标准研究

2023 年第 8 期（总第 30 期）

证标委秘书处　　2023 年 11 月 15 日

投资者个人信息保护工作实践探索

【摘要】证券期货业作为国家金融活动的重要领域之一，汇聚了大量敏感、重要的金融数据和个人数据，是典型的数据规模巨大、数据价值高、数据应用场景复杂的行业。近些年公募基金行业高速发展，业务规模迅速增长，公司各个业务系统存在大量的投资者敏感信息，随着线上应用和交易不断增多，个人信息在互联网的风险暴露面逐步增大，导致数据泄露的风险增加，一是来自互联网的攻击渗透风险不断加大，二是由于内部员工安全意识不足，或对操作使用行为监控不到位，均会导致个人敏感信息泄露。为此，银华基金管理股份有限公司（以下简称“银华基金”）根据自身特点实践并探索针对投资者个人信息保护工作策略和管理规范。

关键词：基金公司　个人信息保护　标准要求　实践探索

一、监管背景

（一）组建国家金融监督管理总局强化投资者保护决心

2023年全国两会期间，根据国务院关于提请审议国务院机构改革方案的议案，组建国家金融监督管理总局。统一负责除证券业之外的金融业监管，强化机构监管、行为监管、功能监管、穿透式监管、持续监管，统筹负责金融消费者权益保护，加强风险管理和防范处置，依法查处违法违规行为，作为国务院直属机构，中国证券监督管理委员会的投资者保护职责划入国家金融监督管理总局，改革方案明确将投资者保护的职责均纳入国家金融监督管理总局的职责范围，进一步体现了金融监管保护金融消费者的决心。

（二）证券期货业网络和信息安全管理办法正式实施

证监会发布《证券期货业网络和信息安全管理办法》将于2023年5月1日起正式实施，《办法》中第三章节，重点提出了关于投资者个人信息保护的具体要求，要求核心机构和经营机构应当遵循合法、正当、必要和诚信原则，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。一是明确核心机构和经营机构处理投资者个人信息的基本原则，要求建立健全投资者个人信息保护体系和管理机制，履行保护义务。二是明确核心机构和经营机构在投资者个人信息处理、共享

环节的安全防护要求。三是提出核心机构和经营机构在网络安全防护边界外处理投资者个人信息的技术要求，防范化解信息泄露风险。四是对核心机构和经营机构收集客户生物特征的必要性和安全性提出评估要求。

（三）证监局发文要求进一步加强投资者信息安全防护，以切实防范泄露信息违法违规行为的出现

2022 年 7 月多地证监局发布通知要求证券、基金和投顾等在内多类机构应提高内控管理水平，进一步加强投资者信息安全防护，以切实防范泄露信息违法违规行为的出现，证监局提出的要求主要有以下四个方面内容：一是健全内控制度。将投资者信息保护纳入公司全面合规和风险管理范畴，规范信息管理；二是加强信息技术系统建设。开展信息技术系统风险自查，全面梳理、识别、监测、防范因使用信息技术手段引发的安全风险；三是加强人员管理。建立健全各项制度，以切实防止员工个人行为造成投资者个人信息泄露或滥用等事件的发生；四是优化防控机制。建立健全信息安全事件应急处理机制，对于突发重大负面舆情，及时发声澄清认识，传递客观信息，防止局部、单一事件蔓延或升级；发生投资者个人信息泄露、损毁、丢失等情况的，及时采取措施，将损失降低到最小。另外，证监局将加大执法力度，把投资者个人信息保护纳入日常重点监管范畴，对辖区内机构的投资者个人信息保护情况开展专项排查，针对严重违反相

关法律法规的行为，坚决依法查处，从严处罚。

（四）中国人民银行关于加强个人信息安全管理开展风险专项自查的通知

中国人民银行于2022年9月发布《关于加强个人信息安全管理开展风险专项自查的通知》，通知要求各机构应高度重视个人信息安全管理，严格落实《通知》相关要求，明确内部牵头部门，压实各方主体责任，从严从实开展个人信息安全风险自查整改工作。同时，以自查整改为契机，查漏补缺、补齐短板，人防技防相结合，构建个人信息安全管理体系。

二、标准要求

（一）证券期货业数据分类分级指引

数据分类分级是数据保护工作中的一个关键部分，是建立统一、准确、完善的数据架构的基础，是实现集中化、专业化、标准化数据管理的基础。证监会于2018年9月正式公布并实施《证券期货业数据分类分级指引》，指引中明确基金经营机构将投资者管理类划归交易条线管理，划分了包括投资者基本信息、投资者开户/账户信息、投资者衍生信息、投资者合约信息等数据子类，要求此类信息按照三级数据进行保护和管理，指引发布后一方面有助于有效甄别合理化的个人信息使用需求，明确关键环节的技术标准，另一方面有助于结合行业发展变化，有效识别新增风险隐患，持续加强

数据安全管理，建立健全数据管理制度，采取必要的防护措施，切实维护投资者合法权益。

（二）证券期货业网络安全等级保护工作指引及要求

2022 年 12 月证监会发布《关于进一步做好证券期货业网络安全等级保护工作的通知》，其中配套下发的工作指引显示，证券期货业网络和信息系统的安全保护等级，应根据网络和信息系统发生服务能力异常或数据损毁、泄露等网络安全事件后，对国家金融安全、社会秩序、投资者合法权益造成的损害程度进行定级，其中交易系统的的注册交易用户数和非交易业务系统的注册的用户数或存储的用户信息数作为了重要了定级指标，参照证监会于 2021 年 9 月发布的《证券期货业网络安全等级保护基本要求》《证券期货业网络安全等级保护测评要求》2 项金融行业标准，对于基金经营机构进一步落实好网络安全等级保护和个人信息保护工作相关要求，具有非常重要的意义。

（三）证券期货业数据安全管理与保护指引

证监会于 2022 年 11 月发布《证券期货业数据安全管理与保护指引》,《指引》的发布，充分体现了数据安全对于证券期货业的重要性和紧迫性，指引中针对证券基金经营机构中投资者个人信息按照《证券期货业数据分类分级指引》要求，作为三级数据进行定级，明确区分数据控制者和数据接触者角色，在可控区域和非可控区域提出管理指引、技术指

引方面的细化要求，指引同时强调从组织、制度、技术方面建立数据安全体系，提高整体防护能力，也须注意数据级别与数据安全防护的差异性，确保实用性，同时也建议各机构依据自身情况，将数据安全管理进行具体落实。

三、实践探索

（一）组织保障

银华基金网络和信息安全工作实行“谁运营，谁负责；谁使用，谁负责”、安全优先、保障业务发展的原则。关于个人信息安全保护工作遵循“人人有责”的原则，任何人都应在接触和使用到个人信息数据时，均需采取必要的措施保障数据安全性，如发现可能损害个人信息数据安全的情况应及时制止和上报，对于违反个人信息保护制度的行为，将根据行业监管要求和公司信息安全工作管理办法进行追责。

针对个人信息安全保护工作，银华基金信息技术部为主要牵头部门，各相关部门共同推进并开展工作，落实各部门职责，形成相互监督、相互制约的管理体制。积极有效整合公司内部资源，完善内部工作制度，明确决策层、管理层和执行层等各层级人员职责，分类处置各类型的个人信息数据，定期举办针对个人信息安全保护的安全意识培训，确保信息保护要求传达畅通，构建相互衔接、全面有效的个人信息保护体系。

（二）职责分工

银华基金开展经营业务遵循合法、正当、必要的原则针对个人信息进行采集、传输、存储和使用，以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则，并接受外部监督，同时满足个人信息主体授权同意的目的所需的最少个人信息类型和数量，采取技术和其他必要的措施保障个人信息的安全，对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任。公司内部针对个人信息保护工作职责区分了以下几类角色并规定了相关职责：

1、数据所有者部门：业务部门作为开展经营业务所需个人信息的数据所有者部门，是本部门所辖范围内投资者个人数据安全保护工作的主责部门，根据最小权限和岗位必需的原则设置投资者个人信息访问权限，制定所辖范围内投资者个人信息技术和管理要求，相关实施部门予以配合。明确所辖范围内投资者个人信息的授权机制，明确访问人员的责任和义务。

2、数据保管部门：配合开展投资者信息泄露风险自查工作，根据国家标准和公司制度要求采取有效措施防范和处置风险，及时弥补技术和管理漏洞，自查中发现的安全风险应及时通知数据所有者部门；参照《证券期货业数据安全管理与保护指引》、《信息安全技术-个人信息安全规范》、《个人金融信息保护技术规范》要求，对投资者信息存储环节应满足存储时间最小化、去标识化、加密、生物识别信息存储要

求等。

3、数据使用部门：配合开展投资者信息泄露风险自查工作，根据国家标准和公司制度要求采取有效措施防范和处置风险，及时弥补技术和管理漏洞，自查中发现的安全风险应及时通知数据所有者部门和信息技术部，参照《证券期货业数据安全管理与保护指引》、《信息安全技术-个人信息安全规范》、《个人金融信息保护技术规范》要求，对投资者信息使用和传输环节应进行安全性评估，采用加密措施进行保护。

（三）制度规范

银华基金针对投资者信息安全保护工作制定了相关管理制度和流程，包括信息安全工作管理办法、保密管理制度、业务系统权限管理制度、网络与信息安全应急管理办法、员工通讯工具管理规定等规章制度，对由业务系统采集的个人信息及公司重要数据进行明确保护范围，梳理重要数据流转过程，厘清重点岗位和人员的日常访问流程和确保制度保障到位，连续两年在公司内部开展云安全文档系统使用培训，每月通过公司 e-learning 平台推送关于信息安全宣传教育视频、海报，定期开展测试考核工作。

（四）技术措施

1、个人信息采集环节

公司在个人信息采集环节首先明确数据所有者部门，按照最小必要、自主选择、公开透明、授权同意等基本原则开

展相关信息采集工作，采集的个人信息的类型与实现产品或服务的业务功能有直接关联，自动采集个人信息的频率是实现产品或服务的业务功能所必需的最低频率，采集过程中数据所有者部门尊重个人信息主体的自主意愿，不强迫个人信息主体接受服务所提供的业务功能及相应个人信息采集请求（法律规章强制要求采集的除外），设定对个人信息主体做出肯定性动作确认后作为服务业务功能的开启条件，开始采集个人信息。采集投资者信息时，向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则，并获得个人信息主体的授权同意，采集投资者敏感信息前，征得了个人信息主体的明示同意，并应确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示。

2、个人信息传输、存储和使用环节

公司在个人信息传输、存储和使用环节首先明确个人信息保管部门和使用部门职责，利用文档资产全生命周期管控的方式，对包含个人敏感信息的文档的从生成、流转、存储到销毁各个环节进行管控，通过对权限申请审批、文件外发、日志审计、溯源追踪和文件回收站等措施实现对敏感文档的精细化管控。在信息传输过程中建立个人信息传输安全策略和规程，采用必要的传输安全控制措施，在传输信息前双方通过有效的技术手段进行身份鉴别和认证，原则上不通过公

共网络传输投资者个人信息，必须进行传输的采用加密通道或数据加密方式。根据开展业务的需要，采用脱敏技术手段对测试数据进行处理，并采取技术和管理方面的措施，将可用于恢复识别个人信息与脱敏后的信息分开存储并加强访问和使用权限管理。按照公司业务系统访问权限要求，对被授权访问个人信息的人员，建立了最小授权的访问控制策略，使其只能访问职责所需的最小必要的个人信息，且仅具备完成职责所需的最少的数据操作权限，避免对个人信息进行批量修改、拷贝、下载等敏感操作，同步完善业务系统功能模块，确保系统生成日志能及时、准确、全面地记录个人信息的查询和下载操作，信息泄露发生后能够及时追溯。

3、信息泄露监测

公司重点加强内外部数据安全及个人信息保护的监测防护体系，根据实际业务场景分析数据泄露风险，按照重要数据流转过程的梳理结果，分析数据泄露的威胁主体及风险、敏感数据的暴露面等，通过第三方监控平台对信息泄露的主要平台进行实时监测，如网盘、Github、暗网等，出现可疑泄露事件后第一时间启动应急处置预案，对数据进行验证并对事件进行甄别及定性。

（五）应急预案

公司根据网络与信息安全应急管理办法规范了投资者信息安全事件处置流程和分工，主要职责包括事件记录及追

溯、投资者告知、舆情监测等，处置基本原则如下：

1、事前防范，加强监控。通过加强信息安全防范意识，加强数据保密和数据防泄露技术措施，完善个人信息的日常监测、发现机制，及时采取有效的应对措施，迅速控制事件影响范围，力争将损失降到最低程度。从而缓解个人信息泄露安全威胁。

2、分级管理。根据个人信息泄露事件的特点和影响，将突发事件分级管理，针对不同等级的突发事件采取不同的应急处理流程。

3、高效处置。当出现个人信息泄露等突发事件后，要明确责任，高效处置，在最短时间内处理因信息泄露可能带来的风险和客户损失。

4、维护权益。当出现投资者信息泄露等突发事件后，要切实保护客户利益，采取一切积极有效措施，尽量减少投资者损失。

参考《证券期货业网络安全事件报告与调查处理办法》事件分级标准，根据个人信息泄漏突发事件的性质、影响和危害，划分为三个级别：重大事件、较大事件、一般事件。将个人信息泄露应急场景分为服务器被入侵、数据库拖库、内部人员泄露等，设置不同类别场景处置过程，根据应急预案职责对舆情监测、客户告知、监管报告等工作进行了分工。

四、深化工作部署

公司持续高度重视投资者个人信息保护工作，积极有效整合公司内部资源，完善内部工作制度，明确决策层、管理层和执行层等各层级人员职责，确保信息保护要求传达畅通，构建相互衔接、全面有效的数据安全和投资者信息保护体系，下一步公司将持续开展投资者个人信息保护工作，主要包括：

1、ISO 27701 隐私信息管理体系，借助成熟的隐私管理体系帮助公司降低个人、组织隐私和数据泄露的风险，提高企业内部的个人隐私信息安全管理规范，改善员工对于个人敏感信息安全及隐私保护风险管理认知。

2、中国网络安全审查技术与认证中心 App 安全及个人信息保护认证，依据国家标准对银华基金生利宝 APP 收集、存储、传输、处理、使用个人信息等活动进行评价，规范和提升个人信息保护能力，符合要求后获得 APP 安全和个人信息保护认证证书。

3、证券期货业 APP 安全认证，进一步提升银华基金生利宝 APP 安全质量水平和交易安全，围绕移动应用程序开发安全和数据安全全生命周期进行安全管控，在移动终端安全、身份鉴别、网络通信安全、数据安全、个人信息保护等多方面不断提高安全防护能力。

（银华基金管理股份有限公司信息技术部总监武庄、总监助理宋晓刚、运维经理朱林供稿）