HANKUN
汉坤律师事务所
Han Kun Law Offices

汉坤专递

2022 年第 2 期（总第 178 期）

新法评述

1、循序渐进：工信部再次征求数据安全管理办法意见

2、基金管理公司反洗钱工作持续赋能 —— 《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法》评述

新法评述

1、循序渐进：工信部再次征求数据安全管理办法意见

作者：段志超丨蔡克蒙[1]

2022 年 2 月 10 日，根据 2021 年 9 月 30 日公布的《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）（“**《管理办法》**”）收到的公开意见，工业和信息化部（“**工信部**”）对该法规草案进行了修改完善，再次面向社会征求意见，反馈截止时间为 2022 年 2 月 21 日。

2021 年以来，针对如何落实《中华人民共和国数据安全法》（“**《数据安全法》**”）以及《中华人民共和国个人信息保护法》（“**《个人信息保护法》**”），工信部和国家互联网信息办公室（“**网信办**”）分别出台了具体的实施细则，并侧重于不同领域。针对工业和信息化领域数据安全管理，工信部出台了上述《管理办法》，对接《数据安全法》等法律法规要求，在工业和信息化领域对国家数据安全管理制度进行细化，明确开展数据分类分级保护、重要数据管理等具体要求，构建工业和信息化领域数据安全监管体系[2]。针对网络数据[3]，网信办于 2021 年 11 月 14 日，公布了《网络数据安全管理条例（征求意见稿）》（“**《网络数据条例》**”）。该条例针对《数据安全法》和《个人信息保护法》中的相关制度设计了实施路径；针对上位法中的相关要求进行细化和明确；并创设增加了一些新的要求，例如重要数据处理者备案要求和年度报告要求、数据出境安全管理义务、网络平台责任等。

目前《管理办法》和《网络数据条例》均处在编写阶段，两者作为数据安全领域的两大主要监管部门工信部和网信办分别出台的实施细则，虽然部分内容存在交叉，但同时也强调了与数据本身属性相关的监管内容，潜在地为工信部和网信办之间的监管范围和路径做出了区别。

修改后的《管理办法》条目由原先的八章四十四条缩减为八章四十一条。

《管理办法》主要修改内容有：

- 强调个人信息单独保护：新增《个人信息保护法》作为目的依据。
- 扩充数据定义：将无线电数据纳入适用范围。
- 明晰监管机构职权范围：明确工信部对地方监管部门的督促指导作用。
- 修改分级分类标准：判定标准和细分标准发生变化。
- 明确备案机制：补充备案申请、审批、变更相关要求。

[1] 实习生赵怡冰对本文的写作亦有贡献。

[2] 参见《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》起草说明，访问地址：https：//www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20219/1d1668e46e644b42b04a95db43854607.pdf。

[3] “网络数据”指任何以电子方式对信息的记录，英文翻译为“cyber data”，不限于利用“网络”（internet 或 network）产生或在其中处理的数据。访问地址：https：//mp.weixin.qq.com/s/3uewzfNMEP_2Rr9SpaULnw。

- 严格主体责任：法定代表人负责制，加强内部管理。
- 更新全生命周期合规要求：取消核心数据不得出境，新增核心数据跨主体处理要求。
- 统筹协调数据安全审查：灵活化安全评估、监督协助等要求。

我们将在下文对比《管理办法》（0930 版）和《管理办法》（0210 版），梳理此次修订的重要内容，并同时提出我们的解读。

一、强调个人信息单独保护：新增《个人信息保护法》作为依据

在《管理办法》（0930 版）的起草说明中曾强调《管理办法》秉承《数据安全法》将个人信息纳入重要数据目录和核心数据目录进行重点保护的工作理念，将个人信息纳入数据全生命周期安全管理，不再单独提出个人信息保护的要求[4]。因此《管理办法》（0930 版）将《网络安全法》、《数据安全法》作为上位法基础，但并未提及《个人信息保护法》。但在此次最新发布的《管理办法》（0210 版）中，新增了《中华人民共和国个人信息保护法》作为目的依据，并且在具体条款中也调整了关于个人信息的规定，例如：

- 在第八条【分级分类方法】的数据分类类别列举中，删除了“个人信息”的表述，保留了原先的管理数据、运维数据、研发数据等非个人信息。
- 在第八章附则中新增第三十七条【个人信息保护】，“开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。”

综上可见，《管理办法》（0210 版）调整了对于个人信息的规制思路，由原先的“纳入重要数据目录和核心数据目录统一管理”到强调个人信息的单独保护。此变化是为了与此前发布的相关法律文件形成统一。在《管理办法》（0930 版）发布后，2021 年 11 月 14 日《网络数据条例》公开向社会征求意见，其中明确了重要数据和核心数据的定义，并不包含个人信息。此外，无论是 2021 年 9 月 23 日全国信息安全标准化技术委员会秘书处发布的国家标准《信息安全技术 重要数据识别指南》征求意见稿（“**《指南》**”）第一版，还是 2022 年 1 月 13 日发布的《指南》修订版，其中重要数据的定义中，均明确说明“重要数据不包括国家秘密和个人信息，但基于海量个人信息形成的统计数据、衍生数据有可能属于重要数据。”为实现法律规定的统一协调，此次《管理办法》（0210 版）中改变了对于个人信息管理的思路，强调《个人信息保护法》作为个人信息保护基础性法律的作用。

二、扩充数据定义：将无线电数据纳入适用范围

《管理办法》（0210 版）在第三条数据定义中修改了如下表述：

- 明晰了工业和信息化领域数据包括三类：即工业数据、电信数据和无线电数据。
- 删除行业领域的具体列举：在《管理办法》（0930 版）中，对工业和信息化领域进行了列举，如“原材料工业、装备工业、消费品工业、电子信息制造业、软件和信息技术服务业、民爆等行业领域”。但是在《管理办法》（0210 版）中，删除了列举表述，而是用“工业和信息化领域”作为统称，此修改更有抽象概括性，避免了无法穷尽列举和实践变化导致的法律不兼容问题。
- 新增无线电数据的定义：即“无线电数据是指在开展无线电业务活动中产生和收集的无线电频率、

[4] 参见《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》起草说明，访问地址：https：//www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20219/1d1668e46e644b42b04a95db43854607.pdf。

台（站）等电波参数数据”。《管理办法》（0210 版）在定义条款中将无线电数据纳入适用范围的同时，还对应修改了配套制度，例如新增“无线电频率、台（站）使用单位”作为工业和信息化领域数据处理者；新增无线电管理机构作为监管机构之一；将电磁所受影响纳入重要数据与核心数据判定标准。

三、明晰监管机构职权范围：明确工信部对地方监管部门的督促指导作用

《管理办法》（0210 版）中对中央和地方主管部门的职权进行了进一步明晰：

- 中央层面：要求工信部的监督管理活动需要遵守国家数据安全工作协调机制统筹安排。此前提的补充是为了解决此前数据监管“九龙治水”的局面，强调数据安全工作的统筹协调。
- 地方层面：《管理办法》（0930 版）中并未明晰层层监管的架构，尤其是中央层面对地方层面的监督。《管理办法》（0210 版）进行了修改，明确了工信部负责督促指导各省、自治区、直辖市及计划单列市、新疆生产建设兵团的地方工业和信息化主管部门、地方通信管理局和地方无线电管理机构；由地方工业和信息化主管部门、地方通信管理局和地方无线电管理机构负责监督本地区的数据处理活动。
- 强调上述行业（领域）监管部门需依照有关法律、行政法规的规定，依法配合有关部门开展的数据安全监管相关工作。

四、修改分级分类标准：判定标准和细分标准发生变化

《管理办法》再次重申了《数据安全法》确立的数据分类分级管理要求，在《管理办法》（0210 版）对分级分类工作要求、方法、一般数据、重要数据以及核心数据判断标准进行了修改调整。主要体现在以下方面：

- 工作要求：《管理办法》（0210 版）中将【分级分类工作要求】提前到第七条；地方工业和信息化主管部门、通信管理局、无线电管理机构新增了重要数据和核心数据具体目录上报更新义务；删除了企业应当坚持先分类后分级的工作方法。
- 分级分类方法：补充新增工业和信息化领域数据处理者可在一般数据、重要数据和核心数据三级基础上细分数据的类别和级别。
- 判定标准：取消“恢复数据或消除负面影响所需付出的代价程度”作为一般数据或重要数据的判定标准；在核心数据判断标准中，新增无线电数据场景。

然而，此次修改并未对“重大影响”、“严重影响”、“重大损害”等判断因素进行量化，故企业如何在实践中落实重要数据和核心数据的分级分类工作仍有待主管部门提供更明确的指引。

五、明确备案机制：补充备案申请、审批、变更相关要求

《管理办法》（0210 版）在《管理办法》（0930 版）的基础上，针对重要数据和核心数据目录备案义务进行了进一步细化和明晰，具体表现如下：

- 备案机构：明确工业和信息化领域数据处理者应当将本单位重要数据和核心数据目录向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）备案。

- 备案内容：调整了语言表述，对原先备案内容进行了更为严谨的整合；并明确备案内容不包括数据内容本身。
- 备案审核时间：要求地方工信部门、通信管理局、无线电管理机构在工业和信息化领域数据处理者提交备案申请的二十个工作日内完成审核工作。
- 审核结果：予以备案应发放备案凭证，同时将备案情况报工信部；不予备案的应当及时反馈备案申请人并说明理由。
- 备案变更要求：重要数据和核心数据的类别或规模变化 30%以上的，或者其它备案内容发生重大变化，工业和信息化领域数据处理者应当在发生变化的三个月内履行备案变更手续。
- 更新备案要求：销毁重要数据和核心数据需要向工信部门、通管局、无线电管理机构更新备案。

六、严格主体责任：法定代表人负责制，加强内部管理

《管理办法》（0930 版）中明确了企业落实数据安全管理义务的第一步将是建立健全数据安全组织架构，并进一步要求企业党委（党组）或领导班子对数据安全负主体责任、主要负责人是数据安全第一责任人、分管数据安全的负责人是数据安全直接责任人。而《管理办法》（0210 版）对原来的第十三条【主体责任】、第十四条【工作体系】、第十五条【关键岗位管理】和第十六条【数据收集】进行了整合，修改删减为第十三条【主体责任】。在内容上也进行相应调整：

- 确定法定代表人负责制：将“本单位党委（党组）或领导班子对数据安全负主体责任”改为“本单位法定代表人或者主要负责人是数据安全第一责任人”。此调整更符合法律责任要求，党委或领导班子是行政上的设计，无法适用于所有的企业，但是法定代表人是公司法制度的核心设计，体现了责任的承担，更适合担任数据安全责任人。
- 严格内部管理制度：针对重要数据和核心数据处理者，新增要求“建立内部登记、审批机制，对重要数据和核心数据的处理活动进行严格管理并留存记录”。

对于可能处理重要数据、核心数据的企业，需要密切关注此项调整，进而重新设计内部组织架构，可能承担责任的法定代表人、主要负责人、直接责任人以及关键岗位人员需提高数据合规重视度，积极参与数据安全的各类培训，提升数据治理专业能力。

七、更新全生命周期合规要求：取消核心数据不得出境，新增核心数据跨主体处理要求

《管理办法》（0210 版）针对数据全命周期的不同环节，再次更新了适用各级别数据的通用要求、以及处理重要数据与核心数据应遵守的额外要求。如下合规变化值得企业关注：

- 数据存储：新增存储重要数据和核心数据的，需定期开展数据恢复测试。
- 数据使用加工：删除“未经个人、单位等同意，不得使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原等加工处理活动”。
- 数据公开：删除“对涉及个人隐私、个人信息、商业秘密、保密商务信息不得公开”。
- 数据销毁：新增“销毁重要数据和核心数据的，应当及时向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）更新备案”。

- 数据出境：取消核心数据不得出境的要求，统一核心数据和重要数据出境监管要求，即确需向境外提供时，应当依法依规进行数据出境安全评估。

- 核心数据跨主体处理：新增第二十四条，要求跨主体提供、转移、委托处理核心数据的，应当评估安全风险，采取必要的安全保护措施，并经由地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报工信部。工信部按照有关规定进行审查。

- 用户权利响应：《管理办法》（0930 版）中第二十九条【举报投诉处理】中曾要求“工业和电信数据处理者应当建立用户投诉处理机制，公布电子邮件、电话、传真、在线客服等便捷有效的联系方式，配备受理用户投诉的人员接收数据安全相关投诉，并自接到投诉之日起 15 个工作日内答复投诉人”，此为强制性义务。但是在《管理办法》（0210 版）中删除了该表述，并改为了“鼓励工业和信息化领域数据处理者建立用户投诉处理机制”，减轻了数据处理者应对用户投诉的合规义务。

八、统筹协调数据安全审查：灵活化安全评估、监督协助等要求

根据此前的《管理办法》（0930 版），国家通过数据安全检测、评估、认证，以及监督检查、安全审查，落实数据安全监督管理。企业需要履行开展安全评估、协助监督检查以及通过数据安全审查的合规义务。此次，《管理办法》（0210 版）对第五章【数据安全监测、认证、评估管理】和第六章【监督检查】进行了灵活化调整，主要体现在以下方面：

- 放宽认证机构管理：此前《管理办法》（0930 版）第三十二条明确要求工业和信息化部和地方监管部门建立数据安全检测、评估与认证机构管理制度，制定机构认定标准，开展机构选拔认定、资质授权、日常管理和推荐目录发布等工作。但《管理办法》（0210 版）中删除了由监管部门开展机构选拔以及资质授权的要求，改为了“工业和信息化部鼓励、引导具备相应资质的机构，依据相关标准开展行业数据安全检测、认证工作”。

- 取消一般数据处理者的自评估要求：《管理办法》（0930 版）第三十三条鼓励一般数据处理者开展安全自评估，但是在《管理办法》（0210 版）中删除了该表述，仅强调重要数据和核心数据处理者应自行或委托第三方评估机构展开评估。

- 取消预留检查接口要求：《管理办法》（0930 版）第三十四条规定，企业有配合行业监管部门开展监督检查、并预留检查接口的义务。对于企业而言，主管部门可通过检查接口访问并审查的数据范围、接口的技术标准与调用条件，可能是企业最为关心的事项。但在《管理办法》（0210 版）中删除了预留检查接口这项要求，仅为笼统地要求企业配合监管部门检查。

- 统筹协调数据安全审查：《管理办法》（0930 版）第三十五条规定，工信部在国家数据安全工作协调机制指导下，对影响或可能影响国家安全的工业和电信数据处理活动开展数据安全审查。另一方面，2022 年 1 月 4 日，网信办、中国证券监督管理委员会等十三部委正式联合出台了修订后的《网络安全审查办法》，其中将数据处理活动纳入了审查范围，其中“核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险”是网络安全审查重点评估的因素。可见，若依据《管理办法》（0930 版）则数据处理者会同时面对基于工信部《管理办法》与网信办《网络安全审查办法》的双重审查。此次《管理办法》（0210 版）中删除了“对影响或可能影响国家安全的工业和电信数据处理活动开展数据安全审查相关工作”的要求，仅强调工信部需在国家数据安全工作协调机制指导下开展数据安全审查工作，对未来工信部和网信办如何统筹协调数据安全审查保留了灵活性。

九、结语

本次《管理办法》（0210 版）修改内容较多，除了以上重要实质合规义务的修改，在语言表述以及法律责任承担上也进行了调整（例如删除了将数据处理者的安全管理责任纳入信用管理和失信名单的要求）。此次调整体现了《管理办法》与相关法律法规的统筹协调，修正了相关概念表述，灵活调整了监管和合规思路。《管理办法》作为工业和信息化领域数据安全管理的顶层设计，提出了多项新增和细化的合规要求，建议工业和信息化领域数据处理者密切关注。

《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）修订对比

蓝色为删除部分，红色为增加内容

	工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）
第一章 总则	第一章 总则
第一条【目的依据】为了规范工业和信息化领域数据处理活动，加强数据安全管理，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家安全和发展利益，根据《中华人民共和国民法典》《中华人民共和国数据安全法》《中华人民共和国网络安全法》等法律法规，制定本办法。	第一条【目的依据】为~~了~~规范工业和信息化领域数据处理活动，加强数据安全管理，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家安全和发展利益，根据《~~中华人民共和国民法典》《~~中华人民共和国数据安全法》《中华人民共和国网络安全法~~》~~《中华人民共和国个人信息保护法》《中华人民共和国国家安全法》《中华人民共和国民法典》等法律法规，制定本办法。
第二条【适用范围】在中华人民共和国境内开展的工业和电信数据处理活动及其安全监管，应当遵守相关法律、行政法规和本办法的要求。	第二条【适用范围】在中华人民共和国境内开展的工业和信息化领域数据处理活动及其安全监管，应当遵守相关法律、行政法规和本办法的要求。
第三条【数据定义】工业数据是指原材料工业、装备工业、消费品工业、电子信息制造业、软件和信息技术服务业、民爆等行业领域，在研发设计、生产制造、经营管理、运维服务、平台运营、应用服务等过程中收集和产生的数据。 电信数据是指在电信业务经营活动中收集和产生的数据。 工业和电信数据处理者是指对工业、电信数据进行收集、存储、使用、加工、传输、提供、公开等数据处理活动的工业企业、软件和信息技术服务企业和取得电信业务经营许可证的电信业务经营者等工业和信息化领域各类主体。	第三条【数据定义】~~工业数据是指原材料工业、装备工业、消费品工业、电子信息制造业、软件和信息技术服务业、民爆等行业领域，在研发设计~~工业和信息化领域数据包括工业数据、电信数据和无线电数据。 工业数据是指工业各行业各领域在研发设计、生产制造、经营管理、运行维护、平台运营、~~应用服务~~等过程中产生和收集的数据。 电信数据是指在电信业务经营活动中产生和收集~~收集和产生~~的数据。 无线电数据是指在开展无线电业务活动中产生和收集的无线电频率、台（站）等电波参数数据。 工业和信息化领域数据处理者是指对工业和信息化领域数据进行收集、存储、使用、加工、传输、提供、公开等数据处理活动的工业企业、软件和信息技术服务企业、取得电信业务经营许可证的电信业务经营者和无线电频率、台（站）使用单位等工业和信息化领域各类主体。
第四条【监管机构】工业和信息化部负责对工业和电信数据处理者的数据处理活动和安全保护进行监督管理。各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门（以下统称地方	第四条【监管机构】~~工业和信息化部负责对工业和电信数据处理者的数据处理活动和安全保护进行监督管理。~~在国家数据安全工作协调机制统筹协调下，工业和信息化部负责督促指导各省、自治区、直辖

	工业和信息化领域数据安全管理办法（试行）（征求意见稿 2022 年 2 月 10 日版）
工业和信息化主管部门）负责对本地区工业数据处理者的数据处理活动和安全保护进行监督管理。各省、自治区、直辖市通信管理局（以下统称地方通信管理局）负责对本地区电信数据处理者的数据处理活动和安全保护进行监督管理。 工业和信息化部及地方工业和信息化主管部门、通信管理局统称为行业监管部门。	市及计划单列市、新疆生产建设兵团工业和信息化主管部门（以下统称地方工业和信息化主管部门）~~负责对本地区工业数据处理者的数据处理活动和安全保护进行监督管理。~~，各省、自治区、直辖市通信管理局（以下统称地方通信管理局）~~负责对本地区电信数据处理者的数据处理活动和安全保护进行监督管理~~和各省、自治区、直辖市无线电管理机构（以下统称地方无线电管理机构）开展数据安全监管，对工业和信息化领域数据处理者的数据处理活动和安全保护进行监督管理。 地方工业和信息化主管部门负责对本地区工业数据处理者的数据处理活动和安全保护进行监督管理。地方通信管理局负责对本地区电信数据处理者的数据处理活动和安全保护进行监督管理。地方无线电管理机构负责对本地区无线电数据处理者的数据处理活动和安全保护进行监督管理。 工业和信息化部及地方工业和信息化主管部门、通信管理局、无线电管理机构统称为行业（领域）监管部门。 行业（领域）监管部门依照有关法律、行政法规的规定，依法配合有关部门开展的数据安全监管相关工作。
第五条【产业发展】行业监管部门鼓励数据开发利用和数据安全技术研究，支持推广数据安全产品和服务，培育数据安全企业、研究和服务机构，壮大数据安全产业，提升数据安全保障能力，促进数据的创新应用。 工业和电信数据处理者研发提供数据开发利用新技术、新产品、新服务，应当有利于促进经济社会和行业发展，符合社会公德和伦理。	第五条【产业发展】行业（领域）监管部门鼓励数据开发利用和数据安全技术研究，支持推广数据安全产品和服务，培育数据安全企业、研究和服务机构，~~壮大~~发展数据安全产业，提升数据安全保障能力，促进数据的创新应用。 工业和信息化领域数据处理者研究、开发、使用数据新技术、新产品、新服务，应当有利于促进经济社会和行业发展，符合社会公德和伦理。
第六条【标准制定】行业监管部门推进工业和信息化领域数据开发利用和数据安全标准体系建设，组织开展行业标准制修订工作。鼓励支持企业、研究机构、高等院校、行业组织等不同主体，开展国际标准、国家标准、团体标准、企业标准制定。引导工业和电信数据处理者开展数据管理、数据安全贯标达标工作。	第六条【标准制定】行业（领域）监管部门推进工业和信息化领域数据开发利用和数据安全标准体系建设，组织开展行业相关标准制修订工作。鼓励支持企业、研究机构、高等院校、行业组织等不同主体，合作开展国际标准、国家标准、行业标准、团体标准、企业标准制定。引导工业和信息化领域数据处理者开展数据管理、数据安全贯标达标工作。

	工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）
第二章 数据分类分级管理	第二章 数据分类分级管理~~-~~
	~~第十一条~~第七条【分类分级工作要求】工业和信息化部组织制定工业和信息化领域数据分类分级、重要数据和核心数据识别认定、数据分级防护等标准规范~~制度规范~~，指导开展数据分类分级~~防护~~管理工作，~~形成~~制定行业重要数据和核心数据具体目录并实施动态管理。 地方工业和信息化主管部门、通信管理局、无线电管理机构组织开展本地区~~工业、电信行业~~工业和信息化领域数据分类分级~~防护~~管理及重要数据和核心数据识别~~认定~~工作，确定~~形成~~本地区行业（领域）重要数据和核心数据具体目录并上报工业和信息化部，目录发生变化的，应当及时上报更新。 ~~工业和电信数据处理者应当建立健全数据分类分级管理制度，将重要数据和核心数据目录报送地方工业和信息化主管部门或通信管理局，并采取措施开展数据分级防护，对重要数据进行重点保护，对核心数据在重要数据保护基础上实施更严格的管理和保护。不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护。~~ 工业和信息化领域数据处理者应当定期梳理数据，按照相关标准规范识别重要数据和核心数据并形成目录。
第七条【分类分级方法】工业和电信数据处理者应当坚持先分类后分级，定期梳理，根据行业要求、业务需求、数据来源和用途等因素对数据进行分类和标识，形成数据分类清单。数据分类类别包括但不限于研发数据、生产运行数据、管理数据、运维数据、业务服务数据、个人信息等。 工业和信息化部按照国家有关规定，根据数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益等造成的危害程度，将工业和电信数据分为一般数据、重要数据和核心数据三级。	~~第七条~~第八条【分类分级方法】~~工业和电信数据处理者应当坚持先分类后分级，~~根据行业要求、特点、业务需求、数据来源和用途等因素，~~对数据进行分类和标识，形成数据分类清单。~~工业和信息化领域数据分类类别包括但不限于研发数据、生产运行数据、管理数据、运维数据、业务服务数据等。~~个人信息等~~ ~~工业和信息化部按照国家有关规定，~~根据数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益等造成的危害程度，~~将工业和电信数据~~工业和信息化领域数据分为一般数据、重要数据和核心数据三级。 工业和信息化领域数据处理者可在此基础上细分数据的类别和级别。

	工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）
第八条【一般数据】危害程度符合下列条件之一的数据为一般数据： （一）对公共利益或者个人、组织合法权益造成较小影响，社会负面影响小； （二）受影响的用户和企业数量较少、生产生活区域范围较小、持续时间较短，对企业经营、行业发展、技术进步和产业生态等影响较小； （三）恢复数据或消除负面影响所需付出的代价小； （四）其他未纳入重要数据、核心数据目录的数据。	第八条第九条【一般数据】危害程度符合下列条件之一的数据为一般数据： （一）对公共利益或者个人、组织合法权益造成较小影响，社会负面影响小； （二）受影响的用户和企业数量较少、生产生活区域范围较小、持续时间较短，对企业经营、行业发展、技术进步和产业生态等影响较小； （三）恢复数据或消除负面影响所需付出的代价小； （四）其他未纳入重要数据、核心数据目录的数据。
第九条【重要数据】危害程度符合下列条件之一的数据为重要数据： （一）对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全相关数据的安全； （二）对工业、电信行业发展、生产、运行和经济利益等造成影响； （三）造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大； （四）引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响； （五）恢复数据或消除负面影响所需付出的代价大； （六）经行业监管部门评估确定的其他重要数据。	第九条第十条【重要数据】危害程度符合下列条件之一的数据为重要数据： （一）（二）对政治、国土、军事、经济、文化、社会、科技、电磁、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全相关数据的安全与国家安全相关的重点领域； （二）对工业、电信行业发展对工业和信息化领域发展、生产、运行和经济利益等造成严重影响； （三）造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大； （四）引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响； （五）恢复数据或消除负面影响所需付出的代价大；经工业和信息化部评估确定的其他重要数据。
第十条【核心数据】危害程度符合下列条件之一的数据为核心数据： （一）对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等构成严重威胁，严重影响海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全相关数据的安全； （二）对工业、电信行业及其重要骨干企业、关键信息基础设施、重要资源等造成严重影响； （三）对工业生产运营、电信和互联网运行和服务等	第十条第十一条【核心数据】危害程度符合下列条件之一的数据为核心数据： （一）对政治、国土、军事、经济、文化、社会、科技、电磁、网络、生态、资源、核安全等构成严重威胁，严重影响海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全相关数据的安全与国家安全相关的重点领域； （二）对工业、电信行业及其重要骨干企业对工业和信息化领域及其重要骨干企业、关键信息基础设

	工业和信息化领域数据安全管理办法（试行）（征求意见稿 2022 年 2 月 10 日版）
造成重大损害，导致大范围停工停产、大面积网络与服务瘫痪、大量业务处理能力丧失等； （四）经工业和信息化部评估确定的其他核心数据。	施、重要资源等造成~~严重~~重大影响； （三）对工业生产运营、~~电信和互联网~~电信网络（含互联网）运行和服务、无线电业务开展等造成重大损害，导致大范围停工停产、大面积无线电业务中断、大规模网络与服务瘫痪、大量业务处理能力丧失等；– （四）经工业和信息化部评估确定的其他核心数据。
第十一条【分类分级工作要求】工业和信息化部组织制定工业和信息化领域数据分类分级、重要数据和核心数据识别认定及数据分级防护等制度规范，形成行业重要数据和核心数据具体目录并实施动态管理，指导开展数据分类分级防护工作。 地方工业和信息化主管部门、通信管理局组织开展本地区工业、电信行业数据分类分级防护及重要数据和核心数据识别认定工作，形成本地区行业重要数据和核心数据具体目录并上报工业和信息化部。 工业和电信数据处理者应当建立健全数据分类分级管理制度，将重要数据和核心数据目录报送地方工业和信息化主管部门或通信管理局，并采取措施开展数据分级防护，对重要数据进行重点保护，对核心数据在重要数据保护基础上实施更严格的管理和保护。不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护。	~~第十一条~~第七条【分类分级工作要求】工业和信息化部组织制定工业和信息化领域数据分类分级、重要数据和核心数据识别认定、数据分级防护等标准规范~~制度规范~~，指导开展数据分类分级~~防护~~管理工作，~~形成~~制定行业重要数据和核心数据具体目录并实施动态管理。 地方工业和信息化主管部门、通信管理局、无线电管理机构组织开展本地区~~工业、电信行业~~工业和信息化领域数据分类分级~~防护~~管理及重要数据和核心数据识别~~认定~~工作，确定~~形成~~本地区行业（领域）重要数据和核心数据具体目录并上报工业和信息化部，目录发生变化的，应当及时上报更新。 ~~工业和电信数据处理者应当建立健全数据分类分级管理制度，将重要数据和核心数据目录报送地方工业和信息化主管部门或通信管理局，并采取措施开展数据分级防护，对重要数据进行重点保护，对核心数据在重要数据保护基础上实施更严格的管理和保护。不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护。~~ 工业和信息化领域数据处理者应当定期梳理数据，按照相关标准规范识别重要数据和核心数据并形成目录。
第十二条【重要数据和核心数据备案管理】工业和信息化部建立工业和信息化领域重要数据和核心数据备案管理制度，统筹建设备案管理平台。备案内容包括数据的数量、类别、处理目的和方式、使用范围、主体责任、安全保护措施等基本情况，数据提供、公开、出境、承接，以及数据安全风险、事件处置等情况。 地方工业和信息化主管部门、通信管理局应当分别对本地区工业、电信行业重要数据和核心数据备案	第十二条【重要数据和核心数据目录备案~~管理~~】~~工业和信息化部建立工业和信息化领域重要数据和核心数据备案管理制度，统筹建设备案管理平台。~~工业和信息化领域数据处理者应当将本单位重要数据和核心数据目录向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）备案。备案内容包括但不限于数据~~的数量~~、类别、级别、规模、处理目的和方式、使用范围、~~主体责任~~责任主体、对外共享、跨境传

	工业和信息化领域数据安全管理办法（试行）（征求意见稿 2022 年 2 月 10 日版）
内容进行审核，对不符合有关备案要求的，应当督促企业及时完善并重新进行备案。 工业和电信数据处理者应当按照有关要求进行备案，备案内容发生变化的，应在三个月内报备变更情况，同时对整体备案情况进行更新。	输、安全保护措施等基本情况，~~数据提供、公开、出境、承接，以及数据安全风险、事件处置等情况~~不包括数据内容本身。 地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）~~应当分别对本地区工业、电信行业重要数据和核心数据备案内容进行审核，对不符合有关备案要求的，应当督促企业及时完善并重新进行备案。~~应当在工业和信息化领域数据处理者提交备案申请的二十个工作日内完成审核工作，备案内容符合要求的，予以备案并发放备案凭证，同时将备案情况报工业和信息化部；不予备案的应当及时反馈备案申请人并说明理由。 重要数据和核心数据的类别或规模变化 30%以上的，或者其它备案内容发生重大变化的，工业和信息化领域数据处理者应当在发生变化的三个月内~~报备变更情况，同时对整体备案情况进行更新。~~履行备案变更手续。
第三章 数据全生命周期安全管理	第三章 数据全生命周期安全管理–
第十三条【主体责任】工业和电信数据处理者应当对数据处理活动负安全主体责任，根据数据的类型、数量、安全 级别、处理方式以及对国家安全、公共利益或者个人、组织合法权益带来的影响和安全风险等，采取必要措施确保数据持续处于有效保护和合法利用的状态。 （一）建立数据全生命周期安全管理制度，针对不同级别数据，制定数据收集、存储、使用、加工、传输、提供、公开等环节的具体分级防护要求和操作规程； （二）明确数据安全管理的主要负责人和责任部门，统筹负责数据处理活动的安全监督管理； （三）合理确定数据处理活动的操作权限，严格实施人员权限管理； （四）制定数据安全事件应急预案，并定期进行演练； （五）定期对从业人员开展数据安全教育和培训； （六）法律、行政法规规定的其他措施。	第十三条【主体责任】~~工业和电信~~工业和信息化领域数据处理者应当对数据处理活动负安全主体责任，~~根据数据的类型、数量、安全 级别、处理方式以及对国家安全、公共利益或者个人、组织合法权益带来的影响和安全风险等~~对各类数据实行分级防护，不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护，~~采取必要措施~~确保数据持续处于有效保护和合法利用的状态。 （一）建立数据全生命周期安全管理制度，针对不同级别数据，制定数据收集、存储、使用、加工、传输、提供、公开等环节的具体分级防护要求和操作规程； （二）~~明确数据安全管理的主要负责人和责任部门~~根据需要配备数据安全管理人员，统筹负责数据处理活动的安全监督管理，协助行业（领域）监管部门开展工作； （三）合理确定数据处理活动的操作权限，严格实施人员权限管理；–

	工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）
	（四）根据应对数据安全事件的需要，制定~~数据安全事件~~应急预案，并定期进行演练； （五）定期对从业人员开展数据安全教育和培训； （六）法律、行政法规等规定的其他措施。 工业和信息化领域重要数据和核心数据处理者，还应当： （一）建立覆盖本单位相关部门的数据安全工作体系，明确数据安全负责人和管理机构，建立常态化沟通与协作机制。本单位法定代表人或者主要负责人是数据安全第一责任人，领导团队中分管数据安全的成员是直接责任人； （二）明确数据处理关键岗位和岗位职责，并要求关键岗位人员签署数据安全责任书； （三）建立内部登记、审批机制，对重要数据和核心数据的处理活动进行严格管理并留存记录。
第十四条【工作体系】涉及重要数据和核心数据的，工业和电信数据处理者应当建立覆盖本单位相关部门的数据安全工作体系，设置专门的数据安全管理责任部门，本单位党委（党组）或领导班子对数据安全负主体责任，主要负责人是数据安全第一责任人，分管数据安全的负责人是直接责任人，明确各部门数据安全职责及人员，建立常态化沟通与协作机制。	~~第十四条【工作体系】涉及重要数据和核心数据的，工业和电信数据处理者应当建立覆盖本单位相关部门的数据安全工作体系，设置专门的数据安全管理责任部门，本单位党委（党组）或领导班子对数据安全负主体责任，主要负责人是数据安全第一责任人，分管数据安全的负责人是直接责任人，明确各部门数据安全职责及人员，建立常态化沟通与协作机制。~~
第十五条【关键岗位管理】工业和电信数据处理者应当确认数据处理关键岗位及人员，签署数据安全责任书，记录数据处理活动。	~~第十五条【关键岗位管理】工业和电信数据处理者应当确认数据处理关键岗位及人员，签署数据安全责任书，记录数据处理活动。~~
第十六条【安全同步】工业和电信数据处理者应当确保数据安全管理和技术保护手段与生产运营、业务发展同步规划、同步建设、同步运行。	~~第十六条【安全同步】工业和电信数据处理者应当确保数据安全管理和技术保护手段与生产运营、业务发展同步规划、同步建设、同步运行。~~
第十七条【数据收集】工业和电信数据处理者收集数据应当遵循合法、正当、必要的原则，不得窃取或者以其他非法方式收集数据。 数据收集过程中，应当采取配备技术手段、签署安全协议等措施加强对数据收集人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行记录。	~~第十七条~~第十四条【数据收集】~~工业和电信数据处理者收集数据应当遵循合法、正当、必要的原则~~工业和信息化领域数据处理者收集数据应当遵循合法、正当的原则，不得窃取或者以其他非法方式收集数据。 数据收集过程中，~~应当采取配备技术手段、签署安全协议等措施加强对数据收集人员~~应当根据数据安全级别采取相应的安全措施，加强重要数据和核心

	工业和信息化领域数据安全管理办法（试行）（征求意见稿 2022 年 2 月 10 日版）
通过间接途径获取数据的，应当要求数据提供方做出数据源合法性的书面承诺，并承担相应的法律责任。	数据收集人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行记录。 通过间接途径获取重要数据和核心数据的，工业和信息化领域数据处理者应当要求数据提供方做出数据源合法性的书面承诺，与数据提供方通过签署相关协议、承诺书等方式，明确双方法律责任。
第十八条【数据存储】工业和电信数据处理者应当依据法律规定或者与用户约定的方式和期限存储数据。存储重要数据的，还应当采用校验技术、密码技术等措施进行安全存储，不得直接提供存储系统的公共信息网络访问，并实施数据容灾备份和存储介质安全管理。存储核心数据的，还应当实施异地容灾备份。	第十八条第十五条【数据存储】工业和信息化领域数据处理者应当依据法律规定或者与用户约定的方式和期限存储数据。存储重要数据和核心数据的，应当采用校验技术、密码技术等措施进安全存储，不得直接提供存储系统的公共信息网络访问，并实施数据容灾备份和存储介质安全管理，定期开展数据恢复测试。存储核心数据的，还应当实施异地容灾备份。
第十九条【数据使用加工】工业和电信数据处理者未经个人、单位等同意，不得使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原等加工处理活动。利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。使用、加工重要数据和核心数据的，还应当加强访问控制，建立登记、审批机制并留存记录。 工业和电信数据处理者提供数据处理服务，涉及经营电信业务的，应当按照相关法律、行政法规规定取得电信业务经营许可。	第十九条第十六条【数据使用加工】未经个人、单位等同意，不得使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原等加工处理活动。工业和电信数据处理者工业和信息化领域数据处理者利用数据进行自动化决策分析的，应当保证决策分析的透明度和结果公平合理。使用、加工重要数据和核心数据的，还应当加强访问控制，建立登记、审批机制并留存记录。。 工业和电信数据处理者提供数据处理服务工业和信息化领域数据处理者提供数据处理服务，涉及经营电信业务的，应当按照相关法律、行政法规规定取得电信业务经营许可。
第二十条【数据传输】工业和电信数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据的，还应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施，涉及跨组织机构或者使用公共信息网络进行数据传输的，应当建立登记、审批机制。跨不同数据处理主体传输核心数据的，还应当通过国家数据安全工作协调机制审批。	第二十条第十七条【数据传输】工业和电信数据处理者工业和信息化领域数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据和核心数据的，应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施，涉及跨组织机构或者使用公共信息网络进行数据传输的，应当建立登记、审批机制。跨不同数据处理主体传输核心数据的，还应当通过国家数据安全工作协调机制审批。。
第二十一条【数据提供】工业和电信数据处理者应当依据行业数据分类分级管理要求，明确数据提供的范围、数量、条件、程序等。提供重要数据的，还应	第十八条【数据提供】工业和电信数据处理者工业和信息化领域数据处理者提供数据，应当依据行业数据分类分级管理要求，应当明确提供的范围、类

	工业和信息化领域数据安全管理办法（试行）（征求意见稿 2022 年 2 月 10 日版）
当采取数据脱敏等措施，建立审批机制。提供核心数据的，还应当通过国家数据安全工作协调机制审批。 工业和电信数据处理者应当事先对数据接收方的数据安全保护能力进行核实，并与数据接收方签订数据安全协议，明确数据提供的范围、使用方式、时限、用途以及相应的安全保护措施、违约责任，并督促数据接收方予以落实。	别、条件、程序等，~~应当事先对数据接收方的数据安全保护能力进行核实，~~并与数据获取方签订数据安全协议，~~明确数据提供的范围、使用方式、时限、用途以及相应的安全保护措施、违约责任，并督促数据接收方予以落实。~~。提供重要数据和核心数据的，应当对数据获取方数据安全保护能力进行评估或核实，采取必要的安全保护措施。
第二十二条【数据公开】工业和电信数据处理者公开数据应当真实、准确，并在公开前开展安全评估，对涉及个人隐私、个人信息、商业秘密、保密商务信息以及可能对公共利益及国家安全产生重大影响的，不得公开。	第十九条【数据公开】~~工业和电信数据处理者~~工业和信息化领域数据处理者公开数据~~应当真实、准确，并在公开前开展安全评估，对涉及个人隐私、个人信息、商业秘密、保密商务信息不得公开。~~应当在数据公开前分析研判可能对公共利益、国家安全产生的影响，存在重大影响的不得公开。
第二十三条【数据销毁】工业和电信数据处理者应当建立数据销毁策略和管理制度，明确销毁对象、流程和技术等要求，对销毁活动进行记录和留存。销毁重要数据和核心数据的，不得以任何理由、任何方式对销毁数据进行恢复。 符合以下情况之一的，工业和电信数据处理者应当销毁相应数据： （一）因业务约定，需要销毁的； （二）个人依据其合法权益请求销毁的； （三）组织基于保护国家安全、社会公共利益目的，且有第三方机构提供证明，请求销毁的。	第二十三条第二十条【数据销毁】~~工业和电信数据处理者~~工业和信息化领域数据处理者应当建立数据销毁制度~~策略和管理制度~~，明确销毁对象、规则、流程和技术等要求，对销毁活动进行记录和留存。个人、组织依据法律规定、合同约定等请求销毁的，工业和信息化领域数据处理者应当销毁相应数据。 销毁重要数据和核心数据的，应当及时向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）更新备案，不得以任何理由、任何方式对销毁数据进行恢复。 ~~符合以下情况之一的，工业和电信数据处理者应当销毁相应数据~~： （~~一~~）~~因业务约定，需要销毁的~~； （~~二~~）~~个人依据其合法权益请求销毁的~~； （~~三~~）~~组织基于保护国家安全、社会公共利益目的，且有第三方机构提供证明，请求销毁的。~~
第二十四条【数据出境】工业和电信数据处理者在中华人民共和国境内收集和产生的重要数据，应当依照法律、行政法规要求在境内存储，确需向境外提供的，应当依法依规进行数据出境安全评估，在确保安全的前提下进行数据出境，并加强对数据出境后的跟踪掌握。核心数据不得出境。	第二十四条第二十一条【数据出境】~~工业和电信数据处理者~~工业和信息化领域数据处理者在中华人民共和国境内收集和产生的重要数据和核心数据，法律、行政法规~~要求在境内存储~~有境内存储要求的，应当在境内存储，确需向境外提供的，应当依法依规进行数据出境安全评估~~，在确保安全的前提下进行数据出境，并加强对数据出境后的跟踪掌握。核~~

	工业和信息化领域数据安全管理办法（试行）（征求意见稿 2022 年 2 月 10 日版）
	~~心数据不得出境。~~ 工业和信息化部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，处理外国工业、电信、无线电执法机构关于提供工业和信息化领域数据的请求。非经工业和信息化部批准，工业和信息化领域数据处理者不得向外国工业、电信、无线电执法机构提供存储于中华人民共和国境内的工业和信息化领域数据。
第二十五条【数据承接】工业和电信数据处理者因兼并、重组、破产等原因需要转移数据的，应当明确数据承接方案，并通过电话、短信、邮件、公告等方式通知受影响用户。涉 及重要数据和核心数据的，应当及时向所在地工业和信息化主管部门或通信管理局备案。 作为数据承接方的工业和电信数据处理者，应当及时向 所在地工业和信息化主管部门或通信管理局备案，承担数据 安全责任和保护义务，不得违反国家有关规定及原数据处理者与用户的约定。 重要数据和核心数据没有承接方且符合销毁条件的，工业和电信数据处理者应当依法进行数据销毁。重要数据和核心数据没有数据承接方且不符合销毁条件的，工业和电信数据处理者应当及时上报所在地工业和信息化主管部门或通信管理局，将数据移交至行业监管部门指定的机构进行保存。	~~第二十五条【数据承接】~~第二十二条【数据转移】~~工业和电信数据处理者~~工业和信息化领域数据处理者因兼并、重组、破产等原因需要转移数据的，应当明确~~数据承接方案~~数据转移方案，并通过电话、短信、邮件、公告等方式通知受影响用户。 涉及重要数据和核心数据的，应当及时向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）更新备案。~~作为数据承接方的工业和电信数据处理者，应当及时向所在地工业和信息化主管部门或通信管理局备案，承担数据安全责任和保护义务，不得违反国家有关规定及原数据处理者与用户的约定。~~ ~~重要数据和核心数据没有承接方且符合销毁条件的，工业和电信数据处理者应当依法进行数据销毁。重要数据和核心数据没有数据承接方且不符合销毁条件的，工业和电信数据处理者应当及时上报所在地工业和信息化主管部门或通信管理局，将数据移交至行业监管部门指定的机构进行保存~~
第二十六条【委托处理】工业和电信数据处理者委托他人开展数据处理活动的，应当对被委托方的数据安全保护能力、资质进行核实，确保符合国家、行业主管部门的相关要求，并通过合同约束、现场核查等方式对被委托方落实数据安全保护措施的情况进行监督管理。委托处理重要数据和核心数据的，还应当委托取得相应认证资质的检测评估机构对被委托方进行安全评估。除法律、行政法规另有规定外，未经委托方同意，被委托方不得将数据提供给第三方。	~~第二十六条~~第二十三条【委托处理】~~工业和电信数据处理者~~工业和信息化领域数据处理者委托他人开展数据处理活动的，应当通过签订合同协议等方式，明确委托方与被委托方的数据安全责任和义务。委托处理重要数据和核心数据的，应当对被委托方的数据安全保护能力、资质进行评估或核实。~~确保符合国家、行业主管部门的相关要求，并通过合同约束、现场核查等方式对被委托方落实数据安全保护措施的情况进行监督管理。委托处理重要数据和核心数据的，还应当委托取得相应认证资质的检测评估机构对 被委托方进行安全评估。~~ 除法律、~~行政法规另有规定外~~行政法规等另有规定

	工业和信息化领域数据安全管理办法（试行）（征求意见稿 2022 年 2 月 10 日版）
	外，未经委托方同意，被委托方不得将数据提供给第三方。
	第二十四条【核心数据跨主体处理】跨主体提供、转移、委托处理核心数据的，应当评估安全风险，采取必要的安全保护措施，并经由地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报工业和信息化部。工业和信息化部按照有关规定进行审查。
第二十七条【安全审计】工业和电信数据处理者应当在 数据全生命周期处理过程中，记录数据处理、权限管理、人员操作等日志。日志留存时间不少于六个月，定期进行安全审计，并形成审计报告，涉及重要数据和核心数据的，应当至少每半年进行一次。	~~第二十七条【安全审计】~~第二十五条【日志留存】~~工业和电信数据处理者~~工业和信息化领域数据处理者应当在数据全生命周期处理过程中，记录数据处理、权限管理、人员操作等日志。日志留存时间不少于六个月~~，定期进行安全审计，并形成审计报告，涉及重要数据和核心数据的，应当至少每半年进行一次~~。
第四章 数据安全监测预警与应急管理	第四章 数据安全监测预警与应急管理
第二十八条【监测预警机制】工业和信息化部统筹建立工业和信息化领域数据安全风险监测机制，建设数据安全监测预警平台，对数据泄露、违规传输、流量异常等安全风险进行监测和预警，及时组织研判重要数据和核心数据安全风险并进行预警。 地方工业和信息化主管部门、通信管理局建设数据安全监测预警平台，组织开展本地区工业、电信行业数据安全风险监测，按照有关规定及时发布预警信息，通知本地区工业和电信数据处理者及时采取应对措施。 工业和电信数据处理者应当开展数据安全风险监测，及时排查安全隐患，采取必要的措施防范数据安全风险。	~~第二十八条~~第二十六条【监测预警机制】工业和信息化部~~统筹~~建立~~工业和信息化领域~~数据安全风险监测机制，~~，对数据泄露、违规传输、流量异常等安全风险进行监测和预警，及时组织研判重要数据和核心数据安全风险并进行预警。~~组织制定数据安全监测预警接口和标准，统筹建设数据安全监测预警技术手段，形成监测、溯源、预警、处置等能力，与相关部门加强信息共享。 地方工业和信息化主管部门、通信管理局和无线电管理机构~~建设数据安全监测预警平台~~建设本地区数据安全监测预警机制，组织开展本地区工业、电信行业~~和无线电~~数据安全风险监测，按照有关规定及时发布预警信息，通知本地区工业和~~电信数据~~信息化领域数据处理者及时采取应对措施。 ~~工业和电信数据~~工业和信息化领域数据处理者应当开展数据安全风险监测，及时排查安全隐患，采取必要的措施防范数据安全风险。
第二十九条【信息上报和共享】工业和信息化部统一汇集、分析、通报工业和信息化领域数据安全风险信息，鼓励安全服务机构、行业组织、科研机构等开展数据安全风险和事件等相关信息上报和共享。	~~第二十九条~~第二十七条【信息上报和共享】工业和信息化部~~统一汇集~~建立数据安全风险信息上报和共享机制，统一汇集、分析、研判、通报~~工业和信息化领域~~数据安全风险信息，鼓励安全服务机构、行

	工业和信息化领域数据安全管理办法（试行）（征求意见稿 2022 年 2 月 10 日版）
地方工业和信息化主管部门、通信管理局汇总分析本地区工业、电信行业数据安全风险和事件信息，及时将涉及重要数据和核心数据的安全风险上报工业和信息化部。 工业和电信数据处理者应当及时将自身数据安全风险情况向所在地工业和信息化主管部门或通信管理局报告。	业组织、科研机构等开展数据安全风险~~和事件等相关~~信息上报和共享。 地方工业和信息化主管部门、通信管理局和无线电管理机构汇总分析本地区工业、电信行业和无线电数据安全风险~~和事件信息~~，及时将~~涉及重要数据和核心数据的安全风险~~可能造成重大及以上安全事件的风险上报工业和信息化部。 ~~工业和电信~~工业和信息化领域数据处理者应当及时将~~自身数据安全风险情况~~可能造成较大及以上安全事件的风险向~~所在地~~地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报告。
第三十条【应急处置】工业和信息化部制定工业和信息化领域数据安全事件应急预案，组织协调重要数据和核心数据安全事件应急处置工作。 地方工业和信息化主管部门、通信管理局组织开展本地区工业、电信行业数据安全事件应急处置工作。涉及重要数据和核心数据的安全事件，应当立即上报工业和信息化部，并及时报告事件发展和处置情况。 工业和电信数据处理者在数据安全事件发生后，应当按照应急预案，及时开展应急处置，涉及重要数据和核心数据的安全事件，应当第一时间向所在地工业和信息化主管部门或通信管理局报告。事件处置完成后应当在规定期限内形成总结报告，每年向所在地工业和信息化主管部门或通信管理局报告数据安全事件处置情况。 工业和电信数据处理者对可能损害用户合法权益的数据安全事件，应当及时告知用户，并提供减轻危害措施。	~~第三十条~~第二十八条【应急处置】工业和信息化部制定工业和信息化领域数据安全事件应急预案，组织协调重要数据和核心数据安全事件应急处置工作。 地方工业和信息化主管部门、通信管理局和无线电管理机构组织开展本地区工业、电信行业和无线电数据安全事件应急处置工作。涉及重要数据和核心数据的安全事件，应当立即上报工业和信息化部，并及时报告事件发展和处置情况。 ~~工业和电信~~工业和信息化领域数据处理者在数据安全事件发生后，应当按照应急预案，及时开展应急处置，涉及重要数据和核心数据的安全事件，应当第一时间向~~所在地~~地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报告。事件处置完成后应当在规定期限内形成总结报告， 每年向~~所在地~~地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报告数据安全事件处置情况。~~工业和电信~~工业和信息化领域数据处理者对可能损害用户合法权益的数据安全事件，应当及时告知用户，并提供减轻危害措施。
第三十一条【举报投诉处理】工业和信息化部委托相关行业组织建立工业和信息化领域数据安全违法行为投诉举报渠道，及时向地方工业和信息化主管部门、通信管理局、工业和电信数据处理者下发相关投	~~第三十一条~~第二十九条【举报投诉处理】工业和信息化部委托相关行业组织建立工业和信息化领域数据安全违法行为投诉举报渠道，~~及时向地方工业和信息化主管部门、通信管理局、工业和电信数据处~~

	工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）
诉举报信息。地方工业和信息化主管部门、通信管理局组织工业和电信数据处理者对举报信息进行核实和依法处理，对涉及重要数据和核心数据安全问题的，开展执法调查。 工业和电信数据处理者应当建立用户投诉处理机制，公布电子邮件、电话、传真、在线客服等便捷有效的联系方式，配备受理用户投诉的人员接收数据安全相关投诉，并自接到投诉之日起 15 个工作日内答复投诉人。	~~理者下发相关投诉举报信息。~~地方工业和信息化主管部门、通信管理局、无线电管理机构建立本地区工业、电信行业和无线电数据安全违法 行为投诉举报机制或渠道，依法接收、处理投诉举报，根据工作需要开展执法调查~~组织工业和电信数据处理者对举报信息进行核实和依法处理，对涉及重要数据和核心数据安全问题的，开展执法调查。~~。鼓励工业和信息化领域数据处理者建立用户投诉处理机制。~~工业和电信数据处理者应当建立用户投诉处理机制，公布电子邮件、电话、传真、在线客服等便捷有效的联系方式，配备受理用户投诉的人员接收数据安全相关投诉，并自接到投诉之日起 15 个工作日内答复投诉人。~~
第五章 数据安全检测、评估与认证管理	第五章 数据安全检测、~~评估与认证管理~~ 认证、评估管理
第三十二条【安全能力认证】工业和信息化部建立数据安全检测、评估与认证机构管理制度，制定机构认定标准，开展机构选拔认定、资质授权、日常管理和推荐目录发布等工作。地方工业和信息化主管部门、通信管理局依据管理制度和认定标准，开展本地区工业、电信行业数据安全检测、评估与认证机构选拔认定、资质授权和管理等工作。	~~第三十二条【安全能力认证】~~第三十条【安全检测与认证】工业和信息化部鼓励、引导具备相应资质的机构，依据相关标准开展行业数据安全检测、认证工作。~~建立数据安全检测、评估与认证机构管理制度，制定机构认定标准，开展机构选拔认定、资质授权、日常管理和推荐目录发布等工作。地方工业和信息化主管部门、通信管理局依据管理制度和认定标准，开展本地区工业、电信行业数据安全检测、评估与认证机构选拔认定、资质授权和管理等工作。~~
第三十三条【安全评估】工业和信息化部制定工业和信息化领域数据安全评估规范，指导检测评估机构开展数据安全风险评估、合规评估等工作。地方工业和信息化主管部门、通信管理局负责组织开展本地区工业、电信行业数据安全评估。 工业和电信数据处理者应当依据数据安全评估规范，开展数据安全评估及整改。 （一）对于一般数据，鼓励开展数据安全自评估，对发现的数据安全风险问题进行及时整改； （二）对于重要数据和核心数据，应当至少每年自行或者委托推荐目录中的检测评估机构开展一次安全评估，并向所在地工业和信息化主管部门或通信管理局报告。	~~第三十三条~~第三十一条【安全评估】工业和信息化部制定行业数据安全评估机构管理制度，开展评估机构管理工作。制定行业数据安全评估规范，指导评估机构开展数据安全风险评估、合规评估、能力评估、出境评估等工作。 地方工业和信息化主管部门、通信管理局和无线电管理机构负责组织开展本地区工业、电信行业和无线电数据安全评估工作。~~ 工业和电信数据处理者应当依据数据安全评估规范，开展数据安全评估及整改。~~ ~~（一）对于一般数据，鼓励开展数据安全自评估，对发现的数据安全风险问题进行及时整改；~~ ~~（二）对于重要数据和核心数据，应当至少每年自~~

	工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）
	~~行或者委托推荐目录中的检测评估机构开展一次安全评估，并向所在地工业和信息化主管部门或通信管理局报告。~~ 工业和信息化领域重要数据和核心数据处理者应当自行或委托第三方评估机构，每年至少开展一次安全评估，及时整改风险问题，并向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）报送评估报告。
第六章 监督检查	第六章 监督检查~~-~~
第三十四条【监督检查和协助义务】工业和信息化部组织制定数据安全监测接口标准。行业监管部门对工业和电信数据处理者落实本规定要求的情况进行监督检查。工业和电信数据处理者应当配合行业监管部门依法开展监督检查，并预留检查接口。	~~第三十四条【监督检查和协助义务】~~第三十二条【监督检查和协助义务】~~工业和信息化部组织制定数据安全监测接口标准~~行业（领域）监管部门对~~工业和电信~~工业和信息化领域数据处理者落实本~~规定~~办法要求的情况进行监督检查。 ~~工业和电信~~工业和信息化领域数据处理者应当对行业（领域）监管部门监督检查予以配合。~~数据处理者应当配合行业监管部门依法开展监督检查，并预留检查接口。~~
第三十五条【数据安全审查】工业和信息化部在国家数据安全工作协调机制指导下，对影响或可能影响国家安全的工业和电信数据处理活动开展数据安全审查。	~~第三十五条~~第三十三条【数据安全审查】工业和信息化部在国家数据安全工作协调机制指导下，~~对影响或可能影响国家安全的工业和电信数据处理活动~~开展数据安全审查相关工作。
第三十六条【保密要求】行业监管部门及其委托的数据安全检测评估机构工作人员对在履行职责中知悉的个人信息和商业秘密等，应当严格保密，不得泄露、出售或者非法向他人提供。	~~第三十六条~~第三十四条【保密要求】行业（领域）监管部门及其委托的数据安全~~检测~~评估机构工作人员对在履行职责中知悉的个人信息和商业秘密等，应当严格保密，不得泄露~~、出售~~或者非法向他人提供。
第三十七条【约谈整改】行业监管部门在履行数据安全监督管理职责中，对未按要求进行重要数据和核心数据备案，或者发现数据处理活动存在重大安全风险或发生安全事件的，可以按照规定权限和程序对工业和电信数据处理者的法定代表人或者主要负责人进行约谈，并要求采取措施进行整改，消除隐患。	~~第三十七条~~第三十五条【约谈整改】行业（领域）监管部门在履行数据安全监督管理职责中，~~对未按要求进行重要数据和核心数据备案，或者~~发现数据处理活动存在~~重大~~较大安全风险~~或发生安全事件~~的，可以按照规定权限和程序对~~工业和电信~~工业和信息化领域数据处理者~~的法定代表人或者主要负责人~~进行约谈，并要求采取措施进行整改，消除隐患。
第七章 法律责任	第七章 法律责任
第三十八条【信用机制】行业监管部门应当将工业和	~~第三十八条【信用机制】行业监管部门应当将工业~~

	工业和信息化领域数据安全管理办法（试行） （征求意见稿 2022 年 2 月 10 日版）
电信数据处理者落实数据安全管理责任情况纳入信用管理。对存在数据安全违法违规行为受到行政处罚的数据处理者，按照有关规定将其列入业务经营不良名单或失信名单。	~~和电信数据处理者落实数据安全管理责任情况纳入信用管理。对存在数据安全违法违规行为受到行政处罚的数据处理者，按照有关规定将其列入业务经营不良名单或失信名单。~~
第三十九条【法律责任】对于违反本办法的，由行业监管部门依照《数据安全法》《网络安全法》等法律和相关行政法规，根据情节严重程度给予公开曝光、没收违法所得、罚款、暂停业务、停业整顿、关闭网站、吊销业务许可证或吊销营业执照等行政处罚；构成犯罪的，依法追究刑事责任。	~~第三十九条~~第三十六条【法律责任】有违反本办法~~规定行为的，~~由行业（~~领域~~）监管部门依照~~《数据安全法》《网络安全法》等法律和相关行政法规~~相关法律法规，根据情节严重程度给予~~公开曝光~~没收违法所得、罚款、暂停业务、停业整顿、吊销业务许可证~~关闭网站、或吊销营业执照~~等行政处罚；构成犯罪的，依法追究刑事责任。
第八章 附则	第八章 附则
	第三十七条【个人信息保护】开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。
第四十条【涉密排除】涉及国家秘密信息、密码使用等数据处理活动，按照国家有关规定执行。	~~第四十条【涉密排除】~~第三十八条【其他规定参照】涉及军事、国家秘密信息、密码使用等数据处理活动，按照国家有关规定执行。
第四十一条【军事数据排除】涉及军事的数据处理活动，按照国家有关规定执行。	~~第四十一条【军事数据排除】涉及军事的数据处理活动，按照国家有关规定执行。~~
第四十二条【政务数据排除】工业和信息化领域政务数据处理活动的具体办法，由工业和信息化部另行规定。	~~第四十二条~~第三十九条【政务数据排除】工业和信息化领域政务数据处理活动的具体办法，由工业和信息化部另行规定。
第四十三条【国防科工、烟草领域】国防科技工业、烟草领域数据安全管理由国防科工局、国家烟草专卖局负责，具体制度参照本办法另行制定。	~~第四十三条~~第四十条【国防科工、烟草领域】国防科技工业、烟草领域数据安全管理由国防科工局、国家烟草专卖局负责，具体制度参照本办法另行制定。
第四十四条【施行日期】本规定自 年 月 日起施行。	~~第四十四条~~第四十一条【施行日期】~~本规定自~~本办法自 2022 年 月 日起施行。

2、基金管理公司反洗钱工作持续赋能 — 《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法》评述

作者：葛音丨毛慧

一、反洗钱新规密集出台

随着国内金融业务发展创新、国际反洗钱要求不断提高，为进一步发挥反洗钱在建设现代金融体系、扩大金融业双向开放等领域中的作用，完善反洗钱法律制度的需求愈发迫切。2021 年全国人大、商务部、中国人民银行等立法机构和反洗钱行政主管部门出台了一系列对反洗钱监管有重大影响的法律法规，从跨境业务、风险评估、尽职调查等多个角度加强及完善了反洗钱相关制度和措施。

2021 年一系列反洗钱领域法律法规的密集出台反映了反洗钱监管要求从以“规则为本”到以“风险为本”的转变趋势，形式合规已无法满足相关监管要求。2021 年出台的主要反洗钱法律法规包括：2021 年 1 月 15 日中国人民银行颁布了《法人金融机构洗钱和恐怖融资风险自评估指引》并于同日生效，2021 年 1 月 19 日中国人民银行、国家外汇管理局颁布了《银行跨境业务反洗钱和反恐怖融资工作指引（试行）》并于 2021 年 2 月 18 日起施行，2021 年 3 月 31 日《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法（修订草案征求意见稿）》（“**《修订草案征求意见稿》**”）向社会公开征求意见，《中华人民共和国反洗钱法（修订草案公开征求意见稿）》也于 2021 年 6 月 1 日向社会公开征求意见。此外，2021 年 4 月 15 日中国人民银行颁布了《金融机构反洗钱和反恐怖融资监督管理办法》并于 2021 年 8 月 1 日起施行。

在此基础上，中国人民银行、银保监会、中国证监会日前联合印发了《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法》（中国人民银行、中国银行保险监督管理委员会、中国证券监督管理委员会令〔2022〕第 1 号）（“**《2022 办法》**”），自 2022 年 3 月 1 日起施行。《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》（中国人民银行、中国银行业监督管理委员会、中国证券监督管理委员会、中国保险监督管理委员会令〔2007〕第 2 号）（“**《2007 办法》**”）同时废止。《2022 办法》施行前发布的客户尽职调查和客户身份资料及交易记录保存的其他规定与《2022 办法》不一致的，以《2022 办法》为准。

二、《2022 办法》核心条款解读

金融机构是监测和打击洗钱活动的第一道防线，因此，对金融机构反洗钱工作的完善是维护金融体系稳健运行、维护公平公正的市场经济秩序的重中之重，对打击违法犯罪和维护社会稳定具有重要意义。公募基金行业兴起时间短，但其交易便捷、资金密集度高的特性给洗钱犯罪提供了便利，逐步成为洗钱行为滋生的新领域。随着洗钱犯罪形势日益严峻、国内外反洗钱标准日趋严格以及反洗钱监管和处罚力度不断加强，建立与基金管理公司业务特点相适应的反洗钱内部控制体系是当前公募基金行业反洗钱工作的重要议题。因此，我们就《2022 办法》项下与基金管理公司履行反洗钱义务相关的核心内容进行解读，以期为行业提供参考。

（一）关于适用范围

伴随着资产管理行业的发展及业务类型的多样化，相较于《2007 办法》，《2022 办法》第 2 条进一步扩大了金融机构的适用范围，增加了开发性金融机构、消费金融公司、贷款公司、理财公司、非银行支付机构、银行卡清算机构等适用主体，效力位阶更加细化。但《2022 办法》未明确基金管理公司子

公司是否纳入适用主体。根据《中国人民银行关于<金融机构反洗钱和反恐怖融资监督管理办法（征求意见稿）>公开征求意见的反馈》（“**《人行反馈》**”），“基金管理公司子公司的反洗钱要求由发起设立该子公司的基金管理公司进行覆盖，是否单独将其纳入反洗钱义务主体，需对基金管理公司子公司的反洗钱系统、人力资源配备等情况进一步梳理研究”，因此，基金管理公司子公司或被列入《2022 办法》所述的“中国人民银行确定并公布的从事金融业务的其他机构”范畴。我们理解，在基金管理公司子公司日常履行反洗钱义务的过程中，仍应参照适用《2022 办法》的相关规定。

值得注意的是，《2022 办法》的适用范围不包括私募基金管理人。根据《人行反馈》，私募基金管理人未被纳入的原因是（1）目前私募基金管理人的法律性质界定仍需进一步明确；且（2）从实践来看，我国私募基金管理人类型复杂、数量众多且工作人员普遍较少，难以统一监管要求并实质开展反洗钱工作。针对私募基金产品可能存在的洗钱风险问题，中国人民银行将会同相关主管部门进一步研究。

（二）关于国内外法律适用

近年来，国际和中国反洗钱形势发生了深刻而复杂的变化，反洗钱工作重心由制度建设转向关注实效，有效性与合规性并重的理念也成为国际共识。《2022 办法》规定了其原则上适用于金融机构境外分支机构和附属机构，并且进一步明确了其与境外分支机构和附属机构驻在国或地区法律规定竞合适用的相关规则。我们理解，基金管理公司及其境外子公司关于客户尽职调查和客户身份资料及交易记录保存义务相关法律法规的适用规则如下：

1. 原则上，基金管理公司及其境外子公司均应执行《2022 办法》的相关要求；
2. 境外子公司所在国家或地区法律有更严格要求的，遵守其规定；
3. 境外子公司所在国家或地区的相关规定更为宽松，但所在国家或地区法律禁止或者限制境外子公司实施《2022 办法》的，基金管理公司应当采取适当措施应对洗钱和恐怖融资风险，并向中国人民银行报告。

对于《2022 办法》新增的“金融机构应当采取适当措施应对洗钱和恐怖融资风险”，对基金管理公司及其境外子公司在上述第（3）类情形下的反洗钱管控能力提出较高的要求。

（三）关于建立信息共享机制

为提高金融机构反洗钱工作效率、便于金融机构对反洗钱风险的统一管理，《2022 办法》对反洗钱信息的同步和共享提出了更高的要求，“金融机构应当在总部层面对客户尽职调查、客户身份资料及交易记录保存工作作出统一部署或者安排，制定反洗钱和反恐怖融资信息共享制度和程序，以保证客户尽职调查、洗钱和恐怖融资风险管理工作有效开展。金融机构应当对其分支机构执行客户尽职调查制度、客户身份资料及交易记录保存制度的情况进行监督管理”。因此，基金管理公司股东、基金管理公司及分公司、基金管理公司子公司在开展反洗钱工作时，应建立相应的联动工作机制，例如建立统一的反洗钱客户尽职调查、客户身份资料及交易记录保存分类标准、风险应对预案、黑名单库等。在实际业务开展过程中，受限于系统、传输接口、代销机构信息保密要求等原因，代销机构客户身份信息的传输方面仍存在较大的改善空间，该情况也是公募基金行业普遍存在的行业共性问题。值得一提的是，该项规定为股东受托代销基金管理公司旗下产品场景下的客户信息的全面传输提供了强有力的支持。

就外资基金管理公司关心的上述“总部层面的统一部署或者安排”以及“信息共享”是否能包含向境外总部传输反洗钱信息的问题，《2022 办法》则并未明确说明。根据文义解释和我们的实践经验，由于中国的反洗钱法律法规并未明确说明如何进行跨境反洗钱信息传输，实践中外资基金管理公司可

以考虑与中国人民银行、中国证监会等反洗钱行政主管部门及时沟通，以便获得监管指示明确允许或禁止跨境传输的反洗钱信息范围。

（四）关于客户尽职调查

1. 《2022 办法》使用“客户尽职调查”取代了《2007 办法》的“客户身份识别”，删除了客户身份初次识别、持续识别、重新识别等概念，并突出强调“把握实质风险”原则。基金管理公司应当根据风险差异确定客户尽职调查措施的程度和具体方式，不应采取与风险状况明显不符的尽职调查措施，把握好防范风险与优化服务的平衡。

2. 《2022 办法》将客户尽职调查分设为“一般规定”和“其他规定”两节，分别明确在一般情形和特殊情形下的客户尽职调查要求。其中，针对高风险情形或客户，《2022 办法》进一步明确了强化尽职调查从事前调查到事后限制的具体措施。针对低风险情形和客户，《2022 办法》参照《金融机构洗钱和恐怖融资风险评估及客户分类管理指引》的规定，适用简化尽职调查程序并进一步明确了简化尽职调查时应当采取的识别方式。相较于《修订草案征求意见稿》，《2022 办法》强调“根据风险高低调整所提供的服务范围和业务功能”，并允许对同类型的客户、业务进行批量处理。

3. 信息技术的不断发展推动了大数据时代的来临，相应的客户身份信息核实手段要求多措并举。《2022 办法》对客户身份信息核实手段予以明确，可以单一使用或结合使用以下方式：

(1) 通过公安、市场监督管理、民政、税务、移民管理等部门或者其他政府公开渠道获取的信息核实客户身份；

(2) 通过外国政府机构、国际组织等官方认证的信息核实客户身份；

(3) 客户补充其他身份资料或者证明材料；

(4) 中国人民银行认可的其他信息来源。

其中，银行履行客户尽职调查义务时，按照法律、行政法规、部门规章的规定需核实相关自然人的第二代居民身份证的，应当通过中国人民银行建立的联网核查公民身份信息系统进行核查。

目前针对基金管理公司的代销客户，相关的客户身份信息核查和验证一般由代销机构开展；而针对基金管理公司的直销客户（包括柜台直销和线上直销），目前大部分基金管理公司也已建立了客户身份信息联网核查机制，一般通过证通或国政通对直销客户进行联网核查，符合《2022 办法》要求的“金融机构运用互联网和移动通信等信息通信技术，依法以非面对面形式与客户建立业务关系或者为客户提供金融服务时，应当建立有效的客户身份认证机制，通过有效措施识别并核实客户身份”的要求。

（五）关于受益所有人识别情形

根据《2022 办法》第 22 条，金融机构开展客户尽职调查时，对于客户为法人或者非法人组织的，应当识别并核实客户身份，了解客户业务性质、所有权和控制权结构，识别并采取合理措施核实客户的受益所有人，即通过以下方式最终拥有或者实际控制法人或者非法人组织的一个或者多个自然人：

1. 直接或者间接拥有法人或者非法人组织 25%（含）以上股权或合伙权益的自然人；

2. **单独**或者联合对法人或者非法人组织进行实际控制的自然人，包括但不限于通过协议约定、亲属关系等方式实施控制，如决定董事或者高级管理人员的任免，决定重大经营、管理决策的制定或者执行，决定财务收支，长期实际支配使用重要资产或者主要资金等；

3. 直接或者间接享有法人或者非法人组织 25%（含）以上收益权的自然人。

金融机构应当综合使用上述三种方式识别并核实客户的受益所有人，当使用上述方式均无法识别受益所有人时，识别法人或者非法人组织的高级管理人员。

《2022 办法》关于受益所有人的识别要求沿用了《非居民金融账户涉税信息尽职调查管理办法》（“**《管理办法》**”）的类似规定，根据《管理办法》第 13 条，公司的控制人按照以下规则依次判定：

1. 直接或者间接拥有超过 25%公司股权或者表决权的个人；

2. 通过人事、财务等其他方式对公司进行控制的个人；

3. 公司的高级管理人员。

合伙企业的控制人是拥有超过 25%合伙权益的个人。

信托的控制人是指信托的委托人、受托人、受益人以及其他对信托实施最终有效控制的个人。

基金的控制人是指拥有超过 25%权益份额或者其他对基金进行控制的个人。

此前《管理办法》关于“控制人”的认定在实际操作中遇到较多障碍，如存在基金管理公司与投资人对于该条款理解和适用存在不一致的情形，或理解和适用达成一致但实际执行存在困难的情形。因此，未来在适用《2022 办法》进行“受益所有人”识别的过程中，基金管理公司还应视业务情形制订具体的内部判定细节方案，并与投资人提前做好沟通。

（六）关于业务中止的适用情形

根据《2022 办法》，若客户先前提交的身份证件或者其他身份证明文件已过有效期，基金管理公司在履行必要的告知程序后，客户未在合理期限内更新且未提出合理理由的，基金管理公司应当中止为客户办理业务。

相较于《2007 办法》，《2022 办法》增加了“履行必要的告知程序”的前置条件。基金管理公司在实际业务开展过程中，应提前做好关于必要告知程序的设计、执行、与客户的互动等环节的相应部署，以实现反洗钱义务履行与客户或有投诉之间的有效平衡。

（七）关于客户风险动态评估

《2022 办法》明确了“风险为本”以及“风险跟踪”的尽职调查原则，要求对客户的相关信息持续关注，并通过及时调整风险等级等方式采取相应措施。基金管理公司应当持续关注客户的风险状况、交易情况和身份信息变化，及时调整客户洗钱和恐怖融资风险等级。基于前述客户风险等级动态评估的前提，《2022 办法》减少了洗钱或者恐怖融资风险等级最高客户的定期审核频次，将审核频次由至少每半年进行一次审核调整为至少每年进行一次审核。

（八）关于客户重新尽职调查

相较于《2007 办法》，《2022 办法》对于重新对客户进行尽职调查的情形进行了优化，触发重新尽职调查的情形包括：客户风险状况发生变化，客户变更经营范围及受益所有人，客户先前提交的身份证件或者其他身份证明文件已过有效期，以及其他情形等。虽然前述内容与《基金管理公司反洗钱客户风险等级划分标准指引（试行）》及《中国人民银行关于证券期货业和保险业金融机构严格执行反洗钱规定防范洗钱风险的通知》的相关要求一脉相承，但《2022 办法》对此进行了进一步的明确，为基金管

理公司反洗钱日常工作开展提供有效抓手。

（九）关于客户身份信息的电子化管理

随着反洗钱工作开展的逐渐系统化、集成化、标准化，《2022 办法》第 45 条新增了对反洗钱信息的电子化管理要求，金融机构应当采取必要的管理措施和技术措施，逐步实现以电子化方式完整、准确保存客户身份资料及交易信息，防止客户身份资料及交易记录缺失、损毁，防止泄漏客户身份信息及交易信息。金融机构客户身份资料及交易记录的保存方式和管理机制，应当确保足以重现和追溯每笔交易，便于金融机构反洗钱工作开展，以及反洗钱调查和监督管理。

我们理解，基金管理公司应当以可稽核、可回溯、强备份、防泄漏的方式保存客户身份资料以及交易信息，同时，《2022 办法》还依据《中华人民共和国个人信息保护法》、《中华人民共和国反洗钱法》等有关个人信息、反洗钱信息保护的相关规定，强化了“依法保护商业秘密和个人信息”。

（十）关于客户身份基本信息要素

根据目前现行的三证合一政策，《2022 办法》对《2007 办法》中关于“客户身份基本信息”的要素进行了调整，包括非自然人客户删除了组织机构代码、税务登记证号码等要素。另外，用“受益所有人”一词取代了“控股股东”或者“实际控制人”的原有表述，并与《2022 办法》全文的其他表述保持一致。

对比《修订草案征求意见稿》，《2022 办法》中在自然人客户信息中删除了“工作单位”要素，与《2007 办法》中关于自然人客户“身份基本信息”的要素保持一致。

三、未来拟重点加强的工作

近年来，为有效应对反洗钱金融行动特别工作组（FATF）对我国的反洗钱和反恐怖融资工作的评估，加强金融行业反洗钱监管，各市场参与主体反洗钱风险管控任务重大。而在履行反洗钱义务的过程中，洗钱风险防控体系不健全，业务、产品洗钱风险评估不足，不能以风险为导向分配反洗钱资源；人员配备、系统建设滞后；客户尽职调查不充分，客户资料不完整；可疑交易监测分析手段不足；未对大额申购资金的来源建立实质性审查机制等，一直是行业探讨较多且有待持续改善和优化的问题。

下一步，针对上述问题及结合《2022 办法》的相关要求，我们认为，基金管理公司应加强如下重点工作的后续推进和开展。

（一）建立客户分类尽职调查机制

根据《2022 办法》第 7 条，金融机构在与客户建立业务关系、办理规定金额以上一次性交易和业务关系存续期间，怀疑客户及其交易涉嫌洗钱或恐怖融资的，或者对先前获得的客户身份资料的真实性、有效性或完整性存疑的，应当开展客户尽职调查，采取以下尽职调查措施：

1. 识别客户身份，并通过来源可靠、独立的证明材料、数据或者信息核实客户身份；
2. 了解客户建立业务关系和交易的目的和性质，并根据风险状况获取相关信息；
3. 对于洗钱或者恐怖融资风险较高的情形，了解客户的资金来源和用途，并根据风险状况采取强化的尽职调查措施；
4. 在业务关系存续期间，对客户采取持续的尽职调查措施，审查客户状况及其交易情况，以确认为客

户提供的各类服务和交易符合金融机构对客户身份背景、业务需求、风险状况以及对其资金来源和用途等方面的认识；和

5. 对于客户为法人或者非法人组织的，识别并采取合理措施核实客户的受益所有人。

金融机构应当根据风险状况差异化确定客户尽职调查措施的程度和具体方式，不应采取与风险状况明显不符的尽职调查措施，把握好防范风险与优化服务的平衡。

为满足上述要求，基金管理公司应建立客户分类尽职调查工作机制，层层递进，例如，基金管理公司对直销个人客户通过证通或国政通进行身份证验证，对直销机构客户通过国家企业信用信息公示系统等网站进行身份核实；通过调查问卷设计、结合客户身份分析等方式对客户的交易目的进行分析；通过建立可疑交易模型进行持续筛查，结合客户历史交易信息进行人工可疑交易甄别；制作材料清单请客户配合提供公司章程、相关证明文件等。

（二）建立事后身份核实工作机制

根据《2022 办法》第 25 条，金融机构应当在建立业务关系或者办理一次性交易时，核实客户及其受益所有人身份。在有效管理洗钱和恐怖融资风险的情况下，对于难以中断的正常交易，金融机构可以在建立业务关系后尽快完成客户及其受益所有人身份核实工作。金融机构在未完成客户及其受益所有人身份核实工作前为客户办理业务的，应当采取适当的风险管理措施。

对于基金管理公司而言，事后进行身份核实的方式可以提高日常业务开展的效率。也即，对于难以中断的正常交易，身份证验证可于每日日终合并完成，通过证通、国政通、国家企业信用信息公示系统等网站进行身份核实的工作也可有条件地适当延后进行，但基金管理公司应建立事后身份核实的风险管理措施，可以考虑采取实行针对身份核实有误、黑名单筛查匹配等情况的后续限制交易、取消事后身份核实待遇等相关措施。

（三）建立强化尽职调查体系

根据《2022 办法》第 29 条，金融机构与客户建立业务关系时或者业务存续期间，综合考虑客户特征、业务关系、交易目的、交易性质、资金来源和用途等因素，对于存在较高洗钱或者恐怖融资风险情形的，或者客户为国家司法、执法和监察机关调查、发布的涉嫌洗钱或者恐怖融资及相关犯罪人员的，应当根据风险状况采取强化尽职调查措施。

根据《2022 办法》第 30 条，对于洗钱或者恐怖融资风险较高的情形以及高风险客户，金融机构应当根据风险情形采取相匹配的以下一种或者多种强化尽职调查措施：

1. 获取业务关系、交易目的和性质、资金来源和用途的相关信息，必要时，要求客户提供证明材料并予以核实；

2. 通过实地查访等方式了解客户的经济状况或者经营状况；

3. 加强对客户及其交易的监测分析；

4. 提高对客户及其受益所有人信息审查和更新的频率；

5. 与客户建立、维持业务关系，或者为客户办理业务，需要获得高级管理层的批准。

金融机构采取强化尽职调查措施后，认为需要对客户的洗钱或者恐怖融资风险进行风险管理的，应

当对客户的交易方式、交易规模、交易频率等实施合理限制，认为客户的洗钱或者恐怖融资风险超出金融机构风险管理能力的，应当拒绝交易或者终止已经建立的业务关系。

针对《2022 办法》所要求的强化尽职调查的场景，“存在较高洗钱或者恐怖融资风险情形的”或“客户为国家司法、执法和监察机关调查、发布的涉嫌洗钱或者恐怖融资及相关犯罪人员的”，基金管理公司应就前述两类情形进一步细化具体场景和适用情形。

针对采取强化尽职调查措施后，“认为需要对客户的洗钱或者恐怖融资风险进行风险管理的”以及“认为客户的洗钱或者恐怖融资风险超出金融机构风险管理能力的”的情形，基金管理公司应就此建立一套完整的评估体系和应对预案，来对应后续的“对客户的交易方式、交易规模、交易频率等实施的合理限制”，以及“拒绝交易或者终止已经建立的业务关系”的处理方式。

（四）建立简化尽职调查体系

根据《2022 办法》第 31 条，金融机构参考以下信息，结合客户特征、业务关系或者交易目的和性质，经过风险评估且具有充足理由判断某类客户、业务关系或者交易的洗钱和恐怖融资风险较低时，可以采取相匹配的简化尽职调查措施：

1. 国家洗钱风险评估报告；
2. 中国人民银行发布的反洗钱、反恐怖融资以及账户管理相关规定及指引、风险提示、洗钱类型分析报告和风险评估报告；
3. 其他法律、行政法规有相关规定的。

金融机构采取简化尽职调查措施时，应当至少识别并核实客户身份，登记客户的姓名或者名称、联系方式、有效身份证件或者其他身份证明文件的种类、号码和有效期限等信息，留存客户尽职调查过程中必要的身份资料。对已采取简化尽职调查措施的客户、业务关系或者交易，金融机构应当定期审查其风险状况，根据风险高低调整所提供的服务范围和业务功能；客户、业务关系或者交易存在洗钱和恐怖融资嫌疑或者高风险的情形时，金融机构不得采取简化尽职调查措施。

简化尽职调查旨在减轻基金管理公司等金融机构日常反洗钱工作开展的负担，基金管理公司应相应建立客户反洗钱分级管理方案。鉴于基金管理公司对简化尽职调查的适用有一定的自由裁量权，可据此建立相应的简化尽职调查评估标准以及后续简化尽职调查的识别及审查方法。同时，目前基金管理公司在履行客户身份识别义务时，对客户进行分级识别的工作机制并不成熟，因此，此项规定对基金管理公司未来适用简化识别情形提出较高的挑战。

（五）梳理与第三方合作机制

根据《2022 办法》第 39 条，第三方应当严格按照法律规定和合同约定履行相应的客户尽职调查义务，并向金融机构提供必要的客户身份信息；金融机构对客户身份信息的真实性、准确性或者完整性有疑问的，或者怀疑客户涉嫌洗钱或恐怖融资的，第三方应当配合金融机构开展客户尽职调查。第三方未按照规定配合金融机构履行客户尽职调查义务的，应当承担相应责任。

目前基金管理公司在开展反洗钱工作过程中，存在代销客户信息完整率较低、存量客户信息亟待补充完善以及基金公司核心系统被个别供应商行业垄断导致相应的系统改造进度缓慢的行业共性问题。对于代销客户信息完整率较低的问题，基金管理公司目前只能通过与代销机构积极沟通的方式，协商客户信息提供方式的优化工作。针对行业呼声较高亟待解决的“由于与代销渠道客户信息传输机制不顺

畅所导致的客户身份基本信息核实、客户风险等级划分有效性不足等问题”，《2022 办法》新增的“第三方未按照规定配合金融机构履行客户尽职调查义务的，应当承担相应责任”，拟改善前述行业痛点，基金管理公司可重新梳理与代销渠道的协议文本、系统对接、日常业务配合等事项，以期未来更顺畅地推进该项工作。

（六）客户尽职调查的查漏补缺

根据《2022 办法》第 51 条，金融机构对该办法施行前已经建立业务关系或者进行交易的存量客户，未满足该办法有关客户尽职调查要求的，应当自该办法施行之日起 1 年内完成较高风险以上存量客户的尽职调查，自该办法施行之日起 2 年内完成全部存量客户的尽职调查。

因此，基金管理公司应对客户进行分层管理，相应梳理客户风险等级，并针对不同风险等级的存量客户安排阶梯式尽职调查规划，并在 2024 年 3 月 1 日前完成全部存量客户的尽职调查。

四、新旧法规对比一览表

点击此处查看新旧法规对比一览表。

特别声明

汉坤律师事务所编写《汉坤专递》的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

如您对上述内容有任何问题或建议，请与汉坤律师事务所的下列人员联系：

北京　金文玉　律师：

电话：　+86 10 8525 5557

Email：　wenyu.jin@hankunlaw.com

上海　曹银石　律师：

电话：　+86 21 6080 0980

Email：　yinshi.cao@hankunlaw.com

深圳　王哲　律师：

电话：　+86 755 3680 6518

Email：　jason.wang@hankunlaw.com

香港　陈达飞　律师：

电话：　+852 2820 5616

Email：　dafei.chen@hankunlaw.com