

资产管理行业数据合规：在摸索中前行

作者：毛慧 | 解石坡 | 刘继炎¹

引言

近年来，在我国居民个人财富不断积累的大环境下，投资者对理财的需求不断攀升，从而使大量个人信息和数据汇聚至资产管理行业。《中华人民共和国网络安全法》（“《网络安全法》”）、《中华人民共和国数据安全法》（“《数据安全法》”）和《中华人民共和国个人信息保护法》（“《个人信息保护法》”）等一系列法规的施行，标志着我国数据合规已步入强监管时代。然而，由于此前资产管理行业对数据合规的重视程度并不足，近年来资产管理机构在个人信息保护和数据合规方面频频出现违反行业规则的情形。据统计，仅 2023 年第 1 季度，中国人民银行及各级银保监会开出的数据罚单就达到了 384 张，罚款金额达到 6.45 亿元，涉及 251 家法人。其中，超千万元的大额罚单达 8 张，罚款金额较 2022 年第 1 季度同比上涨 62.5%。相继爆出的“天价罚单”提醒我国资产管理行业数据合规的重要性，在资产管理领域开展和完善数据合规工作刻不容缓。

资产管理行业的数据合规工作具有法律适用的双重性、数据类型的全面性、敏感性和跨境性以及合规过程的全程性等特点，这要求我们深入分析资产管理领域数据合规的特点和难点，并就特殊问题和关键问题提出具有针对性和实操性的解决方案。本文将详细阐述前述问题并相应提出解决方案，旨在为资产管理领域的数据合规工作提供有益的启示和建议。

一、资产管理领域数据合规现状

（一）资产管理机构合规意识不足

由于数据合规需要以一种全局性的视角开展工作，仅仅依靠数据合规部门难以实现明显成效，这要求机构内部各部门通力合作，并将数据合规工作置于与传统的风险合规防控、反洗钱工作等同等重要的位置。然而目前我国资产管理机构的主动合规意识不足，这导致违规收集、使用、泄露个人金融信息等事件频发。例如，在 2020 年，有报道指出某银行未经当事人同意及出具法定手续，违规将其个人账户交易明细提供给其雇主，最终被银保监会处以人民币 450 万元罚款的行政处罚，其中“主要违法违规事实”包括客户信息收集环节管理不规范、对客户敏感信息管理不善、违规存储客户敏感信息等。由此可见，我国资产管理机构的数据合规意识和数据敏感性亟待加强，这不仅需要合规部门在技术措施上的加强，也需要机构内部所有部门集体培养数据安全意识、提升对数据安全的敏感性。

¹ 实习生左昭阳、张一明对本文的写作亦有贡献。

（二）数据合规技术性工具匮乏

除了合规意识问题，资产管理机构数据合规还面临技术性工具匮乏的问题。《金融行业网络安全研究报告》显示，在引起我国金融行业数据泄露的主要原因中，“网络应用程序攻击、滥用特权和其他错误”占比高达 72%。而对比国外在网络安全上的投入，国内金融机构的网络安全投入仅占总营收的 0.1%，与国外的平均水平 0.4%相比差距明显。因此，仅仅依靠有限的人工对数据进行梳理、分类和保护远远不足，资产管理机构仍需要自动化的技术性工具以提升合规工作的质量和效率。

（三）数据合规理论研究欠缺

总体来看，资产管理机构对于传统的金融监管更为熟悉，而我国个人信息保护和数据合规行业仍属新生领域，相关的法律法规和监管仍处于发展阶段，监管体系也与金融监管存在较大差异，资产管理机构对其总体认识较为有限。此外，在具体适用中，由于各行各业数据的应用场景不同，有关监管部门需要根据监管需求制定配套的数据合规制度。由于数据合规实践的合规基础更新迅速，理论研究往往滞后于实践的发展。而我国资产管理行业缺乏具体的行业操作规范，这导致资产管理机构缺乏完善的理论指引以应对更新频繁的数据合规要求，在一定程度上阻碍了行业数据合规工作的进展。

（四）数据合规人才队伍不充实

资产管理领域的数据合规治理具有多领域、跨学科特征，涵盖了法律、金融、计算机、网络安全、数据治理、个人信息保护、密码、业务流程等多种领域。因此，在资产管理机构开展数据合规工作需要既懂得数据技术、又懂得金融数据合规法律的复合型人才。然而，此类人才需求类别多样且门槛较高，资产管理机构原有的法律人才队伍短期内难以满足此要求。并且，由于数据合规部门更倾向于在幕后为资产管理队伍“保驾护航”，其并不能创造直接的收益。因此，中小型资产管理机构往往囿于经营成本或注重短期效益，难以大量扩充数据合规人才队伍。此外，机构合规团队需同时负担法律诉讼、风险评估及合同审查等日常工作，这进一步加剧了开展数据合规工作的压力。

二、资产管理领域数据合规法律规范体系

鉴于资产管理领域的特殊性，一方面，资产管理机构在投资交易过程中需要收集、流转和处理大量敏感、隐私的个人信息数据，因此受到信息安全和数据保护领域的法律规制；另一方面，作为承载金融系统运行的重要组成部分，其必然面临金融监管机构法律规范的规制。因此，资产管理机构在数据合规方面面临的法律压力来自两方面，即金融监管机构和信息与数据安全部门的双重监管。此外，我们应当看到，随着高水平对外开放格局的形成，各个资产管理机构的业务愈发涉及跨境交易场景，因此也面临着数据跨境合规这一问题。具体而言，我国资产管理机构数据合规面临的法律监管来自如下三方面：

（一）信息安全与数据保护法律规范

信息安全与数据保护的体系由数据保护的“三驾马车”和行业配套的规定与标准构成，各部分所包含的法律规范具体可见下表。从顶层立法、配套规定到行业标准自上而下构成了较为严密的信息数据保护法律体系，这要求资产管理机构在合规管理过程中，需遵循自上而下、由抽象到具体的原则，系统查明相关法律规范，以防出现因遗漏某规定或标准而被处罚的问题。

规范类型	所涉法律法规
<p style="text-align: center;">数据保护的“三驾马车”</p>	<p>信息安全与数据保护的基础框架由数据保护的“三驾马车”构建而成，即《网络安全法》《数据安全法》《个人信息保护法》，这三部法律各有侧重。</p> <p>《网络安全法》的目的是保护网络安全，就网络运行安全、网络信息安全和监测预警与应急处置措施作出总体性规定。</p> <p>《数据安全法》侧重于数据安全的规制，要求包括开展数据处理活动的主体和政府部门等监督机构履行数据安全保护义务，并对数据出境问题作出规定。</p> <p>《个人信息保护法》侧重个人信息处理活动，设置了体系性的权利保护条款以及个人信息处理者的义务，包括查阅、复制、更正、删除权，以及个人信息处理者在个人信息的收集、使用、存储、处理、分享、出境、公开等各方面的义务，其更加侧重于对个人信息的保护。</p>
<p style="text-align: center;">行业配套规定和标准</p>	<p>除数据保护的“三驾马车”外，信息安全与数据保护领域还有一系列配套规定、行业标准和指南，具体包括：</p> <ul style="list-style-type: none"> ■ 《关键信息基础设施安全保护条例》； ■ 《网络安全审查办法》； ■ 《数据出境安全评估办法》； ■ 《个人信息出境标准合同办法》； ■ 《信息安全技术 — 个人信息安全规范》； ■ 《数据出境安全评估申报指南（第一版）》； ■ 《个人信息出境标准合同备案指南（第一版）》； ■ 《信息安全技术个人信息处理中告知和同意的实施指南》； ■ 《网络安全标准实践指南 — 个人信息跨境处理活动安全认证规范》； <p>.....</p>

（二）金融监管法律规范

金融监管的法律架构可以从两个维度进行剖析：一是行业一般性规定，包括但不限于《中华人民共和国证券法》《中华人民共和国反洗钱法》《金融机构反洗钱和反恐怖融资监督管理办法》和《法人金融机构洗钱和恐怖融资风险管理指引（试行）》等，这些法律法规对信息的保密与披露、数据的安全保护等作出了明确的规定。二是针对金融行业数据合规的特定规定和标准，例如金融监管机构业已制定的《个人金融信息保护技术规范》《金融数据安全数据安全分级指南》以及《证券期货业数据分类分级指引》等规定，对信息数据安全的技术要求和等级分类提供了明确指引。

（三）数据跨境流动相关法律规范

随着数据跨境流动的规模不断扩大，资产管理机构在进行数据合规评估时需要将跨境数据流动的

合规作为一项独立的要求。2017年实施的《网络安全法》对数据出境的安全评估提出了原则性要求。2021年，《数据安全法》和《个人信息保护法》正式实施，随之而来地，2022年《数据出境安全评估办法》、2023年《个人信息出境标准合同办法》及一系列配套规范和指南的落地，为我国的数据跨境监管体系提供了完整的法律框架。

将跨境数据合规作为一项独立合规要求的原因在于，一方面，数据跨境将对国家安全和公共利益产生重大影响，国家对此往往采取较为严格的要求和管控措施。而我国关于数据跨境的立法较为分散，这对跨境数据合规的核查工作提出了较高要求。另一方面，数据跨境还需满足全球数据跨境规则的要求，不同国家和地区提出了不同的标准，如欧盟《一般数据保护条例》（GDPR）、《加利福尼亚州消费者隐私法案》（CCPA）和英国数据保护法案等。此外，一系列国际协定就数据的跨境流动也形成了一套严格的保护和规制体系，如《区域全面经济伙伴关系协定》（RCEP）、《数字经济伙伴关系协定》（DEPA）及《全面与进步跨太平洋伙伴关系协定》（CPTPP）。因此，在处理跨境数据流动问题时需要做好不同国家和地区法律规范、国际协定的查明，对不同国家和地区的法律规范及国际协定进行综合考量。

三、资产管理领域数据合规的内涵

（一）保密要求与资质要求

数据合规的基础性要求在于资产管理机构需满足对数据保密性的要求。原因在于金融数据天然具有隐私性与敏感性，其与个人利益、国家经济运行安全紧密相关。因此，相较于其他行业，金融数据具有天然的保密要求和传统。

而资产管理机构开展数据合规治理的另一基础性条件在于满足相关的许可或备案经营资质。作为金融系统运行的核心角色，资产管理机构为投资者提供支付、理财、信贷等金融服务，此时投资者的隐私和信息、国家金融行业的数据暴露在资产管理机构面前。如若允许未取得相关经营资质的经营者进入资产管理领域，将使得资产管理行业鱼龙混杂。此时，数据的安全和保密工作将岌岌可危，毫无基础可言。因此，资产管理机构进行数据合规工作的前提和基础就是满足相关资质要求，并进行有效的保密工作。

（二）个人信息安全

数据合规的重要组成部分是个人信息安全。涉及个人信息安全的数据合规治理应包含如下组成部分：

- 1. 遵循个人金融信息处理的基本原则。**根据《个人信息保护法》，处理个人信息应当遵循合法、正当、必要和诚信原则，具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。此外，处理个人信息应当以告知同意为前提，除非存在法定豁免事由，需要在充分告知个人信息主体相关的信息处理方式和范围的基础上，获取其对个人信息处理活动的同意。而对于特别的个人信息（如敏感个人信息）或处理场景（如个人信息的传输、出境、公开），还需要在加强告知的基础上取得个人的单独同意。
- 2. 保障信息主体的知情权和请求权。**信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向信息主体告知信息处理者的名称或者姓名和联系方式，个人信息的处理目的、处理方式，处理的个人信息种类、保存期限以及信息主体行使法律规定权利的方式和程序等，充分保障信息主体的知情权；个人信息主体依法享有查阅、复制、可携、更正、删除、解释说明的权利，资产管理机构应当及时、便捷响应信息主体的上述请求权。

3. **确保个人金融信息存储和跨境流动安全。**资产管理机构应采取适当的技术措施，制定完善的内部管理制度和操作制度，明确个人信息处理的权限，防止个人信息被不当保存、处理和扩散；同时，面对数据跨境流动的趋势，机构应制定完善的内部风控体系，评估数据跨境的风险。特别是，如果资产管理机构已经掌握了 100 万人以上的个人信息，其业务或管理中涉及个人信息出境的，需要履行数据出境安全评估义务。

（三）重要数据安全

重要数据安全合规应包含如下要素：

1. **重要数据识别：**《金融数据安全 数据安全分级指南》（JR/T 0197 — 2020）（“《分级指南》”）就重要金融数据概念作出了规定。《分级指南》规定，重要数据通常主要用于金融业大型或特大型机构、金融交易过程中重要核心节点类机构的关键业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。数据安全性遭到破坏后，对国家安全造成影响或对公众权益造成严重影响。根据这一标准，重要数据的概念包含两个要素。其范围不涉及国家机密，但与国家安全、经济发展以及公共利益密切相关；其危害后果涉及国家安全、社会公共利益以及个人合法权益。
2. **重要数据保护：**就重要数据的保护，《网络数据安全条例（征求意见稿）》（“《条例》”）明确规定了其负责人、备案机制以及安全评估制度等。

《条例》要求，重要数据的处理者应当明确数据安全负责人，成立数据安全管理机构，落实数据安全保护责任。重要数据的处理者应当在识别重要数据后十五个工作日内向设区的市级网信部门备案，备案内容包括数据处理者的基本信息、处理数据的目的、规模、方式、范围、类型、存储期限、存储地点等。

此外，《条例》规定，处理重要数据或者赴境外上市的数据处理者需要履行数据出境安全评估义务，自行或者委托数据安全服务机构每年开展一次数据安全评估，并在每年 1 月 31 日前将上一年度数据安全评估报告报设区的市级网信部门，安全评估报告的内容包括处理重要数据的情况、数据安全风险及处置措施、数据安全管理制度、国家数据安全法律法规落实情况等。

四、资产管理领域数据合规特点和难点

（一）数据合规风险的全场景要求

资产管理机构面对的数据合规风险是全场景的，需要应对来自数据收集、流转以及处理等全过程的风险并进行有效管理。

具体而言，在数据收集阶段面临的主要问题是未贯彻“告知 — 同意”的处理原则，即未满足充分告知、自愿同意、明确授权、变更再次告知并征得同意、允许撤回同意等完整的规范要求。例如，对于特定身份、账户、行踪轨迹等敏感个人信息，或者对于个人信息传输、出境、公开等特殊场景，只有在具有特定目的和充分必要性时方可采集，且需要取得个人的单独同意，向个人告知处理的必要性以及对个人权益的影响。

在数据流转阶段面临的问题包括：未对敏感信息采取脱敏技术处理，或不当共享某些法律法规禁止共享的特定敏感信息和数据，以及利用自动化工具进行数据共享时，缺乏必要措施防范网络攻击等。在进行数据共享时，资产管理机构还面对共享数据安全审计、建立配套应急响应机制的要求，并应当按照有关要求向监管部门履行数据报送义务，确保数据接收方的身份真实性与数据完整性。并且，涉及数据

跨境的，还应注意履行数据跨境方面的安全评估等合规义务。

在数据处理阶段面临的风险包括超出“告知 — 同意”的范围处理个人信息、处理的合法性、正当性和必要性不足、以及将数据用于违法犯罪活动。“告知 — 同意”规则适用于数据处理阶段要求，在履行“告知 — 同意”义务之后，必须严格按照个人信息主体明确同意的范围进行处理，除非存在法定豁免事由，不得超出事前告知的处理目的和处理方式使用个人信息。尤其是向他人提供个人信息的，应当向个人告知接收方的名称、联系方式、处理目的、处理方式和个人信息种类，并取得个人的单独同意。此外，在处理个人信息等数据时，还应注意是否存在处理信息的必要性。并且，资产管理机构还应防止相关从业人员等将数据用于违法犯罪活动，如非法出售、提供投资者个人信息，将获取的个人信息出售或提供给他人从事犯罪活动等。

（二）数据跨境流动的特殊合规要求

如上文所述，在数据流转过程中，涉及数据跨境的部分，还应特别注意履行数据跨境方面的合规义务。由于资产管理机构处理的数据敏感程度较高、个人信息数量规模较大，很可能达到数据出境安全评估的门槛，因此，在进行数据合规治理时，我们需关注现行法律法规就数据出境安全评估所提出的要求。

《数据出境安全评估办法》规定了应当申报数据出境安全评估的情形，并就数据出境安全评估提出了具体要求。该法规定数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估并明确了重点评估事项。此外，《个人信息保护法》及《个人信息出境标准合同办法》也规定了未达到数据出境安全评估标准的情形下对于个人信息出境需要履行的合规程序。具体而言，数据出境所需履行的合规程序包括：

合规程序	适用场景
<p>需经数据出境安全评估</p>	<ul style="list-style-type: none"> ■ 向境外提供重要数据：重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据； ■ 关键信息基础设施运营者向境外提供个人信息：关键信息基础设施包括公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等； ■ 处理 100 万人以上个人信息的数据处理者向境外提供个人信息； ■ 自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息。
<p>通过订立个人信息出境标准合同开展个人信息出境活动的，需经个人信息保护影响评估</p>	<ul style="list-style-type: none"> ■ 非关键信息基础设施运营者； ■ 处理个人信息不满 100 万人的； ■ 自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的； ■ 自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。

其中，个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。敏感个人信息是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

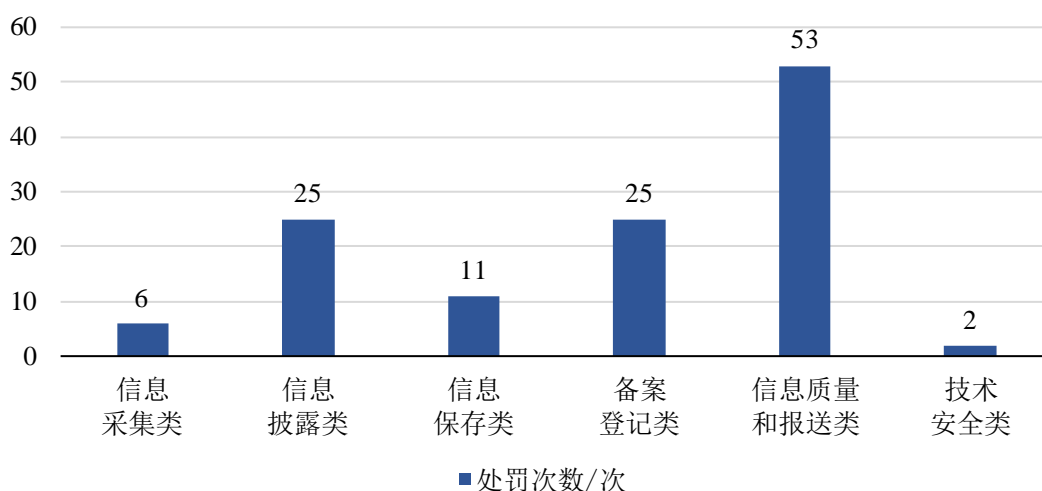
五、资产管理领域数据合规体系构建

（一）塑造科学的数据合规理念，持续跟踪国内外数据合规监管动态

面对渐趋严格的国内外数据合规监管环境，首先，资产管理机构应充分认识到个人信息与数据合规的重要性，在公司内部开展全方位数据合规培训，建立事前防范、事中监控、事后纠正并存的数据合规工作体系。资产管理机构应立足于数据合规风险和特定业务场景进行针对性制度设计。例如，对机构内部涉及重要数据和敏感信息的具体业务操作流程以及相关操作人员的分工、职责提供明确指引，细化使用权限的审批及管理控制流程，并建立常态化数据合规自评制度，定期开展数据合规风险自我审查，以保障数据合规工作制度的有效实施。

其次，资产管理机构应密切关注数据合规监管动态和实践经验。除参照目前已施行的《数据出境安全评估办法》《个人信息出境标准合同办法》等文件开展内部合规自查外，还需重点关注金融监管机构就数据合规颁布的规范和标准。同时，应关注行业内由数据合规问题导致的处罚案例，总结分析行业内数据合规方面易出现问题的情形。根据国家金融监督管理总局机关（“**金融监管总局机关**”）公布的《中国银行保险监督管理委员会行政处罚信息公开表》、中国证券投资基金业协会（“**基金业协会**”）公布的《纪律处分决定书》和中国人民银行公布的行政处罚公示统计，2022年资产管理领域数据合规问题出现频率最高的事由包括数据质量及数据报送违规、信息披露不合规、登记备案信息更新不及时、未按规定保存客户身份资料和交易记录等资料、违反信用信息采集、提供、查询及相关管理规定以及信息系统管控有效性不足等。

资产管理领域数据合规处罚事由统计



资产管理领域数据合规处罚事由统计（2022年）

如图所示，根据金融监管总局机关、基金业协会和中国人民银行公布的行政处罚公示统计，我们可以将资产管理领域数据合规的常见处罚事由分为六大类别。其中，信息采集类包括违反信用信息采集、提供、查询及相关管理规定等；信息披露类包括信息和数据记录不真实、未披露重大信息、信息披露不充分、提供虚假材料、未向投资者风险披露等；信息保存类包括未妥善保管基金募集、投资等相关资料；登记备案类包括登记备案信息更新不及时、产品备案信息与实际不符、未按规定备案登记等；信息质量与报送类包括未及时向基金业协会报送信息、向基金业协会填报的信息不准确、未及时报送重大信息、未按规定报送大额交易报告或者可疑交易报告以及数据质量及数据报送违法等；技术安全类包括信息系统管控有效性不足、信息技术部系统规则缺陷导致数据不真实等。这些问题散布于数据的收集、流转和处理阶段，与上述我们提及的数据合规的报送和评估要求相互印证，是我们开展数据合规工作时需重点关注的问题。

（二）注重复合型数据合规人才队伍建设，建立多部门协同合规机制

鉴于数据合规治理涉及多个领域，跨学科特性显著，资产管理机构不仅需要法律专业人才做好风险防控、降低法律风险，还需要技术人才从事数据合规技术研发，提升数据合规智能化水平。此外，金融人才应结合具体的交易和管理场景，开展合规指导，这也是必不可少的环节。因此，复合型数据合规人才队伍建设尤其必要。一方面，资产管理机构应引进数据合规专业人才，制定自动化、技术化的合规制度；另一方面应加强对合规人才队伍自身的定期数据安全合规培训与考核，提升其专业素质。

同时，数据合规工作无法一蹴而就，仅单独依靠数据合规部门的努力也难以达成目标。数据合规工作对资产管理机构全周期、全场景、全流程合规提出了更高要求，因此建立以数据合规部门为核心，投资研究、营销运营、法律合规等部门协同配合的整体机制已成必要。具体而言，数据合规部门可定期、分别召集各个部门，就相关领域数据合规出现的新法规、新标准进行解读，针对各自领域出现的数据合规问题进行磋商，并根据问题的性质和紧迫程度，分级别制定相应的解决方案和应急预案。此外，应在多部门合规机制中引入自动化、技术化合规工具，实现合规机制的智能化，以建立完善的具体业务场景下多部门协同的数据合规核查流程。

（三）构建合规风险评估、合规尽职调查和合规培训考试三位一体的数据保护合规体系

构建合规风险评估、合规尽职调查和合规培训考试三位一体的数据保护合规体系，首先在于建立严密的风险评估评估制度，对数据处理活动存在的风险点开展定期评估，保存评估报告和处理情况的记录，以检测诸如敏感个人信息、向第三方提供个人信息、数据跨境流动等合规风险点，并在必要时向监管部门报告或备案。其次，针对客户、第三方中介等，在合作前及合作过程中，资产管理机构应做好合规尽职调查工作，及时识别并沟通数据合规风险，以防承担连带责任。最后，应开展数据合规培训考试工作，通过发布数据保护合规政策、制作员工手册、开展培训会议等形式开展培训，并进行相应考试，提高相关部门人员的合规意识和合规能力，并采用录像、照片、签到本等方式，保证培训及考试全程已存留电子或书面记录，以证明公司已进行合规培训考试工作。

（四）注重数据跨境流动工作

首先，应密切关注不同国家和地区的数据立法进展，注重我国的数据合规法律要求与其他国家法律的协调性。除前述中国对数据出境的安全评估和标准合同要求之外，还应密切关注数据从海外传输至中国当地所应履行的合规义务，以实现数据的双向流动。其次，应根据不断变化的国内外数据治理合规要求调整数据处理策略和规则。如金融机构需根据不同国家和地区的标准，把握数据的存储时间长短及数据主体的删除权、修改权、可携带权、被遗忘权、限制处理权等要求。最后，在数据跨境流动过程中，

应注重数据出境的合法性、正当性和必要性，以及个人信息去标识化、匿名化、假名化处理，严格遵循《分级指南》的等级要求。

六、总结

综上所述，资产管理行业的个人信息保护与数据合规治理需要深入把握行业特点，结合具体业务场景，满足传统金融监管和信息安全与数据保护双重立法要求。同时，应注重资产管理领域日益出现的数据跨境趋势，满足数据合规的国际化要求，从合规理念、人员要求、机制建设、智能化管理等方面做好数据合规的全周期、全场景、全流程工作，以更好地利用数据要素，提升资产管理机构的治理水平与工作效率，实现资产管理行业的可持续发展。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

毛慧

电话： +86 21 6080 0506

Email: ellen.mao@hankunlaw.com

解石坡

电话： +86 10 8524 5866

Email: angus.xie@hankunlaw.com