中国人民银行业务领域数据安全管理办法（征求意见稿）

第一章 总则

第一条（目的和依据）为规范中国人民银行业务领域数据的安全管理，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》《中华人民共和国中国人民银行法》等有关法律、行政法规，制定本办法。

第二条（适用范围）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，适用本办法。法律、行政法规或者中国人民银行另有规定的，从其规定。

本办法所称中国人民银行业务领域数据，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，以下简称数据。

第三条（管理原则与目标）数据安全工作遵循“谁管业务，谁管业务数据，谁管数据安全”基本原则。开展数据处理活动应当履行数据安全保护义务，采取有效措施防范数据被篡改、破坏、泄露、不当获取与利用等风险，确保不损害国家安全、公共利益、金融秩序、个人及组织合法权益，遵

守社会公德伦理、商业道德和职业道德。

第四条（协同监督管理）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。

中国银行间市场交易商协会、中国支付清算协会、中国互联网金融协会等金融行业协会应当加强自律管理，建立便捷的投诉、举报渠道，反映会员合理的数据安全意见建议。

第二章 数据分类分级

第五条（数据分类分级保护总体规划）中国人民银行负责组织制定数据分类分级相关行业标准，指导数据处理者开展数据分类分级各项工作，统筹确定重要数据具体目录并实施动态管理。

第六条（数据分类分级制度规程）数据处理者应当建立健全本单位数据分类分级实施制度，规范分类分级工作操作规程。数据分类分级过程实施和结果审批，应当严格遵循操作规程。

第七条（数据分类要求）数据处理者应当参考行业标

准，根据业务开展情况建立业务分类，梳理细化数据资源目录，标识各数据项是否为个人信息、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。

第八条（数据分级要求）数据按照精度、规模和对国家安全的影响程度，分为一般、重要、核心三级。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。数据处理活动中，数据处理者还应当及时准确识别判定所涉及数据是否属于重要数据、核心数据。

第九条（数据敏感性分层级）在数据分级基础上，数据处理者应当参考行业标准，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。结构化数据项应当逐一标识层级；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。

第十条（数据可用性分层级）数据可用性分层级工作纳入信息系统业务连续性分级保障体系统一考虑。数据处理者应当评估信息系统存储数据遭到篡改、破坏后可能对业务连续性造成的影响程度，明确恢复点目标要求。恢复点目标越

严格，数据的可用性层级越高。在此基础上，鼓励数据处理者识别用于支撑最基本业务运转、无法承受彻底灭失风险、需要进一步进行容灾备份的数据。

第十一条（动态更新要求）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。

第三章 数据安全保护总体要求

第十二条（责任落实总体要求）数据处理者应当明确其数据安全管理相关内设部门职责分工，配备足够数量的数据安全管理人员，并细化各类违规数据处理活动的定责问责规程，压实数据安全保护责任。重要数据的处理者还应当书面明确数据安全负责人和数据安全牵头管理内设部门。

第十三条（全流程安全管理制度要求）数据处理者应当建立健全全流程数据安全管理制度，结合数据分类分级结果，明确差异化的安全保护管理和技术措施要求，并制定数据处理活动操作规程，规范各类内部审批和授权流程。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。与母公司、子公司、关联公司或者附属公司等具有关联关系的数据处理者合作开展数据处理活动时，不得降低安全保护管理和技术措施要求。

第十四条（安全培训总体要求）数据处理者应当根据岗位分工，制定数据安全年度培训计划，组织开展相关教育培训，并对培训结果进行评价。培训内容应当包括：

（一）数据安全相关法律、行政法规、部门规章、国家和金融行业标准、内部规定、行为准则和职业操守；

（二）不同岗位的数据安全责任，失职失责或者违法违规数据处理活动应当承担的后果；

（三）针对性的数据安全保护管理和技术措施要求，以及对应的操作规程；

（四）数据安全事件应急处置规程。

第十五条（鼓励创新）鼓励数据处理者积极开展数据安全技术创新应用，在保障安全合规前提下，积极促进数据的高效流通和创新应用，鼓励优秀创新成果申报行业表彰奖励。

第四章 数据安全保护管理措施

第十六条（人员管理要求）数据处理者应当按照最小必

要和职责分离原则，严格管理信息系统各类业务处理账号、数据库管理员等特权账号的设立和权限，人员变动时应当及时调整权限或者收回账号。

数据处理者应当加强账号身份认证管理，可使用第二层级以上数据项的账号应当支持身份验证。可使用第三层级以上数据项的账号应当支持多因素认证或者实现二次授权，相关账号使用人员应当签署保密协议。

第十七条（数据收集保护管理措施要求）数据处理者收集数据应当遵循合法、正当原则，并采取下列安全保护管理措施：

（一）除法律、行政法规明确无需说明的情形外，应当在隐私政策协议或者合同协议中以显著方式、清晰易懂的语言说明数据收集的目的、范围、方式、存储期限，以及数据来源不合法、数据不真实情形对应的违约责任；

（二）接受其他数据处理者委托协助收集数据时，应当通过合同协议与其约定，是否需要代其向相关个人、组织说明委托关系；

（三）非直接面向个人、组织收集数据时，应当要求数据提供方依照法律、行政法规取得个人、组织的同意，对于非书面同意情形，应当要求其出具数据来源说明材料，并依据材料评估其合法性、真实性；

（四）应当针对数据合法性、真实性存疑等情形，明确

业务暂停使用相关数据时的应急处置方案；

（五）应当优先采用数据提供方直接录入或者信息系统间交互的方式收集数据；

（六）因履行无障碍义务或者客观条件限制，采用纸质文件、影像或者代为手工录入等方式收集数据时，应当采取自动识别、人工核验等措施，保障数据录入的及时性和准确性，并按照档案管理要求保存原始数据收集凭证；

（七）停止提供其产品服务，合同协议履约终止或者响应个人、组织合法权益要求时，应当主动停止数据收集活动；

（八）保存数据收集行为对应的合同协议、内部审批记录、数据提供方出具的数据来源说明材料和对应评估结论等信息至少三年。

第十八条（数据存储保护管理措施要求）数据处理者应当根据业务需要，明确数据存储期限。除履行法定职责或者法定义务所必需外，第三层级以上数据项原则上不得在终端设备和移动介质中存储。确需存储的，数据处理者在履行内部审批程序基础上，应当统一明确需在终端设备和移动介质中存储的特定场景、支持此类场景的必要性、应当采取的风险防范措施，并据此开展。风险防范措施至少应当包括仅在授权的终端设备和移动介质中存储，存储期限不得超过审批允许的期限。

数据处理者应当保存终端设备、移动介质中存储第三层

级以上数据项行为的目的说明、内部审批记录、授权设备或者介质识别编号、允许存储期限等信息至少三年。

第十九条（数据使用保护管理措施要求）第三层级数据项原则上不提供导出使用方式，第四层级以上数据项原则上仅提供核验使用方式，确需提供其他使用方式时，应当说明相关必要性，经内部审批并明确对应的风险防范措施后，据此开展。涉及第三层级以上数据项导出使用的风险防范措施，原则上应当优先采取加密、数字水印或者脱敏处理等安全保护措施，确需未经安全保护即导出的，数据处理者应当统一明确相关导出需求场景，并据此开展。

除面向个人、组织展示其数据，履行法定职责或者法定义务必需展示数据的两类情形外，信息系统界面展示第三层级以上数据项时，原则上应当优先实施脱敏处理后再展示。确需明文展示的，数据处理者应当统一明确相关展示需求场景、支持此类场景的必要性和应当采取的风险防范措施，并据此开展。

第二十条（数据加工保护管理措施要求）数据加工前，数据处理者应当审查加工目的与收集约定是否一致，确保数据加工不以垄断经营和不正当竞争为目的，不发生误导、欺诈、胁迫或者干扰等限制个人或者组织正当选择与决策的行为，遵循社会公德伦理。第四层级以上数据项加工，应当经内部审批并明确对应的风险防范措施后，据此开展。

基于加工生成的数据项面向个人提供自动化决策服务时，应当以适当方式说明加工目的、加工依赖数据基本情况和加工基本逻辑，提升决策的透明度。

数据处理者应当保存数据加工行为目的说明、内部审查审批记录、审查对应的加工应用程序源代码、新产生数据项列表等信息至少三年。

第二十一条（促进数据开发利用）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，可视情降低敏感性层级，促进数据依法合规开发利用。

第二十二条（数据传输保护管理措施要求）除履行法定职责或者法定义务所必需外，数据处理者原则上不得采用互联网邮件、即时通讯、在线文件传输、交互性信息服务等互联网信息服务或者通过移动介质交换传输第三层级以上数据项，确有需要的，数据处理者应当统一明确相关传输需求场景、支持此类场景的必要性和应当采取的风险防范措施，并据此开展。

第二十三条（一般性数据提供保护管理措施要求）数据处理者应当针对自身业务开展所需的数据提供行为采取下列安全保护管理措施：

（一）涉及个人信息的数据提供行为，应当评估确认遵

守有关法律、行政法规的规定。其他数据提供行为，应当评估确认不违反与相关组织间事前约定的有关保守商业秘密要求；

（二）通过合同协议方式与数据接收方约定数据提供的目的、方式、范围、规模、允许存储时限、将数据再转移提供至第三方的限定条件，要求接收方及时告知可能发生的数据泄露事件，明确各方数据安全保护责任和至少应当采取的安全保护措施；

（三）向个人、组织提供其数据时，可视情简化合同协议签订和对应内部审批要求，但应当先行核实其身份的真实性；

（四）对于委托处理情形，在合同协议中进一步明确委托处理受托人重要事项报告、及时返还和删除数据的实施方式、接受并配合数据处理者监督其委托处理活动等义务；

（五）有效监督委托处理受托人履约情况，定期评估确认其数据处理活动符合事前约定，并已采取承诺的全部安全保护措施；

（六）对于委托处理以外情形，第三层级数据项应当优先通过查询、固定报表和核验方式向其他数据处理者提供，第四层级以上数据项应当优先通过核验方式向其他数据处理者提供，确需以其他方式提供的，在履行内部审批程序基础上，数据处理者应当统一明确相关提供需求场景、支持此

类场景的必要性和应当采取的风险防范措施，并据此开展；

（七）切实保障提供数据的质量，对提供数据真实性作必要核验，按照约定格式做好数据清洗转换，不得提供虚假数据误导数据接收方、合作方；

（八）保存数据提供行为评估记录、内部审批记录、对应的合同协议内容、监督过程中识别的风险及整改处置情况等信息至少三年。

第二十四条（特殊性数据提供保护管理措施要求）数据处理者向其他数据处理者提供重要数据前，应当依照法律、行政法规要求，说明重要数据的具体信息，从数据接收方数据处理目的方式和范围的合法正当必要性、潜在安全隐患、数据接收方诚信守法和背景情况、合约协议完备性和拟采取的安全保护管理和技术措施等方面做好风险评估并保存报告至少三年。在此基础上，数据处理者还应当通过法律、行政法规明确规定的安全评估。

数据处理者向其他数据处理者提供核心数据前，还应当提请国家数据安全工作协调机制办公室批准。除履行法定职责或者法定义务所明确情形外，数据处理者不得通过拆分等方式规避上述义务。

数据处理者因合并、分立、解散、被宣告破产等原因需要转移数据的，应当通过公告等方式将数据接收方信息告知相关个人、组织，并评估确认不违反与相关组织间事前约定

的有关保守商业秘密要求。重要数据的处理者发生合并、分立、解散或者申请重整、和解以及破产清算等情况时，法律、行政法规有明确要求的，应当事前向中国人民银行报告重要数据处置方案和数据接收方基本情况。

第二十五条（数据融合创新应用管理措施要求）数据处理者采用隐私计算等技术促进数据融合创新应用时，应当确认原始数据未离开自身控制范围，且多个数据提供行为关联后，暴露约定范围外信息的风险可控。

第二十六条（数据出境限制管理措施要求）数据处理者在中华人民共和国境内收集和产生的数据，法律、行政法规有境内存储要求的，应当在境内存储。

数据处理者因自身需要向境外提供数据，存在国家网信部门规定情形的，应当严格遵守其有关规定事前开展数据出境风险自评估并申报数据出境安全评估。数据处理者不得有意拆分、缩减出境数据规模以规避申报数据出境安全评估。

对于因自身需要的数据出境提供行为，数据处理者应当于每年1月底前测算或者估算其上两年内累计出境数据规模与范围，并保存测算估算结果和对应的境外接收方联系方式至少三年。涉及数据出境安全评估的，数据处理者还应当保存有效期内的数据出境风险自评估报告、数据出境安全评估申报书和评估结果。

第二十七条（国际组织和外国金融管理部门数据调取）

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，处理国际组织和外国金融管理部门关于提供数据的请求。非经中国人民银行和其他有关主管部门批准，数据处理者不得向其提供境内存储的数据。

第二十八条（数据公开保护管理措施要求）数据处理者应当履行内部审批手续，审核数据公开行为的目的、数据内容范围、渠道、时限和脱敏处理情况，分析研判可能产生的负面影响，并核验数据的合法性、真实性与有效性。数据公开渠道原则上应当为本单位统一明确的官方渠道。确有需要通过其他渠道公开的，应当经内部审批并明确对应的风险防范措施后，据此开展。

第二层级以上数据项公开时，数据处理者应当保存数据公开行为目的说明、日期、公开渠道、数据范围和内部审批记录等信息至少三年。

第三层级以上数据项原则上应当实施脱敏处理后再公开，数据处理者应当统一明确第三层级以上数据项确需未经脱敏处理即允许公开的特定需求场景、支持此类场景的必要性和应当采取的风险防范措施，并据此开展。

第二十九条（数据删除保护管理措施要求）涉及个人信息的数据，满足法律、行政法规规定应当删除情形时，数据处理者应当主动删除数据。其他数据已超过与组织约定的存

储时限，或者组织提出符合法律、行政法规规定的正当请求时，数据处理者应当主动删除数据。删除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处理。数据处理者应当每年至少对信息系统业务处理账号、特权账号实施一次核验，确认已停止除存储和必要安全保护措施之外处理的数据，不可被访问使用。

数据处理者发生解散、被宣告破产等情况时，合法合规完成自身需要的数据转移处理后，应当及时销毁全部数据存储介质。中国人民银行或其住所地分支机构依据法律、行政法规另有数据转移要求的，还应当按照要求将数据转移至指定接收方后再销毁数据存储介质。

第五章 数据安全保护技术措施

第三十条（账号权限保护技术措施要求）数据处理者应当采取有效技术措施，从严管控业务处理账号的数据使用权限，鼓励建设技术平台，采取统一认证、统一授权策略进一步加强管控。

数据处理者应当统一明确特权账号的使用场景，并通过内部审批授权，严格限定其使用。可使用第三层级以上数据项的特权账号，涉及人工操作的数据库表删除、修改等操作应当逐一进行事前审查和事后审计。

第三十一条（数据处理活动日志保护技术措施要求）数据处理者应当建立统一的日志规范，明确数据处理活动日志应当完整记录的溯源所需信息。第三层级数据项如需在数据处理活动日志中记录原则上应当实施脱敏处理，第四层级以上数据项原则上不记录。确有需要的，数据处理者应当统一明确相关日志记录需求场景、支持此类场景的必要性和应当采取的风险防范措施，并据此开展。

数据处理者应当将数据处理活动日志纳入数据分类分级管理，并落实对应的管理和技术措施要求。数据处理者应当妥善保存数据处理活动日志至少六个月。向其他数据处理者提供涉及个人信息的数据或者重要数据的行为，相关日志应当保存至少三年。

第三十二条（数据收集保护技术措施要求）采用直接录入方式收集第二层级以上数据项，应当核验录入人身份。采用信息系统间交互方式收集第三层级以上数据项，应当对数据提供方身份进行认证，并保障收集数据的完整性。

数据处理者应当采取关联信息交叉核验等技术措施，识别并规避数据项同一内容不合理映射至多个个人或者组织、不同数据项信息相互矛盾等问题，尽可能保障收集数据的准确性，避免损害个人、组织的合法权益。

数据处理者面向个人直接录入方式收集数据时，应当建立健全技术措施，识别法律、行政法规禁止发布或者传输的

信息。

数据处理者采用自动化搜集方式从其他数据处理者收集数据时，应当遵守其数据访问控制协议，不得干扰其网络服务正常运行，不得侵害其原有网络服务合法运营权益。

第三十三条（数据存储保护技术措施要求）数据处理者应当针对数据存储行为采取下列安全保护技术措施：

（一）有效隔离开发测试环境与生产环境数据存储设施设备；

（二）存储重要数据或者一百万人以上个人信息的信息系统应当落实三级以上网络安全等级保护要求，存储核心数据的信息系统应当落实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；

（三）除因业务影响、产业制约，并可提供详细分析报告情形外，应当优先采用商用密码技术对信息系统中第三层级以上数据项实施加密存储，结构化数据项在对数据库文件整体实施加密基础上鼓励进一步采用更细粒度的加密方式，非结构化数据项可仅对拆分的第三层级以上结构化数据项单独实施加密；

（四）按照业务连续性保障等级，加强信息系统数据冗余备份管理，对于恢复点目标要求小于十分钟的信息系统，每天至少验证一次最新冗余备份数据可被正常加载使用；对于其他信息系统应当逐一明确验证频率要求，据此定期验证

最新冗余备份数据可被正常加载使用。

鼓励数据处理者针对需要进一步容灾备份的数据，采取独立于信息系统灾难备份体系以外的备份技术措施。

第三十四条（数据使用保护技术措施要求）数据处理者应当统一明确第三层级以上数据项的脱敏处理策略，降低脱敏数据仍可识别至个人、组织的风险。

数据处理者应当采取数字水印等措施，标识信息系统当前数据使用账号、时间等信息，并在展示后及时清除缓存信息，提升数据展示、打印等使用过程的安全防护和溯源能力。

数据处理者应当建立终端设备安全管控策略，鼓励针对使用第三层级以上数据项的终端，采取安全沙箱、终端行为管控等安全保护措施。

生产环境第二层级以上数据项原则上应当经授权并实施脱敏处理后才能用于开发测试，确需不经脱敏处理即用于开发测试的，数据处理者应当履行内部审批手续，并采取与生产环境一致的安全保护管理和技术措施，确保开发测试数据安全。

第三十五条（数据加工保护技术措施要求）数据处理者应当建立统一的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缓释措施以及退出算法自动化决策的替代方案。

第三十六条（数据传输保护技术措施要求）数据处理者

应当针对数据传输行为采取下列安全保护技术措施：

（一）通过运营商网络传输第二层级以上数据项时，采取专用线路、虚拟专用网络、安全通信协议等安全保护措施；

（二）动态更新记录不同网络安全区域间正常数据传输对应的网络地址、网络协议通信映射关系，加强安全隔离与终端设备准入控制；

（三）第三层级以上数据项传输至其他数据处理者、传输至不同数据中心或者传输至运营商网络时，应当优先使用商用密码技术保障机密性，并根据业务需要使用商用密码技术加强完整性和抗抵赖性保障，未使用商用密码技术进行传输保护的，数据处理者应当统一明确相关传输需求场景、支持此类场景的必要性和应当采取的风险防范措施，并据此开展；

（四）在传输失败或者传输完成后，及时删除不必要的缓存数据；

（五）及时评估调整网络线路的传输承载容量，加强网络线路和相关软硬件设备的冗余备份。

第三十七条（数据提供保护技术措施要求）数据处理者应当针对数据提供行为采取下列安全保护技术措施：

（一）针对持续性数据提供行为建设较为集中的技术平台，并采用前置网关或者应用程序接口方式向其他数据处理者提供数据；

（二）提供从其他数据处理者收集获得的数据项，中国人民银行有明确需公开数据来源要求的，应当以显著方式标识来源；

（三）提供第三层级以上数据项时应当对数据接收方身份进行认证；

（四）采用隐私计算技术提供数据时，应当建立统一的技术风险评估和控制策略，明确安全可验证性、性能可接受性等风险对应的缓释措施；

（五）对于委托处理情形的数据提供行为，应当纳入信息科技外包管理体系统一管理。

第三十八条（数据公开保护技术措施要求）数据处理者应当明确自身已公开数据是否可被自动化搜集的数据访问控制协议，并采取有效技术措施，保障公开数据不被篡改。

第三十九条（数据删除保护技术措施要求）删除数据涉及数据存储介质销毁工作时，数据处理者应当建立统一的数据存储介质销毁策略，明确销毁技术方式和过程监督措施。存储第三层级以上数据项的存储介质不再使用并且离开数据处理者控制范围时，应当及时销毁。

数据处理者应当保存数据存储介质销毁日期、销毁介质识别编号、采取的销毁技术方式、操作执行及复核人等信息至少三年。

第六章 风险监测、评估审计与事件处置措施

第四十条（数据处理活动风险监测）数据处理者应当采取有效措施，强化数据处理活动安全风险监测和告警，推进违规数据处理活动阻断技术措施建设，及时做好风险隐患的溯源排查处置，并核验技术措施的有效性和可靠性。监测告警规则应当重点关注下列事项：

（一）收集、提供的数据存在恶意程序或者法律、行政法规禁止传输的信息；

（二）危害数据安全的漏洞；

（三）终端设备和移动介质未经授权存储第三层级以上数据项；

（四）识别到不明用途的数据存储网络地址；

（五）未授权的数据使用行为，发生时间、网络地址、频率、总量存在明显异常的数据使用行为；

（六）用户身份认证强度较弱；

（七）开发测试环境中使用未授权或者未经脱敏处理的生产环境数据；

（八）对第四层级以上数据项实施加工、提供等行为；

（九）异常的网络通信行为和非授权终端设备接入内部网络的行为；

（十）未经商用密码技术加密传输第三层级以上数据

项；

（十一）终端设备使用互联网邮件、公共即时通讯、互联网文件传输工具传输第三层级以上数据项或者打印第三层级以上数据项；

（十二）网络线路数据传输承载能力不足；

（十三）使用前置网关或者应用程序接口方式提供超出合同协议约定范围数据的异常行为；

（十四）违反数据访问控制协议的公开数据异常访问行为。

第四十一条（数据安全风险情报监测）数据处理者应当加强数据安全风险情报的监测，及时核实并做好必要的数据安全防范处置工作。监测规则应当重点关注下列事项：

（一）本单位非公开数据泄漏至互联网的情况；

（二）兜售本单位数据的情况；

（三）假冒本单位身份非法收集、公开数据，或者对本单位管理的数据进行造谣传谣的情况；

（四）与本单位或者具有关联关系的数据处理者相关的数据安全负面舆情信息；

（五）与本单位合作的数据接收方、委托处理受托人相关的数据安全负面舆情信息。

第四十二条（数据安全通报预警监测）数据处理者应当及时接收、核查和处置中国人民银行或其分支机构通报的数

据安全风险情报，并根据要求按时反馈核查处置结果。

鼓励数据处理者积极向中国人民银行或其分支机构提供可共享的数据安全风险情报，提升联防联控效能。

第四十三条（数据安全风险评估）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。

第四十四条（数据安全审计）数据处理者应当围绕全流程数据安全管理制度和相关操作规程执行情况、数据安全相关投诉处理情况，每年至少开展一次与数据安全相关的合规审计。发生重大以上数据安全事件后，应当及时开展专项审计，督促数据处理活动过程留痕，安全保障责任落实到人。

第四十五条（数据安全风险评估与审计的安全保障）数据处理者应当细化管控数据安全风险评估人员和审计人员使用数据的权限，并采取有效措施确保实施过程安全。鼓励数据处理者建立技术平台，统一建立数据安全风险评估与审计的安全管控策略。

数据安全风险评估报告和审计报告不得记录第四层级以上数据项。报告保存期限不得短于实施过程中使用数据的存储期限，且最短不得低于三年。

委托检测机构、审计机构开展数据安全风险评估或者审计工作时，数据处理者应当在合同协议中明确其数据安全保护责任，并指定本单位人员全程参与评估。

第四十六条（数据安全事件定级判定）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，细化明确各等级数据安全事件对应的定级判定标准：

（一）对于数据被篡改、破坏的事件，定级标准应当考虑不同业务连续性保障等级信息系统无法正常服务的时长、影响的业务笔数与金额、影响的个人或者组织数量、损失的各敏感性层级数据项情况和对应数据规模、带来的舆情影响等；

（二）对于数据泄露事件，定级标准应当考虑涉及的个人或者组织数量、泄露的各敏感性层级数据项情况和对应数据规模、带来的舆情影响等；

（三）涉及核心数据、重要数据的安全事件，应当分别定级为特别重大事件、重大事件。

第四十七条（数据安全事件响应处置）数据处理者应当将数据安全事件纳入网络安全事件应急响应机制统一管理，制定相关应急预案，做好事件定级、处置、总结、报告、整改工作，按照规程向中国人民银行或其住所地分支机构、其他有关主管部门报告事件信息。

数据处理者应当每年至少开展一次针对数据安全事件的应急演练，确保应急处置措施的效率和效果。

合作的数据接收方、委托处理受托人发生与本单位所提供数据相关的数据安全事件时，数据处理者应当立即开展调查评估，督促其及时采取补救措施。

第七章 法律责任

第四十八条（监督管理责任履行）中国人民银行及其分支机构，按照管辖权对数据处理者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组织对数据处理者的执法检查。中国人民银行及其分支机构在执法检查过程中发现数据处理者的数据处理活动存在较大安全风险时，依照《中华人民共和国数据安全法》第四十四条予以处理；发现影响或者可能影响国家安全的数据处理活动线索时，应当及时报国家数据安全工作协调机制办公室，研判是否启动国家数据安全审查。

第四十九条（违反数据安全保护义务行为的处理）在本办法适用范围内，数据处理者未履行数据安全保护义务，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》第四十五条规定予以处理：

（一）未按照本办法第十二条规定，明确或者压实数据

安全保护责任；

（二）未按照本办法第十三条规定，建立健全全流程数据安全管理制度；

（三）未按照本办法第十四条规定，制定数据安全年度培训计划，未组织开展相关教育培训；

（四）除本办法第五十条、第五十一条规定情形外，未对应采取本办法第四章和第五章所规定的数据安全保护管理措施或者技术措施；

（五）未按照本办法第四十条、第四十一条规定，做好数据处理活动风险监测或者数据安全风险情报监测；

（六）未按照本办法第四十二条规定，接收、核查、处置和反馈中国人民银行或其分支机构通报的数据安全风险情报；

（七）重要数据的处理者未按照本办法第四十三条规定，每年组织开展一次全面的数据安全风险评估并按时报送风险评估报告；

（八）发生数据安全事件时，未按照本办法第四十七条规定，做好响应处置各项工作。

数据处理者未履行本办法提出的数据安全保护义务，其他有关法律、行政法规作出规定的，中国人民银行及其分支机构依照相关规定予以处理。

第五十条（违反规定数据出境行为的处理）中国人民银

行及其分支机构执法检查发现数据处理者未履行本办法第二十六条规定的数据境内存储义务，按照《中华人民共和国网络安全法》第六十六条规定和有关法律、行政法规的规定予以处理；发现数据处理者未履行本办法第二十六条规定的数据出境安全评估申报义务，将相关案件信息移送同级网信部门，并配合其依法依规予以处理。

第五十一条（违反规定向国际组织或者外国金融管理部门提供数据行为的处理）数据处理者未履行本办法第二十七条规定，未经中国人民银行和其他有关主管部门批准，向国际组织或者外国金融管理部门提供境内存储的数据时，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》第四十八条第二款规定予以处理；所提供数据涉及个人信息的，依照《中华人民共和国个人信息保护法》第六十六条规定予以处理。

第五十二条（非法获取数据行为的处理）中国人民银行及其分支机构执法检查发现数据处理者存在窃取或者以其他非法方式获取数据的行为时，将相关案件信息移送同级公安机关、国家安全机关，并配合其依法依规予以处理。

第五十三条（处理数据损害合法权益行为的处理）中国人民银行及其分支机构执法检查发现数据处理者开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照《中华人民共和国反不正当竞争法》《中华人民共和国

反垄断法》《中华人民共和国消费者权益保护法》等法律，将相关案件信息移送承担执法职责的有关主管部门，并配合其依法依规予以处理。

第五十四条（监督管理人员违反规定行为的处理）中国人民银行及其分支机构人员在监督管理过程中存在玩忽职守、滥用职权、徇私舞弊情形的，按照法律、行政法规规定给予处分；涉嫌犯罪的，依法移送监察机关或者司法机关处理。

第八章 附则

第五十五条（名词定义）术语定义：

（一）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据，表现形式为由一条或者多条信息记录组成的集合；

（二）数据项，是指描述网络数据结构最基本的、不可分割的单位；

（三）结构化数据项，是指具有预定义的抽象描述数据类型，通常使用数据库二维逻辑表中单一字段指代的数据项；

（四）非结构化数据项，是指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；

（五）数据处理活动，是指数据收集、存储、使用、加工、传输、提供、公开、删除等活动；

（六）数据处理者，是指开展数据处理活动的金融机构和其他机构；

（七）本办法所称“以上”均含本级。

第五十六条（解释权）本办法由中国人民银行负责解释。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。

第五十七条（生效期）本办法自2024年××月××日起施行。