企业合规专业委员会
法律资讯

主编：谢佩之

副主编：王黎君、胡晓光

责任编辑：王英卜

2025 年 2 月

目　录

作者：张善奋 上海功承瀛泰律师事务所[1]

[1] 现任上海律协企业合规专业委员会委员、上海功承瀛泰律所数据合规委委员、律师。拥有 CISP-PIP、CCRC-DCO 等企业合规领域专业资质。张律师曾先后供职于平安、复星、银联等金融企业，负责过企业内部法律、合规、风控、内审等多类职能工作，在金融、大数据行业具有十多年丰富的企业实务积累。现为多家金融机构和企业提供常年或专项法律服务。张律师专业领域有：银行与保险、数字经济与资产、公司与并购、个人财富传承。张律师是公众号“ DataTech 合规实务”的负责人，该号创建以来一直以原创性、研究性、前沿性为特色。张律师坚持研究与实务相结合，从实践需要出发，擅长从企业视角来理解问题、分析问题并解决问题。张律师经常开展各类公开或企业定向培训，主题涵盖了金融消费者权益保护、企业数据合规体系建设、保险业务合规、保险在财富传承中的价值、金融监管文件解读、个人信息保护、数据资产入表、数据资产融资等主题。

银行保险机构数据安全管理办法

第一章　总　则

第一条　为规范银行业保险业数据处理活动，保障数据安全、金融安全，促进数据合理开发利用，保护个人、组织的合法权益，维护国家安全和社会公共利益，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国银行业监督管理法》《中华人民共和国商业银行法》《中华人民共和国保险法》等法律法规，制定本办法。

第二条　本办法所称银行保险机构，是指在中华人民共和国境内设立的政策性银行、商业银行、农村合作银行、农村信用合作社、金融资产管理公司、企业集团财务公司、金融租赁公司、汽车金融公司、消费金融公司、货币经纪公司、信托公司、理财公司、保险公司、保险资产管理公司、保险集团（控股）公司。

开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。国家有关主管部门另有规定的，应当依法遵守其规定。

第三条　本办法所称数据，是指以电子或者其他方式对信息的记录。

数据处理，是指对数据的收集、存储、使用、加工、传输、提供、共享、转移、公开、删除、销毁等。

数据安全，是指通过采取必要措施，对数据处理活动和数据应用场景进行管理与控制，确保数据始终处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

数据主体，是指数据所标识的自然人或者其监护人、企业、机关、事业单位、社会团体和其他组织。

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。

大数据平台，是指以处理海量数据存储、计算、分析等为目的的基础设施，包括数据统计分析类的平台和大数据处理类平台（如数据湖、数据仓库等）。

第四条　国家金融监督管理总局及其派出机构负责银行业保险业数据安全的监督管理，制定并发布监管规章制度，对银行保险机构履行数据安全保护义务情况进行监督检查。

第五条　银行保险机构应当建立与本机构业务发展目标相适应的数据安全治理体系，建立健全数据安全管理制度，构建覆盖数据全生命周期和应用场景的安全保护机制，开展数据

安全风险评估、监测与处置，保障数据开发利用活动安全稳健开展。银行保险机构利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度基础上，履行数据安全保护义务。

第六条　银行保险机构开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、政治安全、经济金融安全、公共利益，不得损害个人、组织的合法权益。

第七条　银行保险机构应当统筹发展和安全，落实国家大数据战略，推进数据基础设施建设，加大数据创新应用力度，促进以数据为关键要素的数字经济发展，提升金融服务的智能化水平，创新普惠金融服务模式，增强防范化解风险的能力。

第八条　银行保险机构应当持续跟踪新兴数据开发利用和科技发展前沿动态，有效应对大数据应用与科技创新可能产生的规则冲突、社会风险、伦理道德风险，防止数据与科技被误用、滥用。

第二章　数据安全治理

第九条　银行保险机构应当建立覆盖董（理）事会、高管层、数据安全统筹、数据安全技术保护等部门的数据安全管理组织架构，明确岗位职责和工作机制，落实资源保障。

第十条　银行保险机构应当建立数据安全责任制，党委（党组）、董（理）事会对本单位数据安全工作负主体责任。银行保险机构主要负责人为数据安全第一责任人，分管数据安全的高级管理人员为直接责任人，明确各层级负责人的责任，明确违规情形和责任追究事项，落实问责处置机制。

第十一条　银行保险机构应当指定数据安全归口管理部门，作为本机构负责数据安全工作的主责部门。其主要职责包括：

（一）组织制定数据安全管理原则、规划、制度和标准；

（二）组织建立和维护数据目录，推动实施数据分类分级保护；

（三）组织开展数据安全评估和审查；

（四）统筹建立数据安全应急管理机制，组织开展数据安全风险监测、预警与处置；

（五）组织开展数据安全宣贯培训，提升员工数据安全保护意识与技能；

（六）建立和维护内部数据共享、外部数据引入、数据对外提供、数据出境的统筹管理机制，牵头对外部数据供应商进行安全管理，统筹大数据应用、数据共享项目的安全需求管理；

（七）向党委（党组）、董（理）事会、高管层报告数据安全重要事项；

（八）其他须统筹管理的数据安全工作事项。

第十二条　银行保险机构应当按照“谁管业务、谁管业务数据、谁管数据安全”的原则，明确各业务领域的数据安全管理责任，落实数据安全保护管理要求。

第十三条　银行保险机构风险管理、内控合规和审计部门负责将数据安全纳入全面风险管理体系、内控评价体系，定期开展审计、监督检查与评价，督促问题整改和开展问责。

第十四条　银行保险机构信息科技部门是数据安全的技术保护主责部门，其主要职责包括：

（一）建立数据安全技术保护体系，建立数据安全技术架构和保护控制基线，落实技术保护措施。

（二）制定数据安全技术标准规范制度，组织开展数据安全技术风险评估。

（三）组织开展信息系统的生命周期安全管理，确保数据安全保护措施在需求、开发、测试、投产、监测等环节得到落实。

（四）建立数据安全技术应急管理机制，组织开展数据安全风险技术监测、预警、通报与处置，防范外部攻击、内外部破坏等危害数据安全活动。

（五）组织数据安全技术研究与应用。

第十五条　银行保险机构应当建立良好的数据安全文化，开展全员数据安全教育和培训，提高数据安全保护意识和水平，形成全员共同维护数据安全和促进发展的良好环境。

第三章　数据分类分级

第十六条　银行保险机构应当制定数据分类分级保护制度，建立数据目录和分类分级规范，动态管理和维护数据目录，采取差异化安全保护措施。

第十七条　银行保险机构应当对机构业务及经营管理过程中获取、产生的数据进行分类管理，数据类型包括客户数据、业务数据、经营管理数据、系统运行和安全管理数据等。

第十八条　银行保险机构应当根据数据的重要性和敏感程度，将数据分为核心数据、重要数据、一般数据。其中，一般数据细分为敏感数据和其他一般数据。

核心数据，是指对领域、群体、区域具有较高覆盖度或者达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或者共享，可能直接影响政治安全、国家安全重点领域、国民经济命脉、重要民生、重大公共利益。

重要数据，是指特定领域、特定群体、特定区域或者达到一定精度和规模的数据，一旦被泄露或者篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。

敏感数据，是指一旦被泄露或者篡改、损毁，对经济运行、社会稳定、公共利益有一定影响，或者对组织自身或者公民个体造成重要影响的数据。

除以上数据之外的，为其他一般数据。

第十九条　银行保险机构应当加强数据安全级别的时效管理，建立动态调整审批机制，当数据的业务属性、重要程度和可能造成的危害程度发生变化，导致原安全级别不再适用的，应当及时动态调整。

第四章　数据安全管理

第二十条　银行保险机构应当按照国家数据安全与发展政策要求，根据自身发展战略，制定数据安全保护策略。银行保险机构应当制定数据安全管理办法，明确管理责任分工，建立包括数据处理全生命周期管控机制，落实保护措施。

银行保险机构应当对数据外部引入或者合作共享、数据出境等，制定安全管理实施细则。

第二十一条　银行保险机构应当建立企业级数据架构，统筹开展对全域数据资产登记管理，建立数据资产地图，以数据分类分级为基础明确数据保护对象，围绕数据处理活动实施安全管理。

第二十二条　银行保险机构在处理敏感级及以上数据的业务活动时，或者开展数据委托处理、共同处理、转移、公开、共享等对数据主体有较大影响的活动时，应当事先开展数据安全评估。数据安全评估应当根据数据处理目的、性质和范围，按照法律法规和伦理道德规范要求，分析数据安全风险和对数据主体权益影响，评估数据处理的必要性、合规性，评估数据安全风险及防控措施的有效性。

第二十三条　银行保险机构应当建立企业级数据服务管理体系，制定数据服务规范，建立专职数据服务团队，统筹内外部数据加工、分析，实施数据服务需求分析、服务开发、服务部署、服务监控等活动。

第二十四条　银行保险机构收集数据应当坚持“合法、正当、必要、诚信”原则，明确数据收集和处理的目的、方式、范围、规则，保障收集过程的数据安全性、数据来源可追溯。银行保险机构不得超出数据主体同意的范围向其收集数据，法律、行政法规另有规定的除外。

银行保险机构向其他银行保险机构收集行业重要级及以上数据，需经国家金融监督管理总局同意。

第二十五条　银行保险机构应当以信息系统为数据收集的主要渠道，限制或者减少其他渠道、临时性数据收集。

银行保险机构停止金融业务或者服务后，应当立即停止相关数据收集或者处理活动，法律、行政法规另有规定的除外。

第二十六条　银行保险机构应当制定外部数据采购、合作引入的集中审批管理制度，纳入外包风险管理体系进行统筹管理，统筹建立数据需求、安全评估、收集引入、数据运维、登记备案和监督评价管理机制，对数据来源的真实性、合法性进行调查，评估数据提供者的安全保障能力及其数据安全风险，明确双方数据安全责任及义务。

第二十七条　银行保险机构开展敏感级及以上数据清洗转换、汇聚融合、分析挖掘等数据加工活动时，应当采用匿名化、去标识化或者其他必要安全措施保护数据主体权益，法律、行政法规另有规定的除外。数据汇聚融合衍生敏感级及以上数据，或者导致数据安全级别变化的，应当及时评估、调整安全保护措施。

第二十八条　银行保险机构应当按照“业务必要授权”原则，对敏感级及以上数据严格实施授权管理，制定数据访问闭环管理机制，并对数据访问行为实施审计。确因业务需要从生产环境提取数据的，应当建立严格的审批程序，并明确数据使用或者保存期限。

银行保险机构利用互联网等信息网络开展数据处理活动时，要落实网络安全等级保护、关键信息基础设施安全保护、密码保护等制度要求。

第二十九条　银行保险机构应当对数据共享使用进行集中安全管控，明确企业级数据共享策略，评估数据共享使用的必要性、合规性、安全性及伦理道德规范的符合度。

银行保险机构应当建立银行母行、保险集团或者母公司与其子行、子公司数据安全隔离的“防火墙”，并对共享数据采取有效保护措施。银行保险机构与其母行、集团，或者其子行、子公司共享敏感级及以上数据，应当获得数据主体的授权同意，法律、行政法规另有规定的除外。不得以数据主体拒绝同意共享敏感数据而终止或者拒绝单家子行、子公司对其提供金融服务，所共享数据属于提供产品或者服务所必需的除外。

第三十条　银行保险机构在委托处理数据时，应当明确所涉数据外部使用和处理的条件、场景、方式。委托处理数据时，应当以合同协议方式约定委托处理的目的、期限、处理方式、数据范围、保护措施、双方的数据安全责任和义务，以及受托方返还或者删除数据的方式等，对数据处理活动进行记录和审计，可对外公开披露的数据除外。银行保险机构应当要求受托方在未取得其同意时，不得转委托其他主体处理数据，不得对外共享数据，不得加工、训练、挪用数据，或者采取其他形式处理数据以谋取合同或者协议约定以外的利益。

第三十一条　银行保险机构应当将数据委托处理纳入信息科技外包管理范围，在实施过程中不得将信息科技管理责任、数据安全主体责任外包，涉及信息科技战略管理、信息科技

风险管理、信息科技内部审计及其他有关信息科技核心竞争力的职能不得外包。供应链服务中涉及敏感级及以上数据处理的，银行保险机构应当加强对供应商的准入和安全管理。

第三十二条　银行保险机构与第三方机构进行数据共同处理时，应当按照“业务必要授权”原则制定方案并采取有效管理和技术保护措施确保数据安全，并以合同协议方式明确双方在数据处理过程中的数据安全责任和义务。

第三十三条　银行保险机构因合并、分立、解散、被宣告破产等需要转移数据的，应当明确数据转移内容，通过协议、承诺等方式约定数据接收方全面承接对应数据的安全保护义务，通过公告等方式告知数据主体。数据转移应当采用安全可靠方式进行，并确保转移过程可追溯。

第三十四条　银行保险机构向外部提供敏感级及以上数据，应当取得数据主体同意，法律、行政法规另有规定的除外。除国家机关依法履职外，银行保险机构核心数据跨主体流动应当按照国家相关政策要求通过风险评估、安全审查。

第三十五条　银行保险机构应当建立对外公开披露数据的审批机制，研判可能产生的影响，数据公开应当在机构官方渠道进行发布，确保数据真实、准确、防篡改，记录审批和发布情况。

敏感级及以上数据不得公开，法律、行政法规另有规定或者取得数据主体授权同意的除外。

第三十六条　银行保险机构向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息，应当承担数据安全主体责任，并按照国家有关政策要求进行安全评估。

第三十七条　银行保险机构应当采取技术措施，对敏感级及以上数据加强重点防护。加强数据备份，制定备份策略，备份数据和生产数据应隔离分开保存，严格管理备份数据的访问权限。制定备份验证计划，确保备份数据完整有效、业务可恢复。

第三十八条　银行保险机构应当制定数据销毁管理制度，按照国家、行业有关规定及与数据主体的约定进行数据删除或者匿名化处理。银行保险机构委托数据处理终止时，应当要求服务提供商及时删除数据，并采取现场检查等有效监督措施，确保数据被销毁、不可恢复。

第五章　数据安全技术保护

第三十九条　银行保险机构应当建立针对大数据、云计算、移动互联网、物联网等多元异构环境下的数据安全技术保护体系，建立数据安全技术架构，明确数据保护策略方法，采取技术措施，保障数据安全。

第四十条　银行保险机构应当将数据安全保护纳入信息系统开发生命周期框架，针对敏感级及以上数据明确安全保护要求，实现数据安全保护措施与信息系统的同步规划、同步建设、同步使用。

第四十一条　银行保险机构应当将数据纳入网络安全等级保护。银行保险机构应当根据数据安全级别，划分网络逻辑安全域，建立分区域数据安全保护基线，实施有效的安全控制，包括内容过滤、访问控制和安全监控等，确保相关措施满足处理和存储最高级别数据的网络安全策略和数据安全保护策略要求。存放或者传输敏感级及以上数据的机房、网络应当实施重点防护，设立物理安全保护区域，对网络边界、重要网络节点进行安全监控与审计。

第四十二条　银行保险机构应当将敏感级及以上数据纳入信息系统保护。在数据全生命周期内采取有效的访问控制管理措施，对于不同区域流转和共享中的数据，应当实施同等水平的安全防护措施。多来源敏感级及以上数据汇聚集中后，应当采取加强性或者至少不低于集中前最高级别数据保护强度的安全措施。

第四十三条　银行保险机构应当严格实施对敏感级及以上数据的管理，制定用户对数据的访问策略，采取有效的用户认证和访问控制技术措施，规范数据操作行为，用户对数据的访问应当符合业务开展的必要要求并与数据安全级别相匹配。敏感级及以上数据的操作应当进行日志记录，包括操作时间、用户标识、行为类型等，核心数据操作日志及其备份数据保存时间不低于三年，重要数据、敏感数据操作日志及其备份数据保存时间不低于一年，如涉及委托处理、共同处理的数据操作日志及其备份数据保存时间不低于三年。应当定期对数据操作行为进行审计，审计周期不超过六个月。

第四十四条　银行保险机构敏感级及以上数据传输应当采用安全的传输方式，保障数据完整性、保密性、可用性。

银行保险机构之间进行数据交换时，参与数据交换的相关机构应当采取有效措施保障信息数据传输和存储的保密性、完整性、准确性、及时性、安全性。

第四十五条　银行保险机构应当对敏感级及以上数据采取安全存储措施，防止勒索病毒、木马后门等攻击。个人身份鉴别数据不得明文存储、传输和展示。敏感级及以上数据应当实施数据容灾备份，定期进行数据可恢复性验证。

第四十六条　敏感级及以上数据达到使用或者保存期限后，应当采取技术措施及时删除或者销毁，确保数据不可恢复。终端和移动存储介质内的敏感级及以上数据应当采取技术保护措施，确保受控安全访问，介质报废或者重用时，其存储空间数据应当完全清除并不可恢复。

第四十七条　银行保险机构应当开展数据安全的技术基础设施建设，支持用户身份管理、数据匿名化、行为监测、日志审计、数据虚拟化等功能的组件化、服务化，保障安全标准在信息系统中执行的一致性。

第四十八条　银行保险机构开发信息系统时，应当明确系统拟处理的数据及其安全级别、访问规则、保护需求，并实施有效的系统安全控制。系统投产上线前应当开展安全测试，确保各项安全要求落实，有效防范数据安全风险。测试环境应当与生产系统隔离，敏感级及以上数据原则上未经脱敏处理不得进入测试环境，防止数据泄露。

第四十九条　银行保险机构应当对大数据平台采取高可用设计、安全加固、数据备份等措施进行重点保护。应当建立大数据服务访问授权机制，动态监测与审计大数据访问行为。

第五十条　银行保险机构开展自动化决策分析、模型算法开发、数据标注等活动，应当保证数据处理透明度和结果公平合理。银行保险机构应当对人工智能模型开发应用进行统一管理，建立模型算法产品外部引入的准入机制，对模型研发过程进行主动管理，实现模型算法可验证、可审核、可追溯。

第五十一条　银行保险机构信息系统、模型算法投入使用前，应当开展数据安全审查，审查数据与模型使用的合理性、正当性、可解释性，以及数据利用对相关主体合法权益的影响、伦理道德风险及防控措施有效性等。

第五十二条　银行保险机构使用人工智能技术开展业务时，应当就数据对决策结果影响进行解释说明和信息披露，实时监测自动化处理与系统运行结果，建立人工智能应用的风险缓释措施，包括制定退出人工智能应用的替代方案，对安全威胁制定应急方案并开展演练。

第五十三条　银行保险机构在建设开放银行、金融生态或者与第三方数据合作时，要实现自身与外部的安全风险隔离，与外部机构的数据交互应当通过集中管理的外联平台或者应用程序接口实施，依据“业务必需、最小权限”原则，采取有效措施对接口设计、开发、服务、运行等进行集中安全保护管理。

第六章　个人信息保护

第五十四条　银行保险机构处理个人信息应当按照“明确告知、授权同意”的原则实施，法律、行政法规另有规定的除外，并在信息系统中实现相关功能控制。

第五十五条　银行保险机构处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，收集个人信息应当限于实现金融业务处理目的的最小范围，不得过度收集个人信息。不得利用所收集的个人信息从事违法违规活动。

第五十六条　银行保险机构处理个人信息前，应当真实、准确、完整地向个人告知其个人信息的处理目的、处理方式、处理的个人信息种类、保存期限，个人行使其信息权利的申请受理和处理程序，以及法律法规规定应当告知的其他事项。

银行保险机构应当制定个人信息处理规则，个人信息处理规则应当公开展示、易于访问、内容明确、清晰易懂。

第五十七条　银行保险机构不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务，处理个人信息属于提供产品或者服务所必需的除外。

第五十八条　银行保险机构在开展涉及对个人权益有重大影响的个人信息处理活动时，应当进行个人信息保护影响评估，评估内容包括个人信息处理的合法性、必要性，对个人权益的影响及安全风险，所采取的保护措施合法性、有效性以及是否与风险程度相适应。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。

第五十九条　银行保险机构与其母行、集团，或者其子行、子公司共享个人信息，及向外部提供个人信息，应当履行向个人告知及取得其同意等相关事项的义务。

第六十条　银行保险机构向中华人民共和国境外提供个人信息的，除满足第三十六条、第五十九条规定的要求外，还应当向个人告知其向境外接收方行使信息权利的方式和程序等事项，法律、行政法规另有规定的除外。

第六十一条　银行保险机构委托第三方处理个人信息的，应当在合同或者协议条款内明确受托人对个人信息的保护义务、保护措施和期限等，并严格监督受托人以约定的处理目的、处理方式等处理个人信息，与第三方传输个人敏感数据必须确保安全，防范数据滥用和泄漏风险。未经银行保险机构同意，受托人不得转委托他人处理个人信息。

第六十二条　银行保险机构在算法设计、训练数据选择和模型生成时，应当采取有效措施，保障个人合法权益。利用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。

第六十三条　发生或者可能发生个人信息泄露、篡改、丢失的，银行保险机构应当立即采取补救措施，同时通知个人并报送国家金融监督管理总局或者其派出机构。通知应当包括下列事项：

（一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；

（二）银行保险机构采取的补救措施和个人可以采取的减轻危害的措施。

银行保险机构采取措施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；监管部门认为可能造成危害的，有权要求银行保险机构通知个人。

第七章　数据安全风险监测与处置

第六十四条　银行保险机构应当将数据安全风险纳入本机构全面风险管理体系，明确数据安全风险监测、风险评估、应急响应及报告、事件处置的组织架构和管理流程，有效防范和处置数据安全风险。

第六十五条　银行保险机构应当对数据安全威胁进行有效监测，实施监督检查，主动评估风险，防止数据篡改、破坏、泄露、非法利用等安全事件发生。监测内容包括：

（一）超范围授权或者使用系统特权账号；

（二）内部人员异常访问、使用数据；

（三）对数据集中共享的系统或者平台的网络安全、数据安全威胁；

（四）敏感级及以上数据在不同区域的异常流动；

（五）移动存储介质的异常使用；

（六）外包、第三方合作中的数据处理异常或者数据泄露、丢失和篡改；

（七）客户有关数据安全的投诉；

（八）数据泄露、仿冒欺诈等负面舆情；

（九）其他可能导致数据安全事件发生的情况。

第六十六条　银行保险机构应当每年开展一次数据安全风险评估。审计部门应当每三年至少开展一次数据安全全面审计，发生重大数据安全事件后应当开展专项审计。银行保险机构委托专业机构进行数据安全审计时，不得使用该机构提供的产品和其他服务。

第六十七条　数据安全事件是指银行保险机构数据被篡改、泄露、破坏、非法获取、非法利用等，对个人或者组织合法权益、行业安全、国家安全造成负面影响的事件。根据其影响范围和程度，分为特别重大、重大、较大和一般四个事件级别。

第六十八条　银行保险机构应当建立数据安全事件应急管理机制，建立机构内部协调联动机制，建立服务提供商、第三方合作机构数据安全事件的报告机制，及时处置风险隐患及安全事件。

（一）制定数据安全事件应急预案，定期开展应急响应培训和应急演练。

（二）发生数据安全事件后，应当立即启动应急处置，分析事件原因、评估事件影响、开展事件定级，按照预案及时采取业务、技术等措施控制事态。

（三）建立数据安全事件报告机制，根据事件安全等级制定报告流程，发生数据安全事件时按照规定报告，同时按照合同、协议等有关约定履行客户及合作方告知义务。

（四）发生数据安全事件或者使用的网络产品和服务存在安全缺陷、漏洞时，应当立即开展调查评估，及时采取补救措施，防止危害扩大。网络产品和服务提供商存在安全缺陷、漏洞隐瞒不报的，银行保险机构应当责令其改正；未按要求整改或者造成严重后果的，应当取消其服务资格，按合同约定予以处罚，并向国家金融监督管理总局或者其派出机构报告。

第六十九条　数据安全事件发生 2 小时内，银行保险机构应当向国家金融监督管理总局或者其派出机构报告，并在事件发生后 24 小时内提交正式书面报告。发生特别重大数据安全事件，银行保险机构应当立即采取处置措施，按照规定及时告知用户并向国家金融监督管理总局或者其派出机构、属地公安机关报告。银行保险机构应当每 2 小时将处置进展情况上报，直至处置结束。数据安全事件处置结束后，银行保险机构应当在五个工作日内将事件及其处置的评估、总结和改进报告报送国家金融监督管理总局或者其派出机构。其他法律、行政法规对数据安全事件应急处置作出规定的，银行保险机构应当执行。

第八章　监督管理

第七十条　国家金融监督管理总局及其派出机构对银行保险机构数据安全保护情况进行监督管理，开展非现场监管、现场检查，将数据安全管理情况纳入监管评级评估体系，依法对银行保险机构数据安全事件进行处罚和处置，实施对数据安全管理的持续监管。

第七十一条　国家金融监督管理总局按照国家数据分类分级要求，制定银行业保险业重要数据目录，提出核心数据目录建议，监督指导银行保险机构开展数据分类分级管理和数据保护。银行保险机构应当按要求向国家金融监督管理总局或者其派出机构报送重要数据目录。重要数据目录发生重大变化应当及时报备更新后的数据目录。

第七十二条　国家金融监督管理总局建立银行业保险业数据安全监测预警、通报处置机制，持续监测数据安全风险，向行业发布风险提示，制定银行业保险业数据安全事件应急预案，处置数据安全风险事件。与国家数据安全管理部门建立联防联控管理机制，实施数据安全信息共享、风险监测预警及数据安全事件处置。

第七十三条　涉及批量敏感级及以上数据的数据共享、委托处理、转让交易、数据转移，银行保险机构应当在处理、合同签署前二十个工作日向国家金融监督管理总局或者其派出机构报告，法律、行政法规另有规定的除外。

第七十四条　银行保险机构应当于每年 1 月 15 日前向国家金融监督管理总局或者其派出机构报送上一年度数据安全风险评估报告，报告内容包括数据安全治理、技术保护、数据安

全风险监测及处置措施、数据安全事件及处置情况、委托和共同处理、数据出境、数据安全评估与审查情况、数据安全相关的投诉及处理情况等。

第七十五条　国家金融监督管理总局及其派出机构对银行保险机构数据安全保护情况进行现场检查、事件调查，对于发现涉嫌违法违规事项的有关单位和个人，依法开展调查。现场检查、事件调查可以委托国家、行业有关专业技术机构或者审计机构予以协助。

第七十六条　银行保险机构违反本办法要求的，国家金融监督管理总局或者其派出机构根据其违规情况，对银行保险机构依法采取风险提示、监管谈话、监管通报、责令改正等监管措施；对涉及违规处理行为的系统或者应用，责令暂停或者终止服务；对有重大违法违规情形，或者迟报、瞒报数据安全事件和案件，或者产生重大数据安全风险、事件、案件的第三方机构进行行业通报，责令银行保险机构暂缓或者停止合作。

第七十七条　银行业金融机构违反本办法要求的，国家金融监督管理总局及其派出机构可以依据《中华人民共和国银行业监督管理法》相关规定，责令银行业金融机构改正，并处以二十万以上五十万以下罚款；情节特别严重或者逾期不改正的，可以责令停业整顿或者吊销其经营许可证。根据违规情况，可以责令银行业金融机构对直接负责的董事、高级管理人员和其他直接责任人员给予纪律处分；银行业金融机构的行为尚不构成犯罪的，对直接负责的董事、高级管理人员和其他直接责任人员给予警告，处五万元以上五十万元以下罚款；取消直接负责的董事、高级管理人员一定期限直至终身的任职资格，禁止直接负责的董事、高级管理人员和其他直接责任人员一定期限直至终身从事银行业工作。构成犯罪的，依法追究刑事责任。

保险业金融机构违反本办法要求的，国家金融监督管理总局及其派出机构可以依据《中华人民共和国保险法》相关规定，责令保险业金融机构改正，处五万元以上三十万元以下的罚款；情节严重的，限制其业务范围、责令停止接受新业务或者吊销业务许可证。根据违规情况，对其直接负责的主管人员和其他直接责任人员给予警告，并处一万元以上十万元以下的罚款；情节严重的，撤销任职资格。构成犯罪的，依法追究刑事责任。

实施过程中如遇《中华人民共和国银行业监督管理法》《中华人民共和国保险法》修订，以修订后的规定为准。

第七十八条　中国银行业协会、中国保险行业协会等行业社团组织应当通过宣传、培训、自律、协调、服务等方式，协助引导会员单位提高数据安全管理水平。

第九章　附　则

第七十九条　本办法由国家金融监督管理总局负责解释和修订。

第八十条　国家金融监督管理总局批准设立的其他银行业金融机构、保险业金融机构、金融控股公司以及总局管理单位参照适用本办法。地方金融管理部门批准设立的金融组织参照适用本办法。

第八十一条　本办法自公布之日起施行，《银行保险机构数据安全办法》（银保监办发〔2022〕118号）同时废止。

附件：数据安全事件分级

数据安全事件分级

一、特别重大数据安全事件

1.核心数据遭到泄露、破坏或者非法获取、非法利用。

2.重要数据遭到泄露、破坏或者非法获取、非法利用，对2个及以上省级区域经济运行秩序造成特别严重影响。

3.敏感级及以上数据遭到大规模泄露、破坏或者非法获取、非法利用，导致下述情形之一的：

（1）对公共利益造成特别严重危害，造成特别重大经济损失，或者产生特别重大社会群体性事件；

（2）对银行业保险业核心业务、系统重要性金融机构、关键信息基础设施等生产经营造成特别严重威胁或者影响，包括导致大面积业务中断、大量处理能力丧失、大面积关键信息基础设施瘫痪等。

4.其他对国家安全、政治安全、经济金融安全、公共利益造成特别严重影响的。

二、重大数据安全事件

1.重要数据遭到泄露、破坏或者非法获取、非法利用，对省级区域经济带来重大影响或者对银行保险行业安全造成影响。

2.敏感级及以上数据遭到泄露、破坏或者非法获取、非法利用，导致下述情形之一的：

（1）对多个银行保险机构的业务、重要信息系统生产运营造成严重威胁或者影响，可能导致区域性或者部分金融机构的业务中断、信息系统中断、处理能力丧失等；

（2）对公众利益造成严重危害，产生大范围社会负面影响，可能导致或者直接造成大面积投诉、社会群体性事件；

（3）对多个个人或者组织权益造成严重影响，包括对党政机关、企事业单位、社会团体等多个组织造成严重经济或者技术损失，对生产经营秩序产生直接影响；多人财产安全受到严重危害、尊严遭受侵害等。

3.其他对国家安全、经济金融安全、公共利益、个人和组织权益造成严重影响的。

三、较大数据安全事件

敏感级及以上数据遭到泄露、破坏或者非法获取、

非法利用，导致下述情形之一的：

1.对个人造成不可消除或者消除代价较大的负面影响，包括个人财产安全遭受损失或者可能产生重大损失，个人名誉尊严受到侵害，产生投诉、诉讼事件等。

2.对组织造成不可消除或者消除代价较大的负面影响，包括造成或者可能造成较大经济或者技术损失，部分业务无法正常开展，声誉受到破坏等。

3.银行保险机构自身部分业务无法正常开展或者本机构声誉受到破坏；银行保险机构重要信息系统安全稳定运行受到威胁或者影响，可能产生较大及以上级别的重要信息系统突发事件。

4.其他对经济金融安全、公共利益造成一般影响，或者对个人和组织权益造成较大影响的。

四、一般数据安全事件

除上述数据安全事件外，对组织或者个人造成一定影响的数据安全事件。

国家金融监督管理总局有关司局负责人就《银行保险机构数据安全管理办法》答记者问

一、《办法》制定的背景是什么？

答：金融数据具有高价值和高敏感性，金融数据安全与国家安全和金融消费者权益密切相关。近年来，银行业保险业数字化变革加速演进，新技术、新业态不断涌现，数据合作共享日益频繁。与此同时，金融领域面临的数据安全风险形势复杂严峻，也给金融机构数据安全管理带来新的挑战。对此，有必要充分发挥监管的“指挥棒”作用，通过强化政策要求引导银行保险机构压实主体责任，完善内部机制，采取有效的管理和技术措施加强数据安全保护，确保客户信息和金融交易数据的安全。

二、《办法》的主要内容和特点是什么？

答：《办法》共 9 章 81 条。包括总则、数据安全治理、数据分类分级、数据安全管理、数据安全技术保护、个人信息保护、数据安全风险监测与处置、监督管理及附则。主要特点包括：

一是落实数据安全责任制。明确银行保险机构党委（党组）、董（理）事会对本单位数据安全工作负主体责任，机构主要负责人为数据安全第一责任人，分管数据安全的领导为直接责任人。

二是明确数据安全归口管理部门。要求银行保险机构指定数据安全归口管理部门，作为本机构负责数据安全工作的主责部门，承担制定数据安全管理制度标准、建立维护数据目录、推动数据分类分级保护、组织开展风险监测、预警及处置等职责。

三是将数据安全风险纳入全面风险管理体系。要求银行保险机构明确管理流程，主动评估风险，对数据安全风险进行有效监测，防止数据破坏、泄露、非法利用等安全事件发生。风险管理、内控合规和审计部门定期对数据安全开展审计、监督检查与评价。

四是强化数据安全评估。要求银行保险机构开展相关数据处理活动时，应事先开展安全评估。根据数据处理目的、性质和范围，分析数据安全风险和对数据主体权益影响，评估数据处理的必要性、合规性及防控措施的有效性。

五是建立数据安全保护基线。将数据纳入网络安全等级保护，对存放或传输敏感级及以上数据的机房、网络实施重点防护，在数据全生命周期内采取有效访问控制管理措施，采用安全有效的传输方式保障数据完整性、保密性、可用性。

三、《办法》在数据分类分级方面提出了哪些具体要求？

答：《办法》要求银行保险机构制定数据分类分级保护制度，建立数据目录和分类分级规范，动态管理和维护数据目录，并采取差异化的安全保护措施。在数据分类方面，对机构业务及经营管理过程中获取、产生的数据进行分类管理，具体类型包括客户数据、业务数据、经营管理数据、系统运行和安全管理数据等。在数据分级方面，银行保险机构应根据数据的重要性和敏感程度，将数据分为核心数据、重要数据、一般数据，其中一般数据细分为敏感数据和其他一般数据；当数据的业务属性、重要程度和可能造成的危害程度发生变化，导致安全级别不再适用的，及时进行动态调整。

四、《办法》规定的数据安全管理职责有哪些？

答：《办法》要求银行保险机构按照国家政策要求，根据自身发展战略，制定数据安全保护策略；根据数据处理目的、性质和范围，按照法律法规和伦理道德规范要求，对相关数据业务处理活动进行安全评估，分析数据安全风险和对数据主体权益影响，评估数据处理的必要性、合规性及防控措施的有效性；收集数据应坚持“合法、正当、必要、诚信”原则，明确数据收集和处理的目的、方式、范围、规则，保障收集过程的数据安全性、数据来源可追溯；在数据集团内部共享的过程中，应建立总行（公司）与其子公司数据安全隔离的“防火墙”，并对共享数据采取有效保护措施；《办法》还对数据加工、委托处理、共同处理、数据转移、数据跨境等具体的数据处理场景分别提出了相应安全管理要求。

五、《办法》在个人信息保护方面有哪些规定？

答：《办法》单独设置“个人信息保护”章节，以进一步落实《数据安全法》《个人信息保护法》等上位法要求，体现保护消费者信息和权益的政策导向。主要规定包括：银行保险机构处理个人信息应按照“明确告知、授权同意”的原则实施，并限于实现金融业务处理目的的最小范围，不得过度收集个人信息。处理、共享和对外提供个人信息时，应当履行必要的告知义务，并取得必要同意。不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务，处理个人信息属于提供产品或者服务所必需的除外。在开展涉及对个

人权益有重大影响的个人信息处理活动时，应当进行个人信息保护影响评估。委托第三方处理个人信息时，应明确受托人对个人信息的保护义务、保护措施和期限等。发生或者可能发生个人信息泄露、篡改、丢失的，银行保险机构应当立即采取补救措施，并向监管部门报告。

六、《办法》规定的数据安全事件应急响应与处置机制包含哪些内容？

答：《办法》将数据安全事件根据影响范围和程度，分为特别重大、重大、较大和一般四个级别。要求机构建立内部协调联动机制和外部服务商、第三方机构的报告机制。具体包括：一是制定数据安全事件应急预案，定期开展应急响应培训和应急演练。二是数据安全事件发生后，立即启动应急处置，分析事件原因、评估事件影响、开展事件定级，按照预案及时采取业务、技术等措施控制事态。三是建立数据安全事件报告机制，根据事件安全等级制定报告流程，发生数据安全事件时按照规定报告，同时按照合同、协议等有关约定履行客户及合作方告知义务。四是发生数据安全事件或者使用的产品和服务存在缺陷时，立即开展调查评估，及时采取补救措施。

银行保险机构应在数据安全事件发生 2 小时内向总局或其派出机构报告，并在事件发生后 24 小时内提交正式书面报告。发生特别重大数据安全事件，银行保险机构应当立即采取处置措施，按照规定及时告知用户并向属地公安机关、金融监管机构报告。银行保险机构应当每 2 小时将处置进展情况上报，直至处置结束。数据安全事件处置结束后，银行保险机构应当在五个工作日内将事件及其处置的评估、总结和改进报告报送属地监管部门。

七、《办法》公开征求意见情况如何？

答：《办法》起草过程中已广泛征求了有关部门及各类银行保险机构意见，并组织部分机构召开专题会议现场听取意见建议。2024 年 3 月至 4 月，总局就《办法》面向社会公开征求意见。各方反馈的相关合理化意见建议均被采纳，未采纳意见主要集中在数据审计周期、监管报送时限等方面。

迎接《银行保险机构数据安全管理办法》，金融机构做好准备了吗?

张善奋　上海功承瀛泰律师事务所

适逢2024年底，金融监管局重磅发布金规〔2024〕24号《银行保险机构数据安全管理办法》（以下简称“《办法》”）。众所周知，金融行业是一个强监管行业。强监管之下，若无明确或严格的监管要求，金融机构可能怠于提高合规标准。截至目前，金融监管部门并未就金融机构数据安全管理单独出台统一性的部门规章或规范性文件，也未对金融机构在数据安全管理采取严格措施，更多的是点到为止。数据安全管理，从2025年开始，是否会成为下一个金融消保，成为金融监管和检查的重点领域，犹未可知。

本文中，笔者将谈谈自己对《办法》部分内容的理解，并提出一些建议供大家参考，以便金融机构管理层了解监管新要求，并考虑是否需要在2025年及后续几年的工作计划或预算中做一些安排，以迎接可能的监管新趋势。

一、关于数据安全治理体系和现行治理结构的融合

金融机构应考虑梳理和调整现有组织架构和部门/岗位职责分工，以期符合数据安全治理体系新要求。

《办法》要求建立四级数据安全管理组织架构，从党委、董事会、高管层到职能部门，明确各自的职责，但是具体落地时，仍有很多问题需要金融机构自行考虑。例如：

1. 《办法》要求明确党委和董事会对本单位数据安全工作负主体责任。为落实该要求，笔者建议将数据安全工作纳入三重一大审议事项。但并非一概而论，金融机构需要评估哪些事项需要提交三重一大审议，并考虑适当的审议和表决的机制。未被纳入三重一大审议范围的，则需要考虑哪些交给高级管理层来决策，哪些交给专属职能部门来决策。

2. 《办法》要求，高管层中，金融机构主要负责人为数据安全第一责任人，分管数据安全的高级管理人员为直接责任人，但同时要求将数据安全管理纳入金融机构全面风险管理工作体系。在很多金融机构中，分管风险的和分管信息安全的高管一般不是同一个人，因为这两类岗位在专业要求上有一些区别。全面风险管理体系一般在风险条线管理，数据（含网络）安全在CTO/首席数据官的管辖下，如何将两条管理线下的工作有机协同起来，是需要金融机构在调整组织架构和职能分工时考虑的问题。

3. 职能部门层面，《办法》要求要指定数据安全归口管理部门、数据安全技术保护主责部门，并要求风险管理将数据安全纳入全面风险管理体系、内控合规将数据安全纳入内控评价体系、审计部门负责数据安全的定期审计工作等。但是，实际执行中就存在很多要解决的职能边界问题。数据安全管理是离不开技术的，风险管理部如果要实质上管理数据安全风险，就必须借助技术部门能力，而这可能与数据安全归口管理部门职能边界存在冲突或重叠，实践中风险管理部是否就沦为全面风险管理报告的收集汇总方，也未可知。

二、关于数据安全制度建设和现行制度体系的衔接

金融机构应盘点现有制度体系，查漏补缺，做好已有制度体系与新增数据安全制度体系的衔接，完善金融机构内部制度建设工作。

《办法》从建立数据安全治理体系、分类分级管理、数据安全管理、个人信息保护、风险监测处置等几方面对金融机构的相关工作提出要求，其中包括了大量的制度建设要求。

结合《办法》的要求，笔者建议，金融机构至少需要就以下这些内容制定或完善相关制度：

序号	制度类型	需增加或调整的制度内容
1	数据安全治理体系	数据安全文化建设
2		三重一大制度
3		章程（董事会和高管层职权中可能存在调整的需要）
4		高管及相关部门考核办法或标准
5	数据分类分级保护	数据目录和分类分级规范
6		数据分类分级动态管理和维护数据目录，数据安全级别的时效管理，动态调整审批机制
7		差异化安全保护措施
8	数据安全管理	数据安全保护策略
9		数据安全管理责任分工
10		数据处理全生命周期管控机制
11		数据共享管理实施细则
12		数据出境管理实施细则
13		数据资产登记管理制度
14		数据服务规范
15		数据合规管理制度
16		外部数据采购、合作引入的集中审批管理制度
17		数据授权、访问及提取管理机制
18		数据委托处理管理制度
19		数据供应商的准入和安全管理
20		数据共同处理的管理制度
21		数据转移的管理制度
22		数据对外公开披露的管理制度
23		数据备份制度
24		数据销毁制度

25	数据安全技术	数据安全技术架构和保护控制基线
26		数据保护策略方法
27		数据安全技术标准规范
28		将数据安全保护纳入信息系统开发生命周期框架
29		将数据纳入网络安全等级保护
30		数据操作日志管理
31		数据存储、传输、删除/销毁等技术措施
32		数据容灾备份制度
33		开发测试投产管理
34		人工智能模型管理制度
35		数据安全应急管理机制
36		数据安全风险隔离机制
37	个人信息保护	个人合法权益保障机制
38		个人信息保护影响评估
39		个人信息出境管理
40		个人信息委托处理管理
41		个人信息安全事件应急管理
42	数据安全风险监测与处置	全面风险管理制度（将数据安全风险纳入）
43		内控评价制度（将数据安全风险纳入）
44		数据安全威胁检测机制
45		审计制度（将数据安全审计机制纳入）
46		数据安全风险评估机制
47		数据安全事件应急管理机制

在数据安全制度体系完善过程中，建议以现有制度为基础，例如如果现有制度中已经对供应商管理做出了规定，那么结合本次《办法》中有关数据方面的供应商管理要求，可做扩充或细化，并不一定需要另行制定新制度。

三、关于个人信息保护与金融消保相关要求的衔接

《办法》中的个人信息保护要求与金融消保相关要求具有一致性，建议金融机构融合两套监管要求，消保部门亦可借数安管理体系的推进完善消保工作，事半功倍。

《办法》第六章对个人信息保护做了专章要求，其中部分要求与《银行保险机构消费者权益保护管理办法》第六章“保护消费者信息安全权”具有一致性。如下图：

《办法》 第六章个人信息保护	《银行保险机构消费者权益保护管理办法》 第六章“保护消费者信息安全权”
第五十四条 银行保险机构处理个人信息应当按照“明确告知、授权同意”的原则实施，法律、行政法规另有规定的除外，并在信息系统中实现相关功能控制。	第四十三条 银行保险机构收集消费者个人信息应当向消费者告知收集使用的目的、方式和范围等规则，并经消费者同意，法律法规另有规定的除外。消费者不同意的，银行保险机构不得因此拒绝提供不依赖于其所拒绝授权信息的金融产品或服务。 银行保险机构不得采取变相强制、违规购买等不正当方式收集使用消费者个人信息。
第五十五条 银行保险机构处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，收集个人信息应当限于实现金融业务处理目的的最小范围，不得过度收集个人信息。不得利用所收集的个人信息从事违法违规活动。	第四十七条 银行保险机构处理和使用个人信息的业务和信息系统，遵循权责对应、最小必要原则设置访问、操作权限，落实授权审批流程，实现异常操作行为的有效监控和干预。
第五十六条 银行保险机构处理个人信息前，应当真实、准确、完整地向个人告知其个人信息的处理目的、处理方式、处理的个人信息种类、保存期限，个人行使其信息权利的申请受理和处理程序，以及法律法规规定应	第四十四条 对于使用书面形式征求个人信息处理同意的，银行保险机构应当以醒目的方式、清晰易懂的语言明示与消费者存在重大利害关系的内容。 银行保险机构通过线上渠道使用格式条款获取个人信息授权的，不得设置默认同

当告知的其他事项。 银行保险机构应当制定个人信息处理规则，个人信息处理规则应当公开展示、易于访问、内容明确、清晰易懂。	意的选项。
第五十七条 银行保险机构不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务，处理个人信息属于提供产品或者服务所必需的除外。	第四十三条 ……消费者不同意的，银行保险机构不得因此拒绝提供不依赖于其所拒绝授权信息的金融产品或服务。 银行保险机构不得采取变相强制、违规购买等不正当方式收集使用消费者个人信息。
第五十八条 银行保险机构在开展涉及对个人权益有重大影响的个人信息处理活动时，应当进行个人信息保护影响评估，评估内容包括个人信息处理的合法性、必要性，对个人权益的影响及安全风险，所采取的保护措施合法性、有效性以及是否与风险程度相适应。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。	
第五十九条 银行保险机构与其母行、集团，或者其子行、子公司共享个人信息，及向外部提供个人信息，应当履行向个人告知及取得其同意等相关事项的义务。	第四十五条 银行保险机构应当在消费者授权同意等基础上与合作方处理消费者个人信息，在合作协议中应当约定数据保护责任、保密义务、违约责任、合同终止和突发情况下的处置条款。 合作过程中，银行保险机构应当严格控制合作方行为与权限，通过加密传输、安全隔离、权限管控、监测报警、去标识化等方式，防范数据滥用或者泄露风险。
第六十条 银行保险机构向中华人民共和国境外提供个人信息的，除满足第三十六条、第五十九条规定的要求外，还应当向个人告知其向境外接收方行使信息权利的方式和程序等事	

项，法律、行政法规另有规定的除外。	
第六十一条 银行保险机构委托第三方处理个人信息的，应当在合同或者协议条款内明确受托人对个人信息的保护义务、保护措施和期限等，并严格监督受托人以约定的处理目的、处理方式等处理个人信息，与第三方传输个人敏感数据必须确保安全，防范数据滥用和泄漏风险。未经银行保险机构同意，受托人不得转委托他人处理个人信息。	第四十六条 银行保险机构应当督促和规范与其合作的互联网平台企业有效保护消费者个人信息，未经消费者同意，不得在不同平台间传递消费者个人信息，法律法规另有规定的除外。
第六十二条 银行保险机构在算法设计、训练数据选择和模型生成时，应当采取有效措施，保障个人合法权益。利用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。	
第六十三条 发生或者可能发生个人信息泄露、篡改、丢失的，银行保险机构应当立即采取补救措施，同时通知个人并报送国家金融监督管理总局或者其派出机构。通知应当包括下列事项： （一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害； （二）银行保险机构采取的补救措施和个人可以采取的减轻危害的措施。 银行保险机构采取措施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；监管部门认为可能造成危害的，有权要求银行保险机构通知个人。	第五十条 银行保险机构发生涉及消费者权益问题的重大事件，应当根据属地监管原则，及时向银保监会或其派出机构消费者权益保护部门报告。

四、关于个人信息保护保护影响评估

《办法》还增加了个人信息保护影响评估（以下简称 PIA）等要求，这些要求在既往消保相关管理要求中并未明确。笔者记忆中，这是金融监管局的部门规章及规范性文件中首次提出 PIA 的要求。

现实中，金融机构在纸质合规层面已经做了不少工作，例如将 PIA 纳入了内部制度中，或写入了与合作方的法律文件中。但是实质合规层面，PIA 报告可能未被真正落实。本次《办法》更是要求，在“开展涉及对个人权益有重大影响的个人信息处理活动时”就要做 PIA。这一要求说明，首先，PIA 不是一份定期的年度总结报告，也不是一份一次性报告，而是一项根据个人信息处理活动发生而触发的工作。其次，金融机构需要有一套配套机制，要明确何为“对个人权益有重大影响”的标准，以及达到标准后的运作机制、审批机制、操作机制和资源配备等，包括谁来做 PIA、需要的成本和人力等。

五、关于数据安全审计与个人信息保护合规审计

本次《办法》中多次提到要将数据安全纳入金融机构的审计，审计内容包括但不限于数据权限的管理、数据访问行为、数据处理活动、数据操作行为和日志等。金融机构常设有信息系统审计等项目，这次《办法》提到的数据安全审计，从内容上来看更像是在原有信息系统等传统审计项目的基础上进行了扩充。

《办法》全篇没有提到个人信息保护合规审计。作为一项《个人信息保护法》规定的法定义务，理应也成为金融机构的法定义务之一。但是本次《办法》并未提到这一点，不免让人疑惑，是金融机构不需要做个人信息保护合规审计，还是金融监管局另有文件再跟进相关要求呢？尚不得而知。

笔者个人认为，本次《办法》所提到的数据安全审计，并不等同于法律规定的个人信息保护合规审计，两者是相对独立的审计项目。数据安全审计，源自金融监管的要求，更侧重在网络和数据安全性层面，与传统的信息系统/IT 审计一脉相承，这也许是和本次办文部门是科技监管司有关。而个人信息保护合规审计，源自法律义务，更侧重于个人信息保护的合规性审查。[1]数据安全审计，并不能代替个人信息保护合规审计。即便本次《办法》并未提到个人信息

保护合规审计，但是笔者认为，金融机构依然需要建立个人信息保护合规审计机制。

六、结语

纵观本次《办法》的全篇内容，作为金融监管局出台的第一份独立的、有关金融数据安全管理方面的监管文件，笔者认为这份文件对规范银行保险业数据处理活动，保障数据安全、金融安全，促进数据合理开发利用，维护社会公共利益和金融消费者合法权益，有着重要的意义。虽然金融机构落地这些要求还需要一点时间，还需要一些调整和资源，但是监管释放的明确态度，有利于金融机构管理层重视数据安全及合规工作，从而有利于内部有关部门推进数据安全及合规工作的开展。

注释

[1] 关于个人信息保护合规审计的具体内容，请查看作者其他文章：《从金融机构角度 谈个人信息保护合规内审机制的搭建（一）》。

上海律协企业合规专业委员会

主　任：

杨伟东 （上海格联律师事务所）

副主任：

李嘉杰（北京市环球律师事务所上海分所）

吴　瑛（上海市汇业律师事务所）

赵何璇（上海市方达律师事务所）

委　员：

陈　兵 陈　敏 仇如愚 陈松竹 丁　亮 董　野 丁志龙 冯　欣 顾丽萍 郭青红 高睿静 葛　舒 葛文昱 胡文兵 胡晓光 江秋杰 蒋　霞 孔　丽 李　擘 刘　畅 陆春晨 刘宏悦 吕晋 李　响 李心军 刘秀丽 林　媛 乔　骄 全开明 钱　莉 盛琬刚 史昭君 田　原 王东升 万海军 王黎君 王　森 王　璇 谢凌云 谢佩之 薛雯雯 邢芝凡 殷慧娟 袁开宇 杨利涛 尹庆 杨　薇 杨晓蓉 张　斌 张　涵 周　航 赵海英 赵嘉炜 张善奋 朱永红

秘书：王英卜