中国人民银行业务领域数据安全管理办法

（2025 年 5 月 1 日中国人民银行令〔2025〕第 3 号公布 自 2025 年 6 月 30 日起施行）

《中国人民银行业务领域数据安全管理办法》已经 2025 年 4 月 2 日中国人民银行第 5 次行务会议审议通过，现予发布，自 2025 年 6 月 30 日起施行。

行　长　潘功胜

2025 年 5 月 1 日

中国人民银行业务领域数据安全管理办法

第一章 总　则

第一条 为规范中国人民银行业务领域数据的安全管理并促进开发利用，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国中国人民银行法》《网络数据安全管理条例》等法律、行政法规，制定本办法。

第二条 在中华人民共和国境内开展与中国人民银行业务领域数据相关的处理活动及其安全监督管理，适用本办法。其他有关主管部门有规定的，还应当依法遵守其规定。

本办法所称中国人民银行业务领域，指依据法律、行政法规，党中央、国务院决定，由中国人民银行承担监督和管理职责的业务领域。

本办法所称中国人民银行业务领域数据，指中国人民银行业务领域内产生和收集的不涉及国家秘密的网络数据（以下简称业务数据）。

本办法所称数据处理者，指金融机构以及经中国人民银行批

准设立或者认定的其他机构。

第三条 业务数据安全工作遵循“谁管业务，谁管业务数据，谁管数据安全”原则。中国人民银行对业务数据安全负指导监管责任。数据处理者应当履行数据安全保护义务，防范业务数据被篡改、破坏、泄露或者非法获取、非法利用等风险，保障国家安全、公共利益、个人及组织合法权益，尊重社会公德伦理，遵守商业道德和职业道德，保障业务数据依法有序自由流动。

第四条 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按照本办法开展业务数据安全监督管理工作，加强与其他有关主管部门间的数据安全监督管理协作配合、信息沟通。

相关金融行业协会应当加强自律管理，依法制定业务数据安全行为规范和团体标准，指导会员加强业务数据安全保护。

第五条 鼓励数据处理者积极开展业务数据安全创新应用，在保障安全合规前提下促进业务数据的高效流通和开发利用，鼓励在行业内推广优秀创新成果。

第二章 业务数据分类分级与总体要求

第六条 中国人民银行负责制定业务数据分类分级保护相关规范标准，指导业务数据分类分级保护工作，组织编制中国人民

银行业务领域重要数据目录并实施动态管理。

第七条 数据处理者应当建立健全业务数据分类分级制度和操作规程。业务数据分类分级实施应当遵循制度规程，分类分级结果应当履行内部审批程序。

第八条 数据处理者应当建立业务数据资源目录，并从业务关联性、敏感性和可用性方面分别做好业务数据分类：

（一）标识各数据项是否为个人信息、是否为外部收集产生、存储该数据项的信息系统清单和关联的业务类别。

（二）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。业务数据的结构化数据项应当逐一标识敏感性，业务数据的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标识的最高敏感性，标识其敏感性。中国人民银行业务领域内的敏感个人信息、可能涉及商业秘密的客户经营信息、应当严格控制知悉范围的业务信息等，应当标识为高敏感性数据项。

（三）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。

第九条 按照国家有关规定，将业务数据分为一般数据、重

要数据、核心数据三级。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，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。

中国人民银行按照国家有关规定组织确定重要数据具体目录，数据处理者应当准确识别、申报本机构存储的全量业务数据是否属于重要数据、核心数据，并填报重要数据具体目录内容。

中国人民银行汇总形成重要数据具体目录，经国家数据安全工作协调机制审定后，确定重要数据的处理者并告知其对应的重要数据。

除单独说明的情形外，本办法所列重要数据的保护义务，均适用于核心数据。

第十条 数据处理者应当每年至少更新一次业务数据资源目录，完整准确记录信息系统所存储数据项和对应标识内容。

第十一条 数据处理者应当切实履行业务数据安全保护责任，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，细化业务数据安全保护

奖惩规程。

面向社会提供产品、服务的数据处理者应当建立便捷的投诉、举报渠道，及时受理并处理业务数据安全有关投诉、举报。

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。管理机构应当切实履行法律、行政法规已明确的各项责任。业务数据的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。

第十二条 数据处理者应当建立健全全流程业务数据安全管理制度，结合业务数据分类分级明确差异化的安全保护措施，制定业务数据处理活动操作规程和业务数据安全相关内部审批授权规程，明确操作实施和审批授权记录的留存要求。

不同敏感性数据项在同一个业务数据处理活动中被处理，且难以采取差异化安全保护措施的，应当采取高敏感性数据项对应的安全保护措施。

第十三条 数据处理者应当根据岗位分工，制定业务数据安全年度培训计划，每年组织业务数据处理活动参与人员开展相关教育培训。培训内容应当包括与业务数据安全相关的制度标准、风险防范常识、岗位责任、保护措施和事件应急处置要求。

第三章 全流程业务数据安全管理要求

第十四条 数据处理者应当严格管理处理业务数据相关信息系统数据库管理员账号等特权账号和各类业务处理账号的权限，人员变动时应当立即调整权限。数据处理者应当与可使用高敏感性数据项账号的人员签订保密协议。

数据处理者存储核心数据的，应当对业务数据的安全负责人和可使用核心数据的关键岗位人员进行安全背景审查。

第十五条 数据处理者收集业务数据应当采取下列安全保护管理措施：

（一）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，收集业务数据时应当依照法律、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。

（二）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。数据提供方未取得个人书面同意或者组织书面授权的，还应当要求其出具业务数据来源依法合规和数据真实性的必要佐证材料。

（三）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，按照相关管理要求留存业务

数据收集原始凭证。

（四）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。

（五）按照与数据提供方合同或者协议中约定的处理目的、方式、范围以及安全保护义务等开展收集和后续的业务数据处理活动。

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。除履行法定职责或者法定义务外，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，数据处理者应当统一规范管理相关需求场景。

第十七条 业务数据使用活动中，数据处理者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。确需采取导出方式使用高敏感性数据项或者采取其他方式使用用于身份鉴别的数据项的，数据处理者应当统一规范管理相关需求场景。

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，数据处理者原则上须实施脱敏处理后再展示高敏感性数据项。确需不脱敏展示的，数据处理者应当统一规范管理相关需求场景。

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；需要训练业务数据的，应当审查训练业务数据的真实性、准确性、客观性、多样性；需要标注业务数据的，应当抽样审查标注的合理性与准确性；需要建立模型评价激励规则的，应当审查评价激励规则是否尊重社会公德伦理、遵守商业道德和职业道德。

业务数据加工活动中，数据处理者加工高敏感性数据项的，应当进一步明确应当采取的安全保护措施，并履行内部审批程序；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。

第十九条 对于业务数据加工活动产生新数据项，经评估其敏感性明显低于加工所使用数据项的，数据处理者可遵循规程降低其敏感性标识，促进依法合规开发利用。

对于业务数据加工活动产生新数据项，经评估其敏感性明显高于加工所使用数据项的，数据处理者应当提高其敏感性标识，并加强业务数据安全保护。

第二十条 除根据个人请求向其传输与其相关业务数据外，数据处理者原则上不使用邮件、即时通讯、在线文件存储等互联

网信息服务或者移动介质传输高敏感性数据项。确有需要的，数据处理者应当统一规范管理相关需求场景。

第二十一条 从事业务所需的业务数据提供活动，数据处理者应当核验数据接收方身份，并采取下列安全保护管理措施：

（一）对于涉及个人信息的业务数据提供活动，应当评估是否遵守法律、行政法规要求。对于其他业务数据提供活动，应当评估是否符合保守商业秘密的约定。

（二）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）按照约定做好业务数据清洗转换，对提供数据的真实性作必要审查，不得误导数据接收方。

（四）除委托处理情形外，原则上不采取导出方式向其他数据处理者提供高敏感性数据项，用于身份鉴别的数据项原则上须采取核验方式提供。确需采取导出方式提供高敏感性数据项或者采取其他方式使用用于身份鉴别的数据项的，数据处理者应当统一规范管理相关需求场景。

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，并重点评估数据接收方数据处理目的和方式的合法正当性、数据项列表的需求合理性、数据活动的潜在安全风险、数据接收方诚信守法情况、合同或者协议内容的完备性、拟采取的安全保护措施等。

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。数据处理者不得通过拆分、转换等手段规避上述义务。

重要数据的处理者因合并、分立、解散、破产等可能影响重要数据安全的，应当依照法律、行政法规要求，事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告重要数据处置方案，在方案中说明重要数据目录内容更新情况、数据接收方的名称或者姓名和联系方式等。

第二十三条 数据处理者采用隐私计算等技术促进业务数据融合创新应用的，应当落实本办法第二十一条第一项至第三项要求，并确认除本机构外其他数据处理者无法使用未加密原始数据、与其他数据融合创新应用活动作关联分析无法泄露约定范围

外的信息。

第二十四条 数据处理者因业务等需要向中华人民共和国境外提供数据，存在国家网信部门规定情形的，应当严格遵守其有关规定；法律、行政法规和中国人民银行相关规定有境内存储要求的，业务数据还应当同时在中华人民共和国境内存储。

符合国家网信部门规定应当申报数据出境安全评估或者开展保护认证等情形的，数据处理者不得对业务数据采取拆分、转换等手段规避相关义务。

第二十五条 中国人民银行根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国金融执法机构关于提供业务数据的请求。

第二十六条 数据处理者应当审核业务数据公开活动的目的、数据项列表、渠道、时限和脱敏处理情况，分析研判可能产生的不利影响，审查业务数据的合法性、真实性，并通过本机构明确的官方渠道公开业务数据。确需通过其他渠道公开的，应当明确采用的安全保护措施并履行内部审批程序。

业务数据处理活动中，数据处理者不得公开用于身份鉴别的数据项，公开其他高敏感性数据项原则上须作脱敏处理。确需不作脱敏处理的，数据处理者应当统一规范管理相关需求场景。

第二十七条 数据处理者应当依照法律、行政法规和中国人民银行相关规定，主动删除处理目的已实现、处理目的无法实现、为实现处理目的不再必要或者约定保存期限已届满等情形的业务数据。

删除业务数据从技术上难以实现的，数据处理者应当停止除存储和采取必要的安全保护措施之外的业务数据处理活动，并每年至少实施一次审查，确认相关业务数据不可被使用。

第二十八条 数据处理者委托处理业务数据，除落实本办法第二十一条第二项要求外，还应当在合同或者协议中明确受托人需报告的重要事项、委托处理事项完成后传输和删除业务数据的实施方式与时限要求、配合本机构监督其委托处理活动等义务，并采取定期评估等方式监督受托人履约情况。涉及核心数据的委托处理活动，数据处理者应当事前对受托人开展尽职调查，进一步加强对其的监督。

数据处理者应当将业务数据委托处理活动纳入业务或者信息科技外包管理体系，加强风险管理。

中国人民银行已明确要求不得以外包形式开展业务的，相关业务数据不得委托处理。

第四章 全流程业务数据安全技术要求

第二十九条 数据处理者应当加强访问控制，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。

数据处理者应当加强安全认证，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。

第三十条 数据处理者应当规范日志记录，明确业务数据处理活动日志记录信息，满足数据安全风险溯源和事件处置需要。

业务数据处理活动日志记录高敏感性数据项原则上须经脱敏处理。确需不脱敏处理的，数据处理者应当统一规范管理相关需求场景。

数据处理者应当将业务数据处理活动日志纳入业务数据分类分级管理，落实安全保护要求。

数据处理者应当留存业务数据处理活动日志至少六个月；对于与存储重要数据信息系统相关的业务数据处理活动日志，应当

留存至少一年；对于与存储核心数据信息系统相关的业务数据处理活动日志，应当留存至少三年。

数据处理者向其他数据处理者提供、委托处理个人信息、重要数据的业务数据处理活动日志等记录，应当留存至少三年。

第三十一条 数据处理者应当优先采用直接录入或者信息系统间交互的方式收集业务数据。采用直接录入方式收集业务数据的，应当验证录入人身份；采用信息系统间交互方式收集高敏感性数据项的，应当验证数据提供方身份。

数据处理者应当采取关联信息交叉核验等技术措施，尽可能保障收集业务数据的准确性。

数据处理者采用自动化工具方式从其他数据处理者收集业务数据的，应当遵守其数据收集的控制规则，不得干扰网络服务正常运行，不得侵害其他机构网络服务合法运营权益。

第三十二条 数据处理者应当针对业务数据存储活动采取下列安全保护措施：

（一）有效隔离信息系统开发测试环境与生产环境。

（二）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。

（三）原则上高敏感性数据项须加密存储，确需不加密存储的，数据处理者应当统一规范管理相关需求场景。中国人民银行对业务数据存储有使用商用密码保护特别规定的，按照其规定执行。

（四）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，按照中国人民银行要求定期验证冗余备份业务数据的可用性。评估备份技术措施是否具备防范生产环境业务数据和冗余备份业务数据同时遭到篡改、破坏等风险的能力，并针对性加强安全保护措施。

第三十三条 数据处理者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。

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。

除开发测试环境与生产环境业务数据安全保护措施完全一致的情形外，生产环境数据项用于开发测试环境的，应当履行内部审批程序并实施脱敏处理。

第三十四条 数据处理者应当建立业务数据加工算法风险评估和控制策略，明确可解释性、脆弱性等风险对应的防范或者缓释措施和停止使用加工算法开展自动化决策时的替代方案。

第三十五条 数据处理者应当针对业务数据传输活动采取下列安全保护措施：

（一）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。

（二）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。

（三）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，数据处理者应当统一规范管理相关需求场景。中国人民银行对业务数据传输有使用商用密码保护特别规定的，按照其规定执行。

（四）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。

第三十六条 数据处理者应当动态维护本机构提供业务数据的前置网关和应用程序接口清单，并在前置网关和应用程序接口变更投产前开展安全测试，发现风险隐患立即采取补救措施。

数据处理者采用隐私计算等技术提供业务数据的，应当建立

技术风险评估和控制策略，明确安全不可验证、性能不可接受等风险的应对措施。

第三十七条 数据处理者应当制定本机构公开的业务数据是否允许自动化工具收集的控制规则，并采取必要技术措施保障公开的业务数据不被篡改。

第三十八条 数据处理者应当明确业务数据存储介质销毁策略，规范销毁实施方式和过程监督程序。

第五章 业务数据安全风险与事件管理

第三十九条 数据处理者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：

（一）存在法律、行政法规禁止发布传输的信息。

（二）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。

（三）高敏感性数据项安全保护措施失效。

（四）异常的业务数据处理活动。

（五）业务数据传输或者存储承载能力不足。

第四十条 数据处理者应当加强对业务数据泄露、业务数据被非法兜售、仿冒本机构身份处理业务数据，以及其他与本机构有关的业务数据安全负面舆情的风险监测，发现相关风险时应当

立即核实处置。

第四十一条 中国人民银行及其分支机构通报与业务数据相关的数据安全缺陷、漏洞等风险时，数据处理者应当立即核实处置，并根据通报要求按时准确反馈情况。

鼓励数据处理者向中国人民银行及其分支机构提供具有行业共享价值的业务数据安全风险情报。

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。除法律、行政法规已明确应当评估的内容外，风险评估报告还应当包含与存储重要数据信息系统相关的人员培训与日常管理情况，与业务数据相关的岗位职责落实情况、网络安全等级保护测评和整改情况、保护措施执行情况、本年度风险监测和事件处置情况，以及中国人民银行要求的其他评估内容。

第四十三条 数据处理者应当按照国家网络安全事件应急预案有关事件分级要求，综合考虑影响范围和程度，明确业务数据安全事件对应的分级标准：

（一）业务数据被篡改、破坏事件分级的标准应当考虑信息

系统数据恢复点目标、无法正常提供服务时长、受影响业务笔数和金额、受影响个人或者组织数量、损失的不同敏感性数据项和对应规模等因素。

（二）业务数据泄露事件分级的标准应当考虑受影响个人或者组织数量、泄露的不同敏感性数据项和对应规模等因素。

（三）涉及核心数据、重要数据泄露或者被篡改、破坏的安全事件，应当分别分级为特别重大事件、重大事件。

第四十四条 数据处理者应当做好业务数据安全事件分级，发生业务数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并按照中国人民银行要求及时、准确、完整报告事件情况。

数据接收方、委托处理受托人发生与数据处理者所提供业务数据相关的数据安全事件的，数据处理者应当开展调查评估，督促相关机构立即采取补救措施并向有关主管部门报告。

重要数据的处理者应当每年至少开展一次针对业务数据安全事件的应急演练，其他数据处理者应当每三年至少开展一次针对业务数据安全事件的应急演练。

第四十五条 数据处理者应当对照法律、行政法规和本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。审计应当重点关注业务数据资源目录是否及时更新、相关信息系统账号权限管理是否严密、业务数据处理活动相关合同或者协议是否完备、高敏感性数据项安全保护措施是否有效、数据委托处理受托人管理职责是否落实、前置网关和应用程序接口是否持续安全维护、数据安全风险监测是否有效、数据安全风险与事件处置是否及时、数据出境是否合规、数据安全投诉处理是否及时等情况。

第四十六条 数据处理者应当加强风险评估人员和审计人员使用业务数据权限的管理，采取必要措施确保实施过程的业务数据安全。

与业务数据相关的风险评估报告和审计报告记录高敏感性数据项时应当进行脱敏处理。

数据处理者委托第三方评估机构、审计机构开展与业务数据相关的风险评估或者审计工作的，应当在合同或者协议中明确其数据安全保护义务和对应责任，指定本机构人员全程参与。涉及会计审计服务的，还应当按照国家网信部门和财政部门要求，进

一步加强相关业务数据安全保护。

第六章 法律责任

第四十七条 中国人民银行及其分支机构发现数据处理者的业务数据处理活动存在较大安全风险时，可以对其进行约谈和要求其采取措施进行整改；发现影响或者可能影响国家安全的业务数据处理活动线索时，可以要求数据处理者按照国家有关规定进行国家安全审查。

中国人民银行及其分支机构按照职责可以对数据处理者与业务数据相关的数据安全保护义务落实情况开展执法检查，必要时可以与其他有关主管部门联合实施执法检查。

第四十八条 中国人民银行及其分支机构发现数据处理者在业务数据处理活动中未履行数据出境安全评估或者保护认证等义务的，应当将相关案件信息移送同级网信部门，并配合其予以处理。

第四十九条 数据处理者未履行本办法规定的数据安全保护义务，有下列情形之一的，中国人民银行及其分支机构依照《中华人民共和国数据安全法》第四十五条予以处罚：

（一）未依照法律、行政法规对应规定，建立健全全流程业务数据安全管理制度的。

（二）未依照法律、行政法规对应规定，组织开展业务数据安全教育培训的。

（三）未依照法律、行政法规对应规定，采取相应的技术措施和其他必要措施，保障业务数据安全的。

（四）重要数据的处理者未明确业务数据安全负责人和管理机构的。

（五）未有效监测业务数据安全风险的。

（六）发现业务数据安全风险未立即采取补救措施的。

（七）发生业务数据安全事件未立即采取处置措施，未及时告知用户，或者未按照要求报告事件情况的。

（八）重要数据的处理者未每年对业务数据开展一次风险评估，或者未按照要求报送风险评估报告的。

第五十条 中国人民银行及其分支机构发现数据处理者开展业务数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照相关法律、行政法规予以处理，属于其他有关主管部门管理职责的，移送相关案件信息并配合其予以处理。

第五十一条 中国人民银行及其分支机构发现数据处理者开展业务数据处理活动，涉嫌构成违反治安管理行为或者构成犯罪的，将相关案件信息移送同级公安机关、国家安全机关等有关主

管部门，并配合其予以处理。

第五十二条 数据处理者发生业务数据安全事件造成危害后果，如能证明本机构已按照规定采取数据安全保护措施，并立即采取补救措施的，应当对其从轻或者减轻行政处罚。

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，应当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，从轻或者减轻行政处罚。

第五十三条 中国人民银行及其分支机构工作人员在业务数据处理活动的安全监督管理过程中存在玩忽职守、滥用职权、徇私舞弊情形的，依法给予处分。

第七章 附 则

第五十四条 术语定义：

（一）数据项，是指描述网络数据结构最基本的、不可分割的单位。

（二）结构化数据项，是指具有预定义的抽象描述数据类型，通常为使用数据库二维逻辑表单一字段指代的数据项。

（三）非结构化数据项，是指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。

（四）终端设备，是指数据处理者在业务数据处理活动中所

用的计算机终端、移动智能终端、音视频和多媒体设备、其他专用终端设备。

（五）导出方式，是指数据使用或者提供活动中，将原本具有严格访问权限控制和访问日志记录的业务数据，转换成未实施严格访问控制或者无访问日志记录的文档文件的操作方式。

（六）核验方式，是指业务数据使用或者提供活动中，经核实验证后，仅反馈与存储业务数据是否匹配的操作方式。

（七）统一规范管理，是指数据处理者在本机构制度或者操作规程中对不执行本办法所提原则性合规要求的情形予以集中列举，并说明保留此类情形的必要性、对应需采取的安全保护措施和需履行的必要内部审批程序。

第五十五条 本办法由中国人民银行负责解释。

第五十六条 本办法自 2025 年 6 月 30 日起施行。