汉坤法律评述

2023 年 7 月 25 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

金融数据监管大幕将启：简评人民银行业务领域数据安全管理办法征求意见稿

作者：权威 | 李珣 | 夏迎雨 | 李烨 | 郑博

一、新规出台背景与影响

2021 年，《中华人民共和国数据安全法》（“**《数据安全法》**”）出台，明确金融等主管部门承担本行业、本领域数据安全监管职责，同时规定国家建立数据分类分级保护制度、各部门按照数据分类分级保护制度确定本部门以及相关行业、领域的重要数据具体目录等。2022 年 12 月发布的《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》进一步指出要加强数据分类分级管理。而在金融数据监管领域，尽管近年来已经陆续出台了若干部门规章、规范性文件以及行业标准，但法规体系并不完善，且与我国最新的数据安全、个人信息保护立法仍存在差距。

为此，2023 年 7 月 24 日，中国人民银行（“**人民银行**”）发布了《中国人民银行业务领域数据安全管理办法（征求意见稿）》（“**新规**”），面向社会进行为期 1 个月的公开征求意见，旨在规范人民银行业务领域数据的安全管理，也填补了本领域数据安全管理制度保障的空白。新规共八章五十七条，对人民银行业务领域数据相关的处理活动提出了覆盖全生命周期的细化管理要求，以数据分类分级为基础，对数据安全保护从管理措施、技术措施等方面提出具体要求，同时涵盖风险监测、评估审计与事件处置措施以解决事中事后可能发生的风险，并明确相关法律责任。

作为人民银行业务领域甚至金融领域的首部数据安全专门性法规，新规衔接《数据安全法》等上位法，核心意义在于确立了人民银行数据安全工作逻辑：数据安全工作的开展以“数据分类分级”为基础，并在此基础上针对不同“类/级/层”的数据，需要匹配对应的管理措施和技术措施，对人民银行业务领域的数据安全管理提出了合规底线要求；而数据处理者也应当明确对应的责任岗位、建立对应的工作制度和业务流程、建立培训机制等。新规的出台为后续的金融数据监管提供了重要的参照标准，其亦是在数据安全管理领域对于功能监管和行为监管有机结合的体现，有助于提升监管质效、构建全方位的数据安全监管体系。

二、新规适用的范围和主体

就新规适用的范围和主体而言，可以从“数据类型”“数据处理活动”“数据处理者”与“监管主体”四个维度分别拆解：

（一）数据类型

新规主要规制的是“中国人民银行业务领域数据”，根据新规第 2 条的定义，主要是指“根据法律、

行政法规、国务院决定和中国人民银行规章，开展中国人民银行承担监督管理职责的各类业务活动时，所产生和收集的不涉及国家秘密的网络数据”。

对于“不涉及国家秘密”以及“网络数据”这两项限定要素，人民银行在新规起草说明中有所提及：一方面，《数据安全法》已经明确对于开展涉及国家秘密的数据处理活动适用《保守国家秘密法》等法律法规，因此无需再适用人民银行的业务领域数据规定；另一方面，新规主要是衔接《数据安全法》以及《网络数据安全管理条例》（虽然目前条例仍为征求意见稿，但已被纳入国务院 2023 年立法工作计划），限定数据范围仅为网络数据（可通俗理解为各种电子数据、信息），而对于统计、档案工作中的数据处理活动（可能涉及非网络数据，如纸质文档）可适用对应的法律法规。

（二）数据处理活动

这一项与前述数据类型息息相关，系指“中国人民银行承担监督管理职责的各类业务活动”，乍一看比较宽泛和抽象，特别是 2019 年的中国人民银行“三定”方案进一步明确了其职责范围，包括宏观与微观层面共二十余项。而本次新规所涉及的数据处理活动，更多是集中于金融数据较为密集、市场主体参与较多的场景，为此新规起草说明也进一步明确，**新规约束的数据处理活动主要包括：货币政策业务、跨境人民币业务、银行间各类市场交易业务、金融业综合统计业务、支付清算业务、货币管理和数字人民币业务、经理国库业务、征信业务、反洗钱业务等领域的数据处理活动**。

（三）数据处理者

新规明确需要适用的数据处理者包括“金融机构”和“其他机构”。直观来看，**人民银行具有直接管辖权的金融业务相关机构包括银行、第三方支付机构、持牌征信机构、银联和网联等清算机构，而消金信托等非银行金融机构以及证券基金期货公司等大概率不适用新规，但不排除国家金融监督管理总局、证监会、国家外汇管理局后续会各自出台法规，以对各自领域内的金融数据/网络数据进行规定**。

此外，**对于新规所提的“其他机构”，目前范围仍不明确**，例如数据处理者是否包含人民银行直属机构如中国人民银行征信中心、中国反洗钱监测分析中心、中国人民银行清算总中心等涉及大量网络数据处理的单位；非持牌的互联网公司、科技公司或者数据服务提供商是否适用新规，以及在多大范围内需要满足新规要求（如作为数据处理者直接适用，还是仅作为委托处理的受托方间接适用），也有待进一步澄清。

仅从目前的规定以及监管现状来看，我们认为商业影响可能主要集中在第三方支付机构以及持牌征信机构，这两类主体需要重点关注。例如互联网系的第三方支付机构可能存在独立性较弱的情形，其人员、系统、数据的混同都会在新规下遭受考验，而把支付牌照视为金融业务集群并对金融业务集群进行整体式业务管理的内部管理模式难以符合合规要求。对于国家金融监督管理总局主管的相关机构，基于“**谁管业务，谁管业务数据，谁管数据安全**”的基本原则，此类主体的数据安全管理工作大概率会由国家金融监督管理总局主导。

（四）监管主体

本次新规明确的监管主体是中国人民银行及其分支机构，但同时也受限于“国家数据安全工作协调机制”的统筹协调，以及“其他有关主管部门”依据职责开展的数据安全监督管理工作，需要注意以下几点：

- **新规仅针对中国人民银行的相关业务活动，虽然指向金融行业，但并不包括所有金融业务领域和金融机构**，未来可能还有国家金融监督管理总局、证监会、国家外汇管理局各自的法规

（本次新规第 56 条就提及“国家外汇领域数据安全管理由国家外汇管理局负责，具体制度可另行制定”），而对于部分金融机构（如银行）在同时满足中国人民银行、国家金融监督管理总局以及国家外汇管理局的数据安全要求过程中，如何避免产生冲突或者割裂，有待观察。

- **金融监管部门将承担主要的数据监管职责，但“多头监管”的现象将仍然存在**。新规明确按照“谁管业务，谁管业务数据，谁管数据安全”的基本原则，明确了中国人民银行及其分支机构的执法权，但亦提及将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，因此公安机关、国家安全机关和国家网信等部门仍然对金融行业市场主体具有一定的数据安全监管职责，监管部门之间也需注意避免重复检查、提高管理效能。

三、数据分类分级

（一）数据分类分级要求：三级、五层、可用性

新规规定由人民银行统筹数据分级分类工作，包括相关行业标准制定、分级分类工作开展、确定重要数据目录并实施动态管理等。新规项下的数据分级分类要求可归纳为**三级、五层、可用性**，具体而言：

- **三级**：是指按照数据精度、规模以及对国家安全的影响程度来划分，将数据分为一般、重要、核心三级。该划分维度主要与《数据安全法》《网络安全法》《数据出境安全评估办法》等网信办主导的数据监管领域的现行规定相衔接。

- **五层**：是指按照数据敏感性来划分，根据风险事件发生时可能对个人、组织、公共利益造成的危害程度，将数据分为一至五共五级。该划分维度主要与《金融数据安全 数据安全分级指南》（JR/T 0197 – 2020）等人民银行主导的金融监管领域的现行规定相衔接。

- **可用性**：是指在信息系统业务连续性保障体系建设过程中，纳入考虑数据可用性分层。新规并未对于可用性分层提出具体要求，仅进行了原则性规定。我们理解，该要求主要参照了今年 5 月刚刚发布的《信息技术服务 数据中心业务连续性登记评级准则》（GB/T 42581 – 2023），该准则将数据中心业务连续性等级划分为起始级、发展级、稳健级、优秀级、卓越级五个等级，对应不同可用性级别的设施、不同的业务连续性管理水平以及维持业务连续性的可靠结果。

就“三级、五层、可用性”，我们认为有以下**两个衔接关系**值得重点关注：

- **新规和现行规定的衔接关系：**

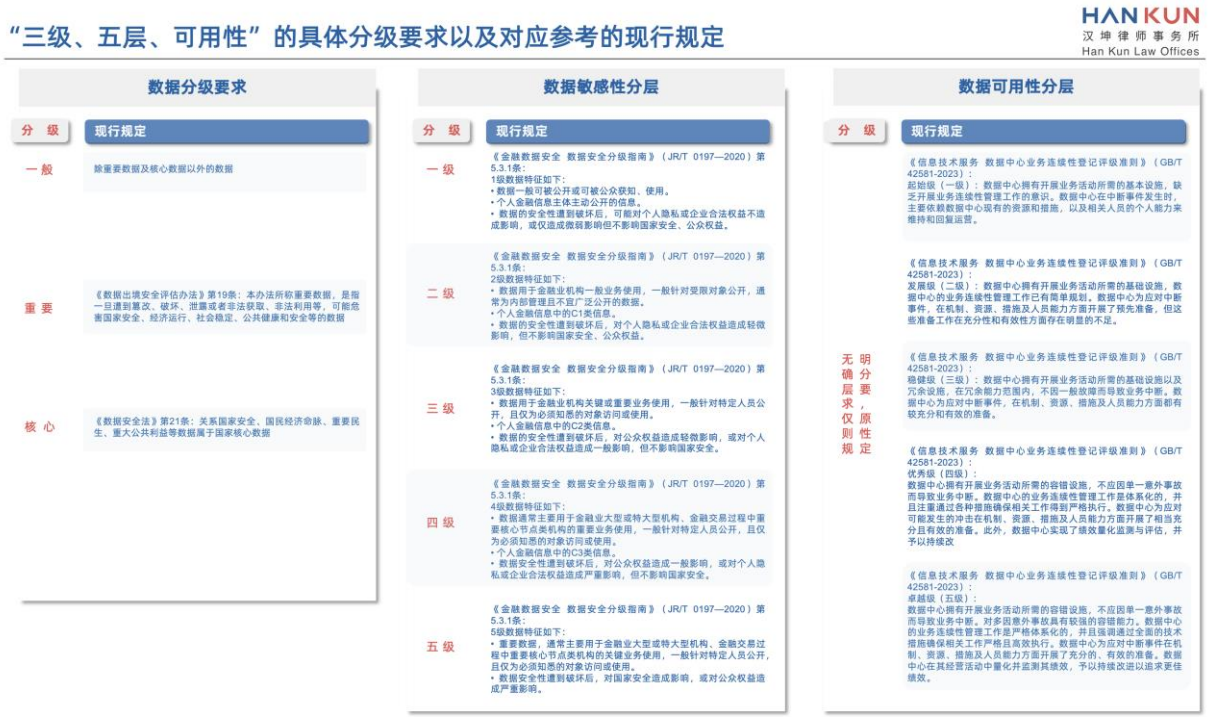
  “三级、五层、可用性”在现行规定中都能找到对应或参考规定。这是否意味着现行规定项下的分级标准可以直接映射到新规中来？我们认为答案显然是否定的。新规起草说明中即明确提出“中国人民银行已相继出台《金融数据安全 数据安全分级指南》（JR/T 0197 – 2020）、《金融数据安全 数据生命周期安全规范》（JR/T 0223 – 2021）等金融业数据安全标准，因数据安全管理要求不断演进，相关标准在内容与术语定义方面，需要根据《办法》作对应调整，后续中国人民银行将加快组织上述标准的修订工作，确保制度与标准适配统一”，可见，人民银行已经计划对于原由人民银行制定的相关标准进行修订，该等修订当然也可能涉及标准中对于数据的分级标准。但另一方面，《数据安全法》《网络安全法》《数据出境安全评估办法》等数据领域的通用监管规定，人民银行并无修订权限，因此，对于这些规定项下的分级标准，新规更可能的是保持一致而非另辟蹊径。此外，对于可用性而言，现有规定仅作为参照，并不存在

适用关系，新规项下作进一步调整的可能性较大。

- **三级和五层的衔接关系：**

  与系统维度的可用性分级要求不同，三级和五层均属于数据维度的分级要求，两者所涉对象是重叠的，因此，三级和五层之间的衔接关系就成为了不可避免的问题。根据现行监管规定，1－4 级数据可能属于一般数据，5 级数据属于重要数据（含核心数据）。尽管如上所述，现行规定项下的分级标准并不能直接映射到新规中来，人民银行还可能对于相关标准进行动态调整，但是我们倾向于认为，三级和五层之间的衔接关系与现行规定相比不会有大的变化，即大概率仍然会沿用原有对应关系。

上述“三级、五层、可用性”的具体分级要求以及对应参考的现行规定可归纳如下图：



（二）数据分类分级的持续动态调整

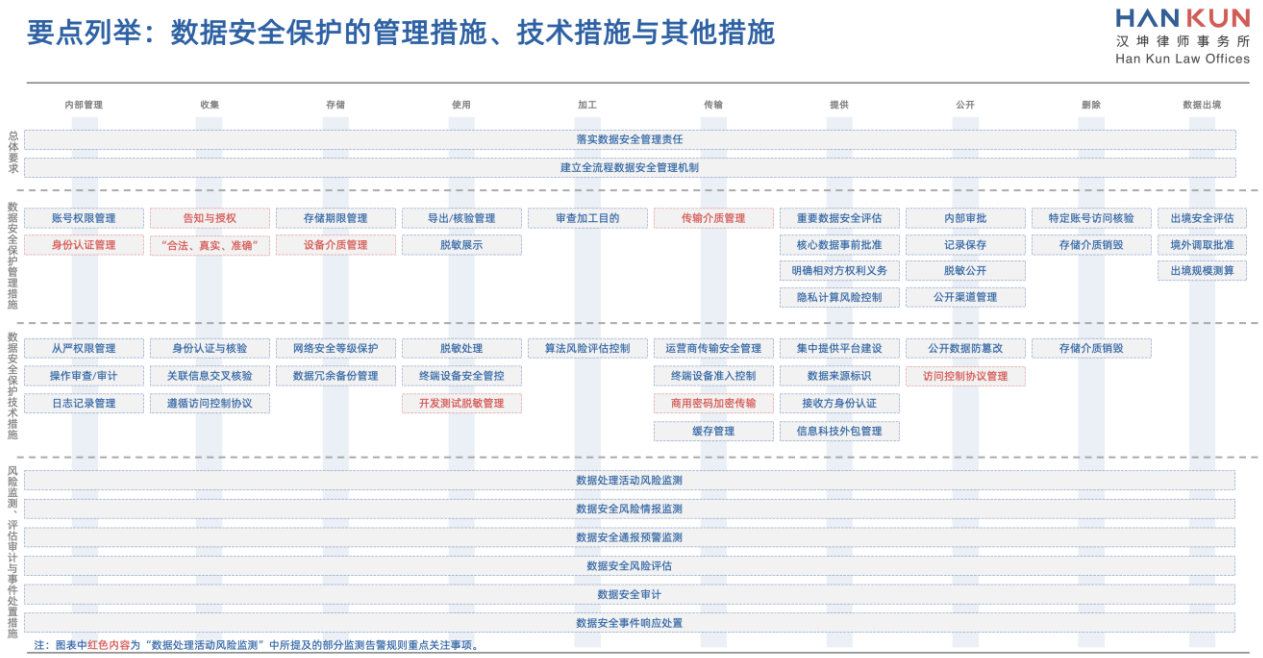
在数据分类分级完成后，并不意味着“高枕无忧”，新规还规定了数据分类分级的持续动态调整机制，即**将数据分类分级监管视为一个持续、动态的过程**，要求数据处理者定期更新、报送数据目录，视具体情况可对相应数据的敏感性层级进行提升或降低，相关规定具体包括：

- 中国人民银行统筹确定重要数据具体目录并实施**动态管理**（新规第 5 条）；
- 在中国人民银行组织下，数据处理者应当准确识别判定本单位信息系统存储的**全量数据是否属于重要数据、核心数据**，并**填写报送重要数据目录内容**，由中国人民银行汇总后确定重要数据具体目录。（新规第 8 条）；
- 数据处理者应当根据数据和信息系统变化情况，每年组织**更新数据资源目录**，避免信息系统所涉及数据项未在数据资源目录中记录、数据项标识信息不完整等情形发生（新规第 11 条）；
- 使用第三层级以上数据项加工后产生的数据项，经评估确认无法识别至特定个人、组织，或者

反映信息敏感程度明显低于原数据项时，数据处理者履行内部审批手续后，**可视情况降低敏感性层级**，促进数据依法合规开发利用（新规第 21 条）。

四、数据安全保护的管理措施、技术措施与其他措施

新规从第三章至第六章以较大篇幅规定了数据安全保护的总体要求、管理措施、技术措施，以及风险监测、评估审计与风险事件处置的措施，我们通过下图进行了部分列举：



就其重点而言，我们理解可以关注如下几个方面：

- **“就高不就低”的总体处理原则**：针对中国人民银行业务领域数据，考虑到实践中可能存在无法拆分的非结构化数据（即没有预定义的抽象描述数据类型，并且不适宜用数据库二维逻辑表展现的数据项，如图像、视频、音频、文档文件等），也可能存在不同敏感层级的数据在同一个数据处理活动中且难以进行差异化管理，在此种情况下如何确定适用数据安全保护管理措施和技术措施，新规也进行了明确 — 采用“就高不就低”的处理原则。

  一方面，非结构化数据项应当优先按照可拆分的各结构化数据项所对应最高层级，标识其层级（新规第 9 条）；另一方面，第五层级数据项应当在第四层级数据项对应的安全保护管理和技术措施基础上进一步从严管理。不同敏感性层级数据项在同一个数据处理活动中被处理，且难以采取差异化安全保护管理和技术措施的，应当统一采取最高敏感性层级数据项对应的安全保护管理和技术措施（新规第 13 条）。此外，与关联方合作开展数据处理活动，也不得降低安全保护管理和技术措施要求，即关联方处理数据无特殊豁免。

- **针对具体环节的管理和技术措施**：新规针对数据处理的八个主要环节 — 收集、存储、使用、加工、传输、提供、公开、删除等都提出了专门且细致的管理措施和技术措施，这在金融行业与数据管理的相关正式立法中并不常见，我们理解大概率是参照原有的个人金融信息保护技术规范、金融数据安全数据安全分级指南、金融数据安全数据生命周期安全规范等行业标准的体例和内容，将其内化并上升为法规的一部分。

根据新规起草说明，明确此类措施主要是为了“压实数据处理活动全流程安全合规底线”，换言之，数据处理者只有做到新规要求的安全保护管理和技术措施，才能被视为总体满足尽职尽责的合规底线要求。从立法技术来看，新规既提出原则上应当采取的措施，又明确特殊情形可通过内部审批、统一场景等方式予以弱化，一定程度上可以避免合规义务“一刀切”的发生。但过于细致的规定是否会给业务开展带来过多的限制（特别是其中包含大量此前的推荐性行业标准要求，且与目前的市场实践存在一定差距），在正式稿发布时是否会进行删减也有待观察。

- **已有法规要求的重申与衔接**：一方面，新规承继了《数据安全法》《个人信息保护法》等法律法规的一部分现有要求并进行了重申，例如新规第 26 条规定境内收集和产生的数据原则上应当在境内存储、在规定情形下向境外提供数据应当申报数据出境安全评估等，第 27 条规定非经主管部门批注不得向境外监管部门提供境内存储的数据（与《数据安全法》第 36 条、《个人信息保护法》第 41 条类似）；另一方面，新规也在现有法规基础上进行了部分补充规定，如第 17 条明确在间接收集数据的场景下，数据处理者应当要求数据提供方提供取得同意的证明或来源说明材料，第 26 条明确了数据出境场景下对于出境数据规模和范围的测算时点是每年 1 月底，第 29 条明确数据处理者应当每年进行账号核验以确保可以响应用户的删除权等。

- **明确隐私计算的可行性，强调爬虫合规**：就数据处理的技术手段上而言，新规提及“隐私计算”这一较为新型的技术概念，并明确在控制风险的范围内可以使用，主要规定如新规第 25 条、第 37 条。事实上，隐私计算由于其“数据不出库、可用不可见”的特点已经在金融行业有所运用，如针对金融产品的智能营销、核查多头借贷与智能风控等。但在目前阶段，隐私计算也不是绝对完美的，不宜将隐私计算与完全的匿名化划等号，在过程中仍可能涉及“梯度值”的传输，也可能被数据接收方进行重新识别，而人民银行也清楚地意识到这点，但为了促进数据高效流通和创新应用，仍然为隐私计算等新技术的运用提供了空间，底线是应确保原始数据未离开自身控制范围、暴露约定范围外信息的风险可控、建立对应的风险缓释措施。不过，新规并未明确隐私计算的含义，某种技术是否足以被理解为隐私计算仍存在模糊之处，因此市场主体对于隐私计算的认定与使用也需要谨慎对待。

  此外，新规第 32 条、第 38 条、第 40 条还多次提及爬虫合规，包括“遵守其他数据处理者的数据访问控制协议”、“明确自身的数据访问控制协议”、“监测违反数据访问控制协议的异常行为”。不过值得商榷的是，数据访问控制协议（常见的是 Robots 协议）在法规层面并无明确定性，其更像是一份“君子协定”或者“道德约束”，司法实践中司法机关也不会以仅仅违反 Robots 协议的这一事实而判定爬虫使用方承担法律责任，但新规第 32 条明确数据处理者“应当遵守”数据访问控制协议，可能与市场实践脱节。

五、小结

总体而言，近两年数据安全领域立法频繁，且此前法规已经提及金融行业的数据分类分级等办法将由行业主管部门自行制定，因此市场主体对于本次新规的出台已经有所预期。**就新规内容而言，也并未创设太多具有“颠覆性”的规定，我们理解更多是基于现有监管规则与金融行业标准进行的细化、总结和延伸补充**。从立法技术上而言，法规条款表述也较为灵活，避免了“一刀切”的规定，尽管在部分条款上可能有商榷空间，但已经具备较高的成熟度了。此外，新规文末已载明将于 2024 年起施行，**我们判断可能会在今年内出台正式稿**。

对市场从业主体而言，数据分类分级的不同将导致面临的合规义务也有较大差别，特别是对于后续数据

的处理使用存在不同限制，**而新规的大量管理措施、技术措施都依赖数据分类分级的完成，对于业务的确切影响暂无法判断，因此建议密切关注后续更新的金融数据分类分级行业标准。就现阶段而言，相关主体可以先考虑初步制定合规制度文本和工作机制流程，新规生效后再视需要进一步调整优化和完善。**

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