个人金融信息全生命周期安全管理实践

卓柳俊[1]，左鹏飞[2]，胡国华[1]，王振东[1]，李 强[1]

（1. 上海北山数据科技有限公司，上海 210203；2. 奇瑞徽银汽车金融股份有限公司，安徽 芜湖 241000）

摘要：对我国金融机构的数据全生命周期管理现状进行调查，分析了金融机构数据安全治理现状。研究表明，金融机构应以数据为中心构建安全合规体系，将数据全生命周期管理视为闭环，综合考虑各数据处理环节的安全合规风险，旨在贯彻数据安全治理理念，提高个人金融信息保护能力，确保个人金融信息在收集、存储、使用、加工、传输、提供、公开、删除等环节都能被有效地、动态地保护和实时监测。

关键词：个人金融信息；数据安全；数据合规；数据生命周期

中图分类号：TP309.2 **文献标志码：**A **文章编号：**1671－1807(2024)22－0184－06

依托大数据、云计算、区块链和人工智能等新兴技术的发展，金融领域应用与技术加速融合，各类业务活动日益依赖对个人金融信息的数据挖掘、分析和共享，由此催生了众多金融基础业务、核心业务和产品服务。随着金融机构处理个人金融信息过程的不断深入，个人金融信息面临越来越严峻的安全合规问题的挑战。

近年来国内学者对个人信息的保护进行了较为深入的研究，其中构建数据全生命周期管理模型来保护个人信息成为学者们的共识。从数据生命周期管理模型内容来看，粟湘等[1]提出了信息生命周期管理模型，涵盖存储、管理和应用三个层次和信息创建、采集、开发等六个阶段；师荣华和刘细文[2]归纳了各派数据生命周期理论，认为数据生命周期是从数据产生，经数据加工和发布，最终实现数据再利用的一个循环过程，其实质是依据科研过程来管理数据。从数据生命周期管理实践落地来看，李卓卓等[3]以大数据生命周期为依托，基于采集和收集数据、组织和处理数据、传播和共享数据、保存和维护数据、访问和利用数据、传播和共享数据，以及用户在各个环节中的综合权利，作为移动应用程序个人隐私信息保护评估的依据；吴丹和马乐[4]以可穿戴设备的医疗健康数据生命周期管理与服务研究成果为对象，从数据获取、传输、集成、交互和反馈等环节来构建医疗健康数据生命周期模型。从数据生命周期管理技术措施来看，林鹭等[5]提出数据生产要素全生命周期安全防护路径，包括构建业务管理平台、创建多方可信计算中台、建设安全运营中心；王蔚萍等[6]认为数据安全是贯穿整个数据全生命周期的，保障身份认证、授权、访问控制、可审计、资产保护等安全体系的五个核心要素的具体落地。

由上述研究看出，数据全生命周期管理是一个以数据为中心，通过政策法规、技术措施、安全组织架构三个维度构建的涵盖数据从收集到删除、再到循环利用的管理体系。尽管已有学者探究数据生命周期管理的价值与实践，但鲜有学者关注数据生命周期管理对个人金融信息的重要意义。本文一方面运用文本分析法对国内数据全生命周期管理的相关政策法规进行梳理，特别是个人金融信息保护内容的解读；另一方面结合实践中各金融机构已经运用的数据全生命周期管理技术措施的优势与不足，积极探索个人金融信息全生命周期管理的发展方向，以期为我国构建以数据为中心的个人金融信息全生命周期管理体系提供参考。

1 个人金融信息全生命周期管理的必要性

1.1 符合个人金融信息强监管趋势

个人金融信息是指个人在金融机构有相关交易记录以及因此提供的个人资料，包括个人的银行

收稿日期：2024-07-02

作者简介：卓柳俊(1992—)，男，广西柳州人，硕士，助理研究员，研究方向为数据安全、数据合规；左鹏飞(1991—)，男，安徽枞阳人，硕士，高级工程师，研究方向汽车金融数据分析、数据中台；胡国华(1977—)，男，江西南昌人，硕士，高级工程师，研究方向为数据安全、数据合规；王振东(1984—)，男，辽宁鞍山人，研究方向为数据安全、数据合规；李强(1972—)，男，山西太原人，研究方向为数据安全、数据合规。

卡账号、存取款情况、贷款和还款情况、信用消费和支付情况等[7]。为加强个人金融信息保护,国家以《中华人民共和国网络安全法》《中华人民共和国数据安全法》(以下简称《数据安全法》)《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)《关键信息基础设施安全保护条例》为基线,辅之以中国人民银行(以下简称"央行")、国家金融监督管理总局(以下简称"金管总局")等机构出台的一系列规范性、指导性文件和技术标准来指导实践,构建了较为完善的个人金融信息保护制度体系。该体系摒弃以系统为中心的传统网络安全建设思路,构建以数据为中心的涵盖数据收集、存储、使用、加工、传输、提供、公开、删除的个人金融信息全生命周期管理体系,主动将隐私保护嵌入金融业务和产品的信息技术开发中,来实现个人金融信息全生命周期安全合规保障。例如,2023 年 5 月 1 日开始实施的《证券期货业网络和信息安全管理办法》明确要求证券期货业机构建立健全投资者个人信息保护体系和管理机制,确保个人信息在收集、存储、使用、加工、传输、提供、公开、删除等全生命周期管理的合规、安全,防止个人信息的泄露、篡改、丢失;再如,2023 年 7 月 24 日公布的《中国人民银行业务领域数据安全管理办法(征求意见稿)》对数据全生命周期的安全保护管理和技术措施提出了具体要求。金融行业有着严格的数据安全合规要求,对个人金融信息进行全生命周期管理符合国家对金融数据强监管的趋势。

1.2 符合数据安全治理理念

金融机构对个人金融信息进行全生命周期管理是一种以数据为中心、以组织为单位的数据安全治理思路。《数据安全治理白皮书 5.0》指出"数据安全治理"强调从战略层面形成由上而下贯穿组织总体架构的对数据安全治理目标的共识,关注数据处理全生命周期安全,重视管理与技术并举,并能够根据安全形势、技术发展和演进趋势等的动态变化,对数据安全治理体系进行持续优化[8]。

"以数据为中心"要求金融机构将数据作为组织中最重要、最核心的资产,将其放在业务和技术决策的中心位置,强调数据作为业务运作的基础,并将其视为需要规划、管理和保护的重要资源,能够支持组织的战略目标,因此金融机构不仅要关注数据的存储和管理,还包括对数据质量、安全性、合规性以及数据使用的全方位进行管理,建立透明的数据流程和规则,确保数据处理的可追溯及可审计。

"以组织为单位"要求金融机构摒弃由个体系统的安全责任人承担各自责任的思路,强调组织内部的不同单位或部门在数据安全治理方面的主导责任和管理控制,各业务单位或部门有责任管理和控制其数据资产,根据自身业务需求和特点来进行数据治理。为防止各业务单位或部门在数据治理过程中的碎片化和非标准化,需要金融机构自上而下协调各单位或部门的数据治理职责,确保整体的数据安全治理战略和目标能够实现。通过对个人金融信息的全生命周期管理,金融机构能够贯彻多元共治、关注数据处理活动安全、管理与技术并举的数据安全治理思路,从而全面掌握个人金融信息的处理情况,有利于监管和追踪数据的变化及使用情况,并有助于识别、发现和管理潜在的数据丢失、盗窃或滥用风险。

1.3 符合个人金融信息全方位保护要求

个人金融信息是个人信息的一部分,来源于证券、银行、保险、宏观经济监管等诸多金融活动,包括金融机构对其在交易过程中获得的静态的客户个人基本信息和动态的交易数据[9]。个人金融信息具有高敏感度和高精准识别性的特点,一旦被泄露或被不当使用,都可能造成严重的经济损失、信用风险等问题。个人金融信息在金融机构中分布广泛且生态复杂,增加了金融机构对个人金融信息管理和安全保护的难度。

为全方位保护个人金融信息,国家相关部门、央行、金管总局出台了一系列规范性、指导性文件和技术标准。国家标准《信息安全技术 个人信息安全规范》(GB/T 35273—2020)规范个人信息处理者在收集、存储、使用、共享、转让、公开披露等信息处理环节中的相关行为。央行发布的金融行业标准《个人金融信息保护技术规范》(JR/T 0171—2020)对金融机构的个人金融信息保护义务提出了全面系统的制度和生命周期技术要求,具有标志性意义;《金融数据安全 数据安全分级指南》(JR/T 0197—2020)为金融数据分类分级提供标准依据。国家互联网信息办公室先后颁布了多部规章,均涉及个人金融信息保护问题,如强化金融等关键基础设施安全防护的《网络安全审查办法》、规范个人金融信息等数据出境的《数据出境安全评估办法》和《个人信息出境标准合同办法》、规范使用个人金融信息等数据和基础模型提供生成式人工智能服务的《生成式人工智能服务管理暂行办法》、规范使用

个人金融信息等数据和算法提供互联网信息服务算法推荐活动的《互联网信息服务算法推荐管理规定》等。

通过对个人金融信息的全生命周期管理，金融机构不仅能够从个人金融信息的收集、存储、使用、加工、传输、提供、公开、删除等方面进行保护，还可以在各阶段的特殊场景中提供防护，如收集和存储阶段的个人金融信息分类分级、使用和加工阶段的生成式人工智能服务和算法推荐活动、提供阶段的数据出境活动等。健全的个人金融信息全生命周期管理能够提高客户对金融机构的信任度，有效管理个人金融信息，保障信息的准确性和安全性，有助于对个人金融信息进行全方位保护。

2 个人金融信息全生命周期管理体系建设内容

国家标准《信息技术 大数据 术语》(GB/T 35295—2017)把“数据全生命周期”定义为将原始数据转化为可用于行动的知识的一组过程，《信息安全技术 数据安全能力成熟度模型》(GB/T 37988—2019)将这一组过程概括为“数据采集”“数据传输”“数据存储”“数据处理”“数据交换”“数据销毁”。《数据安全法》《个人信息保护法》进一步调整为“数据收集、存储、使用、加工、传输、提供、公开、删除”。综合来看，“数据全生命周期管理”就是围绕原始数据的收集、存储、使用、加工、传输、提供、公开、删除等处理活动进行管理和控制的过程。

2.1 全生命周期管理前置工作

个人金融信息全生命周期管理体系建设涉及多个部门，内部组织和协调难度大，需要满足内部和外部各方利益、平衡个人金融信息开发利用与安全合规需求，因此金融机构开展全生命周期管理的第一步是建立数据安全合规工作的组织架构，划分各部门职责分工，协同数据安全治理，为个人金融信息全生命周期管理提供组织支撑。以某城商银行为例，数据安全合规组织架构自上而下包括决策层、管理层和执行层，此外还包括一个贯穿整个数据安全治理过程的监督层对整个过程进行监督、审计，各层级之间通过定期会议沟通等工作机制实现紧密合作、互相协同。由数据安全推进计划发布的《数据安全治理实践指南(3.0)》对各层级之间的关系作了详细解读：决策层指导管理层工作的开展，并听取管理层关于工作情况和重大事项等的汇报；管理层对执行层的数据安全合规提出管理要求，并听取执行层关于数据安全合规执行情况和重大事项的汇报，形成管理闭环；监督层的管理监督小组和执行监督小组分别对管理层和执行层各自职责范围内的数据安全合规工作情况进行监督，并听取各方汇报，形成最终监督结论后同步汇报至决策层[10]。

明确内部数据安全合规组织架构后，金融机构应着手金融数据分类分级工作。金融机构首先应对内部的数据资产进行梳理，明确当前内部存储了哪些数据、数据存储的格式、数据范围、数据流转形式、数据访问控制方式、数据价值高低等内容，并形成数据资产清单。金融机构应在数据资产清单的基础上，参考《金融数据安全 数据安全分级指南》(JR/T 0197—2020)和《个人金融信息保护技术规范》(JR/T 0171—2020)，结合自身业务属性与管理特点，明确数据分类分级的方法、策略和原则。金融机构根据已制定的数据分类原则，定义包含多个层级的数据类别清单，再对数据资产清单中的数据逐个进行分类。完成数据分类之后，金融机构应从数据安全保护的角度，考虑影响对象(如国家、公众、个人、企业)、影响程度(如严重损害、一般损害、轻微损害、无损害)等要素以及实际情况对数据的安全级别进行判定，完成数据定级工作。基于上述数据分类分级工作，金融机构最终形成整体的数据分类分级目录，明确数据类别和级别的对应关系，为执行层落实数据分类分级工作提供依据。在完成数据分类分级的基础上，由管理层依据国家及金融行业领域的安全合规要求，建立数据分类分级保护策略，对数据实施全流程分类分级管理和保护。

综上，金融机构可以根据实际业务流程，在数据安全合规组织的指导下，帮助组织内部更好地识别和管理潜在的数据安全合规风险，结合数据资产清单和数据分类分级目录，帮助组织内部识别哪些数据是敏感的、机密的，从而有针对性地实施个人金融信息全生命周期风险管理措施。

2.2 全生命周期管理数据安全合规实践

2.2.1 敏感数据发现与识别

金融行业通常受到严格的安全合规监管要求，敏感数据发现与识别是确保金融机构符合这些法规和标准的关键步骤，也是确保个人金融信息不被未经授权的访问或泄露的关键一步。通过及时发现和识别敏感数据，金融机构可以采取相应的安全措施来保护客户的隐私权。目前金融机构对敏感数据识别主要依靠人工梳理，存在梳理周期时间长、识别速度慢、识别不够精准和不够系统全面等

问题,即使采用自动化识别的金融机构,也因金融数据存量大、结构复杂、种类多使得自动识别准确度低、对系统影响较大[11]。

为解决上述问题,某股份制商业银行应用了敏感数据识别与检查技术工具,为组织提供了全面、高效、准确的敏感数据识别与检查能力,有效保障了个人金融信息安全合规。敏感数据识别与检查技术工具的关键技术点分别为数据资产发现、敏感数据规则管理、敏感数据自动发现与识别、敏感数据报表等四方面。以下是该银行在这四方面技术应用的实践内容。

(1)数据资产发现是敏感数据识别与检查的第一步,旨在全面梳理和发现银行内部的数据资产。该银行通过静态扫描、动态解析、手动添加等多种资产发现方式,发现与识别数据资产的类型、位置、大小等基本信息;通过收集数据资产的元数据,如数据创建时间、所在系统、所有者、访问权限等,为后续数据管理和分析提供基础。

(2)敏感数据规则管理是建立敏感数据识别标准的重要环节。该银行通过采用机器学习、正则表达、数据指纹等技术,依据金融行业法规和标准,内置大量的敏感数据特征规则,包括正则表达式、关键词匹配、数据类型(如身份证号、银行卡号、电话号码)等,并支持自定义敏感数据规则功能,实现敏感数据规则有效管理。

(3)敏感数据自动发现与识别是技术工具的核心功能。该银行与某科技公司合作,开发自然语言处理(natural language processing,NLP)、机器学习(machine learning)等智能算法,对传统数据环境和大数据环境中存储的数据进行自动扫描,扫描出数据资产存储位置、数据大小、数据属性、数据属主/属组、数据描述等信息,并结合元数据、数据内容、上下文做敏感数据识别。

(4)敏感数据报表是技术工具的输出结果,用于向决策层展示敏感数据的识别结果和分布情况。该银行结合数据分类分级目录和处理结果,列出了敏感数据清单、数据分布图、数据安全风险分析和趋势分析图,帮助全局展示敏感数据的数量与分布等信息,利于直观查看数据库表字段的敏感情况。

2.2.2 数据安全运营管控

数据安全运营管控是定位以数据资产为核心视角、以数据全生命周期管理体系技术支撑为目标,以“识别-保护-检测-响应-恢复”(identify-protect-detect-response-recovery)五大关键安全领域能力落地为主旨构建的一套一站式数据全生命周期管理体系承载和运营的体系能力。数据安全风险监测技术是该体系的关键技术之一,也是实现个人金融信息全生命周期管理的核心能力,以自动化监控视图的方式直观展现出来。自动化监控视图是在数据流图的基础上基于数据分析、用户行为分析、可视化分析等技术,从流量、日志等多维度采集抽取数据进行关联、分析,通过关键节点组合仿真数据处理过程,构建纵向贯通数据处理阶段、横向融通数据安全合规节点的数据安全合规监控视图,以实时自动化的方式研判分析安全合规风险并进行违规报警。数据安全合规监控自动化替代以往人工评估是一个主流趋势,国务院国有资产监督管理委员会于2022年发布的《中央企业合规管理办法》〔国务院国有资产监督管理委员会令第42号〕第三十六条提出应对合规风险进行实时监测与自动处置。

个人金融信息自动化监控视图已经在某股份制证券公司初步应用,通过全面的自动化的数据采集、深入的分析以及有效的处置流程,为个人金融信息的全生命周期管理提供了强有力的保障。自动化监控视图的关键技术点分别为数据安全合规信息采集、数据安全合规信息分析和数据安全合规信息结果处置。以下是该证券公司在这三方面技术应用的实践内容。

(1)数据安全合规信息采集涉及数据采集点设计与数据采集技术实现。该证券公司将数据采集点设计在数据生命周期各阶段的安全合规节点,如数据收集阶段数据采集点设置在采集终端、数据传输阶段数据采集点设置在数据传输的出入两端。当证券公司实际数据处理活动触发安全合规节点风险报警机制时,埋藏于该节点的数据采集点将会自动采集风险信息。上述安全合规节点的设计依据金融证券行业的法律法规、行业标准和内部制度。例如,从《个人信息保护法》提炼总结个人信息处理保护的合法合规要求、从《金融数据安全 数据生命周期安全规范》(JR/T 0223—2021)归纳概括个人金融信息生命周期的技术安全规则、从《证券期货业网络和信息安全管理办法》梳理个人金融信息的管理制度建设要求。数据采集技术通过侵入式(如部署采集探针)或非侵入式(如日志发送)方式实现,但两种方式各有利弊。侵入式能够全面采集到数据合规信息但可能影响采集点的性能与安全,非侵入式不会给采集点带来负面影响但依赖日

志的完整性，因此该证券公司根据不同的数据类型使用不同方案来实现数据采集技术。对于技术方面的安全合规数据，证券公司采用侵入式方案，在数据采集终端、数据处理组件、数据 API 网关等采集点上部署探针，获取技术工具的处理日志；对于管理方面的安全合规数据，证券公司则采用非侵入式方案，要求对管理措施的结果（如组织架构设置与人员任命安排、制度流程规范、安全培训会议纪要）进行电子化归档并形成日志文档，通过日志方式发送数据合规信息至采集点以实现数据采集。

（2）数据安全合规信息分析的关键在于对采集到的安全合规数据进行风险识别。这些安全合规数据包括日志类、网络流量类以及非结构化文本类数据，该证券公司借助 NLP 技术进行解析以提取关键信息，如个人金融信息保护培训会议的人员名单、培训日期和频次、关键培训内容等。分析的难点在于，如何将提取出的关键信息与安全合规节点组成的安全合规知识库进行比对，以判断是否存在安全合规风险。安全合规知识库的构建基于相关法律法规和技术标准，这些法规标准详细规定了个人金融信息保护的各个合规要点，如培训周期（必须定期培训）、参与人员（数据处理人员必须参加）及留存信息（必须保留会议记录）等。以“个人金融信息保护培训”的安全合规节点为例，系统需检查公司培训是否符合规定的周期、是否覆盖所有相关员工、是否记录会议培训的过程。通过解析培训纪要记录的内容，系统能够自动判断培训是否满足合规要求。一旦发现培训周期不足、参与人员不全或培训内容未留存，系统将立即触发安全合规风险报警，并提供详细的分析报告。

（3）数据安全合规信息结果处置主要是将数据安全合规分析后的结果进行展示与处置。数据安全合规信息结果处置的主要工作包括对数据安全合规风险进行定级和对数据安全合规风险状态进行管理。对数据安全合规风险的定级主要根据风险对业务和用户权益影响程度来判断，证券公司把安全合规风险划分为一般、重要、紧急三个等级。一般类风险是不会直接产生数据安全事件的风险，比如召开的个人金融信息保护培训会议的频次没有达到规定要求；重要类风险是可能产生数据安全事件的风险，比如部署的数据防火墙未能配置合理的安全控制策略；紧急类风险是可能产生巨大安全威胁或者已经导致安全事件的风险，比如外部用户可以不受控制访问内网数据，或者数据对外共享未能脱敏或加密。对数据安全合规风险状态进行管理是对发现的数据安全合规风险进行状态跟踪，直到数据安全合规风险被处置并确认风险已解除。对于未能关闭的数据安全合规风险需要能采取措施进行自动处置，比如通过策略联动等技术实现数据访问权限设置，通过网络联动阻断外网不受限访问内网数据等。

3 结语

构建个人金融信息全生命周期管理体系，使金融机构数据资产归口管理清晰、跨部门衔接协作顺畅，在统一的全生命周期管理体系下，能够充分发挥金融机构数据共享和大数据分析的优势，为个人金融信息生命周期中不同的阶段提供安全合规管理的参考依据，实现个人金融信息全生命周期精细化规范化管理的同时，使金融机构业务和产品保值增值，有效提升金融数据的使用效益。

为构建个人金融信息全生命周期管理体系，金融机构应首先建立数据安全合规组织架构，完善数据分类分级目录，为个人金融信息全生命周期安全管理措施的实施提供组织架构和数据资产保障。其次，金融机构应逐渐减少传统人工对个人金融信息进行粗放式管理的方式，提高自动化工具进行全生命周期管理的比例。金融机构可以建立敏感数据发现与识别技术，提高个人金融信息自动化识别与管理能力；还可以构建以数据资产为核心视角、以数据全生命周期管理体系技术支撑为目标的数据安全运营管控能力，以实时监控的自动化监控视图方式可视化地展示个人金融信息处理活动。

由于法律法规、行业监管和技术标准的术语和规则的抽象，一些敏感数据的识别和监控视图中安全合规节点的风险报警无法真正实现自动化处理，这些自动化工具的处理结果还是需要依靠大量人工处理与复查，一定程度上限制了自动化工具在个人金融信息全生命周期管理中的普及程度。随着技术的发展和法律与科技的不断融合，将自动化工具运用于个人金融信息全生命周期管理中会越来越得到金融机构的认可。

参考文献

[1] 粟湘，郑建明，吴沛. 信息生命周期管理研究[J]. 情报科学，2006(5)：691-696.

[2] 师荣华，刘细文. 基于数据生命周期的图书馆科学数据服务研究[J]. 图书情报工作，2011，55(1)：39-42.

[3] 李卓卓，马越，李明珍. 数据生命周期视角中的个人隐私

信息保护——对移动 APP 服务协议的内容分析[J]. 情报理论与实践,2016,39(12):63-68.
[4] 吴丹,马乐. 基于可穿戴设备的医疗健康数据生命周期管理与服务研究[J]. 信息资源管理学报,2018,8(4):15-27.
[5] 林鹭,陶立峰,张博晨. 数据生产要素流通全生命周期安全防护流程研究[J]. 保密科学技术,2021(9):32-38.
[6] 王蔚萍,章学周,郑璐琳. 数据全生命周期安全防护[J]. 中国高新科技,2021(24):64-66.
[7] 张可法. 个人金融信息私法保护的困境与出路[J]. 西北民族大学学报(哲学社会科学版),2019(2):91-97.
[8] 中关村网络安全与信息化产业联盟数据安全治理专业委员会. 数据安全治理白皮书 5.0[R]. 北京:中关村网络安全与信息化产业联盟,2023.
[9] 何渊. 数据法学[M]. 北京:北京大学出版社,2020.
[10] 数据安全推进计划. 数据安全治理实践指南(3.0)[R]. 北京:数据安全推进计划,2023.
[11] 谢锋林,林慧博,林煜豪,等. 敏感数据全生命周期安全防护方案[J]. 电信工程技术与标准化,2020,33(11):61-67.

Personal Financial Information Full Life Cycle Security Management Practices

ZHUO Liujun[1], ZUO Pengfei[2], HU Guohua[1], WANG Zhendong[1], LI Qiang[1]
(1. Shanghai Beishan Data Technology Co. Ltd., Shanghai 210203, China;
2. Chery Huiyin Automotive Finance Co. Ltd., Wuhu 241000, Anhui, China)

Abstract: The current situation of data security governance of financial institutions in China was analysed by investigating the current situation of full life cycle management of data in financial institutions in China. The study shows that financial institutions should construct a security compliance system centred on data, consider the full life cycle management of data as a closed loop, and comprehensively consider the security compliance risks of each data processing link, with the aim of implementing the concept of data security governance, improving the ability to protect personal financial information, and ensuring that personal financial information can be effectively and dynamically collected, stored, used, processed, transmitted, made available, disclosed, deleted, etc., to be protection and real-time monitoring.

Keywords: personal financial information; data security; data compliance; data lifecycle