

律师办理数据资源入表法律业务操作指引（2024）

（来源：北京市律师协会）

第一章总则

第一条【编制目的】为帮助律师办理数据资源入表业务，为出具数据合规确权相关法律意见提供基本操作规范，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》《中华人民共和国个人信息保护法》及其他相关法律法规、规范性文件和行业标准的要求，遵循北京市司法行政机关和北京市律师协会制定的律师执业规则，特编制本指引。

第二条【适用范围】本指引适用于数据资源入表（以下称“数据资源入表”或“入表”）过程中，对委托方指定的标的企业持有或处理的数据的合规确权出具法律意见，以作为数据资源入表时的决策参考。从事其他数据合规业务时，亦可参考本指引。

本指引不应作为判断律师是否勤勉履行委托合同项下律师义务、或是否勤勉开展相关数据资源合规确权工作的依据。

第三条【释义】

（一）标的企业：委托方拟进行数据资源入表的企业或主体。

（二）数据：任何以电子或其他方式对信息的记录。

（三）数据资产：由个人或企业拥有或控制的，能为企业带来未来经济利益的，以物理或电子方式记录的数据资源。其中，满足入表条件的会计准则的资产确认还应当符合成本可计量的要求。

（四）数据资源入表：指将数据资源作为企业的一项资产，按照会计准则进行确认、计量和报告，并在企业的财务报表中予以体现。通常包括：合规性和风险管理、资产确认和分类、成本归集和计量、后续计量和终止确认、列示和披露。

（五）数据处理：指对数据进行收集、存储、使用、加工、传输、提供、公开等行为。

（六）数据持有权/数据资源持有权：指自行持有或委托他人代为持有合法获取的数据，其他人不得非法窃取、篡改、泄露或者破坏权利人持有的数据的权利。

（七）数据使用权/数据加工使用权：指通过加工、聚合、分析等方式，将数据用于优化生产经营、形成衍生数据等的权利。

（八）数据经营权/数据产品经营权：指通过转让、许可、出资或者设立担保等有偿或无偿的方式对外提供数据的权利。

（九）《网安法》：指《中华人民共和国网络安全法》。

（十）《数据安全法》：指《中华人民共和国数据安全法》。

（十一）《个人信息保护法》：指《中华人民共和国个人信息保护法》。

（十二）《民法典》：指《中华人民共和国民法典》。

（十三）《数据二十条》：指2022年12月中共中央、国务院发布的《关于构建数据基础制度更好发挥数据要素作用的意见》。

第四条【一般要求】数据资源入表是将能够给企业创造收益的数据资源按照财政部发布的《企业数据资源相关会计处理暂行规定》（财会〔2023〕11号）的相关规定纳入表内核算的过程，“合法持有或控制”是数据资源入表的核心前提。若被认定为资产的数据资源存在合规问题，将会对会计处理的准确性、恰当性带来负面影响，甚至影响企业的资产化应用。

第五条【法律服务限制】律师事务所仅提供法律服务，尽管在法律尽职调查中不可避免地与技术、安全、会计、评估等方面存在交互关系，律师事务所与相关专业服务机构应独立审查与分工协作，仅在法律相关领域发表独立意见。如法律意见中涉及前述非法律专业事项内容，对有关数据合规涉及的技术、安全、会计、评估等领域内容，律师仅能完成对标的企业提供的书面材料的形式审查或借助工具予以表面核查或抽查，律师可以引用有关机构出具的专业文件和企业或有关人士出具的说明，但该引用不应视为律师对引用内容的真实性与准确性做出任何明示或默示的保证，对于

该等内容律师并不具备查验和作出判断的合法资格，无法也不能发表独立专业意见。

第六条【重视数据应用场景】数据在不同行业和应用场景中可能表现出显著的多样性，律师应深入分析标的企业所在的行业背景及其数据应用的具体场景，以确保法律判断的准确性和适用性。

第七条【数据资源入表步骤】以释放数据价值、促进数据要素流通为目的的数据资源入表的步骤通常应当包括：数据盘点、数据治理、合规确权、会计

核算/评估入表、数据产品作为生产要素进入市场流通。其中数据治理和合规确权是动态交叉的，数据治理的过程可能涵盖了合规整改的情形。

第八条【本指引核心】本指引围绕数据的合规与确权展开，以合规为核心，在合规基础上进一步判断数据权益类型，进而为数据资源入表及后续数据要素流通提供必要的法律意见。

第二章业务受理及尽调内容

第一节业务受理

第九条【沟通委托需求】拟提供法律服务的律师可以通过面谈、电话、邮件、问卷等方式，对委托人需求及其所处的市场、行业等情况进行了解，明确尽职调查的目标、范围、时间表和预算。

第十条【审查利益冲突】拟提供法律服务的律师事务所应当在正式立案、与委托人签署委托协议前进行利益冲突检索和审查，对于法律法规明

确规定不得同时接受对立双方或者利益冲突各方委托的，不得接受委托。如已经或拟同时接受可能会有利益冲突的其他方办理无事实争议具体性事务的委托，应当向委托人说明，并取得相关委托人的书面同意。

第十一条【签署委托合同】办理数据资源入表法律业务，应当由提供法律服务的律师事务所事先与委托人签订书面委托合同。该委托合同通常包括以下内容：

- （一）委托范围及要求；
- （二）法律尽职调查所需资料与信息的提供；
- （三）工作期限；
- （四）工作成果的形式及提交方式；
- （五）报酬、费用及其支付方式和期限；
- （六）违约责任；
- （七）责任限制；
- （八）风险提示；
- （九）其他。

第十二条【组建服务团队】办理数据资源入表法律业务，应当根据法律服务的范围、深度和广度组建相应规模的服务团队。服务团队应包括执业律师，可以包括实习律师及具有一定专业基础的助理人员，并选定一名执业律师为项

目负责人。鉴于数据资源入表业务的交叉性，建议团队配备具有财务和/或计算机等相关专业背景及经验的成员。

第二节 尽调内容

第十三条【尽调内容】一般性数据资源入表法律尽职调查通常包括以下内容：

- （一）标的企业情况；
- （二）数据内容合规审查；
- （三）数据来源合规审查；
- （四）数据处理合规审查；
- （五）数据管理合规审查；
- （六）数据权益界定；
- （七）多主体数据合作合规审查；
- （八）其他。

承办律师可根据标的企业实际情况及尽职调查报告的使用目的适当调整尽职调查内容。

第十四条【尽调清单】服务团队应当根据数据资源入表法律业务项目的具体情况编制尽职调查法律文件清单，并可根据对委托人的具体调查情况编制补充尽职调查文件清单，明确要求委托人或其他当事人严格按照客观、真实、准确、完整的原则提供清单所列明的相关文件，同时要求委托人或其他当事人书面承诺所提供资料不存在虚假、误导性陈述或重大遗漏情况。

第三节 工作底稿编制及归档

第十五条【工作底稿的内容】工作底稿应全面反映律师在办理入表业务的工作过程和结果，可以参照常见非诉业务工作底稿要求，包括但不限于以下内容：

- （一）委托协议及相关补充协议；
- （二）尽职调查材料；
- （三）法律分析及研究报告，包括对相关法律法规、政策的解读和适用分析；
- （四）内部讨论记录、备忘录及工作笔记；
- （五）与客户及其他相关方的沟通记录，如邮件、函件、会议纪要等；

（六）法律意见书、律师工作报告及其他法律文件的草稿和定稿；

（七）其他与业务相关的重要文件和资料，尤其关注涉及数据盘点、治理的相关资料或第三方专业报告。

第十六条【工作底稿编制原则】工作底稿的编制应遵循以下原则：

（一）真实性：工作底稿中的内容必须真实可靠，不得虚构、篡改或隐瞒重要信息。

（二）完整性：应全面收集与业务相关的文件和资料，确保工作底稿能够完整反映业务的全过程。

（三）一致性：应将电子底稿与文档同时刻录光盘或在数据库中以只读文件形式单独保存。

（四）准确性：工作底稿中的信息应准确无误，对事实的描述和法律分析应客观、准确。

（五）规范性：工作底稿的格式和内容应符合一定的规范要求，便于整理、查阅和管理。

（六）保密性：对于涉及客户商业秘密和个人隐私的工作底稿，应严格遵守保密规定，采取必要的保密措施。

工作底稿的编制应按照业务流程和时间顺序进行，确保各环节的工作记录清晰可查。对于重要的文件和资料，应注明来源和取得时间，并由相关人员签字确认。

第十七条【工作底稿归档】工作底稿应在业务办结后及时归档。归档时间一般不得超过业务办结后的三个月。

归档工作应由承办律师负责，档案管理人员协助。归档前，承办律师应对工作底稿进行全面整理和审查，确保工作底稿符合归档要求。

工作底稿的归档应按照以下程序进行：

（一）分类整理：将工作底稿按照业务类型、文件性质等进行分类整理，编制目录。

（二）装订成册：将整理好的工作底稿装订成册，注明案号、业务名称、归档时间等信息。采用刻录光盘等方法保存电子文档的，建议对保存内容计算哈希值并单独保存。

（三）移交档案：将装订好的工作底稿移交档案管理人员，办理移交手续，填写移交清单。

（四）档案管理人员应对接收的工作底稿进行再次审查，确保归档文件完整、准确、规范。如发现问题，应及时通知承办律师进行整改。

（五）工作底稿的保管期限应根据业务性质和重要程度确定。一般情况下，非诉业务工作底稿的保管期限不少于五年。

（六）档案管理人员应定期对工作底稿进行清理和整理，对超过保管期限的工作底稿，按照规定程序进行销毁。

第三章 标的企业情况

第十八条【主要调查内容】对标的企业基本情况进行尽职调查时，包括但不限于以下内容：

- （一）标的企业的基本登记信息；
- （二）标企业的主营业务情况；
- （三）数据资源入表所涉及业务的情况；
- （四）标企业的数据合规管理情况。

第十九条【基本登记信息】对标的企业的基本登记信息进行尽职调查时，应着重于对标的企业的主体资格、企业类型、注册资本（包括实缴资本）、成立时间、经营期限、经营范围、股权（投资）结构与控股股东及实际控制人、治理结构等方面进行审查。

第二十条【主营业务情况】对标企业的主营业务情况进行尽职调查时，应着重于对标企业的主营业务及相关资质、客户范围等进行审查，并重点关注入表相关数据及其未来应用场景与主营业务的关联关系，是否可持续及具有强关联关系。

第二十一条【入表涉及业务的情况】对标的企业入表所涉及的业务进行尽职调查时，应着重于对所涉业务是否已经履行了特定的程序及有效期限，如主管机关的审批、取得必要的经营资质、企业决策机构的批准等；相关数据作为数据资源入表时是否有法律法规或政策上的限制等方面进行审查。

第二十二条【数据合规管理情况】对标的企业的数据合规管理情况进行尽职调查时，应着重于对标的企业的数据内容合规、数据来源合规、数据处理合

规及数据管理合规进行审查。对前述内容进行审查时的要点，请参考本指引第四章至第七章的相关内容。

第四章数据内容合规审查

第二十三条【数据资源的盘点】基于数据资源入表的目的，结合企业的商业模式和数据应用场景，对数据资源进行盘点、梳理和识别，本着成本可计量、现实可控制、未来有收益的原则，形成数据资源盘点或分析报告。

第二十四条【审查依据】

（一）法律法规。包括但不限于《网安法》《数据安全法》《个人信息保护法》、地方性法规、规章等在开展尽职调查时现行有效的相关法律法规及规范性文件等。

（二）国家标准、行业标准（如：GB/T43697-2024《数据安全技术数据分类分级规则》、GB/T36344《信息技术数据质量评价指南》）和规范、重要国家政策、地方政策。

（三）企业内部规章制度，即企业制定的数据管理政策、隐私政策等。第二十五条【审查内容】

（一）合规性审查：审查数据的收集、存储、使用和传输是否符合法律法规的要求。

（二）真实性审查：核实数据的来源是否合法，是否经过验证和审查。检查数据是否存在虚假、错误或误导性信息。

（三）完整性审查：评估数据是否完整，是否存在缺失或损坏的情况。

第二十六条【审查要点】

（一）个人信息合规审查要点

1. 在收集、使用和共享个人信息时是否符合法律法规的规定，是否取得了用户的明确授权。

2. 对个人信息进行的分类、分级管理，是否采取了必要的保护措施。

3. 个人信息泄露事件的应急响应机制是否健全。

（二）企业数据合规审查要点

1. 标的企业业务数据的收集、使用和披露是否符合法律法规和合同约定。

2. 是否建立了完善的数据隐私政策和用户授权机制。

（三）公共数据合规审查要点

1. 数据来源合规性：确认公共数据的收集主体是否在其法定职责范围内进行数据收集及依据。

2. 数据收集的方式：是否遵守法律法规规定、是否取得了数据主体的合法授权及授权范围。

3. 授权主体适格性：授权主体必须是具有法定授权资格的部门或机构；授权主体是否在其权限范围内进行授权，是否超越法定职权进行授权行为。

4. 被授权方资质：评估被授权方的技术能力和安全保障能力；被授权方的信誉、经营状况、过往行政处罚情况，以及是否有能力履行公共数据运营职责。

5. 授权范围及期限：授权运营的公共数据是否明确界定了数据的类型、内容、格式等；被授权方使用目的及用途是否在授权规定的范围内；公共数据的使用是否在授权期限内。

第二十七条【应用场景的数据内容审查】

（一）内部应用场景审查

1. 内部数据使用场景合规性，如数据分析、决策支持、业务优化等。

2. 评估数据收集、使用是否遵循“最小且必要原则”，是否存在数据滥用风险。

3. 内部数据安全管理制度，如访问控制、数据加密、备份恢复等。

（二）外部合作应用场景审查

1. 与外部合作伙伴的数据共享和合作场景合规性。
2. 合作协议中关于数据保护的条款合规性。
3. 新兴技术应用场景合规性审查。
4. 分析新兴技术应用带来的数据安全挑战和风险。

（三）不同应用场景下数据质量影响评估

1. 数据质量评估主要从规范性、完整性、准确性、一致性、时效性和可访问性六个维度展开。

2. 律师办理入表法律业务时应当重视数据应用场景对数据质量的要求，同样的数据在不同场景下对上述六个指标的需求有所差异。

第五章数据来源合规审查

第一节数据来源合规概述

第二十八条【数据来源合规】数据来源的合规是指标的企业在获取和收集数据时，应当遵循相关法律法规、行业规范及道德准则，确保数据取得的合法性、正当性和安全性。

第二十九条【数据获得的渠道】数据的获取主要包括以下几种渠道：内部生成数据、外购数据、公开收集数据、个人授权数据以及其他方式获取的数据。

第三十条【数据来源合规审查的合法性依据】审查数据来源合规的依据主要包括以下内容：

（一）数据收集应符合现行法律法规，尤其是数据相关的法律法规的要求，包括但不限于《网安法》《数据安全法》《个人信息保护法》等。值得注意的是，各垂直领域应考虑不同行业或领域现行专门的法律法规。

（二）数据收集应避免侵害第三方的权益，尤其是从公开渠道获取的数据：属于公共数据源的，应尽基本审慎的义务审查数据来源主体的收集行为是否符合法律法规及行业规范，以及标的企业获取、处理、使用数据集的行为是否符合公共数据源的协议或规则；属于爬取数据的，应审查爬取行为是否具备正当性，不得侵犯其他方的人身权和财产权（包括知识产权）。

（三）通过从第三方购买、授权等数据交易方式外购数据的，应当审查数据交易合同是否违反国家强制性法律规定，明确数据来源，审查交易主体的必要资质和授权、标的数据的授权使用范围、交易主体的网络与数据安全要求，以及出现风险事件的责任承担等条款，确保数据来源的合法性、正当性、安全性。

第三十一条【数据的可追溯性】确保数据能够追溯是合规审查的重要方面，主要包括来源记录和数据流转记录。

来源记录能够确保数据追根溯源，记录内容包括数据的原始提供者、收集时间和收集方式等信息。来源记录有助于在出现问题时快速确定责任主体和解决问题。

数据流转记录能够载明数据在多个主体之间流转情况，记录内容包括每一次流转的目的、接收方和授权情况等。流转记录有助于确保数据在整个生命周期中的合规性。

第二节内部生成数据来源合规审查

第三十二条【内部生成数据】内部生成数据是指标的企业内部业务活动、运营过程、管理决策等所产生的数据集合。这些数据反映了标的企业

的特定业务流程、客户群体、产品和服务的特点以及管理模式等方面的情况。内部生成数据包括但不限于以下内容：业务交易数据、客户信息数据、生产运营数据、财务数据、人力资源数据、研发数据等。

第三十三条【内部生成数据来源合规审查】内部生成数据来源合规审查，主要从以下方面进行合规审查：

（一）数据生成依据审查：检查数据生成是否基于标的企业合规的业务流程和操作规范。确保数据是在遵循相关法律法规、行业标准以及企业内部制度的前提下产生的。

（二）数据生成目的审查：确认数据生成的目的明确、合规且符合标的企业的目标和战略规划，审查是否存在为了不正当目的而生成数据的情况。

（三）数据生成过程审查：评估数据生成过程中的技术手段和方法是否可靠、安全。同时，审查数据生成过程中是否存在干预或篡改数据的风险。确保数据生成过程中的数据生成人员具备相应的资质和权限，且严格按照操作规范和流程执行。

（四）数据质量管理审查：检查标的企业是否建立有效的数据质量管理体系，包括数据质量标准、监控机制和纠错程序等，确保生成数据的准确、完整、一致和及时。同时，评估数据质量问题对业务决策和合规性的潜在影响，对于发现的数据质量问题，审查是否已及时采取纠正措施并对相关责任人进行了必要的问责。

（五）内部审计与监督机制审查：确认标的企业是否设立了独立的内部审计部门或岗位，负责定期对数据生成活动进行监督和审计。同时，检查内部审计的范围、频率和方法是否足以发现潜在的合规问题，审计报告能否得到管理者的重视并及时处理，审计建议落实的情况如何。

第三节 外购数据来源合规审查

第三十四条【外购数据】外购数据是指标的企业从外部供应商、数据提供商处购买或获取的数据资源。

第三十五条【外购数据来源合规审查】外购数据来源合规审查至关重要，它能确定企业所获取的数据是否合法、是否符合道德规范。律师应从以下方面进行合规审查：

（一）供应商的调查：对数据供应商进行全面调查，包括其公司信息、业务范围、信誉度和市场口碑等。了解供应商的经营历史，确认其是否存在法律纠纷或不良记录，这有助于评估其可靠性和合规性。同时，核实供应商是否具有合法的数据采集、处理和销售资质。

（二）数据来源合法性审查：要求供应商明确说明数据的来源渠道。审查数据是否来自合法的途径。对于来源不明或存在疑问的数据，应谨慎对待，避免潜在的法律风险。同时，审查数据采集过程是否符合相关法律法规和道德标准。

（三）数据使用授权的审查：确认供应商是否拥有合法的数据使用授权，并有权将这些权利转让或许可给购买方。审查授权文件的条款和范围，有效控制购买方在使用数据时引发法律纠纷的风险。同时，注意授权的时效性和地域范围。确保数据的使用授权在有效期内，并且适用于购买方的业务范围和运营地区。

（四）数据质量评估：对外购数据的质量进行评估，包括数据的准确性、完整性、一致性和时效性等方面。要求供应商提供数据质量报告或相关证明材料，以便购买方了解数据的质量状况。另外，可以通过抽样检查、数据分析等方式，对数据质量进行进一步验证。如果发现数据质量存在问题，应与供应商协商解决办法。

（五）合同条款审查：在与数据供应商签订合同之前，仔细审查合同条款，确保合同中明确规定了数据的来源、质量、使用授权、保密义务、违约责任等关键事项。注意合同中的免责条款和争议解决条款，确保购买方的合法权益得到充分保护。

第四节公开收集数据来源合规审查

第三十六条【公开收集数据】公开收集数据是指标的企业通过公开的渠道和方式，主动获取各类数据的行为，包括通过互联网平台、政府公开数据平台、公共数据库、线下公开活动等收集数据。

第三十七条【公开收集数据来源合规审查】公开收集数据来源合规审查是确保数据收集行为合法、正当且安全的重要环节。律师应从以下方面进行合规审查：

（一）明确数据收集的目的和范围：在开始审查之前，首先要明确收集数据的具体目的以及所涉及的范围，这有助于确定审查的重点和方向，确保收集的数据仅用于合法、正当且明确的用途，并且不超出必要的范围。

（二）审查数据来源的合法性：确认数据是否来自公开渠道，包括政府公开数据平台、合法的新闻媒体网站、学术研究机构的公开数据库、公共论坛和社交媒体平台等。对于声称来自公开渠道的数据，要仔细核实其来源的真实性和可靠性。同时，检查数据收集是否遵循了相关平台或渠道的使用规则和条款，以免引发法律纠纷。

（三）评估数据收集方法的合规性：如果是通过网络爬虫等技术手段收集数据，要审查其是否遵守了相关的法律法规和技术规范。对网络爬虫的使用可能涉及侵害个人信息权、侵犯网站内容著作权以及违反技术保护措施、Robots协议、对服务器造成过度负担等涉嫌非法利用他人数据获取竞争优势的不正当竞争行为，均需要谨慎评估和处理。同时，对于通过人工方式收集的数据，要确保收集过程符合伦理道德标准，并且获得了被调查者的知情同意。特别是在涉及敏感信息或个人隐私的情况下，更要加强保护措施，确保数据收集的合法性和正当性。

（四）审查数据的质量和准确性：尽管公开收集的数据来源较为广泛，但数据的质量和准确性可能参差不齐。在合规审查过程中，要对数据进行一定的质量评估，检查数据是否存在错误、重复、缺失或不一致等问题。对于

质量较差的数据，要谨慎使用或采取相应的处理措施。同时，需要考虑数据的时效性，对于过时的数据，要进行更新或标注，以免影响决策的准确性。

（五）关注数据隐私和安全问题：在公开收集数据的过程中，可能会涉及个人隐私信息。要审查数据收集和处理过程中是否采取了足够的隐私保护措施，确保个人隐私不被泄露或滥用。同时，评估数据的安全性，防止数据遭到未经授权的访问、篡改或丢失。确保数据存储和传输的环境具备相应的安全防护措施。

（六）建立内部审查机制和流程：为了确保公开收集数据来源的合规性，企业或组织应建立健全内部审查机制和流程。明确负责数据合规审查的部门或人员，制定详细的审查标准和操作指南，定期对数据收集活动进行审查和监督。同时，要加强员工的培训和教育，增强员工的数据合规意识和风险防范能力。

第五节 个人授权数据来源合规审查

第三十八条【个人授权数据】个人授权数据是指个人主体在明确知晓数据使用目的、范围、方式等情况下，自愿给予标的企业使用其相关数据的许可而产生的数据。

第三十九条【个人授权数据来源合规审查】对于个人授权数据，律师应从以下方面进行合规审查：

（一）授权的真实性审查：确认个人确实进行了授权操作，而非他人冒名顶替或伪造授权。可以通过验证授权过程中的身份认证信息、电子签名

等方式来确保授权的真实性。同时，审查授权的方式是否符合法律规定和相关标准。

（二）授权的合法性审查：检查授权行为是否符合相关法律法规的要求。《个人信息保护法》通常规定了个人信息收集、使用和处理的基本原则和规则，审查时应确保授权行为未违反前述法律规定。同时，核实授权是否涵盖了数据使用的所有必要方面，且符合业务的实际需求。

（三）授权的有效性审查：确认授权是否在有效期内。个人授权通常具有一定的期限限制，审查时应确保数据的使用在授权有效期内进行。同时，审查授权是否存在被撤销或变更的情况。个人有权随时撤销或变更其授权，标的企业应向个人提供明确的撤销或变更授权的方式并及时更新个人授权情况，律师审查时也应抽样核实个人信息的最新的授权状态。

（四）数据来源的可靠性审查：尽管个人进行了授权，但仍需审查数据的来源是否可靠。同时，对数据的完整性和准确性进行审查。确保获取的个人授权数据是完整的，没有被篡改或丢失，并且数据的准确性能够得到保证。

（五）审查记录和存档：建立完善的审查记录制度，记录对个人授权数据来源合规审查的过程和结果，包括审查的时间、人员、发现的问题及处理措施

等。同时，对审查记录和相关的授权文件进行妥善存档，以备日后查询和审计。存档的期限应符合法律法规和业务的要求。

第六节 其他方式获取数据来源合规审查

第四十条【其他方式获取的数据】其他方式获取数据是指除了外购数据、公开收集数据和个人授权数据之外，标的企业通过各种非常规或特定途径获取数据的方式，包括但不限于合作交换、数据挖掘与分析、传感器和物联网设备收集、竞赛和众包模式等。

第四十一条【其他方式获取数据来源合规审查】对于其他方式获取的数据来源，律师应从以下方面进行合规审查：

（一）合作与交换：审查合作协议或交换协议，明确双方的数据权利和义务，确保数据的提供和使用符合法律法规及协议约定。核实合作方或交换方的数据来源合法性，要求其提供相关证明材料，如数据采集的授权文件等。

（二）数据挖掘与分析：对于从企业自身数据挖掘得到的数据，审查数据采集和存储的合规性，确保原始数据的获取和处理符合相关规定。若涉及对公开大数据集的二次分析，确认数据集的公开性质和使用许可，遵守相应的使用条款和限制。

（三）传感器和物联网设备收集：审查传感器和物联网设备的数据采集机制，确保其符合隐私政策和相关法规。评估数据传输和存储的安全性，防止数据泄露或被滥用。

（四）竞赛和众包：在竞赛和众包活动中，明确参与者提交数据的所有权和使用权限，制定相应的规则和条款，确保数据来源清晰、合法。同时，对参与者提交的数据进行审查，排除可能存在侵权或违法的数据。

（五）其他：根据其他未列举获取方式的特性进行针对性合规审查。

第六章 数据处理合规审查

第一节 数据处理概述

第四十二条【数据处理者】数据处理者是指在数据处理活动中自主决定处理目的和处理方式的自然人、法人或非法人组织。

第二节 数据收集

第四十三条【数据收集】数据收集是指产生、获取数据的行为，从数据来源的角度，可以将数据收集行为划分为从数据处理者内部系统中新产生的数据和从数据处理者外部系统采集的数据。

第四十四条【数据收集的一般原则】律师应当审查标的企业数据收集是否遵守合法原则、正当原则、诚信原则、权责一致原则。

第四十五条【特定行业/领域数据的收集原则】对于从事特定行业/领域的标的企业，律师应当审查：

（一）汽车行业数据收集的特别原则有：车内处理原则、默认不收集原则、精度范围适用原则、脱敏处理原则。

（二）医疗健康行业数据收集的特别原则有：

1. 从健康医疗大数据的角度，要坚持以人为本、创新驱动的原则，坚持规范有序、安全可控的原则，支持开放融合、共建共享的原则；

2. 从人类遗传资源信息的角度，收集行为要符合伦理原则（尊重人类遗传资源提供者的隐私权，取得其事先知情同意，并保护其合法权益）、禁止买卖人类遗传资源；

3. 从人口健康信息角度，还要遵循“一数一源、最少够用”原则。

（三）金融行业数据收集的特别原则有：合法正当原则、目的明确原则、选择同意原则、最小够用原则、全程可控原则、动态控制原则、权责一致原则。

（四）其他行业特别原则。

第四十六条【个人信息收集必要性的审查】标的企业因自身业务需要直接收集个人信息时，律师应根据标的企业的商业模式及业务功能等审查标的企业收集数据是否符合必要性原则，应符合：

（一）收集的个人信息类型应与企业的产品或服务的业务功能有直接关联（直接关联是指没有上述个人信息的参与，产品或服务的功能无法实现）；

（二）自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率；

（三）间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

第四十七条【个人信息收集授权同意的审查】标的企业因自身业务需要直接收集个人信息时，律师应审查标的企业是否已事前取得个人信息主体的授权同意，具体审查内容包括：

（一）标的企业是否向个人信息主体告知收集、使用个人信息的目的、方式、范围和规则等，并获得个人信息主体的授权同意。收集不满十四周岁未成年人个人信息前，是否取得未成年人的父母或其他监护人的单独同意；

（二）个人信息主体授权是否为有效授权，个人信息收集过程中是否存在强制收集的情形，个人信息收集界面是否未提供跳过或拒绝等选项；

（三）标的企业是否完整保留了个人信息主体签署的《隐私政策》和《用户服务协议》，相关条款约定是否合法、合规，内容是否符合国家标准及行业标准；

（四）如产品或服务提供多项需收集个人信息的业务功能时，标的企业是否存在强迫个人信息主体接受产品或服务所提供的业务功能及相应的个人信息收集请求的情形；

（五）如个人信息主体未给予授权同意的情形下，标的企业是否存在以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务的情形；

（六）未取得个人信息主体的授权同意而收集个人信息的，是否符合法定例外情形。

第四十八条【收集个人敏感信息的审查】标的企业因自身业务直接收集个人敏感信息时，律师应当审查：

（一）标的企业是否就个人敏感信息收集取得个人信息主体的明示同意；个人信息主体的明示同意是否是其在完全知情的基础上自主给出的，是否有具体的、清晰明确的意愿表示；

（二）标的企业是否按照最小必要原则明确收集个人敏感信息；

（三）标的企业是否仅在用户使用业务功能期间收集该业务功能所需的敏感个人信息；

（四）标的企业收集个人敏感信息前，是否已完成个人信息保护影响评估。

第四十九条【收集个人生物识别信息的审查】标的企业收集个人生物识别信息时，律师应当审查：

（一）标的企业是否单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，是否征得个人信息主体的单独明示同意；

（二）如涉及人脸数据，是否按照规定公布人脸识别数据处理规则；

（三）标的企业收集个人生物识别信息是否具有特定的目的和充分的必要性；

（四）标的企业收集个人生物识别信息前，是否已完成个人信息保护影响评估；

（五）标的企业如涉及人脸数据，是否在识别过程中持续告知数据主体验证目的，并通过语言、文字等向数据主体进行提示；

（六）标的企业是否仅收集生成人脸特征所需的最小数量、最少图像类型的人脸图像；

（七）标的企业是否采取安全措施保证人脸识别数据的真实性、完整性和一致性，防止人脸识别数据在收集过程中泄漏或篡改。

第五十条【间接收集个人信息的审查】标的企业间接收集个人信息时，律师应当审查：

（一）标的企业是否制定外部数据采购及审查的相关制度，是否对数据资源提供方的安全保障能力及数据安全风险进行评估，是否对个人信息来源合规性进行审查；

（二）数据资源提供方是否与收集方签署合作协议，明确双方数据安全的责任与义务；

（三）数据资源提供方已获得的个人信息处理的授权同意范围，包括处理目的、处理方式和个人信息的种类，是否能够涵盖数据资源提供方向收集方提供共享信息的范围，个人信息主体是否授权同意转让、共享、公开披露、删除该个人信息数据等；

（四）对于业务开展中所需进行的个人信息处理活动超出个人信息主体授权同意范围的，标的企业是否在获取个人信息后的合理期限内或处理个人信息前，直接或通过数据资源提供方征得个人信息主体的明示同意。

第五十一条【违法收集个人信息的审查】律师应当审查标的企业是否存在违法收集个人信息的情形，包括：

- (一) 以欺诈、诱骗、误导的方式收集个人信息；
- (二) 隐瞒产品或服务所具有的收集个人信息的功能；
- (三) 从非法渠道获取个人信息。

第五十二条【收集非个人信息的审查】收集非个人信息应注意审查：

- (一) 数据处理者是否取得收集相关数据的资质；
- (二) 收集信息的类型、收集使用的目的、收集方式是否符合相关法律法规、规范性文件的规定；
- (三) 如果与第三方合作收集数据的，应关注是否就数据的使用、收益等作出了明确约定。

第三节 数据存储

第五十三条【数据存储】数据存储是指数据处理者在提供产品或服务、开展经营管理等活动时，通过磁盘、磁带、云存储设备等存储媒体，在一定期限内持久化保留、保存数据的行为。

第五十四条【数据存储期限的审查】关于数据存储期限，律师应当审查：

(一) 标的企业对于个人信息的保存期限是否为实现个人信息主体授权使用的目的所必需的最短时间，是否超出收集使用规则中明示的存储期限；

(二) 数据存储的期限是否符合所处特定行业关于存储期限的法律法规及规范性文件的要求，如：

1. 网约车平台采集的个人信息和生成的业务数据，保存期限不少于两年；
2. 住院电子病历保存期限不少于三十年，互联网诊疗病历保存期限不少于十五年，其中图文对话、音视频保存期限不少于三年；
3. 药品网络零售商对处方、在线服务记录的保存期限不少于五年且不少于药品有效期满后一年；
4. 平台经营者对数据信息的保存期限不少于三年；
5. 互联网直播提供者对使用者发布内容和日志的保存期限不少于六十日，对网络交易活动的视频的保存期限不少于三年；
6. 证券登记结算机构对文件和资料的保存期限不少于二十年，证券公司对客户资料等信息的保存期限为至少二十年；
7. 征信机构对个人不良信息的保存期限为五年，超过五年的应当删除；

（三）对于超过存储期限的数据，标的企业是否及时进行删除或匿名化处理。

第五十五条【数据存储安全的审查】律师可从数据存储的行为结构出发，对存储媒介安全、存储系统安全、事故预防机制三个角度把握和管理。

第五十六条【个人信息存储安全措施的审查】关于个人信息存储安全措施，律师应当审查：

（一）标的企业在收集个人信息后，是否进行去标识化处理，是否将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理；

（二）标的企业是否采用物理或逻辑隔离方式分别存储人脸识别数据和个人身份信息等；

（三）标的企业是否直接存储原始个人生物识别信息；

（四）标的企业是否采取数据存储相关安全管控措施，是否按照数据分类分级制度，针对不同类别级别的数据采取差异化数据存储措施；

（五）标的企业是否实施权限管控机制，采用最小授权保障个人信息数据被有效保护，防止被非授权访问或处理；

（六）标的企业是否针对存储介质提供有效的技术和管理手段，防止对介质的不当使用而引发的数据泄露风险，并对存储介质访问和使用行为进行记录和审计；

（七）标的企业是否建立数据备份恢复操作规程，保障数据的可用性和完整性；

（八）标的企业终止运营其产品或服务时，是否将收集的个人信息进行删除或匿名化处理。

第五十七条【数据存储地点的审查】关于数据存储地点，律师应当审查：

（一）根据标的企业处理数据的类型、标的企业所处行业及其性质，判断其数据存储是否需履行本地化储存义务；

（二）审查标的企业数据储存的地点与方式（自行存储或委托第三方存储），判断储存地点是否合法、合规。

第五十八条【数据存储的本地化要求】国家机关处理的个人信息、关键信息基础设施收集和产生的重要数据、汽车重要数据、网约车平台收集的个人信息

息和生成的业务数据、医疗机构产生的人口信息及健康医疗信息等都有数据存储在境内的要求，即数据的本地化存储要求。但也允许在特殊情况下，在取得监管部门审批同意或履行必要的法定义务后，向中华人民共和国境外提供数据。

第五十九条【个人信息删除的审查】关于个人信息删除义务，律师应当审查：

（一）标的企业是否主动删除、受托人是否履行删除义务、标的企业在无法删除时的处置措施。

（二）如果删除个人信息从技术上难以实现，标的企业应当停止除存储和采取必要的安全保护措施之外的处理。

第四节 数据使用

第六十条【数据使用】数据使用是一个集合性的概念。广义上看，数据一经收集即被利用，狭义上看，数据使用可理解为数据处理者对所收集的数据进行利用的行为。如个人信息的使用，包括个人信息的访问、展示，用户画像的使用，个性化展示的使用，以及所收集的個人情報の汇聚融合，信息系统自动决策机制的使用。

第六十一条【数据使用的基本原则】律师应当根据《网安法》《数据安全法》《个人信息保护法》等相关法律法规审查标的企业是否遵守的数据使用原则，包括合法、正当、必要的原则，针对个人信息的使用，还包括使用规则公开透明原则和按照约定使用原则。

第六十二条【访问控制措施的审查】关于标的企业对个人信息访问的控制措施，律师应当审查：

（一）标的企业是否对被授权访问人员建立最小授权的访问控制策略，使其只能访问职责所需的最小必要的个人信息，且仅具备完成职责所需的最少的数据操作权限；

（二）标的企业是否对个人信息的重要操作（如进行批量修改、拷贝、下载等重要操作）设置内部审批流程；

（三）标的企业是否对数据安全管理人员、数据操作人员、审计人员的角色进行分离设置；

（四）标的企业对于因工作需要授权特定人员超权限处理个人信息的情形，是否经内部审批，并记录在册。

第六十三条【展示限制措施的审查】标的企业涉及通过界面展示个人信息的，律师应当审查标的企业是否采取去标识化等处理措施，降低个人信息在展示环节的泄露风险。

第六十四条【使用目的限制的审查】关于标的企业个人信息使用目的，律师应当审查：

（一）标的企业使用个人信息时是否超出与收集个人信息时所声称的目的具有直接或合理关联的范围；如超出范围使用个人信息的，是否再次征得个人信息主体的明示同意；

（二）对于标的企业收集的个人信息进行加工处理而产生的信息，如能够单独或与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，标的企业在使用该等数据时是否遵循收集个人信息时获得的授权同意范围。

第六十五条【自动化决策合规义务的审查】标的企业利用数据进行自动化决策的，律师应当审查：

（一）标的企业是否公示自动化决策的基本原理、目的和主要运行机制，是否向个人提供拒绝自动化的选项；

（二）标的企业利用数据进行自动化决策、数据分析，是否存在对交易条件相同的交易相对人实施差别待遇的情况，法律法规及规范性文件允许例外的除外；

（三）标的企业运营信息系统具备自动决策机制且能对个人信息主体权益造成显著影响的，是否在规划设计阶段或首次使用前开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

（四）标的企业是否在使用过程中定期（至少每年一次）开展个人信息安全影响评估，并依评估结果改进保护个人信息主体的措施；

（五）标的企业是否存在基于人脸识别数据生成用户自身画像和统计分析；是否存在基于人脸识别数据自身进行个性化推荐的情况；

（六）标的企业不应使用人脸识别数据作为汇聚融合的直接关联点；

（七）标的企业是否向个人信息主体提供针对自动决策结果的投诉渠道，并支持对自动决策结果的人工复核。

第六十六条【个性化展示的审查】标的企业产品或服务涉及个性化展示的，律师应当审查：

（一）标的企业业务功能涉及个性化推荐时，是否显著区分个性化展示和非个性化展示的内容；

（二）标的企业业务功能利用用户个人信息和算法进行定向推送，是否同时提供不基于任何个人信息，展示普遍推送商品的功能；

（三）标的企业通过其产品或服务基于用户个人信息进行个性化展示时，是否为用户提供退出或关闭个性化展示模式的选项；

（四）当用户退出或关闭个性化展示模式时，是否向用户提供删除或匿名化定向推送活动所基于的个人信息的选项；

（五）标的企业利用个人信息进行个性化展示时，是否能确保用户可自主控制用于个性化展示的个人信息类型；

（六）用户是否可以通过选择用于个性化展示的个人信息类型，控制个性化展示与用户本身的相关程度。

第六十七条【个人信息使用合规义务的审查】对于标的企业是否履行个人信息使用的合规义务，律师应当审查：

（一）用户画像的合规义务：用户画像系指使用所收集的个人信息，对该等个人信息主体的某些特性进行分析和评估，形成用户标签的数据处理活动。用户画像常见的应用场景包括应用于产品开发和行业分析、精准营销活动和定向推送。如果直接将用户画像提供给第三方，仍需遵循知情、同意原则，如果间接用户画像无法还原个人特征的，符合“匿名化”的特征，不受知情、同意原则的约束。达到群体性画像要求的，符合“匿名化”特征。

（二）个性化推荐的合规要求：个性化推荐是指基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体展示信息内容、提供商品或服务的搜索结果等活动。对个性化推荐活动的合规治理方向，要求个人信息处理者，向个人进行信息推送、商业营销的，应当同时提供不针对其个人特征的选项，或向个人提供便捷的拒绝方式。以算法推荐技术开展个性化推荐的，还要依据相关规定，履行相应的合规义务。

（三）自动化决策的合规义务：自动化决策是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。自动化决策的常见应用场景有小额信贷审查、保险核保、信用评价、劳动用工管理、平台用户管理。自动化决策要坚持决策透明、结果公平公正的原则，对个人信息有重大影响的自动化决策要设置人工干预机制，还要开展个人信息安全影响评估。

（四）其他应注意的合规义务：个人信息处理者还应注意使用个人信息时的去标识化问题、合理关联问题、最小使用问题、超范围使用问题。是否存在基于人脸识别数据自身进行个性化推荐的情况、不应使用人脸识别数据作为汇聚融合的直接关联点等。注意“大数据杀熟”的“不合理”差别待遇问题。

第五节 数据加工

第六十八条【数据加工】数据加工主要是指将原始数据进行编辑、处理、整理、清洗、转换等操作，以便更好地满足数据分析、数据挖掘、业务决策等需求的数据处理过程，以提高数据质量和应用，发挥数据的价值效用。

第六十九条【数据加工一般性合规义务的审查】关于数据加工的一般性合规义务，律师应审查：

- （一）标的企业是否构建数据模型、数据目录；
- （二）标的企业是否开展数据转换、汇聚、清洗、分析等加工活动；
- （三）标的企业是否制定数据清洗、数据分析等管理办法，建立数据加工评价机制、数据操作日志记录及监控审计等技术措施；
- （四）标的企业是否采取测试环境、开发生产环境资源隔离、业务系统身份鉴别及访问控制、数据操作日志及监控审计等技术措施。

第七十条【数据加工汇聚与融合合规义务的审查】关于数据汇聚与融合合规义务，律师应当审查：

- （一）标的企业是否在数据融合之前，根据融合后可能产生的数据内容、处理目的、范围、对个人的影响等对可能的个人信息风险进行评估，并对处理情况进行记录；

（二）标的企业数据融合是否超出数据收集时所声明的使用范围，如超出，是否重新获得信息主体的授权，如涉及个人信息，是否征得个人信息主体同意；如涉及敏感个人信息，是否取得用户的单独同意；

（三）标的企业是否对汇聚融合后产生的衍生数据重新开展数据安全定级工作，根据敏感程度分类分级，并采用相应级别的安全保护措施。

第七十一条【加工健康医疗数据合规义务的审查】标的企业加工健康医疗数据的，律师应审查：

- （一）标的企业是否遵循医疗伦理原则；
- （二）标的企业是否公开个人信息处理规则并取得自然人的个人同意；
- （三）标的企业是否履行保证质量义务。

第七十二条【加工政务数据合规义务的审查】标的企业加工政务数据的，律师应当审查：

- （一）标的企业是否建立健全数据加工处理机制；
- （二）标的企业是否履行保证质量义务、审批和监督义务。

第六节 数据传输

第七十三条【数据传输】数据传输是一个技术层面的概念，是指将数据从一个位置传输到另一个位置的过程，数据传输通常通过传输协议来实现，在传输的过程中可能通过加密保护传输数据的隐私和安全。

第七十四条【数据传输合规的审查】关于数据传输，律师应当审查：

- （一）标的企业是否根据传输的数据类型、级别和应用场景，制定安全策略、操作规程并采取保护措施；
- （二）标的企业是否采取数据传输相关安全管控措施（如传输通道加密、数据内容加密、数据接口传输安全、数据传输终端身份鉴别等）确保数据传输介质和环境安全，保障重要数据和敏感个人信息传输过程的安全性，防范未经授权访问和数据泄露；

（三）标的企业与数据接收方之间是否签署书面合同就数据传输应采取的安全措施明确约定。

第七十五条【重点监管行业数据传输合规义务的审查】如标的企业涉及金融领域、工信领域、健康医疗领域的数据传输，律师应当依据该领域有关标准和规范进行特殊的合规审查。

第七十六条【数据出境的审查】9对于标的企业是否存在数据出境行为及其是否履行合规义务，律师应当审查：

（一）标的企业是否存在向境外提供在中国境内运营中收集和产生的数据的行为；

（二）相关数据是否属于禁止、限制出境的数据；

（三）标的企业内部是否建立健全数据出境相关技术和管理措施；

（四）标的企业是否向个人履行充分告知义务，告知内容包括境外接收方的名称、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使个人信息权利的方式和程序等事项；是否取得个人单独同意；

（五）标的企业是否事前进行个人信息安全影响评估；

（六）标的企业向境外提供重要数据和核心数据的，是否对数据接收方进行数据安全保护能力的评估与核实；

（七）标的企业是否为关键信息基础设施运营者向境外提供重要数据或个人信息，或者非关键信息基础设施运营者向境外提供个人信息数量是否达到国家网信部门规定规模；符合条件的标的企业是否就数据出境通过所在地省级网信部门向国家网信部门申报数据出境安全评估；

（八）如标的企业不涉及关键信息基础设施运营者、重要数据且向境外提供个人信息未达到一定规模的，标的企业是否与境外接收方订立个人信息出境标准合同或者通过个人信息保护认证；

（九）标的企业数据出境行为是否满足相关法律法规、规范性文件规定免于数据出境安全评估、个人信息保护认证、个人信息出境标准合同备案的相关例外情形；

（十）标的企业是否按照法律法规规定期限存留相关日志记录和数据出境审批记录；

（十一）相关数据出境行为是否符合所在行业的其他监管规定。

第七节 数据提供

第七十七条【数据提供】数据提供暂时没有完全统一的定义，与数据收集、存储、使用、加工、传输等都属于数据处理活动。针对数据提供方与接收方之间的法律关系不同，可将数据提供分为数据共享（向第三方数据处理者提供

）、委托处理、转让、共同处理四种主要情形，还包括数据迁移及数据交换等其他数据提供情形。

第七十八条【数据提供通用性合规义务的审查】关于数据提供的通用性合规义务，律师应当审查：

（一）标的企业是否评估数据对外提供行为的风险，是否开展安全影响分析和风险评估；

（二）标的企业是否评估数据接收方的数据合规能力，如数据接收方是否满足网络安全等级制度、是否采取加密措施和访问控制、是否制定了安全制度和数据安全事故的应急响应方案；

（三）标的企业与数据接收方是否签署数据处理协议，就处理数据的类型、处理目的、处理方式等问题进行明确。

第七十九条【政务数据提供合规义务的审查】关于政务数据提供的合规义务，律师应当审查：

（一）被提供的政务数据是否为国家机关在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息，该等数据应予以保密，不得泄露或者非法向他人提供。

（二）如标的企业为政务数据的受托处理方，是否存在擅自留存、使用、泄露或向他人提供政务数据的行为。

第八十条【重要数据提供合规义务的审查】关于重要数据提供的合规义务，律师应当审查：

（一）被提供的数据是否为重要数据。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，可能危害国家安全、公共利益的数据，可以参考相关法律法规或规范性文件关于重要数据的定义及有关部门制定的重要数据目录进行界定。

（二）如涉及重要数据出境，标的企业是否向中央网络安全和信息化委员会办公室或其他主管部门申报数据安全评估。

第八十一条【个人信息提供合规义务的审查】关于个人信息提供的合规义务，律师应当审查：

（一）标的企业是否获得个人信息主体的知情同意；

（二）标的企业是否开展了影响评估；

（三）如涉及向境外提供个人信息的，标的企业是否开展出境安全评估并使用个人信息出境标准合同。

第八十二条【委托处理的审查】如标的企业委托第三方处理个人信息时，律师应当审查：

（一）标的企业是否制定服务供应商评估、管理制度，是否对数据接收方进行事先的数据处理合规技术检测、调研评估其数据保护制度完备情况，并在其提供服务的过程中进行数据处理合规技术抽样检查或通过其他方式监督验证其数据保护能力；

（二）标的企业与受托方是否签署委托协议，是否明确约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等；

（三）标的企业作出委托行为，是否超出已征得个人信息主体授权同意的范围或是否属于法律规定可豁免同意的情形；

（四）标的企业委托处理之前是否进行个人信息安全影响评估；

（五）受托方是否严格按照标的企业的要求处理个人信息；

（六）受托方是否存在再次委托的情况，是否就再委托情况事先征得标的企业的授权；

（七）受托方是否协助委托方积极响应个人信息主体提出的权利请求；

（八）受托方是否发生过安全事件，是否向标的企业反馈；

（九）委托关系解除时受托方是否继续存储相关个人信息；

（十）标的企业是否对受托方进行监督；

（十一）标的企业在向第三方提供数据过程中，是否定期对数据共享接口进行安全审计；

（十二）标的企业对于委托处理个人信息的情况是否准确记录和存储。标的企业委托第三方处理其他数据的，律师可以参照本条第一款审查。第八十三条【数据共享与转让的审查】标的企业共享、转让个人信

息时，律师应当审查：

（一）标的企业转让、共享个人信息之前是否进行个人信息安全影响评估，是否依评估结果采取有效的保护个人信息主体的措施；

（二）标的企业是否已按照法律规定向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型以及可能产生的后果，并事先征得个人信息主体的授权同意；符合法律法规、规范性文件规定的例外情形的除外；

（三）如共享、转让涉及个人敏感信息的，是否事先向个人信息主体告知涉及的个人敏感信息类型、数据接收方的身份和数据安全能力，并事先征得个人信息主体的明示同意；

（四）共享、转让是否涉及生物识别信息，接收方是否具备相应数据安全能力；是否就生物识别信息转让、共享单独取得个人信息主体的明示同意；

（五）标的企业是否与接收方签署协议约定数据接收方的责任和义务；

（六）标的企业是否准确记录和存储个人信息的共享、转让情况，包括共享、转让的日期、规模、目的，以及数据接收方基本情况等；

（七）标的企业是否对数据接收方进行监督，对于接收方违反法律法规及协议约定处理个人信息的行为，是否采取相关措施控制或消除个人信息面临的安全风险。

标的企业共享、转让其他数据时，律师可以参照本条第一款审查。

第八十四条【共同处理】标的企业与第三方为共同处理个人信息时，律师应当审查：

（一）标的企业是否披露各个人信息共同处理者的身份，并明确各方是个人信息共同处理者；

（二）标的企业是否与第三方签署合同确定应满足的个人信息安全要求，以及在个人信息安全方面自身和第三方应分别承担的责任和义务；

（三）标的企业是否向个人信息主体明确告知第三方身份以及在个人信息安全方面自身和第三方应分别承担的责任和义务。

标的企业与第三方为共同处理其他数据时，律师可以参照本条第一款审查。

第八节 数据公开

第八十五条【数据公开】数据公开是指向社会或不特定人群发布数据，使得相关数据处于可被不特定的主体获取、知悉、访问之状态的行为。数据公开可能对国家安全、社会公共利益、个人人格尊严或生命财产安全带来重要影响

。国家制定政务数据开放目录，从政务数据公开后的受众范围上看，有共享政务数据、可开放政务数据、不宜开放共享的政务数据。

第八十六条【数据公开通用性合规义务的审查】关于数据公开的通用性合规义务，律师应当审查：

（一）标的企业数据公开是否尊重社会公德和伦理、是否遵守商业道德和职业道德，是否侵害国家、社会和他人的合法权益；

（二）标的企业数据公开是否采取相应的技术措施，保障数据的安全，确保公开的数据受到保护；

（三）标的企业是否开展对数据公开行为的风险监测，是否在发现数据安全缺陷、漏洞等风险时，立即采取补救措施。

第八十七条【特定行业数据公开的审查】关于特定行业数据，除审查标的企业是否遵守数据公开的通用性合规义务外，律师应对其行业合规要求进行审查，比如工业和信息化领域数据的公开、疾病防治与健康管理领域数据的公开、金融行业数据的公开，都有单独的管理办法或安全规范进行区分、审查数据的公开合规问题；政务数据的公开应遵守公正、公平、便民、及时准确的原则，还要制定政务数据开放目录、构建政务数据开放平台。

第八十八条【个人信息公开披露的审查】个人信息原则上不应公开披露，如标的企业经法律授权或具备合理事由确需公开披露时，律师应当审查：

（一）标的企业是否事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

（二）标的企业是否向个人信息主体告知公开披露个人信息的目的、类型，并事先征得个人信息主体明示同意；

（三）公开披露涉及个人敏感信息的，信息披露前是否向个人信息主体告知涉及的个人敏感信息的内容；是否准确记录和存储个人信息公开披露的情况；

（四）标的企业是否涉及公开披露个人生物识别信息；公开披露中国公民的种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果的情况。

第七章数据管理合规审查

第一节数据管理合规审查要点

第八十九条【一般审查要点】数据管理合规审查的要点包括：数据安全管理制度、数据安全管理机构、数据分类分级管理、人员安全管理、合作外包管理、安全应急管理等。利用互联网等信息网络开展数据处理活动，应一并对所涉及的信息网络的合规情况（包括但不限于网络安全等级保护制度的落实情况等）进行审查。

第九十条【数据安全管理制度审查要点】针对标的企业数据安全管理体系的建设及落实情况，应重点审查：

- （一）数据安全总体策略、方针、目标和原则制定情况；
- （二）数据安全管理工作规划或工作方案制定情况；
- （三）数据分类分级、数据安全评估、数据访问权限管理、数据全生命周期管理、数据安全应急响应、数据合作方管理、数据脱敏、数据加密、数据安全审计、数据资产管理、大数据平台安全等制度建设情况；
- （四）关键岗位的数据安全管理操作规程建设情况；
- （五）制度内容与国家和行业数据安全法律法规和监管要求的符合情况；
- （六）网络安全责任制、数据安全责任制落实情况，网络安全和数据安全事件责任查处情况；
- （七）数据安全管理体系的制定、评审、发布流程建设情况；
- （八）数据安全管理体系的定期审查和更新情况；
- （九）制度发布范围是否覆盖全面，发布方式是否正规、有效；
- （十）数据安全管理制度落实情况，是否具备操作规程、记录表单等制度落实证明材料；
- （十一）制度落实监督检查机制等。

第九十一条【数据安全管理机构审查要点】针对标的企业数据安全管理体系的建设情况，应重点审查：

- （一）数据安全机构和职能设置情况；
- （二）数据安全负责人和职能设置情况；
- （三）单位高层人员参与数据安全决策情况；
- （四）对标的企业内部的数据安全管理执行情况、数据操作行为等进行安全监督的情况；
- （五）数据安全人员和资源投入情况与组织数据安全保护需求适应性等。

第九十二条【数据分类分级管理审查要点】针对标的企业数据分类分级制度的建设及保护情况，应重点审查：

（一）数据分类分级保护制度建设情况，是否符合国家、行业 and 地方的数据分类分级规范要求；

（二）数据分类分级管理情况，及核心数据和重要数据目录建立及维护情况；

（三）是否在相关制度中明确了数据分类管理、分级保护策略，数据分类分级保护措施是否落实在数据访问权限申请、保护措施部署等方面；

（四）数据分类分级变更和审查流程情况；

（五）个人信息分类分级管理情况；

（六）是否对处理的个人信息和重要数据进行明确标识；

（七）按照数据级别建设覆盖全流程数据处理活动的安全措施情况；

（八）数据分类分级标识或数据资产管理工具建设情况，是否具有自动化标识能力，是否具有数据标识结果发布、审查等能力；

（九）按照相关重要数据目录或规定，评估重要数据并进行重点保护的情况；

（十）按照相关核心数据目录或规定，评估核心数据并进行严格管理的情况等。

第九十三条【人员安全管理审查要点】对标的企业的人员安全管理审查包括对人员录用情况、保密协议签订情况、人员转岗离岗管理情况、人员数据安全培训情况四部分内容。

针对人员录用情况，应重点审查：

（一）重要岗位员工录用前背景调查情况；

（二）数据处理关键岗位人员录用，对其数据安全意识或专业能力进行考核的情况。

针对保密协议签订情况，应重点审查：

（一）员工工作纪律和工作要求中是否明确规定员工禁止的数据安全相关行为；

（二）是否与所有涉及数据服务的人员签订安全责任承诺或保密协议，与数据安全关键岗位人员签订数据安全岗位责任协议；

（三）在重要岗位人员调离或终止劳动合同前，是否明确并告知其继续履行有关信息的保密义务要求，并签订保密承诺书。

针对人员转岗离岗管理情况，应重点审查：

（一）在人员转岗或离岗时，是否及时终止或变更完成相关人员数据操作权限，并明确有关人员后续的数据保护管理权限和保密责任；

（二）对终止劳动合同的人员，是否及时终止并收回其系统权限及数据权限，明确告知其继续履行有关信息的保密义务要求。

针对人员数据安全培训情况，应重点审查：

（一）数据安全培训计划制定、更新情况；

（二）开展数据安全意识教育培训，并保留相关记录情况；

（三）是否对数据安全岗位人员每年至少进行一次数据安全专项培训，对关键岗位人员进行定期数据安全技能考核情况。

第九十四条【合作外包管理审查要点】对标的企业合作外包管理的审查包括合作方管理机制、合作协议约束、外包人员访问权限等内容。

针对合作方管理机制建设情况，应重点审查：

（一）数据合作方安全管理机制建设情况，如对合作方或外包服务机构的选择、评价、管理、监督机制；

（二）是否对数据合作方或外包服务机构的安全能力进行评估；

（三）对外包服务机构、人员履行安全责任义务的监督检查情况；

（四）外包人员现场服务安全管理情况；

（五）对外包服务商的技术依赖程度，对委托处理数据的控制和管理能力。

针对合作协议约束情况，应重点审查：

（一）服务合同、承诺及安全保密协议情况，是否通过合同协议等方式对接收、使用标的企业数据的合作方的数据使用行为进行约束；

（二）是否在合作协议中明确了数据处理目的、方式、范围，安全保护责任、数据返还或销毁要求、保密约定及违约责任和处罚条款等；

（三）合作协议中，标的企业与合作方、外包服务商间的数据安全责任界定情况。

针对外包人员访问权限管理情况，应重点审查：

- （一）外包人员对数据与系统的访问、修改权限是否限于最小必要范围；
- （二）能够在测试环境下或使用测试数据完成的，是否向外包人员开放了生产环境权限或真实数据；
- （三）外包人员数据导出操作或数据外发操作的监督管理情况；
- （四）外包人员对敏感数据的访问及操作能否被实时监督或监测；
- （五）数据外包服务账号及访问权限管理情况；
- （六）外包人员远程访问操作系统或数据的情况。

第九十五条【安全应急管理审查要点】针对标的企业数据安全应急管理情况，应重点审查：

（一）近三年发生的网络安全或数据安全事件信息及其处置、记录、整改和上报情况，如事件名称、影响对象、发生时间和频次、发生原因、外部威胁、事件级别、处置措施、整改措施等，重大事件需提供事件调查评估报告；

（二）数据安全事件应急预案制定和修订情况，是否定义数据安全事件类型，明确不同类别级别事件的处置流程和方法；

（三）数据安全应急响应及处置机制建设情况，发生数据安全事件时是否立即采取处置措施，是否按照规定及时告知用户并向有关主管部门报告；

（四）数据安全事件应急演练情况；

（五）数据处理活动安全风险监测情况，发现数据安全缺陷、漏洞等风险时，是否立即采取补救措施；

（六）安全事件对个人、其他组织造成危害的，是否将安全事件和风险情况、危害后果、已经采取的补救措施等通知利害关系人，无法通知的是否采取公告等其他方式告知；

（七）如标的企业是面向社会提供服务的数据处理者，是否建立便捷的数据安全相关投诉举报渠道，以及近三年的数据安全投诉举报处置、记录和整改情况，是否存在侵害用户个人信息合法权益的情况。

第九十六条【数据管理合规审查参考】律师在审查标的企业的数据管理合规情况时，除上述审查要点外，还可以参考相关国家标准、行业标准中的相关规定。

第二节数据管理合规审查实施方法

第九十七条【确定法律依据】检索并确定相关法律法规、国家标准和行业标准对标的企业的数管理合规的要求。

第九十八条【收集资料】为开展数管理合规审查，从标的企业收集相关资料，包括但不限于以下内容：

- （一）数据安全总体策略、方针、目标和原则；
- （二）数据安全管理工作规划或工作方案；
- （三）数据分类分级、数据安全评估、数据访问权限管理、数据全生命周期管理、数据安全应急响应、数据合作方管理、数据脱敏、数据加密、数据安全审计、数据资产管理、大数据平台安全等制度；
- （四）关键岗位的数据安全管理操作规程、与员工签订的保密协议、数据安全培训相关记录；
- （五）相关数据所涉及的各项信息系统的网络安全等级保护备案证明、相关安全资质或评级文件，信息系统的架构图、网络拓扑图、设备清单等技术文档；
- （六）标的企业内审或第三方评估机构出具的网络安全审计、审查或安全测评、风险评估报告；
- （七）标的企业与数据合作方、外包服务商等第三方之间签订的涉及数据的服务合同、数据共享使用协议。

第九十九条【调查问卷】设计针对标的企业员工的问卷调查，了解员工对数管理合规的认识、遵守相关法律法规的情况等。发放问卷并收集，进行统计分析。

第一百条【文档审查】对收集的文档进行审查，对标的企业数管理的总体框架、数管理责任界定、已识别的数管理合规风险及其应对措施有效性进行综合评估。

第一百〇一条【人员访谈】与标的企业的高层管理人员、数据安全负责人、IT部门人员等进行访谈，了解标的企业的数管理的战略、决策过程和执行情况，并询问标的企业员工对数据安全政策的知晓度和遵守情况，以确认相关战略、安全政策等是否落实到位。

第一百〇二条【对第三方审查】审查标的企业与数据合作方、外包服务商等第三方之间的合作关系，评估该等第三方的数据安全水平。检查标的企业对数据合作方、外包服务商等第三方的数据安全要求和监督、审计机制。

第一百〇三条【测试】调查实施阶段，应通过开展穿行测试、符合性测试等测试方法，对标的企业进行审查，保证调查结果准确性。必要时，可以与具备相关从业资质的第三方机构联合开展相关测试。

第一百〇四条【风险分析】汇总调查中发现的数据管理合规风险，分析其潜在影响和发生概率。

第一百〇五条【做出结论】根据分析结果，对标的企业的管理体系有效性、适当性进行评价。基于分析结果，提出具体的改进建议，包括完善相关管理制度、加强人员培训、改进技术措施等。

第一百〇六条【沟通反馈】与标的企业进行沟通，汇报调查结果和建议，解答标的企业的疑问。根据标的企业的反馈意见，对报告进行必要的修改和完善。

第八章数据权益确认

第一百〇七条【数据权益确认及界定依据】

在前期充分尽调的基础上，律师对标的企业是否享有数据资源所有权、数据加工使用权、数据产品经营权的相关权益进行确认。

数据权益界定的依据包括但不限于依据《网安法》《数据安全法》《个人信息保护法》《数据二十条》以及其他相关法律法规、规章、地方性规章、政策文件等确认相关权益。

律师可参考《数据二十条》所提出的“根据数据来源和数据生成特征，分别界定数据生产、流通、使用过程中各参与方享有的合法权利，建立数据资源所有权、数据加工使用权、数据产品经营权等分置的产权运行机制”。目前针对数据权益的确认主要围绕数据资源持有、数据加工使用、数据产品经营三项权益论证。

第一百〇八条【数据资源所有权确认】

（一）数据来源审查

对于标的企业内部生成的数据，根据标的企业内部业务流程、系统记录等，审查标的企业对数据的初始来源合法性。

对来源于其他主体的数据，审查是否有相关授权协议。当数据源于用户，应检查用户注册协议、隐私政策等文件，确认是否明确规定了标的企业对用户数据的获取范围、用途限制等条款，确保标的企业在用户授权范围内持有数据资源。

（二）管理权益确认

1. 根据收集的工作底稿确认标的企业在数据存储、维护、安全保护等方面的管理权益。审查标的企业的数据管理制度，包括数据存储架构、备份策略、安全防护措施等，确保标的企业对数据资源形成有效的管理能力，能够保障数据的完整性、可用性和保密性。

2. 确定标的企业在应对数据合规要求方面的管理责任，在数据跨境传输、数据分类分级、存储删除等数据全生命周期管理方面的措施，以确认标的企业对数据资源管理的全面性。

（三）使用权益确认

根据标的企业业务需求和法律法规限制，确认标的企业对数据资源的使用范围。审查标的企业内部使用数据的流程，确保在使用数据资源时有明确的授权和操作规范，防止滥用数据的情况发生。

第一百〇九条【数据加工使用权确认】

（一）加工使用授权审查

1. 标的企业拟加工使用的数据，应审查是否有合法的授权来源。对标的企业自有数据资源独立进行加工的，应检查标的企业内部决策文件，确认

有权对数据进行加工处理；标的企业委托第三方对数据进行加工的，应审查双方签订的协议中明确了各方数据持有的合规性、加工使用权限、加工目的、加工成果的归属等条款。

2. 对外部数据进行加工的，应当审查标的企业与第三方的协议，确保协议中约定了各方数据持有的合规性、加工使用的权限、加工目的、加工成果的归属等条款。

（二）加工过程合规性

1. 审查标的企业或第三方的数据加工算法、技术手段、使用的软硬件等工具是否符合法律法规之规定。

2. 审查标的企业或第三方对加工过程中产生的中间数据的管理措施，确保中间数据的安全和合规性。

（三）加工使用范围确定：根据标的企业业务和协议约定，确定数据加工使用权范围的合规性、一致性。

（四）加工成果权益：明确数据加工后的成果归属权。标的企业独立完成加工，成果归标的企业所有；与其他主体合作加工，应根据合作协议确定成果的共享、分配等权益。

第一百一十条【数据产品经营权确认】

（一）产品定义与合法性：要求标的企业明确数据产品的定义和应用场景，审查数据产品的生产过程，确认合法合规。

（二）经营权利来源：审查标的企业对数据产品经营的权益来源。依据标的企业内部研发记录、知识产权注册等文件确定标的企业自主研发生产数据产品，确认标的企业享有的经营权益；合作开发数据产品的，应依据合作协议约定确定各方在经营中的权利和义务关系。

（三）市场准入与合规：确定数据产品进入市场所需的资质和许可要求。根据不同行业和地区的规定，检查标的企业是否取得相应的经营许可，数据产品是否符合质量标准、安全标准等要求，确认数据产品能够合法进入市场流通、交易。

第九章多主体数据合作合规审查

第一节合作方及合作情况

第一百一十一条【参与方】按照数据流转过程中参与方的作用，将参与方划分为四方：数据提供方、数据接收方、数据中介、监督机构及平台，其在数据交易和流转过程中的职能包括：

（一）数据提供方通常是数据的持有人，包括具有法定义务或在合同约定的情况下有权或有义务使用 and 提供数据的自然人、法人或其他组织，需要保证数据来源合法合规，数据的收集和处理遵循了数据保护要求，对数据进行分类分级和标识，以确保不包含国家秘密和商业秘密，敏感数据得到有效保护，并且对数据的来源和准确性负责。

（二）数据接收方指接收数据提供方数据的自然人、法人或其他组织，其接收数据的目的通常与其业务属性、所处行业、业务领域、产品、工艺、技术和目标市场相关，包括主动与数据提供方缔约而接收数据，以及用户向

数据持有人提出请求后或根据法律规定或者合同约定向接收方提供数据。数据接收方需要按照数据提供方的需求建立与数据安全性和敏感度相适应的数据安全保护措施，包括加密传输、安全存储和访问控制等，并应当确保数据的使用合法合规并在相关合同约定或允许的范围内，并在数据生命周期结束后按照法律或合同的约定销毁。

（三）数据中介指提供技术基础设施和专业知识，以支持与数据有关的合同签订、履行及数据互操作性，充当协调人，能在数据共享、访问或汇集数据等过程中协助各方完成数据交易的自然人或法人。数据中介通常为数据提供方和接收方提供前沿、创新的技术支持及解决方案，以实现数据提供方和接收方之间的数据共享、处理和使用，其可能同时负有数据控制者和处理者的角色。

（四）监督机构及平台指对数据使用和交易进行监管及提供交易平台的一方，而非国家有关权力机构或监管机构，其需要根据相应的数据保护法规和政策制定具体的操作流程或者交易所规则。

第一百一十二条【最低限度的技术、组织和安全措施】数据交易和流转中，所有参与方应当建立与数据重要性和敏感度相适应的技术、组织和安全措施。数据泄露可能发生在数据流转的任何一个环节中，参与方在选择缔约方过程中应当充分考虑到措施的“短板”效应，实施和部署最低标准技术、组织和安全措施的参与方决定了措施的整体高度。

第一百一十三条【复杂作品客体权利的确认】进行共享的数据如果包含构成作品或者作品的片段，需要尽力核实权利主体的情况，包括权利主体的身份、是否获得权利主体的授权进行二次使用和披露。如尽力核实后仍然无法确认的，应当在合同中约定瑕疵担保和补偿性条款，降低数据接收方和数据中介的法律责任，并反向督促数据的原始提供方以合法方式获得原始数据。

第一百一十四条【复杂客体数据权益的确认】在完成数据资源清理后，或者在数据集的分级分类过程中，如果发现待交易和共享的数据集包含具有多重权利属性，如包含企业数据、个人信息、产品数据、安全数据等，则需要参照

相关法律规定以及本指引其他章节的规定进行逐一确认，确保参与方有权对相关的数据集进行处分。

第二节 合作合同合规审查

第一百一十五条【缔约自由】基于合同自由原则，各方应在数据采集、传输、共享、处理过程中遵循平等协商、缔约自由原则。此类合同在通用合同条款之外，还可以包括技术和组织措施、数据安全措施。

第一百一十六条【公平、合理、无歧视】参与方在缔约过程中应当遵守《中华人民共和国反垄断法》相关规定，按照公平、合理、无歧视的原则进行数据交易和共享。

第一百一十七条【使用性质不公平条款】如果合同条款的使用性质严重偏离了数据访问和使用的良好商业惯例，违反了诚信和公平交易，则该合同条款是不公平的。

第一百一十八条【目的或效力不公平条款】如果合同条款的目的或效力是为了下列目的，则应推定该合同条款是不公平的：

（一）不适当地限制在不履行合同义务情况下的救济方式或在违反这些义务情况下的赔偿责任，或加重对其单方面适用该条款的企业的赔偿责任；

（二）允许单方面施加条款的一方以严重损害另一缔约方合法利益的方式访问和使用另一缔约方的数据，特别是当此类数据包含商业敏感数据或受商业秘密或知识产权保护时；

（三）阻止被单方面施加条款的一方在合同期内使用该方提供或生成的数据，或将该数据的使用限制在该方无权使用、获取、访问或控制该数据或以适当方式利用该数据的价值的范围内；

（四）阻止被单方面施加条件的一方在合理期限内终止协议；

（五）阻止被单方面施加条款的一方在合同期内或合同终止后的合理期限内获得由该方提供或生成的数据的副本；

（六）使单方面施加该条款的一方能够在不合理的短时间通知内终止合同，同时未考虑到另一缔约方转向替代和类似服务的任何合理可能性以及这种终止所造成的经济损失，但有重大理由这样做的除外；

（七）使单方面施加该条款的一方能够实质性地改变合同中规定的价格或与数据的性质、格式、质量或数量有关的任何其他实质性条件。

第一百一十九条【格式条款】如果合同条款是由缔约一方提供的格式条款，而缔约另一方虽经谈判仍不能对条款内容施加影响，则该条款应视

为本条所指的单方面规定的格式条款。提供格式条款一方不合理地免除或者减轻其责任、加重对方责任、限制对方主要权利的，或排除对方主要权利的，该格式条款无效。

第一百二十条【区分定义】要注意到相同法律概念在各法域下的差异，例如，我国《个人信息保护法》下个人信息处理者是指是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人，而在欧盟《通用数据保护条例》下将控制者和处理者区分开来，并赋予不同的权利和义务。

第一百二十一条【合同必要条款】数据交易、共享合同通常包括以下条款：目的和范围、数据所有权和权利、保密性和安全性、数据访问权限及方式、数据质量和完整性、遵守道德准则和法规、责任赔偿、争议解决。涉及数据跨境时，律师应当关注不同法域的合同权利义务的差别。

第一百二十二条【技术合同无效的情形】包含下列情形的数据合作合同可能会被认为属于《民法典》第八百五十条所称的“非法垄断技术”而认定为无效：

（一）限制当事人一方在合同标的技术基础上进行新的研究开发或者限制其使用所改进的技术，或者双方交换改进技术的条件不对等，包括要求一方将其自行改进的技术无偿提供给对方、非互惠性转让给对方、无偿独占或者共享该改进技术的知识产权；

（二）限制当事人一方从其他来源获得与技术提供方类似技术或者与其竞争的技术；

（三）阻碍当事人一方根据市场需求，按照合理方式充分实施合同标的技术，包括明显不合理地限制技术接受方实施合同标的技术生产产品或者提供服务的数量、品种、价格、销售渠道和出口市场；

（四）要求技术接受方接受并非实施技术必不可少的附带条件，包括购买非必需的技术、原材料、产品、设备、服务以及接收非必需的人员等；

（五）不合理地限制技术接受方购买原材料、零部件、产品或者设备等的渠道或者来源；

（六）禁止技术接受方对合同标的的技术知识产权的有效性提出异议或者对提出异议附加条件。

第十章数据确权登记（非入表前置条件）

第一百二十三条【目的】本章旨在说明律师办理入表法律业务时，审查标的企业拟入表的数据是否已经完成了数据确权登记，并不重点阐述数据确权登记类型及其自身需要的核查内容及流程。对于已经完成数据产权登记的，律师可以作为对标的企业数据合规确权的参考。

第一节数据产权登记

第一百二十四条【数据产权】目前我国尚未在法律层面明确数据产权制度，学界较为主流的观点是采取“所有权”与“用益权”两权分离的模式。

《数据二十条》也体现了“来源者数据所有权+处理者数据用益权”两权分离的模式。《数据二十条》提出的“建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制”，实际上暗含着一种分层确权的思路。

第一百二十五条【数据产权登记效力】数据确权登记，目前也仅仅是数据持有者将自己的确权申请提交第三方平台进行登记，第三方平台进行形式审查后，予以登记，甚至发放确权证书。但第三方平台的登记行为，并不能起到法律意义上对申请者数据权益的法律确认，仅仅是一种存证性质。目前，已经有很多第三方平台受理数据持有者提出的数据资源持有权、数据加工使用权、数据产品经营权的登记申请，并发放确权登记证书。

第一百二十六条【数据产权登记审查要点】律师在审查数据知识产权登记时，应当重点审查申请人拟申请登记的数据资源来源，审查其来源是否合规，取得的数据权益的方式和使用情况，办理产权登记的数据是否实际由申请人使用，是否存在拟入表的数据的产权登记主体为关联方或者其他主体控制、占有、使用的情况，是否存在抵押、质押等权利受到限制的情况，是否存在纠纷或者潜在纠纷的情况。

第二节数据知识产权登记

第一百二十七条【数据知识产权】《民法典》规定的八类知识产权种类中只有“法律规定的其他客体”可能包含数据知识产权。虽然国家知识产权局办

公室以发文14的方式确定多地区知识产权局做数据知识产权登记试点工作，但从法律位阶上讲，“数据知识产权”仍然只是一种“类知识产权”。

第一百二十八条【数据知识产权登记审查要点】

- （一）申请人是否取得数据知识产权登记的证书以及证书的有效期；
- （二）申请人取得数据知识产权登记的批准主体，如各地数据交易所、各地的知识产权局等；
- （三）申请人取得数据知识产权登记的方式是否合法合规，是否按照批准主体制定的相关规范履行相应的程序；
- （四）申请人是否就数据知识产权登记事宜委托第三方机构出具合规意见、评估报告等；
- （五）申请人拟入表的数据是否已全部办理知识产权登记；
- （六）申请人已取得的数据知识产权登记是否存在抵押、质押等权利受到限制的情况；
- （七）申请人已办理数据知识产权登记的数据是否与第三方存在权属纠纷的情况，包括与第三方存在不正当竞争纠纷的情况；
- （八）申请人已办理数据知识产权登记的数据是否实际由申请人控制、使用，是否存在关联方或其他主体控制、占用、使用的情况。如有，是否签署相关授权使用文件；
- （九）申请人的数据知识产权标的是否涉及登记机构或国家法律法规、行业惯例中负面清单的内容。

第三节其他登记类型

第一百二十九条【数据资源公证登记】2023年8月，江西省数据资源登记平台正式上线，推出数据资源公证登记服务。该平台采用全链路合规公证模式，为数据资源权益的确认提供了新的途径。

第一百三十条【数据要素综合登记】数据要素综合登记涵盖初始登记、交易登记、信托登记、变更登记、注销登记、撤销登记及续证登记等多个环节。完成登记后，登记主体可部分或全部享有“三权分置”的数据产权及相应的合法财产性权益。2023年11月，贵州省大数据发展管理局颁布《贵州省数据要素登记服务管理办法（试行）》，数据要素综合登记正式实施。

第十一章数据资产列示与披露前法律判断

第一节数据资产列示与披露前法律判断的必要性

第一百三十一条【列示】企业在编制资产负债表时，应当根据重要性原则并结合本企业的实际情况，在存货、无形资产、开发支出科目下增设“其中：数据资源”项目，反映资产负债表日确认为该科目项下数据资源的期末账面价值或支出金额。

第一百三十二条【披露】数据资产的披露是企业在财务报告和信息披露文件中向财务信息使用者提供其数据资源及经济价值相关信息的重要方式，数据资源的披露有强制披露和自愿披露两种方式。

第一百三十三条【入表科目及选择逻辑】根据数据资源的持有目的、形成方式、业务模式，以及与数据资源有关的经济利益的预期消耗方式等，可以将数据资源确认为无形资产、存货或开发支出。

从法律角度而言，判断数据资源计入无形资产或存货的依据是，在对外服务或者交易的过程中，数据或数据产品权属是否发生转移。

开发支出属过渡性科目，反映资产负债表日正在进行数据资源研究的开发项目满足资本化条件的支出金额，在满足特定条件时可以作为无形资产处理。故本指引不对开发支出做法律判断。

第一百三十四条【法律与会计交叉】法律维度侧重于数据资源的合规与确权，会计维度侧重于数据资源的会计核算及计量。

对于不同科目下的数据资产，合规要求会有差异，不同列示类型和披露标准对企业数据资产价值及未来资产变化影响较大。

第一百三十五条【法律判断原则】律师应当在理解数据资产的会计列示与披露类型及标准的基础上，重点关注和提示标的企业入表数据资产在不同科目下披露范围、内容和方式的潜在风险和影响。

数据资源作为无形资产表明，或因该资产为企业所拥有并能够据此通过对外提供服务或对内提高效率与效益而带来增量经济利益。无形资产入表的合规要求相对宽松，律师应当重点关注数据资源的持有权，确保标的企业在日常经营中能够有效控制、合法使用或流动相关数据资源。

数据资源作为存货入表，数据17持有权发生了转移，律师应当重点关注和审查合规链条及权属的完整性，对数据资源的持有权、数据产品经营权进行审查，其合规要求较无形资产更高。

第一百三十六条【数据资产创新应用】数据资源入表后在增信、作价入股、信托管理、质押融资和证券化等创新应用方面发挥重要作用。不同类别的数据资产能够应用的领域不同，律师应根据应用场景、数据限制以及披露要求等作出合规性判断。值得注意的是，对于2024年以前形成的、可以识别为数据资产的、不能入表的数据资源仍然可以评估作价后予以创新应用。

第二节不同科目的数据资产披露前法律判断

第一百三十七条【数据资产作为无形资产披露前的审查要点】

（一）对有限使用寿命的数据资源，披露其使用寿命估计和摊销详情之前，应综合考虑数据资源的法定有效期、合同有效期等因素，以法律角度评估其预计使用寿命的准确性。

（二）对使用寿命不确定的数据资源，在披露其账面价值和使用寿命不确定的判断依据之前，应结合数据资源的法定有效期、合同有效期、行政许可有效期等因素，从法律角度评估其使用寿命不确定性的依据。

（三）对使用权受到限制的数据资源，在披露其账面价值和当期摊销额等信息之前，应结合数据权益界定的路径、数据类型、范围、期限和限制依据、限制内容、限制期限等信息，从法律角度评估数据资源的权利限制状况。

（四）对被用作担保的数据资产，在披露其账面价值和当期摊销额等信息之前，要结合主债权的金额、期限、债务人的偿债能力，以及数据权益的路径、类型、范围、期限和限制等信息，从法律角度评估数据资源的权利限制状况。

第一百三十八条【数据资产作为存货披露前的审查要点】

（一）对使用权受到限制的数据资产，应综合考量数据权益界定的路径、数据类型、范围、期限以及限制依据、限制内容、限制期限等要素，从法律角度对数据资源的使用权限制状况进行评估。

（二）对被用作担保的数据资产，在公布作为担保物的数据资源的账面价值等信息之前，要综合考量主债权的金额、期限、债务人的偿债能力，以及数据权益的路径、类型、范围、期限及限制等要素，从法律角度对数据资源的使用权限制状况进行评估。

第三节自愿披露内容的法律判断

第一百三十九条【自愿披露内容及作用】自愿披露内容主要涵盖数据资源的应用场景描述和分析、来源的合规性、加工投入、应用现状、与重大交易事项相关的信息、相关权利失效情况、权利限制情况的信息，以及其他企业认为有必要披露的相关信息。

自愿披露内容可以帮助企业展示其数据资产管理和运用的透明度，增加投资者和利益相关方对企业的信任和理解，帮助投资者和潜在投资者更好地理解企业数据资源的规范治理和经济价值。

第一百四十条【自愿披露前审查要点】

- （一）应用场景或业务模式的合法合规性。
- （二）原始数据的类型、规模、来源、权属等信息。
- （三）数据资源的加工维护和安全保护情况。
- （四）相关数据产品或服务的运营模式、作价出资、流通交易、服务计费方式等。
- （五）重大交易事项中涉及的数据资源对该交易事项的影响及风险分析，重大交易事项包括但不限于企业的经营活动、投融资活动、质押融资、关联方及关联交易、承诺事项、或有事项、企业/业务重组、债务重组、资产置换等。
- （六）数据资源相关权利的失效情况及失效事由，以及该情形对企业的影响及风险分析等。
- （七）数据资源转让、许可或应用所涉及的地域限制、领域限制及法律法规限制等权利限制。
- （八）企业认为有必要披露的其他数据资源相关信息的法律审查。

第十二章法律风险及特别提示

第一百四十一条【违法处理、不当使用个人信息的法律责任】违法处理个人信息的，需要承担《个人信息保护法》规定的法律责任，包括但不限于责令改正、警告、罚款，承担责任的人员包括直接负责的主管人员和其他直接责任人员。

处理个人信息侵害个人信息权益造成损害的，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

根据《个人信息保护法》关于公益诉讼的相关规定，个人信息处理者侵害众多个人的信息权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。

第一百四十二条【不当使用其他经营者的商业数据的法律责任】在遵守数据抓取约定的情况下，利用抓取的数据提供足以实质性替代其他经营者提供的相关产品或者服务，构成不正当竞争，需要承担相关法律责任。

第一百四十三条【未经授权复制、传播作品的法律责任】进行数据共享的数据如果包含构成作品的或者作品片段的，未经授权的使用可能会侵害著作权中的复制权、修改权、信息网络传播权等权项。从著作权侵权角度而言，复杂客体的数据权属核实通常是不可能或者不现实的，因此有必要在合同中约定瑕疵担保和补偿性条款，降低数据接收方和数据中介的法律责任。

第一百四十四条【交易违规数据的法律责任】市场主体合法处理数据形成的数据产品和服务，可以依法交易，但是交易的数据产品和服务中包含未依法获得授权的数据的、未经依法开放的公共数据的，或者其他法律法规规定禁止交易的情形的，可能由市级市场监督管理部门或者行业主管部门责令改正、没收违法所得，并处以罚款。

第一百四十五条【不当抓取他人公开信息的民事法律责任】未经授权抓取他人公开信息在特定情况下可能会被认为构成违反《中华人民共和国反不正当竞争法》第二条的行为，司法裁判中确立的第二条适用规则为：

（一）《中华人民共和国反不正当竞争法》第二章及《中华人民共和国专利法》《中华人民共和国著作权法》等知识产权专门法对该市场竞争行为未作出特别规定；

（二）该市场竞争行为扰乱市场竞争秩序、损害其他经营者或者消费者合法权益；

（三）该市场竞争行为因违反诚信原则和商业道德而具有不正当性。在互联网环境下的数据共享行为，司法机构可能还将额外考虑其他因素，包括：

（一）该竞争行为所采用的技术手段确实损害了消费者的利益，例如：限制消费者的自主选择权、未保障消费者的知情权、侵害消费者的隐私权等；

（二）该竞争行为破坏了互联网环境中的公开、公平、公正的市场竞争秩序，从而引发恶性竞争或者具备这样的可能性；

（三）对于互联网中利用新技术手段或新商业模式的竞争行为，应首先推定具有正当性，不正当性需要证据加以证明。

第一百四十六条【侵犯公民个人信息的刑事法律责任】违法向他人出售或提供个人信息的，需要承担刑事法律责任，具体而言：

（一）《中华人民共和国刑法》第二百五十三条之一规定，违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

（二）违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

（三）单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照该款的相关规定处罚。

第一百四十七条【其他刑事法律责任】各参与方应当严格审查数据来源，其他与数据收集、使用、处理、共享相关的刑事法律责任，包括但不限于：侵犯公民个人信息罪，破坏计算机信息系统罪，非法侵入计算机信息系统罪，非法控制计算机信息系统罪，提供侵入、非法控制计算机信息系统程序、工具罪，非法利用信息网络罪，帮助信息网络犯罪活动罪，拒不履行信息网络安全管理义务罪，窃取、收买、非法提供信用卡信息罪，非法获取计算机信息系统数据罪，侵犯商业秘密罪等。

第一百四十八条【中介机构法律责任】数据合规确权的法律意见存在虚假记载、误导性陈述或重大遗漏的，可能与委托人承担连带赔偿民事责任，但是能够证明自己没有过错的除外。严重不负责任，出具的证明文件有重大失实，造成严重后果的，可能承担刑事责任。涉及公众公司、特定行业等强监管的，律师事务所及律师或因未勤勉尽责而受到行政处罚。

第一百四十九条【特别提示】数据资源入表具有大量市场需求的同时也将积聚潜在风险，律师事务所作为出具法律意见的中介机构应当重视其中的责任风险，建议在从事入表相关法律业务时，除了办理法律业务本身外，重点关注：委托人类别、标的企业入表目的、数据入表后的用途及其合理性、是否有独

立的第三方数据技术与安全专业意见、对引用的涉及技术与安全、会计、评估等内容不越界发表意见。

第十三章附则

第一百五十条【生效】本指引自发布之日起执行。

第一百五十一条【效力】本指引仅作为北京市范围内的律师从事数据资源入表法律业务的参考，对其他涉及数据合规确权法律业务亦可部分参照适用，但均不具有强制性。

第一百五十二条【解释】本指引解释权归北京市律师协会数字经济与人工智能领域法律专业委员会所有。