

《证券公司投资者个人信息保护技术规范》编制说明

为贯彻落实党中央、国务院关于推进标准化建设的政策部署，进一步推动证券业标准化工作高质量发展，保护投资者合法权益，规范投资者个人信息处理行为，根据国家法律法规要求，参照有关国标、行标，结合证券公司业务特点，中国证券业协会会员单位中泰证券、财信证券联合中国信通院，与万联证券、国泰海通证券、腾讯科技（北京）有限公司、东北证券、国联民生证券、招商证券共同编写了团体标准《证券公司投资者个人信息保护技术规范》（以下简称《技术规范》），现将相关情况说明如下：

一、起草背景

2021年《中华人民共和国个人信息保护法》发布实施，从法律、规章、国家标准、行业标准等不同层面，我国个人信息保护的框架和管理体系正在逐步建立和完善，有些配套规范及工具也在逐步呈现。2023年中国证券监督管理委员会发布了《证券期货业网络和信息安全管理办法》，其中设置了“第三章 投资者个人信息保护”专章，对证券公司投资者个人信息保护提出了总体要求。在证券公司提供多样化的金融产品交易和服务过程中，投资者个人信息“全生命周期”处理环节存在共性运用难点和实践痛点，相关法律、规章、标准众多且分散，因此编制本标准，旨在为证券公司落实投资者个人信息保护要求在技术方面提供工作参考。

二、标准的编写原则和主要编制依据

（一）编写原则

1.全面性原则：依据法律、规章、标准等不同层面有关个人信息保护要求，涵盖投资者个人信息保护有关的管理要求和技术要求，覆盖从主要负责人、各部门、子公司到全体员工的各个层级，覆盖投资者个人信息全生命周期的安全管控要求。

2.可执行性原则：充分考虑现实执行情况，从国家标准、行业标准中汲取规范措施，切实从可执行、可落实角度去指引方向，既符合法律、规章，又侧重于建立体系化管理要求、完善机制、制定有效措施落实；既要达到该落实的要求，又避免要求过高、过细、过严，对于投资者个人信息保护的基本事项，予以明确，对于进一步可以优化提高的要求，也尽量细化梳理。

3.体现行业特性原则：充分结合行业特性，强调证券公司各类业务中，如何落实投资者个人信息保护要求，在生命周期各个环节体现证券业务开展中应落实的保护要求，特别提出分类分级建议、典型应用场景、个人信息保护政策模板等具体化的工作指引。

（二）主要编制依据

1.GB/T 35273—2020 信息安全技术 个人信息安全规范。

2.GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南。

3.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。

4.GB/T 43697—2024 数据安全技术 数据分类分级规则。

5.GB/T 25069—2022 信息安全技术 术语。

6.JR/T 0171—2020 个人金融信息保护技术规范。

7.JR/T 0158—2018 证券期货业数据分类分级指引。

8.JR/T 0250—2022 证券期货业数据安全管理与保护指引。

三、标准主要内容

《技术规范》共 8 章，附加附录 A、附录 B、附录 C。主要涵盖投资者个人信息保护基本原则、分类分级（包含分类分级建议表）、建立健全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基本要求、特定场景投资者个人信息保护等六方面。其中基本原则是开展投资者个人信息保护工作的总纲性要求；个人信息的分类分级作为开展投资者个人信息保护工作的基础性工作，《技术规范》明确了有关分类分级要求和分类分级参照表；建立健全投资者个人信息保护体系涵盖了建立内控制度、组织架构和岗位设置、人员管理、安全防护技术要求和措施、访问控制、投资者个人信息保护影响评估、监控、投资者个人信息安全事件处置、安全

教育与培训、第三方服务机构管理、审计监督等内容；投资者个人信息全生命周期保护基本要求包括了收集、存储、使用、加工、传输、提供、公开、删除等处理要求；特定场景投资者个人信息保护结合证券业务特点列举了6大业务场景的典型应用要求。

四、编制过程及意见收集处理情况

中国证券业协会信息科技部对编制工作进行了全程指导。在行业征集意见阶段共收到171条反馈意见，经编制工作组逐一审慎评估后，共采纳87条，部分采纳36条，未采纳48条，对于未采纳意见均出具未采纳理由。

五、与现行法律、法规和强制性国家标准的关系

《证券公司投资者个人信息保护技术规范》标准的制定，符合现行有关法律、法规的规定，引用了多部现行有效的国内标准文件，做到了与现行的国家、行业标准有机衔接。

《证券公司投资者个人信息保护技术规范》编制工作组

2025年9月25日