汉坤法律评述

2024 年 3 月 26 日

HANKUN
汉坤律师事务所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港 | 海口 | 武汉 | 新加坡 | 纽约

《银行保险机构数据安全管理办法（征求意见稿）》要点分析

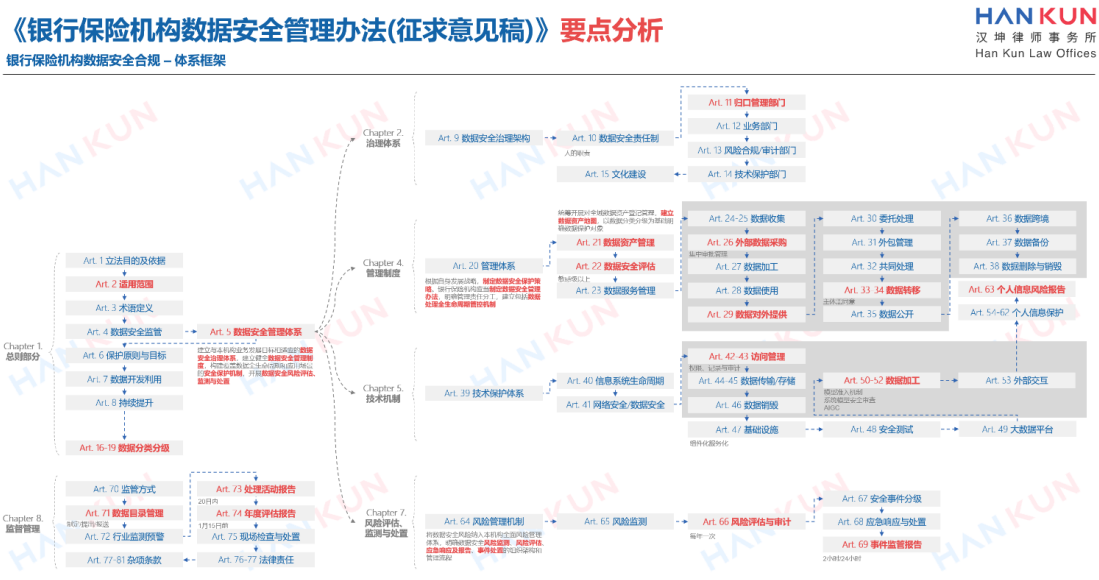
作者：权威 | 李珣 | 夏迎雨 | 李烨 | 洪松

一、新规出台的背景和影响

2024 年 3 月 22 日，《银行保险机构数据安全管理办法》（以下简称“**《银保数安办法》**”）公开征求意见。

作为国家金融监督管理总局（以下简称“**金融监管总局**”）成立后的第一部数据安全立法，《银保数安办法》一方面与《数据安全法》、《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》等数据安全领域的框架性、纲领性文件相衔接，体现了“金融等主管部门承担本行业、本领域数据安全监管职责”的上位要求；另一方面，相较于人民银行于 2023 年 7 月征求意见的《中国人民银行业务领域数据安全管理办法（征求意见稿）》（以下简称“**《人行数安办法》**”），《银保数安办法》亦体现出监管要求及监管方式上的差异性。

整体而言，**《银保数安办法》采取了“主体监管”的监管方式，对于金融监管总局管辖的所有类型金融机构，采取统一的监管标准**。在内容上，《银保数安办法》共八十一条，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、监督管理及附则九个章节，从治理体系、管理制度、技术机制以及风险评估、监测与处置机制等方面进行了系统规范，《银保数安办法》的体系框架可如下图所示：



《银保数安办法》出台的核心意义在于确立了银行保险机构数据安全工作的监管逻辑，但目前的征求意见版本尚有较多细节有待完善。例如在体系上，仍有一定的“技术标准”的痕迹；在术语体系上，仍使用了“提供”、“共享”等近意术语，“企业级”、“闭环”、“多源异构”等语义不够明确的表述，可能会增加实务工作落地的难度，此外还多处使用了“归口”、“主责”、“领导班子”、“宣贯”等在正式立法文件中少见的日常用词，希望在正式稿中可以进一步完善。

二、新规适用的范围和主体

在适用范围和主体上，《银保数安办法》从“两个维度”提出了“全口径”监管要求。

从主体维度上，《银保数安办法》的适用范围包含了开发性金融机构、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；此外，金融监管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、总局管理单位，以及地方金融监管部门批准设立的金融组织亦需参照适用。

可以说，《银保数安办法》在主体监管上采用了“全口径”的监管要求，其直接适用的主体包含了所有银行保险机构及非银行金融机构，且金融监管总局监管的其他金融机构（包括金控公司和地方金融组织）亦全部被兜底纳入“参照适用”的范畴。

从行为维度上，前述机构开展的所有数据处理行为，除涉及国家秘密外，均需要适用《银保数安办法》，即《银保数安办法》在行为监管上亦采用了“全口径”的监管要求。

我们认为，该等“全口径”监管要求从对齐标准、压实责任，避免监管死角和监管套利的角度自然有其积极意义，但考虑到市场实践情况，亦会给部分金融机构带来一定挑战，具体而言：

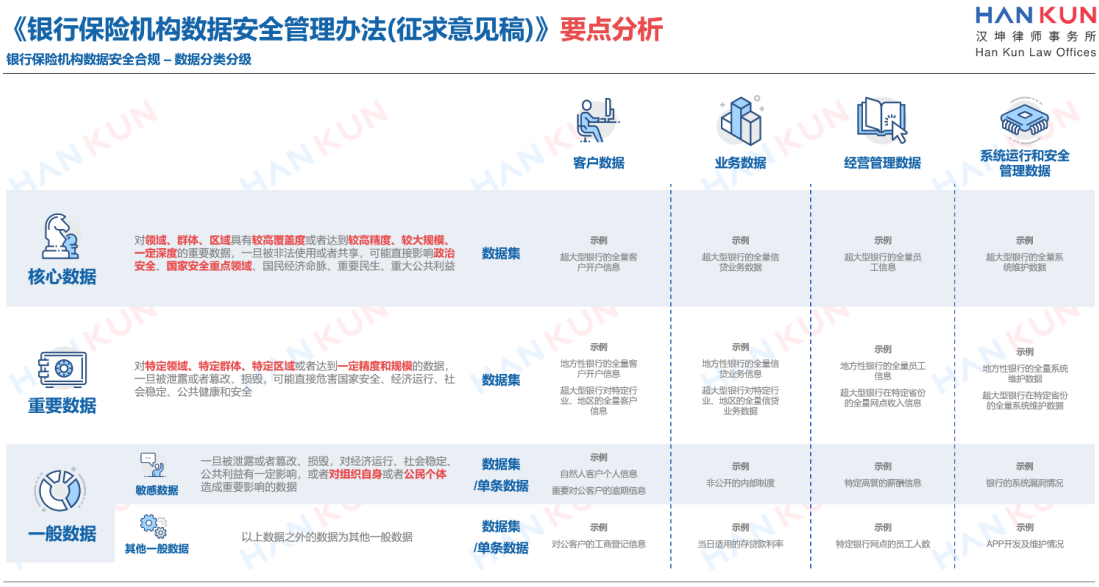
- **机构技术实力存在固有差异**。目前，不同类型金融机构的数据安全管理能力、技术保护能力实际差异较大，《银保数安办法》要求将所有非银行金融机构乃至地方金融组织的监管标准与大型银行、关键信息基础设施运营者拉齐，这可能给中小金融机构的数据安全管理工作带来挑战或造成额外的运营负担；
- **特定数据处理合规要求提升**。《银保数安办法》在较大程度上将针对企业的数据处理活动与针对个人信息的数据处理活动的监管要求拉齐，例如，《银保数安办法》对于不涉及个人信息的敏感级以上数据对外提供行为亦提出了较为严格的授权同意要求，这可能给金融机构带来较大的整改难度，取得同意可能存在困难；
- **与人行规定需要衔接适配**。由于《人行数安办法》亦采取了“行为监管”的监管方式，对于银行金融机构而言，可能面临双重监管的压力，例如，银行金融机构的支付业务、反洗钱业务可能既要执行《人行数安办法》的要求，也要执行《银保数安办法》的要求。由于二者的数据分类分级及合规要求不尽相同，可能会导致机构承担繁重的合规压力。

三、数据分类分级

从数据分类分级角度，**《银保数安办法》规定应当分类管理的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**，该分类方式与《人行数安办法》较为类似，没有实质差异。

在数据分级上，《银保数安办法》则提出了**全新的“三级+细分”分级方式**，与《人行数安办法》的“三

级五层”分级方式存在较大区别，具体而言，《银保数安办法》根据数据的重要性和敏感程度，将数据分为核心数据、重要数据和一般数据，一般数据又细分为敏感数据和其他一般数据，《银保数安办法》项下的数据分类分级方式及相关示例可如下图所示：



《银保数安办法》的分级方式是一个新提法，与人民银行数据监管及国标/行标中的分级方式均存在不同。由于不同级别的数据需要采取差异化和针对性的安全保护措施，实践中的难点在于，对于同一种金融活动（例如银行的反洗钱活动），如果同时适用《人行数安办法》和《银保数安办法》，该以何种分类标准为准进行分类，还是需要分别适用两套分类标准，有必要在金融监管总局和人民银行的后续立法中进行统一和完善。

此外特别值得说明的是，《银保数安办法》目前的版本中依然没能明确“核心数据”和“重要数据”具体的确定机制，仅规定“由金融监管总局制定银行业保险业重要数据目录，银行保险机构在建立自身数据目录及分类分级规范并动态维护的基础上，向金融监管总局或其派出机构报送重要数据目录并在发生重大变化时更新报备。”

根据该逻辑，金融监管总局对于机构上报的目录并无确认或批复的义务，这可能会导致市场主体在进行自身的核心数据、重要数据认定时，都尽可能按照“限缩”范围进行认定，从而尽可能降低自身的合规义务。

四、公司治理

作为《银保数安办法》为金融机构设定的四大核心义务群中的第一项，在治理体系方面，《银保数安办法》在第二章做了专章规定。

较之上位法，《银保数安办法》提出了更为明确的细化要求，要求银行保险机构在机构内部建立涵盖董事会、高管层在内的多层级治理架构，将数据安全归口管理部门、业务部门、风险合规与审计部门、数据安全技术保护部门等部门均纳入到数据安全的治理工作中，并通过建立数据安全责任制压实各层级的数据安全责任，形成“党委（党组）、董（理）事会、高管层领导，数据安全归口管理部门统筹、其他业务部门和职能部门参与执行”的数据安全治理分工。

对于承担统筹管理职能的“归口管理部门”，《银保数安办法》并未强制要求该部门需为独立、专职的

内设部门，亦未强制性指定科技部门、法律合规部门或风控部门牵头相关工作，为银行保险机构的内部管理保留了一定的灵活性，机构可根据实际的内部管理需要确定具体的归口管理部门。

值得关注的是，《银保数安办法》在对业务部门义务的认定上，参照了此前《人行数安办法》首次提出的**“谁管业务、谁管业务数据、谁管数据安全”**的思路和表述，明确开展数据处理活动的具体业务部门应当对相关活动涉及的数据履行数据安全保护义务，而非由技术或风控部门统一归口负责，将会有效降低实践中因各部门间相互推诿而出现责任盲区的潜在风险，体现了近年来结果导向的监管思路。

五、安全管理

在管理措施方面，《银保数安办法》建立了以**“建立数据资产地图”**和**“开展数据安全评估”**为核心抓手的合规思路，并针对包括内部收集、外部采购、加工、使用、对外提供、跨境提供、备份、删除与销毁在内的数据处理全生命周期设置了合规要求。银行保险机构应当据此制定数据安全保护策略和制度，并应当涵盖全生命周期管控机制、数据安全保护措施、数据对外提供和跨境提供等监管重点关注内容。

具体而言，《银保数安办法》第 21 条要求银行保险机构开展“对全域数据资产的登记管理，建立数据资产地图”。该项梳理工作可作为银行保险机构开展数据安全合规工作的起点和重点，在具体实施上建议与内部的数据分类分级工作同步开展。

在此基础上，《银保数安办法》针对银行保险机构**引入了“数据安全评估”这一全新机制**，针对敏感级及以上数据的业务活动和对数据主体有较大影响的业务活动提出了事前评估的合规要求。考虑到数据安全评估的适用客体、触发条件与评估范围等要点与《个人信息保护法》（以下简称“**《个保法》**”）个人信息保护影响评估存在较多相似之处，针对因处理个人信息而触发的“数据安全评估”（因其可能构成“敏感级数据”），应允许两项评估合并为一项工作内容。

针对数据处理的全生命周期管控，**《银保数安办法》借鉴了大量个人信息保护领域的合规思路，并直接复用于数据处理活动**，在实操性和可行性方面可能会存在一定的挑战。例如，《银保数安办法》要求银行保险机构制定外部数据采购、合作引入的集中审批管理制度，实施严格的数据访问授权管理，将数据对外提供规则与现有个人信息对外提供规则基本对齐，均与目前行业数据处理活动的合规水位存在较大偏差。如相关规定最终生效，如何在不影响存量展业活动的情况下完成合规整改工作，值得相关市场主体重点关注。此外，《银保数安办法》还多处提及“可追溯”的要求，包括“数据来源可追溯”、“数据转移过程可追溯”、“模型算法可追溯”，可能进一步压实机构的合规责任。

在个人信息保护方面，《银保数安办法》主要重申了《个保法》的相关内容，包括告知同意原则、目的限制原则等工作原则和影响评估、对外提供、跨境提供、委托处理、自动化决策、个人信息风险报告等合规要求，并未实质性改变或加重银行保险机构的合规义务。

但值得关注的是，《银保数安办法》第 63 条为银行保险机构设定了“个人信息风险报告”的相关制度，要求机构在出现个人信息相关的风险事件时需要向金融监管总局报告。该项要求沿袭了《个保法》第 57 条的相关要求，一定程度上明确了金融监管总局亦构成《个保法》下的“履行个人信息保护职责的部门”。

六、技术保护

在技术保护措施方面，《银保数安办法》主要提出几项原则性的规定，包括建立数据安全技术保护体系和数据安全保护基线，将数据安全保护纳入信息系统开发生命周期框架，以及将数据纳入网络安全等级保护等，并对于数据安全日常工作提出了指导要求。

值得关注的是，针对敏感级及以上数据，《银保数安办法》提出了“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”的要求，意味着对于该等数据的保护措施需要与信息系统高度匹配，对于银行保险机构后续上线新系统提出了进一步的要求。

技术保护措施的另一关注重点在于首次从监管规范层面提出了“数据安全保护基线”这一概念。安全基线作为网络安全领域的技术概念，是指能够保护数据安全与隐私的最低标准和措施。《银保数安办法》针对机构信息系统保护、数据访问控制、数据传输和存储保护、数据销毁管理所设定的基线要求，均应当视为监管部门对银行保险机构数据安全保护工作的底线要求。

此外，针对模型以及人工智能的使用，《银保数安办法》也创新性地设置了“准入机制”等合规要求，对于银行保险机构使用当前较为受关注的金融科技技术提出了新的内控要求。

七、风险监测处置与监督管理

在风险监测与处置方面，《银保数安办法》要求将数据安全风险纳入银行保险机构现有的风险管理体系，定期开展数据安全风险评估（每年一次）和数据安全审计（每三年一次），并划分为事前监测评估、事中处置和事后报告三个阶段，明确机构在各阶段的合规义务。

风险监测与处置的主要合规难点在于持续监测数据安全威胁和数据安全事件分级。一方面，由于《银保数安办法》对“数据安全威胁”的范围界定较为宽泛，将异常访问数据、数据泄露等安全技术问题和客户投诉、负面舆情等公共事务问题均纳入其中，可能导致银行保险机构的技术部门和公共事务部门需共同参与持续监测工作，或需要通过重新划分现有部门职能、建立部际联席工作机制等方式以确保全面覆盖前述问题。

此外，还需要特别关注事后监管报告的时限要求，包括一般数据安全事件发生后 2 小时内的非正式报告、24 小时内的正式书面报告、5 个工作日内的事件处置报告，以及针对特别重大数据安全事件每隔 2 小时定时上报的要求，均需要对于现有应急响应方案和人员部署进行重新梳理。

在监管方面，除常规的监管方式、监管措施及法律责任外，银行保险机构还应当重点关注机构报告义务的变化。根据《银保数安办法》规定，银行保险机构除需要**每年定期报送上一年度数据安全风险评估报告**外，还需要**事先就涉及批量敏感级及以上数据的数据处理活动向监管部门报告**。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

权威

电话： +86 21 6080 0946
Email： wei.quan@hankunlaw.com

李珣

电话： +86 21 6080 0232
Email： xun.li@hankunlaw.com