超期删除等安全功能；
d) 对存储或处理投资者个人信息的系统或设备进行远程访问时，应当采取数据脱敏、数据加密等措施，防范化解投资者个人信息在处理过程中的泄露风险，应对能通过互联网远程方式（如 VPN）访问的涉及投资者个人信息的系统增加限制，如限制通过报备或绑定 MAC 地址的电脑访问，减少因账号密码泄露造成的个人信息安全风险；
e) 对生产网络、开发测试网络、办公网络以及相关非生产网络进行访问控制；
f) 对投资者个人信息访问与投资者个人信息的增删改查等操作进行记录，并保证操作日志的完整性、可用性及可追溯性；系统运维管理类日志不应记录投资者个人信息；
g) 对存储投资者个人信息的数据库及操作日志实施严格的用户授权与访问控制；
h) 对个人信息的重要操作设置内部审批流程，如进行批量修改、拷贝、下载等重要操作；
i) 对安全管理人员、数据操作人员、审计人员的角色进行分离设置；
j) 确因工作需要，需授权特定人员超权限处理个人信息的，经个人信息保护责任人或个人信息保护工作机构进行审批，并记录在册；
k) 对投资者敏感个人信息的访问、修改等操作行为，应在对角色权限控制的基础上，按照业务流程的需求触发操作授权。例如，当收到投资者投诉时，投诉处理人员才可访问该投资者的个人信息。

7.6 投资者个人信息保护影响评估

a) 定义：针对投资者个人信息处理活动，检验其合法合规程度，判断其对投资者合法权益造成损害的各种风险，以及评估用于保护投资者个人信息的各项措施有效性的过程；
b) 责任部门：证券公司应指定个人信息保护影响评估的责任部门、特别工作小组或第三方机构，对评估工作流程的制定、实施、改进以及评估结果负责。该责任部门、特别工作小组或第三方机构应具有独立性，不受被评估方的影响。可进一步采取流程嵌入或纳入奖惩机制等方式，保障影响评估有效开展、评估覆盖范围的完整性等；
c) 适用条件：投资者个人信息保护影响评估的应用场景包括但不限于：
   1) 国家法律法规规定的应当事前进行个人信息保护影响评估的情形：处理敏感个人信息的、利用个人信息进行自动化决策的、委托处理个人信息向其他机构提供个人信息的、公开个人信息的、向境外提供个人信息的、以及其他对个人权益有重大影响的个人信息处理活动；
   2) 法律法规、政策、标准等出现重大变化时重新评估；
   3) 业务模式、互联网安全环境、外部环境等发生重大变化的重新评估；
   4) 发生重大投资者个人信息安全事件后重新评估；
   5) 发生收购、兼并、重组等情形开展评估；
   6) 新产品或新服务（不限于技术平台）需求设计阶段评估；
   7) 新产品或新服务（不限于技术平台）上线初次评估；
   8) 产品或服务在运营过程中发生与投资者个人信息保护相关的重大变更时，需重新开展投资者个人信息保护影响评估；
   9) 产品或服务的年度整体评估等。
d) 评估内容：投资者个人信息的处理目的、处理方式等是否合法、正当、必要；对投资者个人权益的影响及安全风险；所采取的保护措施是否合法、有效并与风险程度相适应；
e) 评估方式：评估实施过程中采用的基本评估方法，包括但不限于访谈、检查和测试；
f) 评估程序：开展评估前，需对待评估的对象进行全面调研，形成清晰的数据清单及数据映射图表，并梳理出待评估的具体的个人信息处理活动。开展评估时，通过分析个人信息处理活动对投资者的权益可能造成的影响及其程度，以及分析安全措施是否有效，是否会导致安全事件发生及其可能性，综合两方面结果得出个人信息处理活动的风险及风险等级，并提出相应的改进，形成评估报告；
g) 评估报告：评估报告的内容通常包括审批页面、评估报告适用范围、实施评估及撰写报告的人员信息、参考的法律、法规和标准、投资者个人信息影响评估对象、评估内容、涉及的相关方等，以及投资者个人权益影响分析结果，安全保护措施分析结果、安全事件发生的可能性分析结果、风险判定的准则、合规性分析结果、风险分析过程及综合评估结果、风险处置等；
h) 投资者个人信息保护影响评估报告和处理情况记录应当至少保存三年。

7.7 监控

监控具体要求如下：

a) 识别并记录相关人员（如管理员用户、业务用户）对投资者个人信息的访问；
b) 对投资者个人信息数据交换网络流量进行安全监控和分析，并存储匹配安全规则的数据，以备事件溯源；
c) 采取技术手段对投资者个人信息全生命周期进行安全风险识别和管控；
d) 通过技术手段建立投资者个人信息泄露监控预警机制，及时发现信息泄露事件。

7.8 投资者个人信息安全事件处置

安全事件处置具体要求如下：

a) 制定投资者个人信息安全事件应急预案，明确安全事件处置流程和岗位职责；
b) 定期组织内部相关人员进行投资者个人信息保护应急预案相关培训和应急演练；
c) 发现因系统漏洞或人为原因造成投资者个人信息遗失、损毁、泄露或被篡改等安全类事件后，及时采取必要措施进行处置，控制事态发展，消除安全隐患，并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受影响的投资者；难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息；证券公司及时采取措施后能够有效避免信息泄露、篡改、丢失造成危害的，可以不通知个人；
d) 发现其他机构、个人违规存储或使用投资者个人信息的，应当排查数据泄露途径、评估影响范围，采取合理可行的整改措施，及时处置风险隐患，并按照中国证监会规定履行报告和调查处理职责。
e) 发现信息技术服务机构等相关方违规存储或者使用投资者个人信息的，应当责令其立即改正并销毁已获取的信息；信息技术服务机构等相关方拒绝配合整改的，应当立即停止与其合作，并采取措施维护自身及投资者的合法权益。
f) 记录事件内容，分析和鉴定事件产生的原因，评估事件可能造成的影响，制定补救措施，并向国家个人信息保护主管部门以及证券期货行业主管部门进行报告；
g) 建立投诉与申诉管理机制，包括跟踪流程，并在规定的时间内，对投诉、申诉进行响应；
h) 采取有效措施开展舆情动态监测，持续跟踪舆情变化，对涉及公司投资者个人信息保护的舆情案件及时研判并报告，并适时进行应急处置；
i) 根据相关法律法规的变化情况以及事件处置情况，及时更新应急预案。

7.9 安全教育与培训

安全教育与培训的要求包括但不限于：

a) 文化宣导：应加强投资者个人信息保护宣传与教育，应每年至少一次或个人信息保护政策、个人信息保护相关法律法规、行业规范发生重大变化时开展全员投资者个人信息安全教育活动，提升员工个人信息保护意识；
b) 应在金融产品或服务提供过程中，通过开展投资者讲堂、报告会、座谈会以及利用投资者回访、网站、App 等方式开展投资者教育和宣传：
   1) 明确告知投资者国家法律法规等所提供的相关权利与义务；
   2) 提升投资者对业务中所涉及的个人信息处理工作的基本认识；
   3) 增强投资者对个人信息保护的总体意识，妥善保护个人身份资料、账户信息等。
c) 应定期(至少每年一次)或在个人信息保护政策发生重大变化时，对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核，确保相关人员熟练掌握个人信息保护政策和相关规程：
   1) 投资者个人信息安全保护工作相关监管动态和处罚；
   2) 最新的法律法规变化；
   3) 引导员工正确有效遵守证券公司关于投资者信息保护的工作原则和要求；
   4) 提升员工对于做好投资者个人信息保护工作是树立证券公司良好声誉的重要部分的意识。
d) 证券公司应结合行业文化建设，健全投资者个人信息保护的合规文化，通过文化建

设凝聚投资者、员工以及第三方服务作机构的合力和共识，形成自觉保护投资者个人信息的一致认识并在工作中自觉执行。

7.10 第三方服务机构管理

除法律法规和中国证监会另有规定外，证券公司不得允许或者配合其他机构、个人截取、留存客户信息，不得以任何方式向其他机构、个人提供未经匿名化处理的投资者个人信息。

证券公司应当记录投资者个人信息的使用情况，并持续监督第三方服务机构（包括外包服务机构与外部合作机构）等相关方落实保密协议的情况。

证券公司将收集的投资者个人信息传输、共享、委托给第三方服务机构（包括外包服务机构与外部合作机构）处理时，应遵循如下要求：

a) 准入要求：应建立第三方服务机构的准入条件，并通过合同等方式约定证券公司与第三方服务机构的权利和义务；
b) 投资者信息保护能力评估：应对第三方服务机构进行评估或要求其提供评估报告，确保第三方服务机构具备足够的信息安全能力，且提供了足够的安全保护措施；
c) 事中监控：应对外部嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）开展技术检测，确保其投资者个人信息收集、使用行为符合约定要求；并根据合同约定对其处理投资者个人信息的行为进行监督和审计，发现超出约定行为且对客户个人信息安全产生影响的，应视后果的严重程度应及时切断接入或通知第三方服务机构在规定的时间内进行整改；
d) 事后处置：在委托关系解除或外包服务终止时，第三方服务机构应按照要求销毁其处理的投资者个人信息，并依据双方协商的期限承担后续的投资者个人信息保护责任；
e) 第三方服务机构转委托时，应当事先取得证券公司同意。

7.11 审计监督

证券公司应根据国家法律法规相关规定，定期对其投资者个人信息处理活动遵守法律、行政法规等情况开展合规审计，具体要求如下：

a) 明确内部开展个人信息保护合规审计的责任部门、审计工作流程、审计频率等内容，形成合规审计报告，并根据审计结果进行整改跟踪，促进个人信息内部合规管理制度、流程的完善；
b) 委托外部专业机构开展合规审计，应当与外部专业机构签订保密协议，要求外部专业机构人员对在审计过程中所知悉的信息进行保密。

8 投资者个人信息全生命周期保护基本要求

8.1 基本要求

证券公司应当遵循合法、正当、必要和诚信原则，在收集、存储、使用、加工、传输、提供、公开、删除等个人信息全生命周期过程处理投资者个人信息，规范投资者个人信息处理行为，履行投资者个人信息保护义务，不得损害投资者合法权益。并建立健全投资者个人信息处理、安全防护、应急处理、审计监督等管理机制，加强投资者个人信息保护，防止个人信息泄露、篡改、丢失。

本章节中有关保护措施未明确具体级别的，一般是指2级及以上的投资者个人信息。

证券公司在处理投资者个人信息前，应向投资者充分履行告知义务，取得投资者的同意。符合以下情形之一的，证券公司无需取得投资者个人同意：

a) 为订立、履行投资者作为一方当事人的合同所必需，或为维护所提供的产品和服务的安全、稳定运行所必需，处理必要的投资者个人信息；
b) 履行法定职责或者法定义务所必需的个人信息处理活动，包括但不限于：履行反洗钱、反恐怖融资、反诈等监管要求；履行投资者适当性管理义务；根据法律法规规定配合执法或司法机关要求；与履行国家法律法规和行业主管部门、行业自律组织有关规定的义务相关的；与国家安全、国防安全直接相关，或与犯罪侦查、起诉、审判和判决执行或国家机关及有权机构协查等直接相关的；
c) 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；
d) 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；
e) 依照国家法律法规规定在合理的范围内处理投资者个人自行公开或者其他已经合法公开的个人信息，包括但不限于：新闻媒体公开报道的信息；司法、行政机关依据法定职责向社会公众公布的信息；个人自行公开且已知悉或应当知悉可被不特定用户访问的个人信息；
f) 出于维护投资者或其他主体的生命、财产等重大合法权益但又很难得到本人同意的；
g) 法律、行政法规规定的其他情形。

8.2 收集

8.2.1 投资者个人信息收集的基本要求

8.2.1.1 投资者个人信息收集的情形

证券公司收集投资者个人信息的情形包括但不限于：

a) 提供服务或产品时通过投资者个人填写、勾选、上传等方式收集个人信息；
b) 按照《证券公司客户交易终端信息管理技术规范》确定的交易终端设备的类型，采集投资者交易终端信息，包括但不限于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；
c) 通过证券公司 App、摄像头等软件程序或硬件设备自动采集投资者个人信息；
d) 证券公司及其工作人员与投资者交互并记录其个人的行为；
e) 从第三方间接获取投资者个人信息；
f) 从非完全公开渠道获取投资者个人信息；
g) 使用大数据、人工智能等技术分析、关联或生成投资者个人信息。

8.2.1.2 收集的基本原则

证券公司收集投资者个人信息需要遵循合法、正当、必要和诚信原则，并满足以下要求：

a) 不得通过误导、欺诈、胁迫等方式非法采集投资者个人信息；
b) 不得隐瞒产品或服务所具有的收集投资者个人信息的功能；
c) 不得违法或过度收集投资者个人信息，或者擅自变更处理目的、范围和方式；
d) 合同约定收集范围、种类应当基于从事证券业务活动的必要限度。

8.2.1.3 合法性之告知

证券公司应当按照法律法规的规定及合同约定收集投资者个人信息，明确告知投资者处理个人信息的目的、方式、范围和投资者个人信息保护政策，在实施告知时注意：

a) 遵守公开透明、有效传达、适时充分、真实明确、清晰易懂的原则，不采用隐藏、故意遮挡等方式诱导投资者略过告知内容，不使用笼统、宽泛的表述；

b） 需结合产品或服务的业务功能特点，选择适当的方式（如一般告知、增强告知、即时提示等）或多种告知方式的组合，友好展示，兼顾差异；

注：一般告知通常采用制定、展示个人信息保护政策的形式进行告知；增强告知系将个人信息处理规则中的关键内容或与特定业务功能处理目的相关的关键规则单独提炼并告知；即时提示系为进一步强化投资者对收集个人信息目的的理解或辅助投资者对个人信息处理规则的理解，证券公司结合产品或服务特点选择如使用弹窗、浮窗或浮层、文字说明、状态栏提示、提示条、提示音、短消息等方式及时、有效传达告知内容。

c） 可以公开且便于查询的方式展示投资者个人信息保护政策（或被称为“隐私协议”“隐私政策”“隐私权政策”等），尽可能全面、清晰的阐述个人信息处理规则；

注：个人信息保护政策的具体内容可参见附录C。

d） 在交互式界面中，将投资者个人信息保护政策完整内容置于产品或服务的基本业务功能开启之前，以弹窗提示、提醒勾选、突出链接等明显方式，引导投资者查阅个人信息保护政策/个人信息处理规则，避免隐私政策等收集使用规则难以访问，如进入App主界面后需多于4次点击等操作才能访问到。无法实现交互式界面展示的，可以发送通知、邮件、提供文档、张贴告示、播放音视频等方式向投资者主动提供或展示；

e） 因产品或服务处理个人信息活动发生变更后更新个人信息保护政策的，可在个人再次使用产品或服务时，使用增强告知或即时提示的方式告知个人信息保护政策中更新的内容。

8.2.1.4 合法性之同意

证券公司收集投资者个人信息依法应当取得个人同意的，应当确保投资者在充分知情的前提下自愿、明确作出同意：

a） 不使用默认勾选方式取得同意；

b） 不采用捆绑方式强迫投资者一次性同意多种业务功能可能收集的个人信息或多个处理活动；

c） 应使用可广泛适用且兼顾特定群体的同意方案，对于线上办理业务的情形，证券公司可通过由投资者在客户端或H5页面勾选同意或弹框确认的形式，事先取得其同意；对于线下办理业务的情形，证券公司可提示投资者现场签署相关协议条款后开展业务办理；

d） 应设置撤回同意的实现机制，并告知投资者行使撤回同意权的具体路径；

e） 不得以投资者不同意处理其个人信息或者撤回同意为由，拒绝向投资者提供服务，为投资者提供服务所必需、履行法定职责或者法定义务的除外。

8.2.1.5 特定对象或场景收集注意点

未成年投资者信息收集：提供产品或服务的业务功能主要面向不满十四周岁未成年人的，证券公司需制定专门的未成年人个人信息保护政策并予以发布。产品或服务涉及收集不满十四周岁的未成年人个人信息的，可通过增强告知方式提示需要向未成年人的监护人告知收集个人信息的情形，以及收集未成年人个人信息的目的、必要性、监护人可代为行使的权利及实现机制等规则。

证券经营场所采集：证券经营场所内安装图像采集仅应用于维护公共安全和履行法定要求目的，并在营业场所设置显著的提示标识告知。

证券App采集信息：

a） 除法律法规另有规定，证券App收集个人生物识别信息、精准地理位置等敏感个人

信息前，应向用户告知处理敏感个人信息的目的、方式、范围等个人信息处理规则以及处理敏感个人信息的必要性和对个人权益的影响（其中证券 App 收集个人生物识别信息前需单独向用户告知），通过弹窗等方式告知并取得用户的单独同意，同时采取严格保护措施；

b) 用户开启业务功能后方可收集其个人信息；

c) 用户选择关闭或退出特定业务功能后，应停止该业务功能的个人信息收集活动；

d) 不得仅以改善服务质量、提升使用体验、研发新产品、增强安全性等为由，强制要求用户同意收集个人信息。

注：证券App、经营场所处理投资者个人信息见附录B。

8.2.1.6 间接获取个人信息

间接获取投资者个人信息时，证券公司应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认；了解个人信息提供方已获得的授权内容，包括使用目的、个人信息主体是否授权同意提供、公开披露等情况；因业务需要证券公司确需超出原授权范围处理个人信息的，应在处理个人信息前取得投资者的明示同意；在停止提供金融产品或服务时，及时停止继续收集个人信息的活动。

8.2.2 投资者个人信息收集环节的保护措施

8.2.2.1 个人信息采集安全策略

投资者个人信息的收集环节具体保护措施和安全策略如下：

a) 3 级、4 级的信息不应委托或授权无金融资质的机构收集；

b) 确保信息来源的可追溯性；

c) 投资者个人信息的采集进行严格的输入合法性验证、准确性验证；

d) 在证券业务信息系统中，应采取具有信息输入安全防护、即时数据加密功能的安全控件对投资者个人信息的输入进行安全保护，并采取有效措施防止合作机构获取、留存投资者个人信息；

e) 证券公司利用生物特征进行客户身份认证的，应当对其必要性、安全性进行风险评估，不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的客户身份认证方式，强制客户同意收集其个人生物特征信息；

f) 对于 4 级的信息，通过证券公司提供的客户端应用软件方式收集时，应使用加密等技术措施保证数据的保密性，防止其被未授权的第三方获取；

g) 涉及嵌入的第三方代码、插件（如 SDK 等）收集个人信息的，应说明第三方身份，以及收集个人信息的种类、目的、方式等；

h) 投资者通过 App 确认同意的记录应在后台进行留存。

8.2.2.2 个人信息质量保证

证券公司收集投资者个人信息需实施质量控制，对投资者个人信息的来源、真实性、时效性、可靠性等进行评估，确保其质量；定期对个人信息进行核查，确保个人信息的准确性和完整性；证券公司应提供投资者个人信息的更正和补充机制，对于投资者提出的更正、补充请求，证券公司应当对其个人信息予以核实，并及时更正、补充。

证券公司受理投资者账户业务时通过中国证券登记结算有限责任公司等提供的身份信息核查接口验证投资者姓名、证件号等信息的真实性和有效性。

8.2.2.3 金融科技运用评估

证券公司运用大数据技术、人工智能、区块链技术为投资者提供产品或服务前，应当对信息采集身份关联、信息流转知情权保障等进行全面测试和评估，构建具有安全性、保密性和专用性的数据处理环境。

8.3 存储

8.3.1 存储地点

a) 投资者个人信息原则上应存储在境内。如因开展业务需要，确需出境的，应提前开展数据出境自评估和申报，详见 8.6.2；
b) 投资者个人信息应存储在证券公司可控区域内，不得通过公有云等非可控方式存储，法律法规与监管机构认可的方式除外；
c) 应尽量避免在公共信息中暴露证券公司投资者个人信息存储的物理地点。

8.3.2 存储期限

8.3.2.1 最小化存储要求

a) 投资者个人信息存储期限应为实现投资者个人信息主体授权使用的目的所必需的最短时间；
b) 超出上述投资者个人信息存储期限后，应对投资者个人信息进行删除或匿名化处理，详见 8.9；
c) 通过投资者个人信息衍生的相关信息应同样遵循最小化存储要求。

8.3.2.2 必要化存储要求

法律法规、监管规定对投资者个人信息存储期限有最低时限要求的，证券公司应遵照相关规定执行。投资者个人信息包括但不限于：

a) 投资者开户个人资料与录像；
b) 投资者委托、交易、转账记录；
c) 投资者交易终端信息；
d) 投资者应用程序使用记录。

8.3.3 存储管理

8.3.3.1 安全管理

a) 应对投资者个人信息存储方式、存储介质、承载的信息系统等内容进行登记管理；
b) 应尽量提高投资者个人信息存储复用性，减少投资者个人信息多余存储；
c) 应以最小化原则建立投资者个人信息存储的权限控制机制，严格控制投资者敏感个人信息授权。

8.3.3.2 安全防护措施

a) 应针对投资者个人信息分级与存储方式采取合适的安全防护措施确保存储安全；
b) 投资者个人信息应结合信息系统维度、是否结构化等因素进行分开存储；
c) 存储投资者敏感个人信息时，可采用加密或安全级别等同的其他防护措施；
d) 投资者个人鉴别信息任何时刻不得以明文存储；
e) 应采取技术措施确保投资者个人信息存储的完整性；
f) 应针对投资者个人信息建立备份机制，防止信息丢失。

8.3.3.3 其他注意事项

a) 不得在移动互联网应用程序客户端明文存储投资者敏感个人信息；
b) 不得在信息系统日志中记录未加密或未脱敏的投资者敏感个人信息；
c) 应针对存储投资者敏感个人信息的移动介质采取两种及以上安全防护手段。

8.4 使用

8.4.1 投资者个人信息使用的情形

证券公司使用投资者个人信息的情形包括但不限于：

a) 证券公司在提供金融产品交易和服务过程中根据交易行为管理、反洗钱管理、尽职调查等要求对投资者个人信息进行监测、分析和展示；
b) 基于证券公司内部经营管理需要对投资者个人信息进行统计、分析等；
c) 其他依据法律规定或合同约定使用投资者个人信息的情形。

8.4.2 投资者个人信息使用限制

证券公司遵循合法、正当、必要和诚信原则，按照法律法规的规定、经投资者确认的个人信息保护政策以及相关协议约定处理投资者个人信息，不得超出正常业务范围使用投资者信息，不得泄露未公开信息。如需将投资者个人信息用于个人信息保护政策未载明或合同约定之外的其他用途的，应再次征求投资者个人信息主体的同意；属于投资者敏感个人信息的，应取得单独同意。

8.4.2.1 合理使用情形

证券公司使用投资者个人信息时，应遵循目的限制原则，不得违背与法律规定的可合理使用的目的，也不得超出与收集个人信息时所告知的目的具有直接或合理关联的范围。证券公司及其工作人员的合理使用的情形有：

a) 根据投资者个人信息主体要求签订和履行合同所必需的；
b) 根据客户交易行为管理相关法律法规的要求开展投资者异常交易行为监测与分析等工作所必需；
c) 开展客户尽职调查、可疑交易监测与分析等反洗钱管理工作所需要；
d) 用于维护所提供的产品或服务的安全稳定运行所必需的，且产品或服务无法安全、稳定运行将可能导致个人权益产生重大影响的，如为发现、处置产品或服务的故障等；
e) 根据法律法规和证券监管规定，为了日常风险管理与监测所需要；
f) 为维护金融产品交易或改善、优化服务，或用于信息系统开发运维测试所必需，该种情形下可对投资者个人信息进行去标识化处理后再开展分析和处理；
g) 将所收集的投资者个人信息用于投资者教育分析、学术研究，属于与收集目的具有合理关联的范围，应在展示结果中对所包括的个人信息进行去标识化处理；
h) 法律法规规定的其他情形。

证券公司不得使用非法获取或来源不明的数据，通过短信、邮件等非自主运营渠道发送投资者敏感个人信息的，应当将投资者账号信息、身份证号码等投资者敏感个人信息进行脱敏处理。

8.4.2.2 特殊使用情形注意事项

证券公司利用算法、画像技术、人工智能等技术分析、加工生成的能识别或关联为投资者个人的衍生信息为投资者个人信息，在使用时需注意：

a) 证券公司应重点关注用户画像所使用的内容，不得包含违法违规情形、侵犯侵害公民、法人和其他组织的合法权益等，应尽量消除明确身份指向性，避免精准定位到特定个人；
b) 运用于个性化推荐、广告推送、精准营销的，不得强制用户使用定向推送功能，需保障投资者知情权和拒绝权；
c) 证券公司应保证自动化决策的透明度和结果公平、公正，以及为个人提供解释说明权、选择权和拒绝权等；
d) 信息汇聚融合的，证券公司应当遵循目的限制原则，并根据汇聚融合后个人信息所用于的目的，开展个人信息保护影响评估，采取有效的个人信息保护措施；
e) 在算法推荐的场景中应避免以下问题：
   1) 未在个人信息保护政策中对用户画像、个性化展示的应用场景及对用户可能造成的影响进行说明；
   2) 未取得用户的明示同意；
   3) 未提供非定向推送信息的选项；
   4) 未向用户提供拒绝接收定向推送的选项；
   5) 未明示信息发送者的真实身份和联系方式；
   6) 以其他不合理的方式影响用户正常使用服务；
   7) 使用非法的用户标签，对用户进行歧视性或偏见性的设置和管理；
   8) 证券公司利用投资者个人信息进行自动化决策时对投资者在交易价格等交易条件上实行不合理的差别待遇。

8.4.3 投资者个人信息使用控制

a) 证券公司应明确投资者个人信息的查询和使用程序，明确数据调用审批程序，建立健全分级审批、双人控制等查询使用制度，防止工作人员行为不当造成投资者个人信息泄露或滥用；
b) 对投资者个人信息进行后台操作应以“一事一议”为原则进行授权、采取双人复核或全程监控方式同时进行操作留痕，并建立检查或审计机制；
c) 其他具体控制措施参见 7.5 访问控制。

8.4.4 投资者个人信息展示控制措施

a) 证券公司提供业务办理与查询等功能的应用软件，及其后台管理与业务支撑系统，在投资者个人信息展示环节具体保护措施如下：依据业务需要，对通过计算机屏幕、客户端应用软件、受理终端设备、自助终端设备、字面等界面展示的投资者个人信息，应采取屏蔽或截词等措施，降低投资者个人信息在展示环节的泄露风险；
b) 在未登录的状态时，不应展示投资者相关的 2 级及以上的信息；
c) 在登录的状态时，不应明文展示 4 级投资者个人信息；对于可直接或组合后确定投资者主体的信息，应进行屏蔽展示或者由投资者选择是否屏蔽展示，如需完全展示，应进行身份鉴别，并做好有关记录，防范此类信息泄露的风险；
d) 在登录状态时，涉及其他投资者的 3 级及以上类别个人信息时，除以下情况外，不直接以明文展示：
   1) 其他方主动发起的活动包含的信息，应展示必要的信息以供活动接收方对活动内容进行确认；
   2) 与其他方已建立信任关系（间接授权），活动发起方应确认发起活动的必要信息的正确性。

8.4.5 投资者个人信息使用中的技术措施

投资者个人信息使用环节具体保护措施和安全策略：

a) 客户交易等重要信息系统应确保运行始终处于证券公司自身控制范围内，不将重要信息系统的运维、日常安全管理交由信息技术服务机构独立实施；
b) 应严格将未经加密、脱敏的投资者个人信息控制在证券公司的网络防护边界内，通过各类技术手段对相关信息进行保护，建立应对网络攻击的反应机制，加强系统防火墙的建设。如应用系统界面中个人信息的必要脱敏展示、技术人员对投资者个人信息有关数据库的脱敏访问、BI 数据分析及数据报告按需自动对投资者敏感个人信息脱敏等；
c) 在防护边界外使用投资者个人信息时，例如外部服务机构协助证券公司进行系统运维、因业务所需与外部合作机构进行有关数据传输等，均需要对投资者个人信息进行加密或脱敏处理，有效降低投资者个人信息的泄露风险；
d) 针对自定义的数据集和用户组，配置并执行访问控制策略，同时支持根据投资者个人信息的分类分级来配置访问控制策略。如引入虚拟账号口令方式代替数据源真实账号口令，降低数据源口令的泄露风险；实施细粒度到人的即时管控，以及监管高危特权；对于高风险数据库操作语句可以根据指令配置访问控制策略，阻断高风险指令的执行；
e) 可采用技术手段对个人信息使用记录进行留痕处理。

8.4.6 投资者个人信息使用中的委托处理

在符合法律法规和中国证监会规定的前提下，证券公司将收集的投资者个人信息委托给第三方机构处理时，可采取以下具体保护措施：

a) 对委托行为开展个人信息保护影响评估，并依据评估结果采取有效措施保护投资者权益；
b) 委托行为保持在已取得的投资者授权同意的范围，同时准确记录和保存委托处理个人信息的情况；
c) 受托人需要严格按照证券公司的要求处理投资者个人信息，如因特殊原因受托人未能按照要求处理个人信息，及时告知证券公司，并采取补救措施以保护个人信息的安全，必要时终止其对个人信息的处理；
d) 与受托人以订立合同等方式约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等。未经书面授权，受托人不应将其处理的个人信息再次委托给其他机构进行处理；
e) 对委托处理的信息采用去标识化等方式进行脱敏处理，降低投资者个人信息被泄露、误用、滥用的风险；
f) 对外部嵌入或接入的自动化工具开展技术检测，确保其投资者个人信息收集、使用行为符合约定要求；并依据合同约定对其收集投资者个人信息的行为进行监督和审计，发现超出约定行为时，立刻切断接入；
g) 委托关系解除时，受托人需要按照证券公司的要求销毁其处理的投资者个人信息，并依据双方协商的期限承担后续的个人信息保密责任。

8.5 加工

8.5.1 投资者个人信息加工的情形

证券公司加工投资者个人信息包括但不限于以下情形：

a) 基于投资者多维度的数据处理加工后形成标签组成的，用于精准地描述一个或者是一类客户特征的用户画像；
b) 将不同产品或服务所收集的投资者个人信息进行汇聚融合；
c) 基于用户画像的自动化决策；
d) 基于用户画像的客户交易行为管理；
e) 投资者个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的去标识化；
f) 投资者个人信息经过处理无法识别特定自然人且不能复原的匿名化；
g) 经纪业务中运用系统自动化匹配投资者分类与产品或服务分级，并出具适当性匹配意见；
h) 反洗钱方面，基于投资者个人信息划分客户风险等级、进行可疑交易预警等，为反洗钱涉密信息，存储于反洗钱系统中，用于金融机构反洗钱履职和洗钱风险管理。

证券公司加工投资者个人信息包括但不限于以下业务类型：经纪、财富管理、资管等业务中（两融、深沪港通、新三板、北交所等业务开通；客户金融产品购买、金融产品投后跟踪；客户投顾产品购买；客户营销展业；客户服务（资讯分享、产品推广、日常运营、好友促活等）；资管产品推荐），在开展相关业务前，判断是否需开展个人信息保护影响评估，具体参见7.6投资者个人信息保护影响评估。

8.5.2 基本原则和要求

应当确保投资者个人信息在加工处理过程中的合规、安全，防止个人信息的泄露、篡改、丢失。

8.5.3 加工处理的防护措施

a) 应采取必要的技术手段和管理措施，确保在投资者个人信息清洗和转换过程中对信息进行保护，对 3 级、4 级信息，应采取更加严格的保护措施；
b) 应对匿名化或去标识化处理的数据集或其他数据集汇聚后重新识别出投资者个人信息主体的风险进行识别和评估，并对数据集采取相应的保护措施；
c) 应建立投资者个人信息防泄露控制规范和机制，防止投资者个人信息处理过程中的调试信息、日志记录等因不受控制的输出而泄露受保护的信息；
d) 应具备信息化技术手段或机制，对投资者个人信息滥用行为进行有效的识别、监控和预警；
e) 应具备完整的投资者个人信息加工处理操作记录和管理能力，记录内容包括但不限于日期、时间、主体、事件描述、事件结果等；
f) 汇聚融合的数据不应超出收集时所声明的使用范围。因业务需要确需超范围使用的，应再次取得投资者个人信息主体明示同意，具体参见 8.2.1.3 合法性之告知和 8.2.1.4 合法性之同意；
g) 应根据汇聚融合后的投资者个人信息类别及使用目的，判断是否开展投资者个人信息保护影响评估。

8.6 传输

8.6.1 境内传输一般要求

a) 证券公司投资者个人信息内部传输应根据法律法规相关要求实施安全技术措施，保证投资者个人信息传输安全性与完整性，包括但不限于：
   1) 运用合适的加密技术和手段，保障投资者个人信息在传输过程中的安全性；

注：采用密码技术时应遵循密码管理相关国家标准。

2) 采取安全传输通道或安全传输协议进行数据传输。
3) 传输投资者个人信息前，通信双方通过有效技术手段进行身份鉴别和认证；
4) 投资者个人信息传输的接收方对接收的信息进行完整性校验；
5) 对投资者个人信息传输安全策略进行审核、监控和优化；
6) 采取有效措施保证数据传输可靠性和网络传输服务可用性。

b) 证券公司使用物理介质（主指移动介质）传输投资者个人信息，应对物理介质采取密码设置等安全措施；
c) 证券公司通过文件传输投资者个人信息，应采取文件加密等必要的安全手段防止信息泄露；
d) 证券公司通过物理介质（主指移动介质）传输投资者个人信息，应设置介质使用期限，到期后及时回收介质并清理投资者个人信息；
e) 向国家机关、证券行业主管和监管单位传输数据，应按照国家及行业相关管理要求进行传输。

8.6.2 跨境传输特别要求

a) 在中华人民共和国境内运营中收集和产生的投资者个人信息向境外传输的，应遵循国家法律法规和中国证监会的规定；
b) 在境内提供证券服务过程中收集和产生的投资者个人信息，应在境内处理。确需向境外机构（含总公司、母公司或分公司、子公司及其他为完成该业务所必需的关联机构）传输投资者个人信息的，应遵守法律法规和中国证监会的相关规定，并按照以下要求执行：
1) 取得投资者个人单独同意，法律法规另有规定的除外；
2) 依据国家、行业有关部门制定的办法与标准开展投资者个人信息保护影响评估，确保境外机构数据安全保护能力达到相应要求；
3) 充分统计评估向境外机构提供投资者个人信息与投资者敏感个人信息的数据量，对照国家相关法律法规要求履行必要的前置审批程序；
4) 应针对投资者个人信息跨境传输开展定期审查。当出现前置审批有效期临期或向境外提供投资者个人信息的目的、范围、种类、敏感程度、方式、保存地点发生变化或境外接收方处理个人信息的用途、方式发生变化或境外接收方当地法律法规发生变化等情形时，应遵循国家相关法律法规要求及时重新完成前置审批程序。
c) 应对境外传输的投资者个人信息进行监控，当发生或可能发生个人信息安全事件时，应当采取补救措施并及时向行业监管部门、省级以上网信部门等相关部门报告；
d) 投资者个人信息处理者及接收方注册于(适用于组织)/位于(适用于个人)粤港澳大湾区内地部分，即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市，或者香港特别行政区的，互相之间发生个人信息传输，可遵循《粤港澳大湾区(内地、香港)个人信息跨境流动标准合同实施指引》的规定。如所处地区对跨境传输有特别规定的，遵照相关规定执行，如《中国（上海）自由贸易试验区临港新片区数据跨境流动一般数据清单操作指南（试行）》。

注：免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证等情况应遵循《促进和规范数据跨境流动规定》。

注：如国家相关法律法规有新增或变化，应遵循国家最新相关法律法规的规定与要求。

8.7 提供

除法律法规和中国证监会另有规定外，证券公司不得以任何方式向其他机构、个人提供投资者个人信息，不得允许或者配合其他机构、个人截取、留存未经匿名化处理的投资者个人信息。

8.7.1 向第三方提供投资者个人信息的情形

证券公司向第三方提供投资者个人信息包括以下情形：

a) 证券监管机构、公安机关、司法机关等有权机关为调查金融领域违法违规、刑事犯罪行为，需要证券公司提供相关投资者的交易数据等个人信息；
b) 开展司法协助业务，根据司法要求配合监管机构提供证券公司客户账户与交易信息；
c) 产品成立或存续期内执行产品报送、报备等要求，如资产管理计划成立、备案及存续运作需向证券监管机构、行业自律组织报送产品投资者信息；
d) 证券公司履行相关法定义务向有关部门报告与报备；
e) 配合证券监管机构、证券交易所、行业自律组织的检查与调查，按要求提供所涉投资者的个人信息；
f) 因合并、分立、解散、被宣告破产等原因转移投资者个人信息；
g) 依据法律法规和中国证监会规定的其他情形。

8.7.2 向第三方提供投资者个人信息的安全防护要求

在向第三方提供投资者个人信息的过程中，具体保护措施如下：

a) 部署信息防泄漏监控工具，监控及报告投资者个人信息的违规传递行为；
b) 部署流量监控技术措施，对共享、转让的信息进行监控和审计；
c) 对投资者个人信息的导出进行操作授权时，应采用口令、密码技术、生物识别技术等两种或两种以上组合的鉴别技术，且其中一种鉴别技术使用密码技术实现，并对导出操作进行细颗粒度的访问控制与全过程审计；
d) 定期检查或评估信息导出通道的安全性和可靠性；
e) 执行严格的审核程序，并准确记录和保存投资者个人信息向第三方提供情况。记录内容包括但不限于日期、规模、目的、范围，以及数据接收方基本情况与使用目的等，并确保提供过程可被追溯；
f) 采取有效技术防护措施，防范信息转移过程中被其他个人、组织和机构截获和利用；
g) 因合并、分立、解散、收购、兼并、重组、破产等情况，对投资者提供金融产品或服务的证券公司主体变更而发生投资者个人信息共享、转让时，证券公司应通过逐一告知（或公告）等方式通知投资者。接收方对其接收运营的金融产品或服务继续履行投资者个人信息保护责任。接收方如变更其在收购、兼并重组过程中获取的个人信息使用目的，接收方应重新取得投资者明示同意或授权。

以上要求仅适用于法律法规和中国证监会规定的向第三方提供投资者个人信息的情况。

8.7.3 投资者个人信息向境外提供的实施要点

a) 除法律法规另有规定，向境外提供个人信息的，需向个人告知境外接收方的身份、联系方式、处理目的、处理方式，个人信息的种类、保存时间、保存区域（至少具体到国家或地区）以及个人向境外接收方行使相关权利的方式等内容，并取得个人的单独同意；

注：个人在自行了解境外接收方所公布的个人信息处理规则后，主动以邮件、短信息、点击启动服务、在线提交信息或直接确认等方式向境外接收方发送涉及其个人信息内容的，可视为个人行为或作出了单独同意。

b) 如产品或服务中涉及个人信息出境的业务功能可与其他业务功能相分离的，证券公司应将涉及个人信息出境的业务功能与其他业务功能区分，以便个人针对个人信息出境作出单独同意；
c) 提供的个人信息仅限于实现处理目的所需最小范围；
d) 个人拒绝涉及个人信息出境的业务功能后，不能影响其他业务功能的正常使用；
e) 收集个人信息时已事前单独就个人信息出境取得个人同意，满足出境其他条件的前提下，后续在出境时可不再次取得个人单独同意。

注：涉及跨境传输的规范参见8.6.2跨境传输特别要求。

8.8 公开

8.8.1 投资者个人信息公开的基本要求

8.8.1.1 投资者个人信息公开的情形

证券公司公开投资者个人信息包括但不限于以下情形：
a) 证券公司在开展证券承销与保荐等投资银行业务的过程中，根据法律法规、监管规定、自律规则等规定或要求，披露投资者的持股情况等个人信息；
b) 证券公司自身在融资过程中，通过发行文件、申报材料等披露与投资者相关的重大交易、诉讼（仲裁）等信息；
c) 投资者通过证券公司组建的群组发言、对证券公司官方社交媒体账号（如官方微博、微信公众号等）发布的信息进行评论回复、参加证券公司组织的抽奖、投票、比赛、评选、宣传、推介等活动也可能导致个人信息被公开；
d) 其他基于法律、法定程序、有权机关强制性规定或要求等，公开投资者个人信息；
e) 其他基于履行法定义务、法定职责或维护国家安全、公共利益，公开投资者个人信息。

8.8.1.2 公开的原则和要求

证券公司原则上不得公开所收集的投资者个人信息，经法律授权或具备合理事由确需公开时，应符合以下要求：
a) 事先开展个人信息保护影响评估，并依据评估结果采取有效的保护个人信息主体合法权益和信息安全的保障措施，防止信息被篡改、滥用等风险；
b) 除法律另有规定外，事先应向投资者告知信息公开的目的、类型，并取得投资者的明示、单独同意；
c) 公开投资者的敏感个人信息前，还应事先告知投资者涉及的敏感个人信息的内容；
d) 相关法律法规、监管规定、自律规则或与投资者签订的合同对信息公开有明确规定或约定的，应严格按照规定或约定的范围、时间、渠道、方式、程序等规则实施信息公开具体行为；
e) 不得公开投资者的个人生物识别信息以及种族、民族、政治观点、宗教信仰等敏感个人信息的分析结果；
f) 建立、维护、更新投资者个人信息公开记录，准确记录和保存投资者个人信息公开的情况，包括公开的日期、信息类型及具体内容、公开目的、公开渠道、公开方式、处理信息公开的人员等情况；
g) 根据法律法规或合同约定，承担因不当公开行为损害投资者合法权益的相应责任。

8.8.2 投资者个人信息公开环节的保护措施

证券公司在公开投资者个人信息时，应采取以下措施保护投资者个人信息安全：

a) 明确投资者个人信息公开的管理部门及人员，并对相关人员开展具体工作有关的管理与培训；
b) 明确涉及投资者信息公开相关工作的操作规程，建立复核机制，避免因信息公开错误等不当行为给投资者造成不利后果或影响；
c) 有效开展投资者个人信息公开前的保护影响评估；
d) 建立投资者个人信息公开安全事件应急处置和报告、安全事件告知、补救及损害救济机制；
e) 开展投资者个人信息保护相关的教育活动，帮助投资者了解信息公开与保护的规则、机制；
f) 将投资者信息公开相关的活动纳入个人信息安全与保护的审计范围，对相关制度流程、保护政策和安全措施的有效性进行审计，及时发现并处理投资者个人信息公开违规行为；
g) 通过客服热线等方式受理投资者对证券公司信息公开规则或公开活动存在的疑问或异议，及时对投资者进行解释说明或采取补救措施。

8.9 删除

8.9.1 基本要求

证券公司在处理投资者个人信息过程中应保障投资者个人信息删除权，证券公司可制定内部数据安全及档案管理相关制度，根据各业务的需要，综合考虑各项因素后（如是否已销户、是否存在纠纷、诉讼时效等）确定各业务涉及的个人信息保存期限及保存的具体方式等，并向投资者明确告知权利、权利例外、删除时限、删除渠道以及替代删除手段，并在业务环节中建立投资者个人删除的落地措施。

8.9.2 投资者个人信息删除环节的保护措施

a) 在公司制度和操作细则中明确删除投资者个人信息的“双向主动”属性：投资者有权利主动要求证券公司删除“最小必要”原则之外的个人信息，证券公司也可按照法律法规要求主动删除“最小必要”原则之外的投资者个人信息；
b) 因业务、产品终止或撤回同意，投资者提出删除其个人信息的要求，证券公司应依据法律法规、证券期货行业主管部门有关规定及与投资者的约定予以响应；
c) 与证券公司提供产品或服务非直接相关投资者个人信息，如仅为改善服务、提升系统功能体验而收集的投资者个人信息，在满足法定情形、确认没有法定或主管部门规定的保存期限或超出保存期限且没有继续保存的必要性的个人信息应予以删除；
d) 证券公司提供产品或服务时依法或者依照合同约定收集的投资者个人信息，在投资者主动提出删除要求时，应首先判断是否符合已满足法定及主管部门规定的最低保存期限。如仍在法定或主管部门规定的保存期限内或存在其他应履行的法定职责或义务需要继续保存客户个人信息的情形，证券公司可拒绝删除并告知投资者理由；如已超过法定或主管部门规定的保存期限，可对投资者进行个人信息删除后果的告知，并由投资者签署书面申请后再进行具体的删除操作；
e) 证券公司可在信息保存满足法律法规和监管要求的基础上，结合投资者个人信息分级和监管存储期限要求，在公司制度和操作细则中针对不同分类分级的投资者个人信息，提出相应的删除时间要求。

8.9.3 证券公司删除投资者个人信息的情形

a) 符合以下情形，根据法律法规要求，或投资者要求证券公司删除个人信息的，应及

时删除个人信息:

1) 违反法律法规规定，收集、使用投资者个人信息的；
2) 违反与投资者的约定，收集、使用投资者个人信息的；
3) 处理目的已实现、无法实现或者为实现处理目的不再必要；
4) 证券公司停止提供产品或者服务，且满足有关行业监管规定时；
5) 其他法律法规要求删除投资者个人信息的情形。

b) 证券公司违反法律法规规定或违反与投资者的约定向第三方共享、转让投资者个人信息,且投资者要求删除的，证券公司应立即停止共享、转让的行为，并通知第三方及时删除；

c) 证券公司违反法律法规规定或违反与投资者的约定，公开披露投资者个人信息，且投资者要求删除的，证券公司应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。

8.9.4 委托处理、共同处理、共享处理的情况下的删除

证券公司除自身保障客户删除权的行使外，还应注意委托处理、共同处理、共享处理的第三方相应删除义务的履行情况，保障投资者对于第三方信息删除的权利：

a) 证券公司如作为投资者个人信息委托处理的委托方,应当在委托合同中明确在不生效、无效、被撤销或者终止的情况下,受托方有义务及时返还个人信息或予以删除,证券公司应通过技术手段及违约责任等方式切实约束受托方,确保受托方履行上述返还或删除义务，保障投资者信息删除权的实现；

b) 涉及到共同处理的情况下,证券公司除应慎重选择共同处理方及在相关的协议中约定各方的责任及追偿等条款外，还应在客户要求删除相关个人信息时，提示客户存在共同处理的情形，如客户要求共同处理方删除，应将客户相关要求转达给共同处理方；

c) 证券公司向其他个人信息处理者提供其处理的投资者个人信息的,为了避免接收方在未单独征求投资者单独同意的前提下超出原授权的处理目的和方式使用客户信息，在投资者要求删除其个人信息时，可再次提示投资者存在信息共享的情形，并根据投资者的要求协助转达删除申请。

8.9.5 建立合理合规的删除制度机制

证券公司在开户告知书、App 用户协议、第三方机构合作协议、证券公司个人信息保护政策等环节确保下列事项的明确沟通：

a) 删除权利告知；
b) 收到投资者删除请求的处理方式和时限；
c) 向投资者通知证券公司如何对个人信息进行删除或匿名化处理；
d) 明确投资者请求删除的渠道；
e) 告知投资者行使删除权可能对其造成的影响，以助于其作出行使相关权利的判断；
f) 第三方机构删除投资者个人信息的明确义务和操作机制。

注：删除权的告知应在收集个人信息阶段完成，具体告知规范参见 8.2.1.3 合法性之告知。

8.9.6 请求删除的渠道

证券公司在履行主动删除义务的同时，应为投资者提供请求删除的渠道，如：

a) 证券公司 App 或官方网站提交删除申请；
b) 现场或电话提交删除申请；
c) 被授权人代提交删除申请。

8.9.7 例外情形

证券公司应在提供产品或服务前，向投资者明示删除投资者个人信息的例外情形：

a) 监管有保存期限法律法规要求的个人信息，包括：客户开户资料、委托记录、交易记录和与内部管理、业务经营有关的各项信息；登记、存管和结算的原始凭证及有关文件和资料；监控档案；做市业务，对报价和成交数据；证券投资顾问业务档案等；

b) 技术难以实现删除的个人信息，如：云存储的情形下，除非全部清空用户的数据，否则无法删除个人信息的情形等；

c) 证券公司可关注新技术带来的删除权例外情形。

注：此处的技术难以实现指现有的技术根本无法删除个人信息或者在现有的技术条件下需要付出不合理成本才能删除。

8.9.8 保障措施

证券公司在信息不可删除的情形下，应采取合理措施充分保护投资者个人信息：

a) 受监管存储期限限制，不可删除的个人信息，应做到明确告知投资者；

b) 在监管存储要求期限内，应建立安全的个人信息储存系统和健全的硬件设施，确保在技术上妥善保护投资者个人信息；

c) 停止除存储和采取必要的保护措施之外的处理；

d) 监管存储期限到期后，证券公司应谨慎评估继续保存的必要性，并对无必要继续保存的投资者个人信息进行及时删除；采取去标识化等脱敏技术手段，降低个人信息对投资者的关联程度。

附录 A
（资料性）
投资者个人信息分类分级参考表

个人信息	子类	说明	敏感	分级
投资者个人基本信息	/	开展证券交易的自然人、法人、非法人组织，以及依法设立的金融产品所涉及的自然人的个人基本信息,包含姓名、性别、民族、出生日期、年龄、联系地址、移动电话、电子邮件、国籍等信息。	/	3
投资者个人身份信息	个人身份证件信息	投资者个人证件类型、证件号码、证件地址、证件有效期、签发机关等。证件类型包括身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等。	是	3
	特定身份信息	残障人士身份信息、犯罪人员身份信息、特定工作信息（如军人、警察）等个人信息。	是	3
投资者个人鉴别信息	投资者账户认证	投资者的账户认证信息，包含投资者用于身份认证的账户密码、数字证书、动态口令、口令保护答案、短信验证码等。	是	4
	个人生物识别信息	用于投资者鉴别的个人生物识别信息。指纹认证信息、人脸认证信息等。	是	4
投资者个人账户信息	开户/账户信息	投资者与业务活动相关的识别信息，包含账户名称、投资者标识、账户类别、账户编码、账户用途、账户状态代码等信息。	是	3
	投资者编码	投资者在证券公司的内部统一编码。	/	2
投资者个人交易信息	成交信息	投资者买卖证券产品的成交相关信息，包含证券账户编码、银行账户编码、市场代码、证券代码、成交金额、成交数量、成交时间、成交价格、成交日期、委托编号、席位代码、经手费、证管费、印花税、佣金等。	是	3
	委托信息	投资者买卖证券产品的委托相关信息，包含证券账户编码、市场代码、证券代码、委托价格、委托数量、委托方向、委托类型、委托时间、委托日期、委托渠道、席位代码等。	是	3
	银证转账	投资者通过三方存管账户进行的资金划转相关信息，包含营业部编码、账户编码、银行代码、发生金额、发生日期、发生时间、渠道代码等。	是	3

	交易业务参数信息	证券产品交易业务规则中定义的，完成交易所需的参数，如账户编码、交易时段、涨跌幅、交易单元等。	/	2
	交易日志信息	投资者行为相关信息，可分为注册登录日志、信息变更日志等多类，包含发生日期、发生时间、来源等信息。	/	3
	其他交易信息	有关规定要求的反映交易真实情况的合同、业务凭证、单据、业务函件和其他资料。	/	3
投资者个人财产信息	持仓信息	投资者持有某一证券、期货、基金等品种的信息，包含证券账户编码、市场代码、证券代码、持仓数量、持仓日期、市值等。	是	3
	银行账务信息	投资者开立的用于交易、结算业务的账户信息，包含开户网点信息、银行账户、币种代码等。	/	3
	资金状况信息	投资者资金账户余额信息，包含币种代码、银行账户、资金余额、个人收入状况等。	是	3
投资者个人信用信息	/	指投资者的信用相关信息，包含信用账户编码、信用等级、信用额度、融资融券偿还情况以及投资者在交易活动中形成的，能够反映其信用状况的其他信息。	是	3
投资者个人合约合同	/	指参与交易活动所产生的契约信息，包含账户编码、流水号、合同号、市场代码、证券代码、证券数量、发生金额、归还日期等。	是	3
投资者个人行为信息	/	投资者在 App、网站中的行为埋点信息、操作日志等。	/	2
投资者衍生信息	/	一般指对投资者交易及行为数据进行处理、分析所形成的反映特定投资者某些情况的信息，包含:投资者分类、投资能力、投资意愿、行为习惯、兴趣偏好等。	/	2
投资者个人设备信息	可变更的唯一设备识别码	AndroidID、、广告标识符（IDFA）、应用开发商标识符 （IDFV）、开放匿名设备标识符（OAID）等，以及机型、系统版本、存储位置等在内的描述个人常用设备基本情况的信息。	/	3
	不可变更的唯一设备识	包括硬件序列号、设备 MAC 地址、唯一设备设别码（如 IMEI/Open UDID/GUID/SIM 卡 IMSI 信息等）。	/	3

	别码			
	应用软件列表	用户在终端上安装的应用程序列表。	/	3
投资者个人位置信息	粗略位置信息	仅能定位到行政区、县级等的位置信息，如地区代码、城市代码等。	/	2
	行踪轨迹信息	包括精准定位信息、经纬度等。	是	3
个人健康生理信息、医疗信息	健康状况信息	与个人身体健康状况产生的相关信息，如体重、身高、体温、肺活量、血压、血型等。	是	3
	医疗健康信息	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。	是	3
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、成绩单等。	/	3
个人其他信息	/	宗教信仰、性取向、婚史、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、网页浏览记录等。	是	3
客户关系信息	/	证券公司与投资者之间在销售、营销和服务上的交互信息数据。	/	3
客户服务信息	/	指证券公司开发新投资者及维护老投资者形成的对客户的联系、服务、售后等信息定期管理的记录。	/	3
客户经营关系	/	指证券公司对投资者交易、持仓和资金情况的分析数据，例如对投资者的盈利、交易量、资产等情况的汇总数据。	/	2
渠道信息	/	指证券公司对投资者进行营销、客户服务等活动中所使用的信息渠道信息。	/	2
市场营销推广信息	/	证券公司对投资者进行营销推广活动中产生的数据信息。	/	2

服务机构和人员信息	/	证券公司提供投资者服务的部门基本信息，证券公司提供投资者服务的人员开展业务服务所需的基本信息。	/	2

注：投资者个人信息分类分级参考表中未包含的类型，可参考 GB/T 43697-2024《数据安全技术 数据分类分级规则》附录 B。

附录 B
（资料性）
特定场景中的投资者个人信息保护

B.1 场景一：证券公司营业场所场景下的投资者个人信息保护

B.1.1 概述

证券公司营业场所场景包括：

一般营业场所：出于安全的目的，在办公地等公共场所安装图像采集、个人身份识别设备[1]。

客户交易区：根据《关于加强证券期货经营机构客户交易终端信息等客户信息管理的规定(2022 修正)》（证监会公告[2022]43 号）规定[2]在客户交易区安装监控录像设备。

B.1.2 收集的内容

可能被采集的个人信息种类通常包括人脸图像等。

B.1.3 信息的处理

B.1.3.1 使用

a) 在营业部等经营场所安装摄像头等采集的影像信息不得使用人脸识别技术进行人脸验证、辨识或者分析；

b) 应安排专人对监控信息进行管理，对查阅、复制、调取信息资料的人员、时间、用途及去向等情况进行登记；

c) 公安机关等行政主管部门因执法工作需要查阅、复制或者调取公共安全视频图像信息系统的信息资料或者直接接入监控系统的，应当依据有关法律、法规的规定执行；

d) 除维护公共安全的目的以外，未经个人单独同意，不得公开或者向他人提供其收集的个人图像、身份识别信息。

B.1.3.2 收集

除落实本规范第 7 章和第 8 章的要求外，其他实施要点如下：

a) 基于公共安全或监管规定安装监控录像设备，属于可免于同意情形；

b) 在营业部等公共场所通过设备采集个人信息时，需以显著方式向用户展示个人信息处理规则。显著方式通常是指在醒目位置张贴、播放简短易懂的告知内容，同时告知获取更多相关信息的途径；

c) 在摄像头安装处张贴告示向用户告知简要的个人信息处理规则；

示例：为保障用户人身财产安全，此处摄像头将记录个人影像信息，我们承诺会保护数据安全，了解详情可拨打电话或扫描二维码；

d) 注意客户交易区安装的监控录像设备位置，不得从录像设备获取投资者交易密码等资料。

B.1.3.3 存储

[1]部分地方政府曾发布公共安全视频图像信息系统相关规定，如《广东省公共安全视频图像信息系统管理办法》。

[2] 《关于加强证券期货经营机构客户交易终端信息等客户信息管理的规定》第十二条第二款规定：证券期货经营机构应妥善保存交易时段客户交易区的监控录像资料，保存期限不得少于 6 个月。

除落实本规范第 7 章和第 8 章的要求外，其他实施要点如下：

a) 客户交易区的监控录像资料，保存期限不得少于 6 个月；其他位置的监控录像资料，不得低于地方政府规章规定的保存期限；

b) 监控系统应按当地地方政府规定进行备案。

B.2 场景二：非现场开户场景下人脸识别中的个人信息处理

B.2.1 概述

目前，非现场开户包括见证开户和网上开户。见证开户是指证券公司工作人员面见客户，通过适当的方式或信息技术手段验证客户身份、见证客户签署开户相关协议后，按规定程序为客户办理资金账户开户。网上开户是指证券公司通过网上开户系统，以适当的方式或信息技术手段验证客户身份，并与客户签署开户相关协议后，按规定程序为客户办理资金账户开户。

非现场开户中，投资者身份验证涉及单向视频活体检测以及人脸识别比对等。

B.2.2.收集的内容

可能被采集的个人信息种类通常包括人脸图像、人脸认证信息等。

B.2.3 信息的处理

B.2.3.1 收集

a) 收集人脸识别信息时，应向投资者告知人脸识别信息的相关事项，包括但不限于数据处理者的名称和联系方式、处理规则、必要性依据等，收集开户所必需的信息可以免予同意；收集非开户所必需信息时需取得投资者单独同意；

b) 采用需要投资者主动配合的措施收集人脸识别信息，应在识别过程中持续告知投资者验证目的，并通过语言文字等向投资者进行提示；

注：需要投资者主动配合的措施包括要求投资者直视收集设备并做出目光注视、特定姿势、表情，或者通过标注了人脸识别应用的文字、图示、图标或符号的专用收集通道等。

c) 应仅收集生成人脸识别所需的最小数量、最少种类的人脸图像；

d) 应采取安全措施保证人脸识别数据的真实性、完整性和一致性，防止人脸识别数据在收集过程中泄漏或篡改。

B.2.3.2 使用

a) 处理人脸识别信息应当事前进行个人信息保护影响评估；

b) 应采取数据完整性校验、数据加密等措施保障人脸识别数据传输安全；

c) 人脸信息原始样本应在完成认证功能后，立即删除、不得保存。

B.2.3.3 提供、公开

a) 除非经投资者单独同意或书面同意，不应公开人脸识别数据；

b) 不应向第三方提供或委托处理人脸识别信息。符合法律法规和中国证监会规定下的提供或委托处理，应按照本规范的第 7 章进行有关评估与告知。公安系统联网验证应属于可免于单独同意情形。

B.2.3.4 存储

a) 因非现场开户所必需收集人脸识别信息，按照监管规定，保存至客户关系终止后 20 年；

b) 因其他业务需要收集的人脸识别信息，应按照与投资者的约定时限及时删除。

B.2.3.5 评估

a) 事前评估

人脸识别技术使用者处理人脸信息，应当事前进行个人信息保护影响评估，并对处理情况进行记录。个人信息保护影响评估主要包括下列内容：

1） 是否符合法律、行政法规的规定和国家标准的强制性要求，是否符合伦理道德；
2） 处理人脸信息是否具有特定的目的和充分的必要性；
3） 是否限于实现目的所必需的准度、精度及距离要求；
4） 采取的保护措施是否合法有效并与风险程度相适应；
5） 发生或者可能发生人脸信息泄露、篡改、丢失、毁损或者被非法获取、非法利用的风险以及可能造成的危害；
6） 可能对个人权益带来的损害和影响，以及降低不利影响的措施是否有效。

b) 持续评估

在使用人脸识别技术过程中，应当对设备的安全性及处理人脸信息的目的、方式等事项进行持续评估与审计，并记录评估、审计过程和结果，根据检测评估情况改进安全策略，调整置信度阈值，采取有效措施保护图像采集设备、个人身份识别设备免受攻击、侵入、干扰和破坏。

B.3 场景三：代销金融产品场景下的个人信息处理

B.3.1 概述

代销金融产品，是指证券公司接受金融产品发行人的委托，为其销售金融产品或者介绍金融产品购买人的行为。

B.3.2 收集的内容

a) 投资者基本信息。自然人的姓名、住址或邮寄地址、学历、年龄、联系方式（邮箱及手机号码）、有效身份证件、出生地、出生日期、性别、国籍等基本信息、开展金融相关业务资格证明、机构负责人或者法定代表人信息、经办人身份信息、联系方式；税收居民身份证明；金融账户信息；产品份额持有人、实际控制投资者的自然人和交易的实际受益人等；

b) 投资者资产状况。收入来源和数额、资产、债务等财务状况及对应的证明文件；

c) 投资者投资经验。投资相关的学习、工作经历、投资经验（包括投资期限、实际投资产品类型、投资金融产品的数量、参与投资的金融市场情况）及对应的证明文件；

d) 相关专业资质。包括获得职业资格认证的从事金融相关业务的注册会计师和律师等资格及对应的证明文件；

e) 投资风险偏好。投资目的、投资期限、品种、期望收益等投资目标；风险偏好及可承受的损失；

f) 诚信记录。包括征信信息、资本市场相关诚信记录查询；

g) 适当性管理过程相关录音录像材料；

h) 投资者购买产品所生成的金融资产相关信息。包括但不限于所持有的份额的数量、净值等信息；份额变动信息，包括认购/申购、赎回、转让、质押、冻结、清算等；

i) 投资者敏感个人信息。投资者的特定身份、金融账户，部分登录系统的还可能涉及指纹认证信息、人脸认证信息、行踪轨迹等信息；

j) 法律法规、自律规则规定的投资者相关信息，以及其他必要信息。

B.3.3 信息的处理

除落实本规范第 7 章和第 8 章的要求外，其他实施要点如下：

B.3.3.1 收集

证券公司作为代销机构，因适当性管理、洗钱风险管理、账户实名制管理、网络安全管理、投资者资金安全等履行法定职责或者法定义务所必需，或为投资者认购/申购、赎回所必需收集、处理投资者个人信息，属于免于同意的情形。

B.3.3.2 提供

如管理人根据本行业或机构需要要求证券公司提供其自身管理范围之外的信息或者基金合同等文件约定之外的个人信息，宜审慎评估；如不属于法定义务或履行合同所必需的信息，应按照委托处理情形取得投资者单独同意。

B.3.4 代销协议个人信息保护条款要点

确认委托人与证券公司均为个人信息处理者；明确代销场合个人信息处理的目的；明确双方各自在个人信息保护相关的权利义务。要点如下：

示例：《金融产品销售协议之个人信息保护条款》参考要点

甲方：**基金管理有限公司
乙方：**证券股份有限公司
一、个人信息保护

（一）释义

本协议所指的“个人信息”是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。

本协议所指的“投资者敏感个人信息”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，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

本协议所指的“个人信息的处理”包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

（二）个人信息的处理

1.依据法律法规规定及《销售协议》的约定，为配合甲方履行其反洗钱、投资者适当性、反恐怖融资、反贿赂、制裁、非居民金融账户涉税信息(CRS)尽职调查等法定义务，以及履行投资者作为一方当事人的合同所必需之目的，乙方应向甲方提供其处理的投资者个人信息。就此，甲乙双方应当依据法律法规的规定就各自的个人信息处理活动向相关信息主体履行必要的告知义务；

依据法律法规及《销售协议》的约定，为向投资者提供持续信息服务，甲方将向乙方提供相关基金投资者份额确认等信息，将涉及投资者个人信息的处理。

2.依据法律法规规定，为实现向投资者提供服务等本条第 1 款所述之外的目的，乙方应向甲方提供其处理的投资者个人信息(具体信息种类、处理目的、处理方式见下文第 3 项)。就此，乙方应当依据法律法规的规定向相关个人履行必要的告知义务，并取得个人的单独同意；

甲方要求乙方提供经相关个人确认后的同意函等证明文件(原件、复印件或扫描件)时，乙方应当及时提供。乙方拒绝提供证明文件(原件、复印件或扫描件)的，视为未取得相关个人的同意，并视为乙方违反《销售协议》之约定，甲方有权据此终止《销售协议》。

为履行《销售协议》而涉及个人信息收集的，甲、乙方应当限于实现处理目的的最小范围，不得过度收集个人信息。

3.为实现 2 所述之目的，乙方应当向甲方提供的投资者个人信息种类、甲方处理目的、处理方式如下:

（1）列举为实现除履行法定义务及履行个人作为一方当事人合同之外的目的，乙方应当向甲方提供的投资者个人信息；

（2）列举为实现除履行法定义务及履行个人作为一方当事人合同之外的目的，甲方就乙方提供的投资者个人信息的处理目的；

（3）列举为实现除履行法定义务及履行个人作为一方当事人合同之外的目的，甲方就乙方提供的投资者个人信息的处理方式；

乙方应根据第 2 项的要求，向个人告知上述个人信息的种类、处理目的和处理方式、信

息接收方的名称和联系方式等要素。涉及投资者敏感个人信息的，乙方还应当向个人告知处理投资者敏感个人信息的必要性以及对个人权益的影响。

如因甲乙双方业务需求变化等原因导致上述内容变更的，乙方应当重新取得个人同意。

4.乙方依照法律法规要求和《销售协议》约定向甲方提供的投资者个人信息，甲方的处理目的应限于前述目的，处理方式应限于为实现前述目的的最小必要范围。如甲方超出前述范围处理个人信息，应自行取得个人的单独同意。

5.甲、乙方确保双方就个人信息的传输方式、传输手段、处理方式等均符合法律法规的规定，采取必要的技术防护措施，降低个人信息转移或交换或处理过程中的安全风险。

6.如未来法律法规或甲乙双方业务需求发生变化，甲乙双方可就个人信息的处理达成补充协议。签署本协议并不构成甲方与乙方共同处理个人信息，亦不构成甲方委托乙方处理个人信息。未经一方同意，另一方不得以与该方为共同个人信息处理者或该方的代理人/受托方名义处理个人信息。

二、违约责任

（一）甲乙双方应严格遵守《中华人民共和国个人信息保护法》的规定及本协议约定，在各自义务范围内履行投资者个人信息保护义务。

（二）违反投资者个人信息保护义务的，由甲、乙方各自向投资者承担责任。

三、其他

（一）除双方另有约定外，本协议适用于甲方已经发行的及今后发行的并经乙方销售的各基金。

（二）甲乙双方为履行本协议所相互提供的信息以及本协议本身均属保密信息，未经对方书面同意，不得向第三方披露，但法律、法规另有规定或监管部门另有要求的除外。

B.4 场景四：互联网营销场景下自动化决策中的个人信息处理

B.4.1 概述

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。《中华人民共和国个人信息保护法》侧重于销售端的自动化决策，如向个人进行信息推送、商业营销等。

B.4.2 收集的内容

B.4.2.1 投资者填写

a) 基本信息：申请开户时间、客户姓名、出生日期、客户年龄、有效身份证件的类型和号码、手机号码、电话号码；
b) 个人背景：兴趣爱好、毕业院校、所处行业、所在单位、婚姻情况、家庭人口数、子女数量、血型、性格类型、偏好、联系方式、邮箱、微信；
c) 财务背景：个人年收入、家庭年收入、收入来源、家庭资产规模、家庭资产组成、置业情况、金融资产、保险、借贷情况、证券投资比重、负债率、家庭人均年收入、月均还贷支出、家庭月均支出、家庭备用金情况、家庭人口数、赡养负担、配偶具体情况、子女具体情况；
d) 投资经验：投资风格、投资收益目标、预期回报率、从事投资年限、行业偏好、投资决策方法、投资证券经验、曾参与投资品种。

B.4.2.2 系统生成

a) 基本信息：开户成功时间、风险等级、风测到期日期、普通账户佣金率、信用账户普通交易佣金率、信用账户信用交易佣金率、开户营业部、风险承受能力；
b) 客户资产：可用资产、股票资产、理财产品、两融余额；
c) 客户交易：证券代码/证券名称、成交数量、成交价格、成交金额、实收佣金、柜台净佣金。

B.4.2.3 证券公司填写

行为特征：客户分类、操作方式、投资板块、投资行业、投资题材、持仓偏好、交易习性、活跃程度、资产规模、账户盈亏情况、交易频次、客户年龄层、投资性格、服务偏好、产品偏好、服务内容需求、交易风格、客户操作依据、性格特征。

B.4.3 自动化决策过程

证券公司的信息系统首先对收集的投资者个人信息基础数据进行清洗，过滤明显偏离正常范围的数据，通过既定的满足外规要求和业务需求的规则对基础数据进行加工和分类，形成标签，标签应通过系统间加密流转和自动化加工形成。单个投资者拥有多维度的标签后，形成用户画像。

目前自动化决策更多地运用于经纪、财富管理、资管等业务中。基于用户画像的自动化决策将进行精准营销及产品推荐，需重点关注数据来源的合法合规性、控制信息泄露和滥用的风险。

B.4.4 自动化决策注意事项

自动化决策涉及处理投资者个人信息，应公开或告知投资者个人信息处理规则，明示处

理的目的、方式和范围并取得投资者的同意，具体参见 8.2.1.3 合法性之告知和 8.2.1.4 合法性之同意。

证券公司利用投资者个人信息进行自动化决策应当事前进行个人信息保护影响评估，并对处理情况进行记录。

评估点应至少包括但不限于以下内容：

a) 是否向用户说明了自动化决策的基本原理或运行机制；

b) 是否定期对自动化决策的效果进行评价；

c) 是否对自动化决策使用的数据源、算法等持续优化；

d) 是否向用户提供针对自动化决策结果的投诉渠道；

e) 是否支持对自动化决策结果的人工复核。

证券公司利用投资者个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对投资者在交易价格等交易条件上实行不合理的差别待遇。向不同特征的投资者推荐同样的产品或服务时，应提供一致的价格。

通过自动化决策方式向投资者进行信息推送、商业营销，应当同时提供不针对投资者特征的选项，让投资者可在通用的信息推送、产品和服务营销以及量身定做的信息推送、产品和服务营销中进行选择；或者向投资者提供便捷的拒绝接受为其量身定做的信息推送、产品和服务营销的方式。

通过自动化决策方式作出对投资者个人权益有重大影响的决定，证券公司应让投资者知晓其有权要求证券公司予以说明，投资者有权拒绝证券公司仅通过自动化决策的方式作出决定。如自动化决策用于内部反洗钱管理，基于客户信息自动划分客户风险等级、进行可疑交易预警；用于适当性管理，经纪业务中运用系统自动化匹配投资者分类与产品或服务分级，并出具适当性匹配意见等对投资者个人权益有重大影响的决定时，证券公司应让投资者知晓其有权要求证券公司予以说明，并有权拒绝证券公司仅通过自动化决策的方式作出决定。

B.5 场景五：证券公司移动互联网应用程序（App）的投资者个人信息保护与合规评估

B.5.1 概述

证券公司涉及投资者个人信息处理的移动互联网应用程序（以下简称App）主要包括证券交易类App与业务办理类App。证券公司应针对相关App建立个人信息保护机制及个人信息处理合规评估机制。

B.5.2 证券公司App个人信息处理内容

B.5.2.1 证券交易类App处理的个人信息内容主要包括：

a) 个人基本资料：个人姓名、电话号码、出生日期等；
b) 网络身份标识信息：App主体账号、内外网IP地址等；
c) 个人财产信息：银行账号、资金账号、密码口令、资产信息、委托交易流水、转账流水等；
d) 个人上网记录：App操作记录、订阅信息等；
e) 个人常用设备信息：MAC地址、IMEI、IDFV、注册手机号码、App登录手机号码、设备品牌型号、操作系统版本、App版本等。

B.5.2.2 业务办理类App处理的个人信息内容主要包括：

a) 个人基本资料：个人姓名、手机号码、出生日期、民族、国籍、联系地址等；
b) 个人身份信息：身份证、港澳台证件、护照、驾驶证、军官证等；
c) 个人生物识别信息：人脸认证信息、双录视频等；
d) 网络身份标识信息：App主体账号；
e) 个人教育工作信息：学历、职业、工作单位、收入等；
f) 个人上网记录：App操作记录、订阅信息等；
g) 个人位置信息：定位信息等。

B.5.3 证券公司App个人信息保护实施要点

证券公司App应遵循本规范中投资者个人信息全生命周期保护基本要求，以下具体实施要点可供参考。

B.5.3.1 收集

a) 投资者在同意个人信息保护政策前，确保App不收集任何个人信息；
b) 证券公司App应以最小化、必要性为原则收集个人信息。不得因投资者拒绝非必要个人信息收集，影响投资者使用证券交易、业务办理等基本功能；
c) 当App功能更新引起个人信息收集发生变化时，证券公司应及时更新个人信息保护政策；
d) 证券公司App应根据法律法规要求准确收集记录投资者个人交易终端信息；
e) 证券公司App应建立已收集个人信息清单并在二级菜单中展示，应简洁、清晰列出App（包括内嵌第三方软件工具开发包SDK）已经收集到的投资者个人信息基本情况，包括信息种类、使用目的、使用场景等。
f) 证券公司App在后台运行期间，不应收集投资者个人信息。

B.5.3.2 存储

a) 不得在App服务端、客户端等日志中记录未脱敏或未加密的敏感个人信息；
b) 不得在App客户端明文存储密码口令类用户鉴别信息；
c) 人脸信息原始样本应在完成认证功能后立即删除、不得保存；
d) 在信息系统中个人生物识别信息应与个人身份信息分开保存。

B.5.3.3 使用

a) 三方存管银行账号、资产信息等投资者敏感个人信息在App客户端默认屏蔽显示；
b) 证券公司开展App测试过程中不得使用未脱敏的投资者敏感个人信息；
c) App向投资者提供资讯推送等个性化展示时，应同时为投资者提供简单直观的退出个性化展示的选项；
d) App基于投资者个人信息进行自动化决策，如对投资者个人主体权益造成显著影响，证券公司应建立自动化决策结果投诉反馈渠道，由人工审核自动化决策结果并反馈；
e) 证券公司App应建立与第三方共享个人信息清单并在二级菜单中展示，应简洁、清晰列出App与第三方共享的投资者个人信息基本情况，包括与第三方共享的个人信息种类、使用目的、使用场景和共享方式等。

B.5.3.4 删除

a) 投资者主动提出删除个人信息要求时，App应揭示告知个人信息删除的处理措施与证券法律法规针对相关个人信息必要存储的最小期限；
b) App应提供资金账号、证券账号等注册账号的销户功能，销户过程中不得设置不合理与不必要的额外要求。

B.5.3.5 身份鉴别

a) App应设置一定强度的密码安全策略，防止投资者设置易于猜测的密码；
b) App登录宜支持多种认证方式，包括但不限于密码、短信、图形手势、生物特征等；
c) 投资者进行鉴别信息修改时应采用合适方式进行身份认证；
d) 针对银行账号、身份信息等投资者敏感个人信息查询，App应采用合适方式进行二次认证；
e) 后台系统直接采信客户终端鉴别结果的，应特别关注客户终端人脸信息保护环节和鉴别结果欺诈问题，并做好风险评估、落实安全管控措施。

B.5.4 证券公司App个人信息保护合规评估生命周期管理

针对App的个人信息保护合规评估应涵盖系统需求分析与设计、系统开发与测试、系统上线、系统后续运维等阶段。

B.5.4.1 需求分析与设计阶段

在系统需求分析与设计阶段，App研发方应梳理投资者个人信息处理内容与事项，设计全面、可行的个人信息保护技术方案。

B.5.4.2 系统开发与测试阶段

App研发方应根据投资者个人信息保护技术方案进行开发，在测试阶段充分验证投资者个人信息保护相关功能的有效性，并记录测试结果。

B.5.4.3 系统上线阶段

系统上线前，证券公司应针对 App 开展专项个人信息保护合规评估，评估通过后进行系统上线。

B.5.4.4 系统后续运维

当 App 涉及个人信息相关功能发生重要变更时，证券公司应针对变更前后差异内容开展个人信息保护合规评估，评估通过后执行变更。重要变更包括但不限于：

a) App 变更个人信息收集范围；
b) App 变更个人信息使用范围；
c) App 变更隐私协议内容。

证券公司应定期聘请第三方安全检测机构针对 App 进行个人信息保护合规评估。

B.5.5 证券公司App个人信息保护合规评估

证券公司 App 应按照《GB/T 35273—2020 信息安全技术 个人信息安全规范》《App 违法违规收集使用个人信息行为认定方法》等法规、标准接收合规评估，证券公司 App 个人信息保护合规评估典型评估项与违规示例：

B.5.5.1 是否公开收集使用规则、是否进行展示方式的优化。

违规示例：

a) App 中无个人信息保护隐私政策；
b) 未向投资者提供 App 个人信息保护政策摘要。

B.5.5.2 是否明示收集使用投资者个人信息的目的、方式和范围。

违规示例：

a) 未逐一列出 App 收集投资者个人信息的目的、方式和范围；
b) 收集使用投资者个人信息范围发生变化时，未以适当方式通知投资者。

B.5.5.3 是否存在未经投资者同意收集使用个人信息的情况。

违规示例：

a) 取得投资者同意前 App 就开始收集投资者个人信息；
b) 投资者明确不同意个人信息收集后 App 仍收集个人信息。

B.5.5.4 是否存在违反必要原则，收集与证券公司服务无关的投资者个人信息的情况。

违规示例：

a) 在投资者拒绝非必要个人信息收集时，影响与非必要个人信息无关的功能使用；
b) App 安装使用期间提前申请超出功能服务范围的个人信息相关权限。

B.5.5.5 是否存在未经投资者同意向第三方提供个人信息的情况。

违规示例：

App 接入第三方应用未经投资者同意直接向第三方应用提供个人信息。

B.5.5.6 是否按法律规定提供删除或更正个人信息功能或未公布投诉、举报方式等信息。

违规示例：

a) App 未向投资者提供有效的删除个人信息或注销账号的功能；
b) App 未向投资者公布个人信息安全的投诉反馈通道与方式。

B.5.5.7App 是否存在频繁自启动和关联启动等情况。

违规示例：

未经投资者同意，App 频繁自启动或关联启动其他 App。

B.5.5.8 是否存在误导投资者下载 App 及开屏信息等侵害投资者权益的情况。

违规示例：

App 开屏信息无法跳过。

B.5.5.9 应用分发平台上的 App 信息是否明示到位。

违规示例：

证券公司自有应用分发平台未明示 App 运行所需权限列表及用途、收集使用个人信息的内容、目的、方式和范围。

B.5.5.10 应用分发平台管理责任是否落实到位。

违规示例：

证券公司自有应用分发平台 App 上架审核不严格、违法违规处理不及时。

B.6 场景六：证券公司信息披露中的投资者个人信息公开与保护

B.6.1 概述

证券公司信息披露涉及投资者个人信息公开的场景包括：

a) 证券公司在提供证券承销与保荐等投行服务的过程中，根据法律法规、监管规定、自律规则等规定或要求，披露投资者的持股情况等信息；

b) 证券公司自身在融资过程中，根据法律法规、监管规定、自律规则等规定或要求，披露与投资者相关的重大交易、诉讼（仲裁）等信息。

B.6.2 信息公开的内容

证券公司履行上述信息披露义务时，可能被公开的投资者个人信息种类通常包括个人基本信息、身份信息、交易信息等。

B.6.3 信息公开的实施与保护要点

a) 严格按照《证券法》等法律法规及证监会、证券交易所发布的信息披露相关内容、格式准则的要求披露投资者个人信息，确保相关信息真实、准确、完整；

b) 确保披露场所或渠道符合《证券法》等法律法规及证监会、证券交易所的要求；

c) 设置管理信息披露事务的职能部门，安排专人实施具体工作，并对相关人员开展具体工作进行管理与培训；

d) 建立信息披露管理制度，明确涉及投资者个人信息公开相关工作的操作规程，建立复核机制，避免因信息公开错误等不当行为给投资者造成不利后果或影响；

e) 通过客服热线等方式受理投资者对证券公司信息披露存在的疑问或异议，及时对投资者进行解释说明或采取补救措施。

附录 C

（资料性）

****个人信息保护政策

****公司（以下简称****或我们）深知个人信息对您的重要性，高度重视个人隐私和信息安全。我们将恪守权责一致、目的明确、选择同意、最少够用、确保安全、主体参与、公开透明的原则，按照法律法规的规定保护您的个人信息及隐私安全。

您浏览****互联网平台或使用我们的互联网平台服务时，我们将按照本《****个人信息保护政策》（以下称“本政策”）处理您的个人信息。如您使用****互联网平台提供的某项或某几项服务有其单独的个人信息保护政策的，该单独的个人信息保护政策将与本个人信息保护政策一起构成一份完整的个人信息保护政策。

本政策发布时间：****年*月。

本政策更新时间：****年*月。

本政策生效时间：****年*月。

根据《常见类型移动互联网应用程序必要个人信息范围规定》，*****App 属于投资理财类，基本功能服务为“股票、期货、基金、债券等相关投资理财服务”，必要的个人信息包括：

1、注册用户移动电话号码，微信号;

2、投资理财用户姓名，证件类型和号码，证件有效期限、证件影印件;

3、投资理财用户资金账户、银行卡号码或支付账号。

本政策将帮助您了解以下内容：

1、我们如何收集和使用您的个人信息

2、我们如何使用 Cookie 和同类技术

3、我们如何共享、转让、公开披露您的个人信息

4、我们如何保护您的个人信息

5、您的权利

6、我们如何处理敏感个人的个人信息

7、本政策如何更新

8、如何联系我们

请在使用我们的产品（或服务）前，仔细阅读并理解本政策。

一、我们如何收集和使用您的个人信息

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，不包括匿名化后的信息。前述信息的来源包括：您通过****互联网服务渠道或其他合法途径向我们提供的信息；您自行向社会公众公开的信息；您通过合法公开渠道（如合法的新闻报道、政府信息公开等）披露或合法留存于第三方的信息等。****仅会出于本政策所述的以下目的，收集和使用您的个人信息:

1、基本业务功能

为实现 App 的业务功能，我们可能需要向您收集以下个人信息。若您拒绝收集，则无法使用相应服务。

1.1、为了完成注册及接收推送

为了您能使用注册功能，且注册后的账户可以使用积分、礼券、进行收藏操作，并接受我们的推送服务，您需要向我们提供您的手机号码，我们会向您发送短信验证码，以验证您的身份。

1.2、为了办理开户

为了您能开通资金账户、证券账户、理财账户，我们会根据监管机构要求收集您的个人

身份信息、个人账户信息及办理网上开户业务所需要的其他信息，包括您的个人基本信息，包括姓名、性别、出生日期、手机号码、国籍、邮箱、住址；个人身份信息，包括身份证件类型、身份证件号码、地址、签发机关、有效期、身份证彩色照片；个人鉴别信息，包括密码信息；个人生物识别信息（指纹认证信息、人脸认证信息、个人视频、个人照片）；个人教育工作信息，包括职业、学历；开户行名称、银行卡卡号、征信信息；风险测评所采集的相关信息（参见第 3 条）；其他业务要求采集的信息。

根据中国证券登记结算有限公司、沪深交易所、北交所、基金公司及三方存管银行相关机构要求，我们将您填写的个人信息报送至以上机构，以便根据您的申请为您开通资金账户、股东账户、OTC 账户、基金账户、建立三方存管、查询及各业务权限开通。

1.3、为了风险测评

当您使用“风险测评”功能时，需要确认您的个人基本信息（姓名、职业、年龄、学历、家庭信息、联系方式）、财务状况、投资经验、投资目标。“风险测评”收集这些信息是用于对您的风险承受能力进行评估，如您拒绝授权此类信息的，我们可能无法为您提供风险评估结果及与此相关的投资服务，但不影响我们为您提供的其他服务的正常使用。

1.4、为了身份验证

当您在开户、交易、业务办理过程中，需要进行身份验证时，我们将会在获取您授权的情况下采集您的生物信息（指纹认证信息/人脸认证信息/视频/照片）。在您的设备上完成对应信息验证后，我们仅接收验证结果，并在法律法规规定时间范围内安全存储相关验证信息。

1.5、为了登录交易账户

在您进行交易登录时，根据证券法及监管要求需记录您的 IMEI、UUID、IP 地址、MAC 地址、IP 端口号、硬盘序列号、硬盘分区信息、系统盘卷标号、PC 终端设备名、PC 终端设备序列号、CPU 序列号、ICCID、IDFV、IMSI、AndroidID、IDFA、设备传感器、应用安装列表、实际使用手机号码、注册手机号码、操作系统版本、交易终端软件名称及版本，并生成登录日志进行存储。

1.6、为了资产查询及转账

为了您能使用银证转账和资产信息查询，需获取您的 IMEI、UUID、IP 地址、MAC 地址、IP 端口号、硬盘序列号码、硬盘分区信息、系统盘卷标号、PC 终端设备名、PC 终端设备序列号、CPU 序列号、ICCID、IDFV、IMSI、AndroidID、IDFA、设备传感器、应用安装列表、实际使用手机号码、注册手机号码、操作系统版本、交易终端软件名称及版本、交易账号、姓名、身份证件类型、身份证件号码、身份证件有效期、银行卡卡号、银行预留手机号码信息。

1.7、为了交易及业务办理

当您使用股票、信用、期权、理财产品交易及业务办理时，根据证券法及监管要求需记录您的 IMEI、UUID、IP 地址、MAC 地址、IP 端口号、硬盘序列号、硬盘分区信息、系统盘卷标号、PC 终端设备名、PC 终端设备序列号、CPU 序列号、ICCID、IDFV、IMSI、AndroidID、IDFA、设备传感器、应用安装列表、实际使用手机号码、注册手机号码、操作系统版本、交易软件版本、证券账号、姓名、身份证信息、身份证件照片、性别、生日、民族、国籍、税收身份及税号，生成交易日志并按照监管要求进行存储。

1.8、为了使用行情软件、投顾服务、投资工具及协议签署

当您使用行情、投资工具、投顾服务时，我们会记录您的设备信息，包括：IMEI、UUID、IP 地址、MAC 地址、IP 端口号、硬盘序列号、硬盘分区信息、系统盘卷标号、PC 终端设备名、PC 终端设备序列号、CPU 序列号、ICCID、IDFV、IMSI、AndroidID、IDFA、设备传感器、应用安装列表、实际使用手机号码、注册手机号码、操作系统版本、交易软件版本进行相关校验。当您使用的产品功能涉及到您与****签署投资顾问服务协议、产品风险揭示

书、适当性匹配，我们将会使用您的账户登录功能对身份信息进行验证，确保协议签署的有效性。

1.9、为了发送必要的通知

为了履行法定和约定的通知义务，我们会将您的电话号码提供给我们合作的通信运营商，这类提供是为提供服务所必须进行的。否则，您将无法收到必要的通知，您将存在资金损失的风险。

2、扩展业务功能

2.1、为了保障账户、资金和服务安全

为保障我们能正常地向你提供服务，维护我们服务的正常运行和改进优化我们的服务体验以及保障您的账户、资金安全，预防您的账户被他人不法侵害，我们会收集您的账户信息、IMEI、UUID、IP 地址、MAC 地址、IP 端口号、硬盘序列号、硬盘分区信息、系统盘卷标号、PC 终端设备名、PC 终端设备序列号、CPU 序列号、ICCID、IDFV、IMSI、AndroidID、IDFA、设备传感器、应用安装列表、实际使用手机号码、注册手机号码、操作系统版本、交易终端软件名称及版本、位置信息，这类信息是为提供服务必须收集的基础信息。如您选择关闭收集位置功能，我们将停止对您的位置信息的收集；这样做不会影响您进行交易，但可能会影响我们对安全状况的判断效果。

2.2、为您提供个性化服务及改进服务质量

为改进服务质量、防范风险、提升您的服务体验，或为您推荐更优质或更适合的服务，我们会收集您使用****互联网平台服务时的搜索记录、浏览信息。（还会向我们的关联公司和合作伙伴收集其合法留存的您的行为信息，用于向您展示和推荐更适合的****互联网平台服务）。

为了客户服务，我们会使用您提供的个人信息，包括联系方式、姓名、性别、年龄、资金账号、投资信息，以及您使用的服务类别和方式、使用服务时的操作信息、交易信息。

当您需要在微信上接收****互联网平台服务的推送消息，您可以将****资金账户与您的微信账号进行绑定，通过微信及时接收****互联网平台的推送消息。如您不再想要接受微信推送消息，您可以前往****微信服务号退订消息的推送设置。

为提升处理效率、降低处理成本、提高处理准确性，我们可能会委托具备相关能力的****关联公司提供这方面的服务，并且我们会要求该公司遵守严格的保密义务，禁止其将该信息用于未经您授权的用途。在特定场景下本平台需要使用设备定位、相机、麦克风情况下，本平台会在获取您的授权情况下调用相应功能。您可以随时关闭相关的授权。本平台不会在超出功能范围之外向您索取相关的授权。

如果您不希望接收到我们为您推送的个性化内容，您可以随时关闭。对于*****App，您可以通过“个人中心”里的“个性化推荐”开关进行关闭。

3、其他情形

在法律法规允许的范围内，我们可能会在出现以下任一情形时收集并使用您的个人信息而无需取得您的授权同意:

（1）与国家安全、国防安全直接相关的；

（2）与公共安全、公共卫生、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；

（5）所收集的个人信息是个人信息主体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）根据个人信息主体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）个人信息控制者为新闻单位且其在开展合法的新闻报道所必需的；

（10）个人信息控制者为学术研究机构，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；

（11）法律法规规定的其他情形。

如需将您的个人信息用于本政策未载明的其他用途，我们会以确认协议、具体场景下的文案确认动作等形式再次征求您的同意。

申请的设备权限如下具体所述：

在提供服务过程中，我们会调用您的一些设备权限，以下是调用涉及个人信息的权限对应的业务功能和调用权限的目的。您可以选择是否授权开通以下权限：

1、读写存储空间的权限

由于行情、资讯、应用日志存储功能需要在手机本地读写文件，因此需要获取存储权限。

2、访问相册的权限

当您进行身份认证需要提交证明材料或导入图片上传自选股、向在线客服发送照片时，您可以从本地相册中选择图片上传，因此需要获取访问相册的权限。

3、获取定位的权限

为了您能方便地进行在线办理业务，查询附近的营业部信息及保障账户安全，需要获取您的地理位置信息，因此需要获取访问定位的权限。

4、访问摄像头的权限

为了您可以通过摄像头进行身份校验（身份证识别、人脸识别、视频验证）、银行卡号码识别及其他证明材料采集，需要获取摄像头权限。

5、获取麦克风的权限

为了您能通过麦克风使用视频通话和语音识别功能进行身份验证、在开户或业务办理过程中视频验证、向在线客服发送语音时，需要获取麦克风的权限。

6、获取电话的权限

为了更好的提供服务，满足投资交易的监管要求或当您需要直接拨打客服热线时，我们需要获取您的电话权限。

7、通知权限

应用程序启动时，如果您没有打开通知权限，我们会向您询问是否打开，如果您不提供通知权限，将无法接收到系统消息推送，但不影响您使用软件的其他功能。

8、访问剪切板的权限

为方便您复制账号、卡号、资讯内容，我们需要获取您设备的剪切板权限，并在 App 启动、前后台切换时读取剪切板信息。

二、我们如何使用 Cookie 和同类技术

（一）Cookie

为确保以 html 技术实现的网页正常运转，我们会在您的计算机或移动设备上存储名为 Cookie 的小数据文件。Cookie 通常包含标识符、站点名称以及一些号码和字符。

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。您可以清除设备上保存的所有 Cookie，大部分网络浏览器都设有阻止 Cookie 的功能。但如果您这么做，则需要在每一次访问我们的网站时亲自更改用户设置。如需详细了解如何更改浏览器设置，您可以通过互联网搜索引擎获得不同浏览器的操作方法。

（二）网页信标和像素标签

除 Cookie 外，我们还会在网页上使用网页信标和像素标签等其他同类技术。例如，我们向您发送的短信或电子邮件可能含有链接至我们网站内容的。如果您点击该链接，我们则会跟踪此次点击，帮助我们了解您的产品或服务偏好并改善客户服务。网站信标通常是一种嵌入到网站或电子邮件中的透明图像。借助于电子邮件中的像素标签，我们能够获知电子邮件是否被打开。如果您不希望自己的活动以这种方式被追踪，则可以随时与我们联络进行退订。

（三） Do Not Track （请勿追踪）

很多网络浏览器均设有 Do Not Track 功能，该功能可向网站发布 Do Not Track 请求。目前，主要互联网标准组织尚未设立相关政策来规定网站应如何应对此类请求。但如果您的浏览器启用了 Do Not Track,那么我们的所有网页都会尊重您的选择。

三、我们如何共享、转让、公开披露您的个人信息

我们承诺对您的信息进行保密，不会与任何公司、组织和个人共享、转让、公开披露您的个人信息，以下情况除外：

1、在获取您明确同意的情况下；

2、根据法律法规、法律程序、政府的强制命令或司法裁定及要求共享的范围共享您的个人信息；

3、在您所参与的抽奖、竞赛或类似推广活动中，将您提供的信息用于管理此类活动。在前述情形下，如您中奖，我们可能会将您的手机号码或注册名进行脱敏后公布在中奖名单或竞赛名单中。如该活动系我们和第三方联合推广，我们可能与该第三方共享活动过程中产生的、为完成该等活动所必要的个人信息（如参加活动的用户数、中奖名单、中奖人联系方式），以便第三方能及时向您发放奖品或为您提供服务；

4、为了向您提供更完善、优质的产品和服务，如我们和第三方联合推广，为进行对账等数据统计需求，我们可能与该第三方共享推广过程中完成对账所必要的个人信息。

同时，我们会与合作第三方签署严格的保密协定，要求他们严格按照我们的说明、本政策以及其他任何相关的保密和采取安全措施来处理您的个人信息。我们将要求合作方无权将共享的个人信息用于任何其他用途。如果您拒绝我们的合作方在提供服务时与我们共享我们收集的为提供服务所必需的您的个人信息，将可能导致您无法在我们的平台上使用该服务；

5、在获取您同意的情况下，为了维护和改善我们的服务、处理您的相关交易或根据相关交易及业务规则进行客户账户管理，我们会使用具有相应业务能力的第三方服务 SDK 来为您提供服务，详见《个人信息第三方共享清单》https://******，个人信息权限清单，详见《系统权限申请与使用》https://******，个人信息收集与使用，详见《个人信息收集与使用》https://******；

6、根据法律法规及相关规定要求，我们需要将您在使用****互联网平台过程中的注册信息、交易信息报送给证券交易所、中国证券登记结算有限公司、金融产品发行方等机构，用于完成这些机构对交易过程的确认、结算及监督。

四、我们如何存储及保护您的个人信息

我们收集和产生的个人信息将存储在中华人民共和国境内。

我们承诺将使信息安全保护达到合理的安全水平。我们通过建立数据分类分级制度、数据安全管理办法来管理规范个人信息的存储和使用，并建立数据安全专职岗位、数据安全应急响应机制来推进和保障个人信息安全。为保障您的信息安全，我们致力于使用各种网络安全层软件（SSL）进行加密传输、信息加密存储、严格限制数据中心的访问、使用专用网络通道及网络代理等安全技术及配套的管理体系来防止您的信息被泄露、毁损或者丢失。

我们将按照相关法律法规及行业监管要求的保存期限对您的个人信息进行保存。

请您理解，由于技术水平限制及可能存在的各种恶意手段，实践中我们对您的信息保护

仍然可能因我们可控制范围外的因素而存在不确定性。

如我们停止运营，我们将及时停止收集您个人信息的活动，且对所持有的个人信息进行删除或匿名化处理。

五、您的权利

按照中国相关的法律、法规、标准，以及其他国家、地区的通行做法，我们保障您对自己的个人信息行使以下权利:

（一）查询您的个人信息

您有权查询您的个人信息，法律法规规定的例外情况除外。如果您想行使数据访问权，可以通过以下方式自行访问:

用户信息——您可通过个人中心查询及管理您的用户信息，包括绑定微信、手机号码、地址等；

交易相关的账户信息——如果您希望查询或编辑您的账户中的个人资料信息和账户信息、更改您的密码、添加安全信息，您可以通过访问业务办理功能中的账户查询及资料修改模块执行此类操作。

搜索信息：您可以在搜索栏中查询或清除您的搜索历史记录、查看相关数据。

如果您无法通过上述方式查询这些个人信息，您可以随时联络我们的官方客户热线*****，或发送电子邮件至*****@*****.com.cn。我们将在 15 个工作日内回复您的访问请求。

对于您在使用我们的产品或服务过程中产生的其他个人信息，只要我们不需要过多投入，我们会向您提供。如果您想行使数据访问权，请发送电子邮件至*****@*****.com.cn。

（二）更正您的个人信息

当您发现我们处理的关于您的个人信息有错误时，您有权要求我们做出更正。您可以通过“业务办理”功能提出个人信息更正申请。

如果您无法通过上述链接更正这些个人信息，您可以随时联络我们的官方客户热线*****，或发送电子邮件至*****@*****.com.cn。我们将在 15 个工作日内回复您的访问请求。

（三）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:

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，却未取得您的同意；

3、如果我们处理个人信息的行为违反了与您的约定；

当您从我们的服务中删除信息后，我们可能不会立即从备份系统中删除相应的信息，但会在备份更新时删除这些信息。

您可通过电子邮箱*****@*****.com.cn 或拨打客服热线*****申请删除您的个人信息。我们将尽快审核您的申请，并在验证您的用户身份后的十五个工作日内回复。

（四）个人信息副本获取

如您需要您的个人信息的副本，您可以通过本政策提供的方式联系我们，在核实您的身份后，我们将向您提供您在我们的服务中的个人信息副本(包括基本资料、身份信息)，但法律法规另有规定的或本政策另有约定的除外。

（五）撤回同意或改变您授权同意的范围

您总是可以选择是否向我们披露个人信息。每个业务功能需要一些基本的个人信息才能得以完成（见本政策“第一部分”）。您可以通过撤回个人信息授权、关闭设备权限、注销账户等方式改变您授权我们继续收集信息的范围或撤回您的授权。

当撤回授权后，我们无法继续为您提供撤回授权所对应的服务，也不再处理您相应的信

息。但您撤回授权的决定，不会影响此前基于您的授权而开展的信息处理。

（六）注销账户

您随时可注销此前注册的****互联网平台账号。在您主动注销之后，我们将停止为您提供服务，并依据您的要求，删除您的个人信息，但法律法规、监管规定、自律规则等另有规定的除外，您在使用****互联网服务期间提供或产生的信息我们仍需按照上述规定要求的时间进行保存，且在该保存的时间内依法配合有关机关的查询。

在 App 中，您可以通过 App 左上角头像—个人资料—手机号码—注销账号进行账号注销。注销后，与该账号有关的积分、礼券、订阅、收藏、消息、自选股等信息将不再保留。

您还可以通过拨打*****客户热线进行注销，我们将根据适用法律及相关规定的要求在 15 个工作日内完成核查和处理。

（七）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。

我们将在十五个工作日内做出答复。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。

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、国防安全直接相关的；

2、与公共安全、公共卫生、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、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；

6、涉及商业秘密的。

六、我们如何处理敏感个人的个人信息

如您为未成年人，请您的父母或监护人阅读本政策，并请您在取得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。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。****将根据国家相关法律法规的规定保障未成年人的个人信息的保密性及安全性。

七、本政策如何更新

我们的个人信息保护政策可能变更。

未经您明确同意，我们不会削减您按照本个人信息保护政策所应享有的权利。我们会在本页面上发布对本政策所做的任何变更。

对于重大变更，我们还会提供更为显著的通知（包括对于某些服务，我们会通过系统公告发送通知，说明个人信息保护政策的具体变更内容）。

本政策所指的重大变更包括但不限于：

1、我们的服务模式发生重大变化。如处理个人信息的目的、处理的个人信息类型、个人信息的使用方式等；

2、我们在所有权结构、组织架构等方面发生重大变化。如业务调整、破产并购等引起的所有者变更等；

3、个人信息共享、转让或公开披露的主要对象发生变化；

4、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；

八、如何联系我们

对于您个人信息权利方面的投诉、举报可以通过以下方式与我们联系。

公司名称：******公司

公司地址：******

电子邮箱：*****@*****.com.cn

客服热线：*****

我们将尽快审核您提出的问题，并在验证您的用户身份后的十五个工作日内回复。

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行为损害了您的合法权益，双方应通过友好协商解决，协商不成，您还可以通过向******人民法院提起诉讼的方式寻求解决方案。

参 考 文 献

[1] 中华人民共和国个人信息保护法（2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过）

[2] 中华人民共和国证券法(2019年12月28日第十三届全国人民代表大会常务委员会第十五次会议第二次修订）

[3] 证券基金经营机构信息技术管理办法（证监会令[第179号] 2021年修正）

[4] 证券期货业网络和信息安全管理办法（证监会令[第218号]）

[5] 证券期货业网络安全事件报告与调查处理办法(证监会公告[2021]12号)

[6] 证券经纪业务管理办法（证监会令[第204号]）

[7] 数据出境安全评估办法（国家互联网信息办公室令[第11号]）

[8] AFCA—FTCC std 0003—2022个人金融信息保护指南

[9] 人脸识别技术应用安全管理办法（国家互联网信息办公室 中华人民共和国公安部令第19号）

[10] 个人信息保护合规审计管理办法（国家互联网信息办公室令[第18号]）

[11] 个人信息保护法理解与适用（程啸 著）

[12] 证券公司客户资金账户管理规则(协会第七届理事会第16次会议表决通过2023年6月9日发布并生效）

[13] 粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引（国家互联网信息办公室香港创新科技及工业局公告2023年3号）

[14] 证券期货业已发布标准术语汇编（2004年—2023年）

[15] 证券公司客户交易终端信息管理技术规范（证保发[2020]9号）

[16] ISO/IEC 29100:2024 Information technology-Security techniques-Privacy framework

[17] 网络数据安全管理条例(中华人民共和国国务院令[第790号]，2024年8月30日国务院第40次常务会议通过)