

数据驱动策略与数据合规:

《金融信息服务数据分类分级指南》简析

作者: 吕红 | 罗黎莉 | 赵一旭

近年来,随着人工智能、机器学习和大数据的快速发展,全球资本市场的博弈愈发依赖数据获取与计算能力。对于量化对冲基金、自营交易机构以及采用科技驱动策略的资产管理机构,海量、多维的市场与行业数据已成为其生成交易信号、挖掘超额收益的核心资源。就境外机构而言,无论是通过合格境外投资者、沪深港通等渠道直接投资于中国市场,还是通过收益互换等金融衍生工具间接投资于中国市场,获取全面、准确、持续的中国市场及行业数据,对于其投资及交易策略的落地至关重要。

在跨境与本土数据需求持续增长的驱动下,国内涌现并逐步发展成熟了一批专业的金融信息服务机构(如万得、同花顺、东方财富等),亦有外国机构经批准在中国境内提供金融信息服务(如 Bloomberg、Dow Jones 等)(合称“数据服务商”)。这些数据服务商广泛收集、处理并向境内外市场参与者提供多维度的金融信息服务,涵盖股票、商品、期货、指数等金融市场数据,贸易、投资、财政等宏观经济数据,行业资讯、研究报告、政策法规等资讯报告数据,食品饮料、交通运输、旅游酒店等行业指标数据。在数据赋能金融创新的同时,数据安全与数据跨境的规范和管理也日益强化,就金融信息服务领域而言,监管逻辑已从对“金融信息服务提供者”的机构审批及报备管理,进一步拓展至对“金融信息服务数据”本身的管理。

2026 年 6 月 13 日,国家互联网信息办公室(“国家网信办”)、中国人民银行、国家金融监督管理总局、中国证券监督管理委员会、国家统计局、国家外汇管理局联合印发《金融信息服务数据分类分级指南》(“《指南》”),旨在规范金融信息数据处理活动,提升金融信息服务数据安全水平。对于高度依赖数据输入以实现策略运作的资产管理机构、量化对冲基金及自营交易机构而言,《指南》绝不仅仅是针对数据服务商的合规要求。数据服务商在落实分类分级标准后,其数据采集的颗粒度、敏感数据的脱敏处理方式、可提供数据服务的范围以及跨境数据传输等环节,都可能发生实质性变化,从而为依赖特定数据源的量化模型或数据驱动策略带来潜在影响。

一. 《指南》的适用对象

《指南》适用于在中国境内从事金融信息服务的金融信息服务提供者开展数据分类分级和重要数据识别工作。根据《金融信息服务管理规定》,“金融信息服务”是指向从事金融分析、金融交易、金融决策或者其他金融活动的用户提供可能影响金融市场的信息和/或者金融数据的服务。

根据《指南》,“金融信息服务提供者”是指从事金融信息服务的法人、非法人组织,不包括国家机关和法律、法规授权的具有管理公共事务职能的组织。同时,结合《关于开展境内金融信息服务报备工作的通知》《外国机构在中国境内提供金融信息服务管理规定》等相关规定,以及国家网信办公布的相关许可及报备名单,《指南》的适用对象应主要为向专业机构或投资者等金融市场参与主体提供金融资讯、金融数据、金融行情等服务的金融信息服务机构。目前,国家网信办已公布的金融信息服务机构名单主要包括境内金融信息服务机构、境外机构在中国境内投资设立的提供金融信息服务的企业以及在中国境内提供金融信息服务的境外机构¹,相关机构应重点予以关注。

¹ 第一批境内金融信息服务机构报备清单: https://www.cac.gov.cn/2022-01/04/c_1642894644935908.htm
第二批境内金融信息服务机构报备清单: https://www.cac.gov.cn/2022-10/28/c_1668509064248761.htm
第三批境内金融信息服务机构报备清单: https://www.cac.gov.cn/2023-11/21/c_1702230143102599.htm
第四批境内金融信息服务机构报备清单: https://www.cac.gov.cn/2026-02/14/c_1772800146857074.htm
境外机构在中国境内提供金融信息服务许可名单: https://www.cac.gov.cn/2026-04/30/c_1779276540918311.htm
境外机构在中国境内投资设立企业提供金融信息服务许可名单: https://www.cac.gov.cn/2026-04/30/c_1779276540092438.htm

二. 《指南》的核心内容

《中华人民共和国数据安全法》在法律层面确立了数据分类分级保护制度，《网络数据安全管理条例》进一步要求各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录。《指南》是在金融信息服务这一细分领域对前述原则性要求的具体落实。

1. 数据分类分级

在数据分类方面，《指南》参照国家标准《数据安全技术 数据分类分级规则》确定的“先行业领域分类、再业务属性分类”的数据分类思路，在金融信息服务行业领域，按照金融信息服务数据的业务属性进行分类，其中一级分类为业务数据、用户数据和企业数据 3 类，在此基础上进一步细分二级分类 9 类、三级分类 67 类，以实现金融信息服务不同场景数据的全方位覆盖与精细化管理。

- 业务数据包括反映金融市场动态和资产状况的金融市场数据、反映国家或地区经济运行状况的宏观经济数据、金融市场参与主体的组织机构数据、反映行业领域运行状态、市场供需等的行业指标数据，以及与金融市场相关的新闻、评论、资讯等资讯报告数据。
- 用户数据分为个人用户数据和机构用户数据。个人用户数据进一步分为基本信息、交易数据和生物特征识别信息，机构用户数据进一步分为基本信息和交易数据。
- 企业数据指金融信息服务企业自身的数据，分为经营管理数据和系统运维数据两类。

不过，从行业前沿交易的实际需求来看，《指南》尚未覆盖部分新兴另类数据类型，例如，消费者交易数据、消费习惯、网络抓取数据、网页浏览量、浏览习惯、卫星图像、地理位置、社交媒体、市场情绪、舆情数据、供应链、海关、航运等，可能无法完全解决量化对冲基金、自营交易机构等专业机构在另类数据采购及跨境传输方面的问题。

在数据分级方面，《指南》参照国家标准《数据安全技术 数据分类分级规则》，根据金融信息服务数据在经济社会发展中的重要程度和敏感程度，以及一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度，将数据从高到低分为四级，分别为核心数据、重要数据、敏感一般数据、常规一般数据。

值得关注的是，《指南》结合金融信息服务领域的特殊性和所掌握数据的敏感性，在国家数据分类分级保护制度框架下，对一般数据作了细分，将一般数据进一步划分为“敏感一般数据”和“常规一般数据”。这一细分的主要标准在于数据是否公开、涉及境内或境外情况，以及一旦被泄露或篡改、损毁，对经济运行、社会稳定、公共利益，或者对组织自身或者公民个体造成的影响程度。举例而言，根据《指南》附录 A 的示例：

- 以“公开状态”为区分标准：基金数据中，未公开的私募基金数据属于敏感一般数据，其他的属于常规一般数据；研究报告中，金融持牌机构公开发布的属于常规一般数据，其他的属于敏感一般数据。
- 以“境内/境外”为区分标准：宏观经济数据(如国民经济核算、价格指数、贸易、投资、金融、财政等)以及各行业指标数据中，境内数据原则上属于敏感一般数据，境外数据则属于常规一般数据。

2. 重要数据识别

根据《指南》第 5.5 条，数据级别应在分级要素识别、影响对象和影响程度分析的基础上综合确定，结合《指南》提供的数据级别判定标准，概括而言：

- 凡对国家安全造成任何程度危害的数据，原则上即构成重要数据乃至核心数据。
- 对经济运行、社会秩序、公共利益造成“严重危害”的，构成重要数据；造成“一般危害”的，构成敏感一般数据。
- 仅影响组织权益、个人权益的，原则上为敏感一般数据或常规一般数据。

此外，《指南》还确立了“就高从严”原则，即数据集级别按其所含数据项的最高级别确定。同时，《指南》还明确，凡被相关部门、地区依据其分类分级标准识别，或告知、公开发布为核心数据、重要数据的，相应定为核心数据或重要数据。

结合《指南》附录 A 的示例，金融信息服务领域可能落入重要数据范畴的情形主要包括：

- 高颗粒度的境内行业及商品数据：境内各行业指标数据(如能源、钢铁、有色金属、汽车、医药生物等)及商品数据，原则上为敏感一般数据，但若其覆盖度、时间跨度、精度等高于有关部门公开发布的水平(包括历史上曾公开的)，并能够反映省级行政区及以上范围情况的，即升级为重要数据。这意味着，比官方更精准、更详实、覆盖面更广的境内宏观与行业数据是重要数据识别的重点。
- 达到一定规模的用户²数据集：例如 1,000 万人及以上的个人用户基本信息数据集、100 万人及以上的个人用户交易数据集、10 万人及以上的生物特征识别信息数据集、100 万及以上机构用户基本信息数据集、10 万及以上机构用户交易数据集，均构成重要数据。
- 可能直接影响国家安全的机构交易数据：机构用户交易数据如一旦泄露或篡改可能直接影响国家安全的，属于重要数据。

² 此处的“用户”应特指采购金融信息服务的用户，并非泛指各行各业的消费者或客户。

根据《指南》第 5.6 条，数据级别并非一成不变。当数据内容、时效性、规模、使用场景、加工处理方式发生变化，或因数据融合、国家及有关部门要求等导致原定级别不再适用时，应及时更新。这意味着数据服务商对同一数据的处理方式(如提高颗粒度、延长历史跨度、进行多源融合)本身即可能改变数据级别，并可能触发重要数据的认定。

三. 《指南》对数据服务商的影响

相关数据服务商应当根据《指南》的要求开展数据分类分级工作，并针对不同类别、不同级别的金融信息服务数据采取相应的差异化保护措施，以履行数据处理者的合规义务。《指南》载明了较为完整的分类分级步骤供数据处理者参考，包括数据资源梳理、数据分类、数据分级、形成数据分类分级清单、报送重要数据目录、动态更新管理。

1. 全面梳理数据资源、建立分类分级清单

数据服务商首先需对其数据资源进行全面梳理，明确数据库表、数据项、数据文件等数据资源的基本信息、描述对象与业务属性等，形成数据资源清单。在此基础上，按照业务数据、用户数据、企业数据的一级分类，逐级落实至二级、三级分类，并通过分级要素分析综合研判数据级别，最终审核确定并形成数据分类分级清单与重要数据目录。

2. 重点履行重要数据目录报送义务

对识别出的重要数据，数据服务商需按照主管部门要求的频度和格式报送重要数据目录。根据《指南》附录 B 的模板，报送内容相当详尽，涵盖数据基本情况(名称、分类分级依据、级别、载体、来源、数据量、存储总量、覆盖类型及占比)、责任主体(数据处理者名称、机构代码、所在地、数据安全负责人)及数据安全情况(信息系统名称、网络安全等级保护情况、是否为关键信息基础设施、是否开展数据安全风险评估及评估结论)等。此外，当重要数据条目数量、存储总量等变化达 30%以上或其他重要内容发生重大变化时，应及时重新报送。

3. 差异化保护与数据出境合规

分类分级的意义在于据此实施差异化的安全保护与跨境管理。一旦数据被识别为重要数据，将依法触发数据出境安全评估等更为严格的合规要求；而对于“敏感一般数据”，虽然在出境层面没有强制性的安全评估义务，但因其“敏感”属性，数据服务商在对外提供(尤其是向境外提供)时仍将审慎把握。这使得数据服务商在数据采集的颗粒度、敏感数据的脱敏处理方式、可对外提供的范围以及跨境传输安排等环节，都可能作出相应调整。

4. 对数据加工与产品策略的潜在影响

值得注意的是，《指南》将“覆盖度、时间跨度、精度高于有关部门公开发布水平并能反映省级行政区及以上范围情况”作为境内行业及商品数据升级为重要数据的关键标准。这实际上对数据服务商的核心竞争力构成了一定约束，即数据服务商越是通过深度加工、多源融合提供比官方

更全、更细、更精的境内数据，越可能触及重要数据红线。因此，数据服务商在产品设计与数据加工策略上，需要在提升数据价值与控制合规级别之间审慎权衡，并通过分级标注、脱敏处理、控制颗粒度与覆盖范围等方式管理合规风险。

四. 数据采购方的关注要点

1. 合作与准入层面：核查数据服务商的合规落实情况

对于量化对冲基金、自营交易机构等数据采购方而言，首要关注点在于交易对手方(即数据服务商)是否已按照《指南》要求开展数据分类分级，以及其所提供的数据在分类分级项下的合规属性是否清晰。将《指南》要求融入尽职调查、合作准入、合同约束等全流程管理中：

- 尽职调查与合规核查：在建立合作前，对数据服务商开展合规尽职调查。重点核查其是否已建立符合《指南》要求的数据分类分级制度，是否已形成完整的数据资产清单，并评估其数据安全能力与合规历史记录。
- 数据范围与级别披露：要求数据服务商对所提供数据的类别、级别(特别是是否涉及“敏感一般数据”或更高级别的数据)进行清晰界定和披露，有明确可识别的数据分类定级标签。
- 合同条款约束：在合作协议中明确约定数据合规陈述与保证内容，要求数据服务商承诺所提供数据来源合法、分类分级准确。
- 跨境传输合规责任的分配：针对涉及数据出境的合作场景，在合作协议或安全协议中清晰界定双方在数据跨境传输中的合规义务、申报主体责任等。
- 动态调整与通知机制：建立常态化沟通机制，约定当数据服务商的数据分类分级结果发生变更(如常规一般数据升级为敏感一般数据)，或监管政策调整影响数据提供范围时，数据服务商应及时履行通知义务，并启动合作方案的动态调整程序。

2. 数据范围：可采购数据的边界可能发生变化

数据分类分级规则的明确，将直接影响数据服务商可对外提供的数据范围。

就境外机构直接向境内数据服务商采购数据的情形而言，以往受限于重要数据识别、数据出境等不确定性，境内数据服务商目前在实践中整体偏于审慎、从严，能够直接提供给境外机构的数据范围相对较窄，有时难以满足境外交易策略对数据广度和颗粒度的需求。

《指南》出台后，随着分类分级标准趋于明确，境外机构可采购的数据范围存在拓展的空间。例如，对于明确不落入重要数据范畴的“敏感一般数据”，由于其不涉及安全评估等前置程序，理论上具备向境外提供的可行性，数据服务商在边界清晰后或可能会适度放开此类数据的供给。

不过需要指出的是，“敏感一般数据”虽不需要履行安全评估程序，但因其“敏感”属性，数据服务商从数据安全及风险控制的角度，对于直接向境外机构提供此类数据仍可能存在顾虑，尤其在出境环节，数据服务商可能因难以把握处理尺度而不愿承担相应的合规负担。因此，“敏感一般数据”在实践中的可获得性，仍可能受到数据服务商风险偏好的制约。

3. 架构安排：设立境内主体的价值与挑战

鉴于“敏感一般数据”在跨境传输中可能面临的供给约束，对于数据需求多元且深入的境外机构而言，设立境内主体进行过渡与处理可能是一种替代方案。

从数据可获得性的维度来看，不同级别数据的出境限制存在本质差异：

- 重要数据：因涉及严格的安全评估等法定程序，无论采购主体在境内还是境外，可合理预见的是，实践中均较难获取并出境。
- 一般数据：原则上无需安全评估即可采购。但其中的“敏感一般数据”受限于部分数据服务商的风险偏好，直接跨境供给或存在阻碍。

据此，境外机构可以考虑在境内设立主体(例如以数据收集、处理为主要业务活动的非持牌外商独资企业)，由该境内主体直接向境内服务商采购数据。在境内完成数据的本地化清洗、脱敏与整合后，再依法合规地向境外关联方传输，以支持境外交易策略。实践中，已有外资机构采用此种架构，在境内设立专门的数据公司。

不过，需要关注的是，设立境内主体亦面临多方面的成本负担：

- 合规监管：境内主体需全面遵守中国相关法律法规，履行相关数据安全义务，并接受境内监管机构的监管。
- 基础设施布局：需在境内部署 IT 基础设施、系统、服务器等，并妥善处理由此带来的数据本地化与安全管理问题。
- 知识产权与技术保护：在境内运营过程中，需妥善处理核心算法、交易模型及关键技术的跨境共享与知识产权保护边界。
- 运营成本：不仅包括初期设立成本，还包括后续的人力、运营、合规等持续性成本。

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@linkslaw.com



罗黎莉
+86 21 3135 8732
lily.luo@linkslaw.com



赵一旭
+86 21 6043 3937
neil.zhao@linkslaw.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@linkslaw.com

上海

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

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

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

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

伦敦

1/F, 3 More London Riverside
London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.linkslaw.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 2026