银行保险机构数据安全管理办法

（公开征求意见稿）

第一章　总　则

第一条　（立法目的及依据）

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　（适用范围）

在中华人民共和国境内设立的开发性金融机构、政策性银行、商业银行、农村合作银行、农村信用社，保险集团（控股）公司、保险公司、保险资产管理公司、金融资产管理公司、信托公司、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、理财公司适用本办法。

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。

第三条 （术语定义）

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 （数据安全监管）

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 （数据安全管理体系）

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 （保护原则与目标）

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、金融安全、公共利益，不得损害个人、组织的合法权益。

第七条 （数据开发利用）

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 （持续提升）

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 （数据安全治理架构）

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 （数据安全责任制）

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，

分管数据安全的领导为直接责任人，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　（数据安全归口管理部门）

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　（业务部门）

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　（风险合规与审计部门）

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　（数据安全技术保护部门）

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，防范外部攻击行为。

（五）组织数据安全技术研究与应用。

第十五条　（数据安全文化建设）

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　（总体要求）

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　（数据分类）

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　（数据分级）

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。

除以上数据之外的数据为其他一般数据。

第十九条　（动态调整）

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　（管理体系）

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　（数据资产管理）

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　（数据安全评估）

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　（数据服务管理）

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　（数据收集）

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　（数据收集）

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　（外部数据采购）

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　（数据加工）

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　（数据使用）

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　（数据共享及集团内部共享）

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　（数据委托处理）

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　（外包管理）

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。

第三十二条　（数据共同处理）

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　（数据转移）

银行保险机构因兼并、重组、破产等需要转移数据，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　（数据转移）

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　（数据公开）

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、行政法规另有规定的或者取得数据主体授权同意的除外。

第三十六条　（数据跨境）

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　（数据备份）

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　（数据删除与销毁）

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中止时，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　（数据安全技术保护体系）

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　（信息系统生命周期的数据安全）

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　（网络安全与数据安全保护）

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　（数据安全保护基线-信息系统保护）

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　（数据安全保护基线-数据访问控制）

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3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1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3年。应当定期对数据操作行为进行审计，审计周期不超过6个月。

第四十四条　（数据安全保护基线-数据传输保护）

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　（数据安全保护基线-数据存储保护）

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　（数据安全保护基线-数据销毁管理）

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　（数据安全基础设施）

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　（数据安全测试）

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　（大数据平台安全）

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　（数据加工）

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　（数据加工）

银行保险机构信息系统、模型算法投入使用时，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　（数据加工）

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　（外部交互数据安全）

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　（处理原则）

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　（处理原则）

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　（告知义务）

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　（告知义务）

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　（影响评估）

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　（共享和外部提供）

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　（跨境传输）

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　（委托处理）

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　（自动化决策）

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　（个人信息风险报告）

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　（数据安全风险管理机制）

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　（风险监测）

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　（风险评估与审计）

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　（数据安全事件分级）

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　（应急响应与处置）

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　（事件监管报告）

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。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　（监管方式）

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　（数据目录管理）

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　（行业监测预警）

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　（机构报告）

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　（机构报告）

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　（现场检查与事件处置）

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　（监管措施与法律责任）

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　（监管措施与法律责任）

银行业金融机构违反本办法要求的，国家金融监

督管理总局或者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可以依据《中华人民共和国保险法》相关规定，责令保险机构改正，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　（行业协会职责）

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　（解释和修订）

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　（参照执行）

国家金融监督管理总局批准设立的外国银行分行、其他金融机构、金融控股公司以及总局管理单位参照适用本办法。地方金融监督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　（生效日期）

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

附件

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。