# 对于银保数安办法草案(征求意见稿)的修改建议

作者：潘永建 | 王祎 | 朱晓阳 | 牛映辉 | 左嘉玮

2024 年 3 月 22 日，国家金融监督管理总局发布了《银行保险机构数据安全管理办法(公开征求意见稿)》(以下简称“《办法》”)，该文件是国家金融监督管理总局于 2023 年 5 月成立后发布的第一部安全领域的行业管理办法，旨在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。国家金融监督管理总局面向社会公众征集对于《办法》的修改意见，反馈期限已于 2024 年 4 月 23 日截止。

通力大合规业务团队与保险业务团队一道，共同研读《办法》，结合各自团队在数据合规和银行保险业务领域的经验，选择了《办法》中的重点条款，以逐条分析的方式提供了解读和修改建议。相关修改意见已经发送国家金融监督管理总局，也供银行保险领域的企业参考《办法》生效后的数据安全合规思路。

## 一. 总则

### 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。

**解读与建议**

《办法》采取“全口径监管”的适用范围——涉及 16 类银行机构、保险机构及非银保金融机构，以及 2 类 5 项参照执行机构。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

一方面，鉴于“全口径监管”所涉机构数量众多、范围广大，而各机构在规模、业务性质、数据管理能力、资源配备等方面均存在程度不等的差异，如一次性将所有相关机构的管理要求提高至同一水平，在实践中可能将造成监管与被监管方的双重压力。

我们注意到，近期发布的《商业银行资本管理办法》(“《资本新规》”)已根据商业银行的业务规模、风险差异将其划分为三档层级，配以差异化的监管与评估原则，并为特定项目提供了过渡方案。此外，原银保监会等部门 2018 年发布的《关于规范金融机构资产管理业务的指导意见》(“《资管新规》”)同样曾规定过渡期，并在近年实践中得到了落实。

我们建议，可以考虑在立法层面参考《资本新规》对商业银行的分级监管举措，对《办法》所规制的银保机构探索分类分级管理，例如，可以考虑机构的展业区域(全国或地方性)、规模(大中小)、业务性质(领域类型，如银行、保险、资管、金融等；流通场景，如是否需要跨境、行业内流通、集团内共享等)，设定不同的管理要求。而在执法监管层面，我们建议可综合考虑各机构的能力资源差距、新设制度的实施难易程度等因素，为《办法》的落地预留合理的缓冲期，为各类银保机构预留适当升级管理资源、精进管理能力的时间。

另一方面，鉴于央行此前发布《中国人民银行业务领域数据安全管理办法(征求意见稿)》(“《央行数安办法草案》”)旨在规制“数据处理者在中华人民共和国境内开展的中国人民银行业务领域数据相关的处理活动”，但尚未明确具体地划分判断标准，导致与本《办法》所规制银保机构的相关数据处理活动在范围上或有部分重合，例如，商业银行为反洗钱业务开展的数据处理活动就可能同时涉及央行业务领域数据。考虑到两部拟定办法效力层级相近，如后续《央行数安办法草案》正式出台实施，在实务中可能造成与《办法》的交叉监管问题。

我们建议，为更好地提高各方理解、落实新规的效率，可以考虑在立法或执法层面明确与央行监管范围之间的关系或边界，例如，一方面，可参考《央行数安办法草案》第 4 条第一款关于协同监督管理的规定，在立法层面增加协同监督管理机制条款；另一方面，可以考虑梳理总结可能同时涉及央行业务领域数据的典型场景，并为此类交叉范围提供法律理解与适用方面的指引。

附：《央行数安办法草案》第 4 条第一款
“在国家数据安全工作协调机制统筹协调下，中国人民银行及其分支机构，依据本办法开展数据安全监督管理工作，积极支持其他有关主管部门依据职责开展数据安全监督管理工作,必要时可以与其他有关主管部门签署合作协议，进一步约定数据安全监督管理协作模式。”

**第三条 术语定义**

……

**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。
……

**解读与建议**

《办法》第 3 条在法规层面新创“数据主体”概念，其范围除自然人外，还涵盖自然人的监护人、企业、机关、事业单位、社会团体和其他组织。我们理解该定义应该系参照“个人信息主体”创设，或许旨在强化银保机构的数据保护义务，从而全面提升金融领域的数据安全治理水平。

一方面，现有“个人信息”概念明确指可以识别到个人的信息，但拓展至其他类型的“数据”却不一定都能够识别或关联(“标识”)企业、事业单位、社会团队等其他主体。

另一方面，目前数据如何进行确权也尚未在法律层面得到明确规定，《办法》如在该领域法律空白期出台实施，可能会引发实践中认定“数据主体”的混乱。

我们建议，可以适当斟酌“数据主体”的现有定义是否完整、准确，以及是否确有必要在银保金融领域率先创设这一定义。

**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。

**解读与建议**

《办法》第 5 条、第 66 条和第 74 条提到了“数据安全风险评估”，在第 11 条、第 22 条、第 74 条又提到了“数据安全评估”。

一方面，《办法》现阶段对“数据安全风险评估”与“数据安全评估”的相应描述偏向原则性表述，尚未明确两者之间的关系，也未作具体区分。

我们建议，可以进一步细化“数据安全风险评估”与“数据安全评估”各自的定义具体内容，明确两者所(分别)适用的场景以及两者之间概念上、开展顺序上等方面的关系。如两者实际为同一概念，我们建议适宜统一其用词表述，并将相应规则以专节/专章等形式集中整理展示，以防疏漏。

另一方面，《办法》现阶段未提供“数据安全风险评估”的具体实施要求，尚未明确开展该评估的主体等信息。

我们建议，可考虑在后续版本中澄清“数据安全风险评估”的开展主体等关键信息，明确是仅限于银保机构自身，还是同样允许委托外部机构。例如，可适当参考《央行数安办法草案》第 43 条“重要数据的数据处理者应当自行或者委托检测机构，每年组织开展一次全面的数据安全风险评估工作……”。

## 二. 数据安全治理

### 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。

**解读与建议**

《办法》新设“数据安全第一责任人”、“直接责任人”、“主体责任”等数据安全职位与职责。我们理解该举旨在通过明确高层权责，强化银保机构内部的数据安全治理能力。

鉴于此前已有《网络安全法》下“网络安全负责人”、《数据安全法》下“数据安全负责人”、《个人信息保护法》下“个人信息保护负责人”等类似职位，如在此基础上新增“数据安全第一责任人”等要求，可能会与部分银保机构现有的管理架构出现重合，或造成一人担任多职、数人担任一职的情况。

我们建议，可以考虑以上新设职位职责能否与现行法规相关职位职责保持一致，或明确相关职位能否由上述职位的人担任或兼任。

### 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。

**解读与建议**

《办法》新设“数据安全归口管理部门”。我们理解所有银保机构均需“指定”该部门。而“指定”暂未限定其具体形式，或可理解为“指定新设”该部门，也可理解为“指定现有”的数据安全部门担任该归口管理职责。

一方面，考虑到实践中各类银保机构的部门规模、既有数据保护组织情况等方面存在差异，如一次性要求所有相关部门均“指定新设”该数据安全归口管理部门，可能会加重中小机构的合规负担，也可能造成大型机构既有合规架构的冗余。

我们建议，可考虑在理解与监管层面对该条中“指定”采取开放式解释，允许合规体系完善的机构将新设归口管理部门与其现有的数据安全保护部门相融合，从而提升合规资源的利用效益。

另一方面，考虑到各类银保机构在业务所涉数据类型、级别、处理活动类型等方面同样存在差异，如一概强调设立同类归口管理部门，可能并不一定有利于实践中各类机构合规资源的调配。

我们建议，可考虑根据机构规模、业务处理数据分类分级水平等因素，对该部门的设立设置差异性要求，从而灵活适配不同机构的情况，提升《办法》落实后的监管效率。例如，《央行数安办法草案》第十二条同样新设类似的“数据安全牵头管理内设部门”，但仅要求“重要数据的处理者”设立。

## 三. 数据分类分级

**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。

**解读与建议**

《央行数安办法草案》第七条同样提出数据分类要求，但分类标准为“是否为个人信息、数据来源(生产经营加工产生、外部收集产生等)、存储该数据项的信息系统清单和应用的业务类别”，与《办法》所采标准并不完全一致。

鉴于《办法》和《央行数安办法草案》位阶较相同且受规制的金融机构存在一定重合，实践中金融领域各适用机构在对接时可能会产生分类标准上的理解差异，进一步影响后续合作与管理。

我们建议，可以与央行进一步协调，探讨能否达成数据分类方面的共识，尽量在立法层面为金融领域数据设置一套统一的分类标准与判断规则。此外，还可以考虑增加对照条款或推出解释，以明确其他相关文件中的分类如何衔接、对应《办法》所采数据分类标准。

**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。

**解读与建议**

该条提出“三级两类”的数据分级要求——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，又进一步将一般数据细分为敏感数据和其他一般数据。

一方面，《办法》所采分级标准与此前《央行数安办法草案》、金融行业推荐标准《金融数据安全 数据安全分级指南》(JR/T 0197-2020)有所差异:

1) 《央行数安办法草案》按照精度、规模和对国家安全的影响程度，分为一般、重要、核心三级，并进一步要求参考行业标准，根据数据遭到泄露或者被非法获取、非法利用时，可能对个人、组织合法权益或者公共利益等造成的危害程度，将数据项敏感性从低至高进一步分为一至五共五个层级；此外，二者针对不同级别数据的数据安全管理要求也不同(例如，《办法》明确要求敏感级及以上数据严格实施授权管理，而《央行数安办法草案》则就数据处理提出普遍告知义务);
2) 《金融数据安全 数据安全分级指南》(JR/T 0197-2020)则将个人金融信息按敏感程度从高到低分为 C3、C2、C1 三个类别。

鉴于三部金融领域办法草案及行业标准均未在数据分级标准上达成一致，且《办法》在适用范围上与《央行数安办法》存在交叉监管可能，或将进一步增加银保机构及其他金融机构开展数据分级及相应管理工作的难度。我们建议，可考虑后续针对数据分级标准及相应管理进一步澄清与其他相关文件的衔接、优先级别等问题。

另一方面，《办法》新设“敏感数据”这一级别数据并在后文设置多项针对“敏感级及以上数据”的安全义务，我们理解“敏感数据”将成为实践中机构改革与监管关注的重点。但目前《办法》仅给出其基本定义，第七十一条虽提及后续将推出的“银行业保险业重要数据目录”、“核心数据目录建议”，但并未涉及“敏感数据”的官方目录。

我们建议，可考虑进一步澄清设立“敏感数据”的立法考量因素，以及后续是否有制定“敏感数据”官方目录或建议的计划，或提供更为详细、可落地的具体判断细则，以供实践层面更好理解、执行。

## 四. 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**。

**解读与建议**

该条提出“制定数据安全管理办法”以及“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”的双重要求，从内部治理制度角度强调银保机构数据安全保护的一般与特殊场景合规义务。

鉴于“数据安全管理办法”经《数据安全法》等上位法铺垫，在实务中已有一定参考样本；而针对数据外部引入或者合作共享、数据出境等特殊活动的“安全管理实施细则”，目前对各机构而言仍缺乏适应银保行业的指引与经验，在落实层面可能存在一定难度。

我们建议，可考虑在未来公布《办法》的同时发布配套指南性文件或示范性细则，在其中明确该等针对银保机构开展数据出境等特殊活动的“安全管理实施细则”的必要条款、整体框架等具体内容，从而提升各机构落实要求的效率。

**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。

**解读与建议**

《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。我们理解，这一制度创新旨在提升银保机构的数据安全水平，通过落实安全评估机制这一实操要求，全面提升各机构对敏感级及以上数据处理的风险意识与合规水平。

一方面，考虑到现阶段《办法》所描述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》下的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”), 我们建议在《办法》或其他指引性文件中明确, 至少针对个人信息而言, 《办法》下的“数据安全评估”是否可以与《个人信息保护法》下的个人信息影响评估工作合并。

另一方面, 相较仅针对个人信息的“个人信息保护影响评估”, 《办法》下的“数据安全评估”首次创新地将评估对象拓展至非个人信息, 有助于全面提升银保领域数据安全的保护水平。但鉴于目前国内尚未确立针对非个人信息安全评估的规范基础, 国际上也同样比较缺失该领域的实践经验, 我们建议可考虑在《办法》或后续指引性文件、标准文件中进一步明确该机制各项要求的具体落地方案细节, 提供评估参考示例, 并释明针对非个人信息类数据的细化理解, 例如, 如何评估非个人信息类数据对数据主体权益影响的水平等。

**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。

**解读与建议**

该条强调除法律、行政法规另有规定外, 银保机构收集数据应限于“数据主体同意的范围”, 提出数据收集环节的“获取同意”义务。

一方面, 《办法》规制范围还包含大量非个人信息, 而现行法律规范仅提供针对个人授权同意的具体要求, 仍缺失针对非个人主体的相关参考基础。

我们建议, 为提高银保机构的操作效率, 可考虑进一步结合数据主体类别及数据的分类情况, 评估对于所有个人信息以外数据的收集均需“数据主体的同意”的适当性, 并进一步评估是否根据数据的重要性划分明确某些非个人数据主体或某些类别数据的收集无需取得“数据主体的同意”。

此外, 可考虑进一步通过指引性文件明确如何判断个人以外“数据主体的同意”, 释明同意的具体方式、类别、参考示例等, 例如, 企业主体就相关业务签署相应的合同是否即可视为同意?同意是否包括“默示同意”, 还是仅包括“明示同意”?此外, 还可考虑针对非个人数据的分类分级, 对不同主体或不同类别的数据分别适用“默示同意”或“明示同意”。

另一方面, 参照《个人信息保护法》相关规定, 除个人信息主体同意要求外, 该法还提供“履行合同所必要”“人力资源管理所必要”等豁免同意的条件。

鉴于银保机构收集和处理的大量数据往往依赖相关机构之间的基础业务框架，实践中未必都会签订具体的细分合同，因此，我们建议，可考虑是否将“履行合同所必要”“金融业务所必要”等金融领域特殊场景纳入数据处理的合法基础范围内，从而提升《办法》的落实效率。

此外，结合《办法》的规制范围，该条规定银行保险机构收集所有数据均应当坚持“合法、正当、必要、诚信”原则。《个人信息保护法》第五条及第五十六条规定，个人信息的处理应当遵循“合法、正当、必要和诚信原则”，且对个人信息影响评估应当包括“个人信息的处理目的、处理方式等是否合法、正当、必要”；相较而言，《数据安全法》第三十二条第一款规定,任何组织、个人收集数据，应当采取合法、正当的方式，《数据安全法》并未含有“必要性”的要求。因此，我们建议考虑进一步评估是否区分个人信息及非个人信息类数据收集所遵循的原则，即收集非个人信息类数据是否需要遵循“必要性”原则。

**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。

**解读与建议**

除上一条所提及“同意”问题外，针对集团公司内部共享场景，当前实践中一些集团公司开展数据融合相关工作时会要求其子行、子公司提供客户数据、业务数据等，而这类集团公司内的数据共享往往是为风控目的或者更好地为消费者提供金融服务，如在采取严格安全措施的前提下开展，并不会损害个人信息主体或其他主体的权益。

根据《办法》该条规定，如要求子行、子公司对于敏感级以上的数据共享均需严格获得数据主体的授权同意，尤其在目前仍缺乏非个人主体授权同意规则的背景下，可能会在实操性上给相关子行、子公司带来相当的挑战。

我们建议，可以考虑对于需要获取授权的数据等级进行适当上调，例如“重要级及以上数据”才需授权同意。或可参照我们上一条的建议，为数据共享场景增加除授权同意之外的合法性基础。

**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。

**解读与建议**

该条提出数据转移场景下，银保机构获取数据主体同意的义务。

鉴于实践中银保机构从相关数据主体获取“敏感级及以上数据”后，除仅仅使用该等数据本身之外，多见将该等数据与自有或者其他方的数据进行汇聚融合使用，进而改变原始数据的范围及性质的情形。

我们建议，可进一步释明，对于此类数据融合所形成新的数据，机构向外部提供时是否仍然需要取得数据主体的同意?如需要，建议可考虑在《办法》或后续指引性文件中明确此类加工、融合场景具体应如何取得同意。

**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。

**解读与建议**

该条提出数据公开场景下，除另有规定外，银保机构应取得数据主体授权同意的义务。

鉴于实践中企业类型的数据主体往往已经通过个人授权同意等方式掌握一定个人信息，对数据的权属可能存在多层关系。我们建议，可进一步明确，对于这部分多层权属数据的公开，机构是否仅需获得最终对接企业等数据主体的授权同意，还是也需要追溯前手主体、同时获得前手个人信息主体的授权同意。

**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**。

**解读与建议**

该条提出数据跨境场景下，银保机构应当进行安全评估的义务。

鉴于个人信息数据出境场景下，现行法律规范除安全评估外，还提供了“出境备案”、“认证”等其他出境路径，而《办法》似乎并未提及该等其他路径。我们建议，可适当参考《促进和规范数据跨境流动规定》等最新要求，在《办法》中进一步明确，银保机构是否同样可以通过安全评估以外的其他路径进行数据跨境流通。

## 五. 数据安全技术保护

**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。

**解读与建议**

该条提出投入使用信息系统、模型算法场景下，银保机构应当开展数据安全审查的义务。

鉴于《数据安全法》规定，只有当数据处理活动“影响或者可能影响国家安全”时，才需要进行数据安全审查。如《办法》该条所指“数据安全审查”仅指银保机构内部审查，可能会与前述《数据安全法》所指机制产生一定混淆。

我们建议，可考虑明确本条中数据安全审查与《数据安全法》下的“数据安全审查”外延、内涵是否一致。如不一致，建议可采取其他更贴近“投入使用信息系统、模型算法”场景且不易混淆的表述。

## 六. 数据安全风险监测与处置

**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。

**解读与建议**

我们建议，可适当参考《央行数安办法草案》对数据安全风险评估的具体要求(下附)，在后续立法或指引性文件中进一步明确《办法》下“数据安全风险评估”机制的具体要求、评估对象、评估内容、实施细则等具体要求，从而提升各机构理解、落实的效率。

附: 《央行数安办法草案》第四十三条

“重要数据的数据处理者应当自行或者委托检测机构，每年组织开展一次全面的数据安全风险评估工作，于下年度一季度末前向中国人民银行或其住所地分支机构报送风险评估报告，并按照行政法规要求向对应的网信部门报送。除法律、行政法规已明确的内容外，风险评估报告还应当重点评估下列风险，并提出改进应对措施:

(一) 数据分类分级实施制度、违规数据处理活动定责规程和问责处罚措施、数据处理活动全流程数据安全管理制度和相关操作规程的建设情况;

(二) 数据安全决策、管理、执行、监督各层面职责划分和对应岗位设置是否明确、合理，实际职责落实情况;

(三) 人员培训和日常管理情况;

(四) 重要数据识别判定情况，处理重要数据的目的、范围、规模、方式、类型、存储期限和存储地点等情况;

(五) 重要数据相关的数据处理活动记录信息的真实性与完整性;

(六) 重要数据相关的数据处理活动全流程管理和技术措施执行情况及其有效性;

(七) 存储重要数据信息系统的网络安全等级保护测评和问题整改落实情况;

(八) 重要数据相关的数据处理活动风险监测预警和溯源排查情况;

(九) 数据安全事件定级判定标准建设情况，应急预案、应急处置流程设计与演练实施情况，以及本年度发生的数据安全事件及处置情况;

(十) 向其他数据处理者提供重要数据的风险评估报告。”

另外，鉴于目前尚未有正式生效的数据专项审计相关监管规则，且尚处于征求意见阶段的《个人信息保护合规审计管理办法》仅针对个人信息而不包括非个人信息类数据，故对于银保机构的专项审计工作参考性可能不足，因此，我们建议，可考虑适当在后续立法或指引性文件中进一步明确《办法》项下“专项审计”的具体要求、审查重点等，从而为银保机构提供专项审计工作的参考指南。

**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。

**解读与建议**

鉴于《办法》尚未明确所有级别数据安全事件具体如何处置及未能及时处置的补救措施、后续措施等，仅明确了特别重大级别的应对措施，且现有“处置措施”“立即”“及时”等表述含义较为模糊；且此类报告的具体形式及内容均未明确。

我们建议，可适当参考《网络安全事件报告管理办法(征求意见稿)》(下附)，将《办法》的相应规定与之统一，明确该条所提及报告的必要内容等具体要求，从而降低实践中机构在理解与落实上的难度。

附：《网络安全事件报告管理办法(征求意见稿)》
第四条
“运营者在发生网络安全事件时，应当及时启动应急预案进行处置。按照《网络安全事件分级指南》，属于较大、重大或特别重大网络安全事件的，应当于 1 小时内进行报告。
网络和系统归属中央和国家机关各部门及其管理的企事业单位的，运营者应当向本部门网信工作机构报告。属于重大、特别重大网络安全事件的，各部门网信工作机构在收到报告后应当于 1 小时内向国家网信部门报告。
网络和系统为关键信息基础设施的，运营者应当向保护工作部门、公安机关报告。属于重大、特别重大网络安全事件的，保护工作部门在收到报告后，应当于 1 小时内向国家网信部门、国务院公安部门报告。
其他网络和系统运营者应当向属地网信部门报告。属于重大、特别重大网络安全事件的，属地网信部门在收到报告后，应当于 1 小时内逐级向上级网信部门报告。
有行业主管监管部门的，运营者还应当按照行业主管监管部门要求报告。
发现涉嫌犯罪的，运营者应当同时向公安机关报告。”
第五条
“运营者应当按照《网络安全事件信息报告表》报告事件，至少包括下列内容：……”

## 七. 监督管理

**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。

**解读与建议**

可参见我们在上文第三章-第十八条(数据分级)部分的具体分析及建议。

**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。

**解读与建议**

针对敏感级以上的客户个人信息出境(如果构成“批量”), 参考该条要求, 无论是签署标准合同, 还是申请数据出境安全评估, 均需要事先履行监管报告手续。

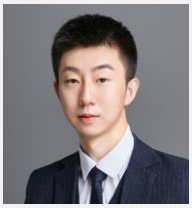
鉴于目前《办法》尚未明确, 对于其他一般类客户个人信息出境签署标准合同是否需要履行监管报告手续规定; 此外, 由于标准合同备案和数据出境安全评估中可能存在多轮申请文件修订, 因此可能还会存在在先履行监管报告材料是否需要继续更新的问题。

我们建议, 可考虑在后续立法及规范性文件中对上述问题予以明确。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

王 祎
+86 10 5081 3888
yi.wang@llinkslaw.com



朱晓阳
+86 21 3135 8683
nigel.zhu@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

| 上海 | 北京 | 深圳 |
| --- | --- | --- |
| 上海市银城中路 68 号<br>时代金融中心 19 楼<br>T: +86 21 3135 8666<br>F: +86 21 3135 8600 | 北京市朝阳区光华东里 8 号<br>中海广场中楼 30 层<br>T: +86 10 5081 3888<br>F: +86 10 5081 3866 | 深圳市南山区科苑南路 2666 号<br>中国华润大厦 18 楼<br>T: +86 755 3391 7666<br>F: +86 755 3391 7668 |
| 香港 | 伦敦 | |
| 香港中环遮打道 18 号<br>历山大厦 32 楼 3201 室<br>T: +852 2592 1978<br>F: +852 2868 0883 | 1/F, 3 More London Riverside<br>London SE1 2RE<br>T: +44 (0)20 3283 4337<br>D: +44 (0)20 3283 4323 | |

www.llinkslaw.com

Wechat: LlinksLaw

**本土化资源 国际化视野**