筑牢金融数据防线
——《中国人民银行业务领域数据安全管理办法》解读

作者：杨迅 | 李依然

《中国人民银行业务领域数据安全管理办法》("**《银行数据管理办法》**")已于 2025 年 5 月 1 日发布，并将自 2025 年 6 月 30 日起施行。作为金融数据安全领域的重要法规，该办法依据《网络安全法》《数据安全法》《个人信息保护法》等上位法制定，聚焦于规范中国人民银行业务领域数据的安全管理与开发利用。该办法不仅为金融机构及其他数据处理者提供了明确的合规指引，强化了数据安全保护义务，还在保障国家金融数据安全、保护个人和组织权益等方面发挥着关键作用。

一. 《银行数据管理办法》简介

(一) 适用范围

《银行数据管理办法》第二条规定，在中国境内开展的中国人民银行业务领域数据相关处理活动及其安全监督管理适用该办法。根据 2025 年 5 月 9 日中国人民银行有关部门负责人就《银行数据管理办法》答记者问[1]，具体包括金融机构及经中国人民银行批准或认定的其他机构在中国境内开展的中国人民银行业务领域数据相关处理活动，包含在货币信贷、宏观审慎、跨境人民币、银行间市场、金融业综合统计、支付清算、人民币发行流通、经理国库、征信和信用评级、反洗钱等业务领域内的数据处理活动。

(1) 从"人"的监管角度，中国人民银行并非商业银行等银行金融机构的主管机关，但其仍然是信用评级、征信业等行业的主管机关，对该行业经营者的数据处理活动有直接的监管职能。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

[1] 中国人民银行有关部门负责人就《中国人民银行业务领域数据安全管理办法》答记者问

(2) 从“行为”的监管角度，中国人民银行负责的反洗钱、支付清算等活动是几乎所有金融机构必须完成的业务环节，《银行数据管理办法》亦适用于该些业务环节涉及的数据。

(二) 立法过程

2023 年 7 月 24 日，《银行数据管理办法》征求意见稿就已发布，并向社会公开征求意见。根据公开征求意见的反馈[2]，在此后的一个月间，共收到有效反馈意见 103 条。在此基础上，《银行数据管理办法》最终稿作了大量的调整，主要调整如下:

(1) 精简数据全流程管理要求

《银行数据管理办法》大幅精简了第三章“全流程业务数据安全管理要求”和第四章“全流程业务数据安全技术要求”所列的内容，即简化了对金融业务中的数据(《银行数据管理办法》中称: “业务数据”)的管理和技术安全要求。例如，第四章征求意见稿中要求数据处理者针对数据收集、存储、使用、加工、传输、提供、公开和删除等各环节采取特定管理和技术措施，正式稿则更注重明确各环节的基本安全原则与要求，简化了对具体操作流程的详细规定，使数据处理者在遵循法规时更具灵活性，可依据自身业务特点制定更适应的管理措施。

(2) 数据出境灵活性提升

《银行数据管理办法》删除了征求意见稿中第二十六条关于保存出境数据规模测算估算结果的要求，在正式稿第二十四条中强调数据处理者因业务等需要向境外提供数据时，应严格遵守国家网信部门有关规定，但不再要求其保存测算估算结果等。这赋予了数据跨境流动一定的灵活性，既确保数据出境符合国家总体要求，又避免了繁琐流程对金融业务的不必要限制。

(3) 明确监督管理协作

《银行数据管理办法》第四条进一步明确了中国人民银行及其分支机构与其他主管部门间的监督管理协作配合、信息沟通。相较于征求意见稿，正式稿第二条强调了其他有关主管部门有规定的，数据处理者还应当依法遵守其规定。同时，根据正式稿第四十七条，中国人民银行必要时可联合实施执法检查，避免了监管真空与重复监管，凝聚了行业监管合力。

(4) 增加从轻减轻处罚情形

《银行数据管理办法》第五十二条增加了从轻减轻行政处罚的适用情形，包括数据处理者发生业务数据安全事件造成危害后果，但能证明已按规定采取数据安全保护措施并立即采

[2] 关于《中国人民银行业务领域数据安全管理办法(征求意见稿)》公开征求意见的反馈

取补救措施的；以及数据处理者积极提供数据安全风险情报，协助及时发现重大业务数据安全风险的，对其未履行数据安全保护义务但尚未造成危害后果的行为。这一修改旨在激励数据处理者更好地履职尽责，主动防范和化解数据安全风险。

(三) 与其他法律的关系

《银行数据管理办法》是《网络安全法》《数据安全法》和《个人信息保护法》的下位法，是网络安全和数据保护领域要求在银行业务领域的落地。

(1) 与《网络安全法》的关系

《银行数据管理办法》落实了《网络安全法》下的安全要求。《网络安全法》第三十七条要求关键信息基础设施运营者在境内存储重要数据，确需出境的则需进行安全评估。显然，银行的有关业务系统很有可能属于关键信息基础设施。《银行数据管理办法》第二十四条细化了相关业务数据跨境传输的规定，明确数据处理者在向境外提供数据时需遵守国家网信部门规定，且在法律、行政法规和中国人民银行规定有境内存储要求时，数据必须同时在境内存储。此外，《银行数据管理办法》第三十五条还要求数据处理者采取加密传输等技术措施保障数据传输安全，与《网络安全法》关于保障网络运行安全的要求相呼应。

(2) 与《数据安全法》的关系

《银行数据管理办法》强化了《数据安全法》下的数据安全责任和数据安全措施。《数据安全法》第三条确立了数据安全保护的总体原则，《银行数据管理办法》第三条据此提出“谁管业务，谁管业务数据，谁管数据安全”的责任制度，明确数据处理者需履行数据安全保护义务。《数据安全法》第二十一条要求建立数据分类分级保护制度，《银行数据管理办法》第六条至第九条细化了业务数据分类分级的标准和流程，规定数据处理者应建立健全相关制度和操作规程，并确定重要数据和核心数据的具体目录，以实现对不同级别数据的差异化保护。

(3) 与《个人信息保护法》的关系

《银行数据管理办法》体现了《个人信息保护法》下对个人信息保护的具体要求。《个人信息保护法》第十三条明确个人信息处理的合法性基础，《银行数据管理办法》第十五条据此规定，收集业务数据时，除收集自行公开或已合法公开的数据外，需取得个人同意或组织授权，并落实告知义务。《个人信息保护法》第五十一条要求个人信息处理者采取措施保障个人信息安全，《银行数据管理办法》第三十一条、第三十三条和第三十五条分别从数据收集验证、脱敏处理、传输加密等方面提出了具体要求，确保个人信息在业务数据处理活动中的安全性。

二. 银行业务数据的分级分类

《银行数据管理办法》第七条明确，数据处理者应遵循《数据安全法》第三条确定的原则，建立健全业务数据分类分级制度和操作规程。数据处理者需履行内部审批程序，保证分类分级结果的准确性和合理性，使数据分类分级工作符合法律法规要求和自身业务实际，为后续的数据安全管理奠定坚实基础。

(一) 数据类别和级别标准

《银行数据管理办法》第八条要求数据处理者依据业务数据的业务关联性、敏感性和可用性等因素，对数据进行全面梳理和分析，以此为基础明确数据的类型。业务关联性要求数据处理者识别数据在不同业务流程中的作用，例如在支付清算业务中，交易明细数据与资金流动数据紧密相关，需明确其在业务链条中的位置和作用。敏感性分类则需评估数据泄露或非法使用对个人隐私、企业利益、公共利益、社会稳定的潜在影响，如个人信用报告数据属于高敏感性信息。可用性分类强调数据在业务连续性中的价值，例如核心业务系统数据应具备高可用性，确保业务在异常情况下的持续运行。

具体就数据定级而言，《银行数据管理办法》第九条规定，业务数据依据其重要程度和敏感性分为一般数据、重要数据、核心数据三级。一般数据是指对业务影响较小、敏感性较低的数据；重要数据是指在特定领域、特定群体、特定区域或者达到一定精度和规模时，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据；核心数据则是指对领域、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，一旦被非法使用或者共享，可能直接影响政治安全的重要数据。

此外，根据《银行数据管理办法》第八条，数据处理者还需根据业务数据遭到泄露或者被非法获取、非法利用时对个人、组织合法权益或者公共利益等造成的危害程度开展敏感性分类；根据业务数据遭到篡改、破坏后对业务正常运行造成的影响程度；明确信息系统差异化的数据恢复点目标，视为对业务数据的可用性分类。通过这样的分类分级标准，数据处理者可以清晰地识别不同数据的风险等级，从而有针对性地制定和实施相应的安全保护策略。

(二) 金融机构的分级义务和程序

金融机构作为重要的数据处理者，需严格遵循《银行数据管理办法》第六条、第八条等规定，承担起数据分类分级管理的义务。首先，金融机构应建立健全数据分类分级制度和操作规程，明确数据分类分级的标准、方法和流程，确保数据分类分级工作的规范化和制度化。其次，金融机构要依据相关制度和规程，定期开展本机构的数据分类分级工作，对存储的全量数据进行全面梳理和分析，明确数据的类型和级别。在此过程中，金融机构需充分考虑业务数据的关联性、敏感性和可用性等因素，结合自身业务特点和风险状况，做出准确的分类分级判定。然后，金融机构应将分类分级结果履行内部审批程序，以保证结果的准确性和权威性。最后，金融机构应及时填

写并报送重要数据目录内容，确保监管部门能够准确掌握金融机构数据的分类分级情况，以便实施有效的监管和指导。

金融机构在进行数据分类分级的过程中，需特别关注重要数据的认定工作，包括按照《银行数据管理办法》第九条的标准，对本机构存储的全量数据进行逐一筛查和判定，准确识别哪些数据属于重要数据。在此基础上，金融机构需填写重要数据目录内容，并按照规定的程序和要求报送至中国人民银行。中国人民银行汇总各金融机构报送的重要数据目录后，形成重要数据具体目录，并经国家数据安全工作协调机制审定。之后，中国人民银行将确定重要数据的处理者，并将其对应的重要数据告知相关金融机构。金融机构应针对被认定的重要数据，进一步强化安全保护措施，确保其安全性和合规性。

三. 业务数据管理要求

根据《银行数据管理办法》，金融机构在业务数据管理方面需要遵循以下合规要点，具体条文如下:

(一) 人员管理

从职责分工角度，《银行数据管理办法》第十一条要求，金融机构应明确业务数据安全保护相关内设部门职责，配备与业务范围和服务规模相适应的数据安全专业人员。其中，重要数据的处理者应当明确业务数据的安全负责人和管理机构，安全负责人应当符合法律、行政法规已明确需具备的条件，并确保其能够有效履行数据安全保护义务，有权直接向中国人民银行报告业务数据安全情况。

同时，《银行数据管理办法》第十一条还要求面向社会提供产品、服务的金融机构应建立便捷的投诉、举报渠道，及时受理并处理业务数据安全有关投诉、举报。

(二) 流程管理

《银行数据管理办法》对业务数据的全流程管理提出了要求，具体包括:

(1) 数据收集

在数据收集阶段，根据《银行数据管理办法》第十五条，收集业务数据时，除收集自行公开或者其他已经合法公开的业务数据的情形外，应当依照法律、行政法规和中国人民银行相关规定取得个人同意或者组织授权，并落实相应告知义务。非直接面向个人、组织收集其尚未公开的业务数据的，应当在合同或者协议中明确数据提供方保障业务数据来源合法性、真实性的义务。

从数据准确性考虑，采用人工录入方式收集业务数据的，应当采取必要校验措施保障业务数据录入的准确性，并按照相关管理要求留存业务数据收集原始凭证。

同时，考虑到原则上不收集图像等原始个人生物识别信息，确需收集的，应当统一规范管理相关需求场景。

(2) 数据使用

对于高敏感性数据，根据《银行数据管理办法》第十七条，使用高敏感性数据项，原则上不采取导出方式，使用用于身份鉴别的数据项原则上仅采取核验方式。除根据个人请求向其展示与其相关业务数据，以及履行法定职责或者法定义务所需外，原则上须实施脱敏处理后再展示高敏感性数据项。

就数据加工而言，根据《银行数据管理办法》第十八条，数据处理者应当审查业务数据加工目的与业务数据收集约定是否一致，确保数据加工活动的合法性。

基于加工生成的数据项面向个人提供自动化决策服务的，应当以适当方式向个人解释说明处理目的、用于加工的个人信息种类和加工规则。

(3) 数据储存

总体而言，根据《银行数据管理办法》第十六条，数据处理者应当根据业务需要，明确业务数据保存期限，避免数据的长期留存风险。

对于高敏感性数据项，原则上不在终端设备和移动介质中存储，确需存储的，应当统一规范管理相关需求场景。同时，根据《银行数据管理办法》第三十二条，原则上，高敏感性数据项须加密存储，确需不加密存储的，应当统一规范管理相关需求场景。

此外，根据《银行数据管理办法》第三十二条，业务数据需要开展定期备份和验证：即，应对照信息系统数据恢复点目标，做好生产环境业务数据冗余备份，定期验证冗余备份业务数据的可用性。

(4) 数据共享

根据《银行数据办法》第二十二条，数据处理者向其他数据处理者提供、委托处理、共同处理重要数据前，应当依照法律、行政法规和中国人民银行相关规定进行风险评估。除履行法定职责或者法定义务外，数据处理者向其他数据处理者提供核心数据达到国家规定情形的，在提供业务数据之前应当经中国人民银行报国家数据安全工作协调机制开展风险评估。

此外，根据《银行数据办法》第二十一条，向其他数据处理者提供业务数据涉及个人信息和重要数据的，应当在合同或者协议中明确各自的数据安全保护义务，需要采取的安全保护措施，数据提供的目的、方式、范围，数据允许存储时限，数据提供至第三方的限制和数据安全事件告知义务，并对数据接收方履行约定义务的情况进行监督。

(三) 安全评估与合规审计

(1) 风险评估

根据《银行数据管理办法》第四十二条，重要数据的处理者应当自行或者委托第三方评估机构，每年对业务数据开展一次风险评估，并于每年 1 月 15 日前向中国人民银行或者住所地中国人民银行省级分支机构报送上一年度风险评估报告。

(2) 合规审计

根据《银行数据管理办法》第四十五条，数据处理者应当对照法律、行政法规和《银行数据管理办法》所列安全保护措施要求，以及本机构业务数据安全相关管理制度和操作规程的执行情况，每三年至少开展一次业务数据安全合规审计。重要数据的处理者应当每年至少开展一次与重要数据安全相关的合规审计。发生重大或者特别重大事件后，应当开展专项审计。

四. 业务数据技术安全要求

根据《银行数据管理办法》，金融机构在技术安全方面需要遵循以下合规要点:

1. 权限管理

根据《银行数据管理办法》第二十九条，金融机构应当加强访问控制，采取有效技术措施管控业务数据处理账号的数据使用权限，明确特权账号的使用场景并加强使用时的内部审批授权。使用特权账号实施业务数据新增、删除、修改等人工操作时应当逐一开展事前审批和事后审查。使用特权账号开展自动化操作前应当对操作正确性和安全性进行必要检查。此外，还应加强安全认证，保障业务数据处理账号和特权账号认证口令的强度，限制验证失败重试次数，可使用高敏感性数据项的账号应当支持多因素认证或者二次授权确认，并建立超时退出、访问通信地址变化等情形的重新验证机制。

2. 存储安全

根据《银行数据管理办法》第三十二条，金融机构应当针对业务数据存储活动采取下列安全保护措施:

(1) 有效隔离信息系统开发测试环境与生产环境。
(2) 存储重要数据的信息系统应当满足三级网络安全等级保护要求，存储核心数据的信息系统应当满足四级网络安全等级保护要求或者关键信息基础设施保护要求，并优先采购安全可信的网络产品和服务。
(3) 原则上高敏感性数据项须加密存储，确需不加密存储的，应当统一规范管理相关需求场景。
(4) 及时评估并调整业务数据存储承载容量，对照信息系统数据恢复点目标，做好生产环境业务数据冗余备份，定期验证冗余备份业务数据的可用性。

3. 传输与接入安全

根据《银行数据管理办法》第三十五条，金融机构应当针对业务数据传输活动采取下列安全保护措施:

(1) 优先采取专用线路、虚拟专用网等技术加强业务数据传输安全保护。
(2) 健全访问控制和安全隔离策略，加强相关终端设备准入控制。
(3) 原则上高敏感性数据项须加密传输至其他数据处理者、其他数据中心或者互联网。确需不加密传输的，应当统一规范管理相关需求场景。
(4) 及时评估并调整通信线路的传输承载容量，加强通信线路和相关软硬件设备的冗余备份。

4. 脱敏技术

根据《银行数据管理办法》第三十三条，金融机构应当明确高敏感性数据项的脱敏处理策略，切实降低脱敏业务数据仍可识别至特定个人、组织的风险。此外，数据处理者应当建立终端设备安全管控策略，明确安全防护措施要求。业务数据展示、打印时应当采取技术措施标识当前使用业务数据的业务处理账号和使用时间。

5. 风险监测

根据《银行数据管理办法》第三十九条，金融机构应当加强业务数据处理活动风险监测，有效识别下列风险并立即采取补救措施:

(1) 存在法律、行政法规禁止发布传输的信息。
(2) 存在计算机病毒、木马、勒索等恶意程序，数据安全漏洞、认证口令强度偏低等缺陷。
(3) 高敏感性数据项安全保护措施失效。
(4) 异常的业务数据处理活动。
(5) 业务数据传输或者存储承载能力不足。

如您希望就相关问题进一步交流，请联系：

杨 迅
+86 21 3135 8799
xun.yang@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 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野

免责声明：
本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2025