筑基固本，添翼附羽——简述《网络数据安全管理条例》对公募基金公司数据安全管理工作的影响

作者：吕红 | 陈颖华 | 袁莹娅

2024 年 9 月 30 日国务院颁布第 790 号令，正式发布《网络数据安全管理条例》(以下简称“《条例》”)，《条例》将于 2025 年 1 月 1 日起施行。作为《网络安全法》《数据安全法》《个人信息保护法》的配套行政法规，《条例》填补了我国在网络数据安全管理领域行政法规层级的空白，细化和落实了上位法中的相关制度性安排和原则性规定，为网络数据安全管理工作提供了明确的法律支撑和具体实施路径，为这一领域的法律法规体系完善了关键一环。

中国证监会作为行业监管机构，历来高度重视公募基金公司(下称“基金公司”)等证券基金经营机构对其业务数据和客户信息的安全管控。此前，围绕数据安全及客户信息保护，证监会已先后发布了《证券基金经营机构信息技术管理办法》《证券期货业网络安全事件报告与调查处理办法》《证券期货业网络和信息安全管理办法》等部门规章及相关配套行业标准，指导证券基金经营机构践行更高标准的数据安全管理义务。因此，从实践层面，《条例》的部分要求已在基金公司现实落地。但同时，《条例》也不乏对现有网络数据安全管理规范的增补，这对基金公司日常的网络数据安全管理工作提出了新的要求与挑战。本文聚焦《条例》的主要内容，并对照现有行业监管规则，以期为基金公司更好地理解和执行《条例》提供有益思路。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

一.《条例》的主要内容

(一) 网络数据处理者的基本义务规范

《条例》第二章“一般规定”旨在通过提炼网络数据安全工作的关键环节，压实网络数据处理者主体责任。证券基金经营机构从事金融业务，掌握着敏感的数据信息，其数据安全管理是整个行业乃至国家安全的重要环节。近年来，证监会等行业主管部门已全方位构建对基金公司网络数据安全的监管体系，下文我们将对照现行的行业监管规范，梳理基金公司执行《条例》下基本义务规范的具体方向与细化标准。

1. 现行行业监管规范对《条例》的映射

《条例》要求	基金行业监管规范	
(1) 在网络安全等级保护的基础上，加强网络数据安全防护	证监会部门规章	《证券期货业网络和信息安全管理办法》 第十四条 核心机构和经营机构应当**落实网络安全等级保护制度，依法履行网络安全等级保护义务，按照国家和证券期货业网络安全等级保护相关要求，开展网络和信息系统定级备案、等级测评和安全建设等工作。** ……
	其他	- 相关行业标准：《证券期货业网络安全等级保护基本要求》《证券期货业网络安全等级保护测评要求》《金融行业信息系统信息安全等级保护实施指引》 - 行业自律规则：《网上基金销售信息系统技术指引》《基金管理公司网络和信息安全三年提升计划(2023-2025)》
(2) 建立健全网络数据安全管理制度	证监会部门规章	《证券期货业网络和信息安全管理办法》 第九条 核心机构和经营机构应当具有完善的信息技术治理架构，**健全网络和信息安全管理制度体系，建立内部决策、管理、执行和监督机制**，确保网络和信息安全管理能力与业务活动规模、复杂程度相匹配。 ……
		《证券基金经营机构信息技术管理办法》 第二十九条 证券基金经营机构应当结合公司发展战略，**建立全面、科学、有效的数据治理组织架构以及数据全生命周期管理机制**，确保数据统一管理、持续可控和安全存储，切实履行数据安全及数据质量管理职责，不断提升数据使用价值。

		其他	- 相关行业标准：《证券期货业数据安全管理与保护指引》《证券期货业信息系统运维管理规范》《证券期货业信息系统审计指南第 6 部分：基金管理公司》《金融数据安全 数据生命周期安全》 - 行业自律规则：《证券期货经营机构信息技术治理工作指引(试行)》《网上基金销售信息系统技术指引》《基金管理公司网络和信息安全三年提升计划(2023-2025)》
(3) 采取加密、备份、访问控制、安全认证等技术措施和其他必要措施，保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用		证监会部门规章	《证券期货业网络和信息安全管理办法》 第十九条 核心机构和经营机构应当构建网络和信息安全防护体系，**综合采取网络隔离、用户认证、访问控制、策略管理、数据加密、网站防篡改、病毒木马防范、非法入侵检测和网络安全态势感知等安全保障措施**，提升网络和信息安全防护能力，及时识别、阻断相关网络攻击，保护重要信息系统和相关基础设施，防范信息泄露与损毁。 第二十条 核心机构和经营机构应当**建立本地、同城和异地数据备份设施**，重要信息系统应当每天至少备份数据一次，每季度至少对数据备份进行一次有效性验证。
			《证券基金经营机构信息技术管理办法》 第三十一条 证券基金经营机构应当**完善网络隔离、用户认证、访问控制、数据加密、数据备份、数据销毁、日志记录、病毒防范和非法入侵检测等安全保障措施**，保护经营数据和客户信息安全，防范信息泄露与损毁。
		其他	- 相关行业标准：《证券期货业数据安全管理与保护指引》《证券期货业信息系统运维管理规范》《证券期货业信息系统审计指南第 6 部分：基金管理公司》《个人金融信息保护技术规范》《金融数据安全 数据生命周期安全》 - 行业自律规则：《网上基金销售信息系统技术指引》《基金管理公司网络和信息安全三年提升计划(2023-2025)》
(4) 处置网络数据安全事件，	i. 发现网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报	证监会部门规	《证券期货业网络和信息安全管理办法》 第三十六条 核心机构、经营机构和信息技术系统服务机构发现网络和信息安全产品或者服务存在**安全缺陷、安全漏洞等风险隐患的，应当及时核实并加固整改**；可能对证券期货业网络和信息安全平稳运行产生较大影响的，**应当向中国证监会及其派出机构报告**。

防范针对和利用网络数据实施的违法犯罪活动	告; 涉及危害国家安全、公共利益的，网络数据处理者还应当在 24 小时内向有关主管部门报告。	章	《证券期货业网络安全事件报告与调查处理办法》 第三章 **事件报告**
		其他	- 相关行业标准:《证券期货业信息系统运维管理规范》《证券期货业信息系统审计指南第 6 部分: 基金管理公司》 - 行业自律规则:《网上基金销售信息系统技术指引》《基金管理公司网络和信息安全三年提升计划(2023-2025)》
	ii. 建立健全网络数据安全事件应急预案，发生网络数据安全事件时，应当立即启动预案，采取措施防止危害扩大，消除安全隐患，并按照规定向有关主管部门报告。	证监会部门规章	《证券期货业网络和信息安全管理办法》 第三十七条 核心机构和经营机构应当根据业务影响分析情况，**建立健全网络安全应急预案，明确应急目标、应急组织和处置流程，应急场景应当覆盖网络安全事件**、自然灾害和公共卫生事件、本机构网络和信息安全相关重大人事变动、主要信息技术系统服务机构退出等情形。 第三十九条 核心机构和经营机构**应当建立应急处置机制，及时处置网络安全事件，尽快恢复信息系统正常运行，保护事件现场和相关证据，向中国证监会及其派出机构进行应急报告，不得瞒报、谎报、迟报、漏报**。 ……
			《证券基金经营机构信息技术管理办法》 第三十六条 证券基金经营机构借助信息技术手段从事证券基金业务活动的，应当建立信息技术应急管理的组织架构，确定重要业务及其恢复目标，**制定应急预案**，配置充足资源，**稳妥处置信息技术突发事件**，并积极开展应急演练和信息技术应急管理的评估与改进。
			《证券期货业网络安全事件报告与调查处理办法》 第十八条 核心机构和经营机构应当建立**网络安全应急处置机制，及时处置网络安全事件，尽快恢复系统的正常运行，保护事件现场和相关证据，并按照下列要求进行应急报告**: ……
		其他	- 相关行业标准: 《证券期货业数据安全管理与保护指引》《证券期货业信息系统运维管理规范》《证券期货业信息系统审计指南第 6 部分: 基金管理公司》《个人金融信息保护技术规范》《金融数据安全 数据生命周期安全》 - 行业自律规则:《证券期货经营机构信息技术治理工作指引(试行)》《网上基金销售信息系统技术指引》《基金管理公司网络和信息安全三年提升计划(2023-2025)》

	iii. 网络数据安全事件对个人、组织合法权益造成危害的，网络数据处理者应当及时将安全事件和风险情况、危害后果、已经采取的补救措施等，以电话、短信、即时通信工具、电子邮件或者公告等方式通知利害关系人。	证监会部门规章	《证券期货业网络和信息安全管理办法》 第四十一条 核心机构和经营机构发生网络安全事件，对投资者造成影响的，**应当及时通过官方网站、客户交易终端、电话或者邮件等有效渠道通知相关方可以采取的替代方式或者应急措施，提示相关方防范和应对可能出现的风险**。
		其他	- 相关行业标准:《个人金融信息保护技术规范》《金融数据安全 数据生命周期安全》 - 行业自律规则:《基金管理公司网络和信息安全三年提升计划(2023-2025)》

2. 《条例》对基金公司提出的新要求

针对网络数据环境和技术的快速演进，《条例》在以下方面提出了更具体严格的操作指导和合规标准:

(1) 明确数据交互的“标准动作”

对于个人信息、重要数据的委托处理、向其他数据处理者提供及共同处理，《条例》在重申数据交互各方基本的安全保障责任外，进一步明确应通过合同等方式落实数据处理各方目的、方式、范围以及安全保护义务等内容。在此之前，《个人信息保护法》仅提及个人信息委托处理场景需要该等合同约束。中国人民银行关于金融数据、个人金融信息的行业标准，虽也鼓励通过合同等方式约束各方责任，但该等标准并不具有强制执行力。因此，《条例》的落地进一步将合同或其他具有约束力的法律文件的签署安排扩展至包括个人信息对外提供在内的数据交互环节。

此外，《条例》规定个人信息、重要数据的相关处理记录应当至少保存 3 年。

(2) 建立面向公众提供服务主体的社会监督机制

公募基金面向公众销售，随着互联网的发展，已成为居民创造财富的重要投资工具。因此，基金公司属于《条例》第二十条规定的“面向社会提供产品、服务的网络数据处理者”，应当建立便捷的网络数据安全投诉、举报渠道，公布投诉、举报方式等信息，及时受理并处理网络数据安全投诉、举报。

(二) 个人信息保护

1. 规范个人信息处理规则的展示和内容要求

结合网信、工信等多部门治理 APP 侵害个人信息权益的执法经验，《条例》第二十一条在《个人信息保护法》的基础上对个人信息处理规则的展示及必备内容做了进一步的细化与补充，将散见在规范性文件中的重要内容上升为行政法规的要求，包括:

a. 个人信息处理规则应当集中公开展示、易于访问并置于醒目位置;
b. 列明个人主张个人信息权利(查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意)的方法和途径;
c. 以清单等形式列明，收集个人信息和向其他网络数据处理者提供个人信息的目的、方式、种类以及接收方信息;
d. 就处理不满十四周岁未成年人个人信息，应专门制定的个人信息处理规则。

2. 提供实现个人信息权利主张的具体路径

《条例》呼应了《个人信息保护法》关于保障个人查阅、复制、更正、补充、删除、撤回同意权利行使的要求，增加个人就限制处理其个人信息、账户注销等个人信息权利的行使，并明确了个人信息转移权的具体操作路径。网络数据处理者应当及时响应并提供便捷的行使权利方式，不得无理拒绝或设置障碍。对于符合条件的个人信息转移请求，网络数据处理者也应提供必要的支持。

3. 明确在特定情况下处理个人信息的规范

《条例》第二十四条对网络数据处理者在利用自动化采集技术过程中无法避免采集到非必要个人信息或未获得个人同意的情况下，以及在个人注销账号时，如何处理个人信息提供了具体规范。如果技术上可行，网络数据处理者应删除或匿名化处理这些个人信息；如果技术上难以实现，应限制进一步处理，停止除存储和采取必要安全保护措施之外的处理。

4. 细化个人信息保护的合规审计要求

《条例》再次强调网络数据处理者应定期开展个人信息处理合规审计的要求，并明确了合规审计可自行或者委托专业机构开展。

结合国家网信办《个人信息保护合规审计管理办法(征求意见稿)》及配套国家标准对于该项合规审计的细化要求，个人信息保护的合规审计与证监会《证券基金经营机构信息技术管理办法》项下的 IT 审计侧重各有不同，难以简单替换。

(三) 重要数据安全

2016 年的《网络安全法》首次提出“重要数据”，《数据安全法》进一步确立数据分类分级保护机制，规定重要数据目录由国家有关部门制定，并对重要数据加强保护。《条例》则在行政法规层

面明确重要数据的定义，即特定领域、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。

《条例》重申了重要数据目录应由各地区、各部门依据数据分类分级保护制度来确定。行业监管方面，在 2024 年 3 月 20 日国务院关于《扎实推进高水平对外开放更大力度吸引和利用外资行动方案》(简称"《行动方案》")政策例行吹风会上，中国人民银行国际司负责人介绍了人民银行正在会同其他金融管理部门，明确金融领域重要数据目录。未来，人民银行、证监会层面将发布金融证券基金领域的重要数据目录。地方上，根据天津自贸区管委会发布的《中国(天津)自由贸易试验区企业数据分类分级标准规范》，天津自贸区将金融机构安保信息、国防军工企业、关系国家安全企业的相关信息列为重要数据。关于后者，基金公司应关注相关敏感企业的投研信息是否会被视为重要数据，进而肩负更重大的安全保护职责。

根据《条例》，网络数据处理者应当主动识别、申报重要数据，如涉及处理重要数据，则应履行网络数据安全保护责任:

a. 指定网络数据安全负责人和设立网络数据安全管理机构;
b. 在提供、委托处理、共同处理重要数据前进行风险评估;
c. 在发生合并、分立、解散、破产等情形时，采取措施保障数据安全并履行报告义务;
d. 定期开展网络数据处理活动的风险评估，并提交评估报告。

特别指出，处理 1000 万人以上个人信息的网络数据处理者，需参照执行上述第 a 项和第 c 项的要求。因此，即便行业监管机构或部分地区尚未发布重要数据目录，但因处理个人信息达到一定量级，上述规定仍将适用于大部分基金公司。

(四) 数据跨境管理

网络数据跨境安全管理方面，《条例》秉持《行动方案》关于便利数据跨境流动，服务高水平对外开放的基本原则，沿袭了《数据安全法》《个人信息保护法》下个人信息、重要数据的出境管控要求，并在行政法规层面认可了国家网信办《促进和规范数据跨境流动规定》("《数据跨境流动规定》")规定的个人信息出境豁免情形[1]，将数据出境的管控重点放在个人信息和重要数据上，并未采纳征求意见稿将管控范围扩展至一般数据的操作。具体而言:

1. 法定需通过数据出境安全评估的情形

(1) 向境外提供重要数据。

注: 未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

[1] 具体可参阅本团队此前的解读——《春风化冻——数据跨境流动新规出台》

(2) 非关键信息基础设施运营者(“关基单位”)自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息(不含敏感个人信息)。属于下文第 3 项豁免情形的除外。

(3) 非关基单位自当年 1 月 1 日起累计向境外提供 1 万人以上敏感个人信息。属于下文第 3 项豁免情形的除外。

(4) 关基单位向境外提供个人信息。属于下文第 3 项豁免情形的除外。

2. 法定需与境外接收方订立标准合同或者个人信息保护认证的情形

(1) 非关基单位自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息(不含敏感个人信息)。属于下文第 3 项豁免情形的除外。

(2) 非关基单位自当年 1 月 1 日起累计向境外提供不满 1 万人敏感个人信息。属于下文第 3 项豁免情形的除外。

3. 可豁免第 1、2 项路径的情形

(1) 非关基单位自当年 1 月 1 日起累计向境外提供不满 10 万人个人信息(不含敏感个人信息)。

(2) 为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息。

(3) 按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息。

(4) 紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息。

(5) 为履行法定职责或者法定义务，确需向境外提供个人信息。

值得注意的是，第(5)项为本次《条例》新增的豁免情形。对于基金公司而言，此项或为跨境业务(如 QDII 业务)涉及的数据出境提供合法路径。

此外，国家允许有条件的自由贸易试验区和自由贸易港可以自行制定区内需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单等，即自贸区负面清单机制。目前天津自贸试验区、上海自贸试验区临港新片区[2]、北京自贸试验区已相继发布相关清单，在数据跨境流动管理方面展开了重要探索，与《个人信息保护法》《条例》《数据跨境流动规定》等法律法规共同构成了数据跨境流动的清晰法律框架和实践指南。

[2] 关于上海自贸试验区临港新片区对于公募基金公司的数据出境新动向可参阅本团队此前的解读——《临港新片区公募基金一般数据清单机制简析》

(五) 网络平台服务提供者的特别要求

对于通过官方网站、APP 或微信小程序等平台开展线上基金销售的基金公司，应关注《条例》第六章关于网络平台服务提供者义务的内容:

1. 基金公司官网、APP 或微信小程序等平台通过接入第三方 SDK 实现人脸识别、支付处理、数据分析和推送服务等业务功能的，应当通过平台规则或者合同等明确接入其平台的第三方 SDK 的网络数据安全保护义务，并督促第三方 SDK 加强网络数据安全管理。如第三方 SDK 违反法律法规或者平台规则及相关合同约定开展网络数据处理活动，对用户造成损害的，基金公司将根据其责任范围承担相应的法律责任。因此，基金公司应特别注意前述义务和责任分配。

2. 基金公司通过自动化决策方式向个人进行信息推送的，应当设置易于理解、便于访问和操作的个性化推荐关闭选项，为用户提供拒绝接收推送信息、删除针对其个人特征的用户标签等功能。

3. 如基金公司线上销售平台达到一定标准，即注册用户 5000 万以上或者月活跃用户 1000 万以上，业务类型复杂，相关数据处理活动对国家安全、经济运行、国计民生等具有重要影响的，将被视为“大型网络平台”，并履行更为严格的网络数据安全管理义务(如年度发布个人信息保护社会责任报告)。

二. 对基金公司后续行动的初步建议

《条例》将自 2025 年 1 月 1 日起施行，结合上文对《条例》的梳理，我们将就基金公司可采取的后续行动提供初步建议，以协助机构更好落实《条例》的新要求，确保数据处理活动的合法合规:

1. 进一步加强网络数据安全防护

尽管行业主管部门已对证券基金经营机构的网络数据安全责任建立了完善的规则体系，但因网络数据安全管理不足而导致的风险事件仍时有发生。如券商经纪系统故障影响投资者的系统登录及正常交易；部分公司因网络安全防护能力不足而遭受病毒感染或爬虫程序攻击，导致官网无法访问、网站被黑客篡改等。这些事件都凸显了行业机构加强网络安全防护的紧迫性。

本次《条例》在行政法规层面进一步夯实机构网络数据安全主体责任，并构建了分工与协同相结合的网络数据监督管理体制机制。可预见到的，国家相关职能部门将形成监管合力，纵深推进金融机构的网络数据安全监管，这将给基金公司带来重大的监管挑战。

2. 健全网络数据安全管理制度

基金公司应全面梳理并检视公司现有的网络数据安全管理相关制度，对照《条例》的新要求予以更新，特别是在落实个人信息保护、数据出境管理、第三方管理以及网络平台服务等方面。

3. 加强第三方合作管理

在与外部机构的合作中，监管部门就曾通报个别公司存在与外部机构的协议约定允许保密信息对外披露、外包人员拥有较高系统权限致使重要信息存在泄露风险。基金公司与第三方合作时涉及业务数据、客户信息处理的，若疏于监督管理，不仅可能承担行政处罚风险，还可能因侵害投资者权益而承担民事风险。故我们建议机构:

- ✓ 与第三方(如代销机构、外包机构、SDK 服务商等)的合作涉及个人信息、重要数据的委托处理、对外提供及共同处理的，应梳理并更新与该等合作方签订的合同或补充签订相关约束性文件。
- ✓ 加强对数据接收方和第三方 SDK 履约情况的监督管理。
- ✓ 确保按照《条例》要求保存个人信息、重要数据委托处理、对外提供的处理记录。

4. 完善个人信息处理规则的内容与展示方式

对照《条例》及工信部门的相关要求，更新和完善个人信息处理规则，并确保其集中公开展示、易于访问并置于醒目位置；以清单方式列明个人信息的收集和对外提供的情形；就处理不满十四周岁未成年人个人信息专设规则。

5. 建立并公开网络数据安全投诉和举报渠道，同时制定有效的响应和处理工作机制。

6. 完善个人信息权利行使响应机制

为投资者提供便捷的个人信息权利行使途径，包括查阅、复制、更正、补充、删除个人信息，或注销账号、撤回同意，以及个人信息转移等；通过自动化决策方式向投资者推送信息的，提供拒绝接收推送信息、删除针对其个人特征的用户标签的功能选择。

7. 建立个人信息保护合规审计机制并定期开展审计工作。

如您希望就相关问题进一步交流，请联系：

吕 红
+86 21 3135 8776
sandra.lu@llinkslaw.com

陈颖华
+86 21 3135 8680
tracy.chen@llinkslaw.com

袁莹娅
+86 21 3135 8773
leah.yuan@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