数据资产入表法律实务——微观篇

作者：潘永建 | 朱晓阳 | 邓梓珊 | 左嘉玮 | 李佳琪

结合团队实操经验与各地各行业最新实践，通力数据合规服务团队将陆续推出“数据资产入表与交易”主题的系列实务文章。

本篇文章介绍数据资产入表在法律合规层面的实务要点，包括数据资产的定义、数据资产入表的法律合规路径，以及律师在数据资产入表合规评估时需要关注的关键要点，包括主体合规、数据资源合规、数据安全管理能力合规。

一. 数据资源与数据资产

根据《企业会计准则——基本准则(2014 修改)》第 21 条和第 22 条的规定，“资产”是指由企业过去的交易或者事项形成的、由企业拥有或者控制的、预期会给企业带来经济利益的资源。具体而言，“由企业拥有或者控制”，是指企业享有某项资源的所有权，或者虽然不享有某项资源的所有权，但该资源能被企业所控制。

除上述条件外，数据资源符合资产定义还需满足以下两项要件:

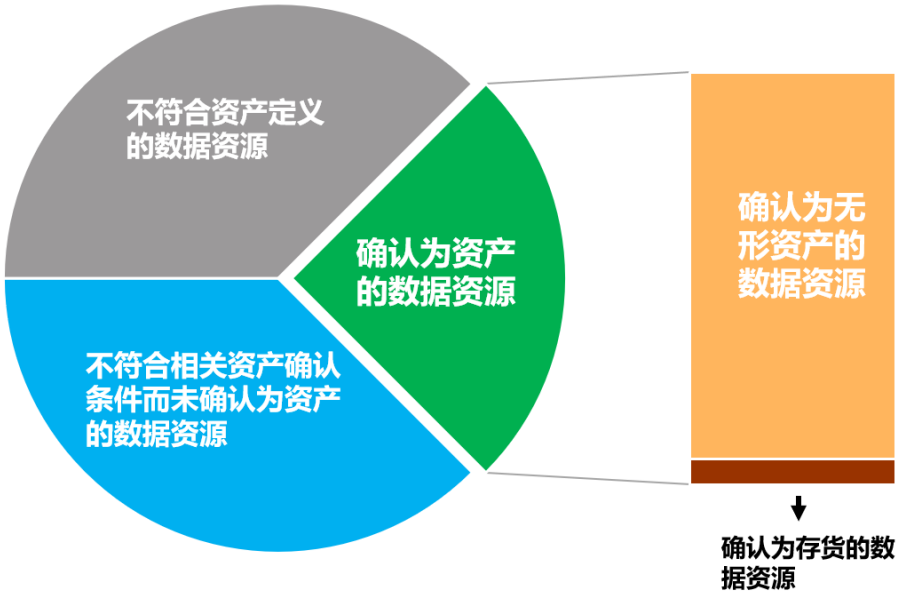
1. 与该资源相关的经济利益很可能流入企业
2. 该资源的成本或价值能够可靠地计量

只有同时满足所有这些条件的数据资源才能被确认为数据资产。据此，数据资源可以大致分为以下三类(如下图所示):

1. 确认为数据资产的数据资源
2. 不符合资产定义的数据资源
3. 不符合相关确认条件而未确认为资产的数据资源

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com



图源：财政部会计司《暂行规定》专题培训

二. 数据资产入表的法律合规

在数据资产入表的过程中，律师的核心职责是评估数据资源是否满足“由企业拥有或者控制的”这一要件。为此，律师需要从法律角度深入理解和分析“拥有”“控制”的内涵及其在实践中的适用。

当前，我国在法律层面尚未明确数据确权制度，数据权属问题存在较大分歧。特别是在大数据时代背景下，数据资源往往并非企业独立生产，而是通过用户、合作方等多方渠道获取。若企业以“合法拥有”(即，对拟入表的数据资源享有所有权)作为入表路径，可能缺乏充分的法律支撑。

因此，现阶段企业在数据资产入表时，更为可行的路径是证明其对于数据资源的“合法控制”。关于“合法控制”的具体论证方式，目前业界尚未完全形成共识。一般认为，企业需至少确保以下维度的合规性:

1. 主体合规：企业应当具备合法的主体资格、必要的资质和许可，且不存在重大经营风险或法律纠纷
2. 数据资源合规：从原始数据的采集到加工、生成数据产品或服务的整个流程，均应当遵循相关法律法规
3. 数据安全管理能力合规：企业应当具备良好的数据安全管理能力，建立完善的数据管理制度和技术防护措施，以确保数据资源的完整性、保密性和可用性

三. 主体合规评估

对主体合规的评估是数据入表合规评估的第一步，律师需要从企业基本信息到具体业务资质，再到特殊监管要求进行全面的审查。

1. 企业基本信息

- 主营业务是否与其注册的经营范围相符，是否存在超范围经营的情况
- 查询企业的信用记录、是否存在诉讼、失信被执行情况
- 近期(三年)受到行政处罚及有关主管监管部门调查及整改情况，特别是网络和数据安全相关情况

2. 业务资质

确认企业是否已取得必要的业务资质，并审查其有效期限、适用范围等是否符合要求:

- 对于某些业务领域，企业应当获得特定的行政审批和许可，例如征信业务需要取得征信资质
- 对于涉及电信业务的企业，应当根据业务类型申请相应的证照，例如 EDI 证、ICP 证等

3. 特殊主体的监管要求

法律法规对于特殊主体提出了监管要求，律师需注意对企业是否适用该等监管要求进行甄别。具体包括:

- 重要互联网平台：提供重要互联网平台服务、用户数量巨大、业务类型复杂的企业，应当履行建立外部独立监督机构、发布个人信息保护社会责任报告等义务
- 关键信息基础设施运营者：被认定为关键信息基础设施运营者的企业，应当按照相关规定采取严格的安全保护措施，例如“三同步”建设、本地化存储
- 行业监管规定：对于医疗健康、金融、汽车等行业，律师需重点关注行业主管部门出台的专门监管规定
- 核心数据、重要数据处理者：国家实施数据分类分级保护制度，涉及处理核心数据、重要数据的企业，应当履行特别的数据安全保护义务，例如定期开展安全风险评估并报送有关部门等

四. 数据资源合规评估

数据资源合规是数据资产入表合规评估中的核心环节，对于拟入表的数据资源，律师应当深入了解其处理(“处理”包括收集、存储、使用、加工、对外提供、删除等一系列操作)涉及的业务流程，分析其从原始数据到形成数据产品或服务的全流程合规情况。

1. 一般要点

就原始数据的来源而言，可以分为自行生产、公开收集、直接收集、间接获取等。

(1) 自行生产的数据是指企业在日常经营活动中产生的数据，对此类数据的评估应关注“自行性”:

- 评估企业是否具备相应的人员和技术能力，以及是否拥有相关的知识产权，如专利、软件著作权等
- 对于数据处理涉及的信息系统、设备等的情况，可要求企业提供服务器处理日志作为证明

(2) 公开收集的数据通常通过网络爬虫或类似技术获取，对此类数据的评估需考虑以下要点:

- 是否遵守被访问网站的 Robots 协议
- 是否突破或绕开被访问网站设置的反爬措施
- 是否妨碍网站的正常运行(例如，爬虫收集的网站流量不应超过网站日均流量的三分之一)
- 是否涉及爬取商业模式相同或相似主体的主营业务数据

(3) 直接收集的数据是指企业直接从数据主体(参照《银行保险机构数据安全管理办法(征求意见稿)》的定义，数据主体是指数据所标识的自然人或者其监护人、企业、机关、事业单位、社会团体和其他组织)处收集的数据。对此类数据的评估要点包括:

- 收集方式、收集目的等是否符合法律要求，包括收集目的是否合理且符合业务场景
- 是否通过隐私政策、数据授权协议等方式取得数据主体的授权同意

(4) 对于通过第三方数据源间接获取的数据，评估时主要关注“授权链条”的完整性:

- 上游数据源是否已合法获得数据授权，包括对外提供数据的授权
- 企业是否与上游数据源签署购买协议、合作协议或许可使用协议等
- 与上游数据源签署的协议是否对授权时间、使用范围等进行限制

2. 特定类型数据的合规评估

若数据资源(或其原始数据)涉及受到特别监管的数据，律师应当根据数据类型开展进一步的评估。

(1) 个人信息

- 是否公开个人信息处理规则，明示处理的目的、方式和范围
- 是否获得个人信息主体的授权同意，包括单独同意(如需)。企业应提供同意记录作为证明
- 个人信息的处理(包括加工形成数据资源等)是否符合最小必要原则
- 依据其他合法性基础(例如合同履行所必需、法定义务所必须等)收集个人信息的，处理是否处于该合法性基础范围内

(2) 公共数据

- 公共数据来源和获取方式是否合法，授权链条是否完整，是否获得数据源部门或地方数据主管部门的授权

- 授权范围是否涵盖公共数据运营(即将公共数据加工形成产品、服务，并对外提供)
- 是否符合地方公共数据授权运营相关政策(如有)要求
- 公共数据可能对国家安全、公共利益具备一定的影响程度，需评估是否可能构成重要数据。如是，进一步评估企业是否遵守重要数据的处理规定
- 宜按照“原始数据不出域、数据可用不可见”的要求，以模型、核验等产品和服务等形式向社会提供

五. 数据安全管理能力合规评估

《网络安全法》《数据安全法》《个人信息保护法》对于企业的网络安全保护、数据安全保护、个人信息保护义务进行了规定。

条文	具体规定
《网络安全法》第二十条	国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改: (一)制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任; (二)采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施; (三)采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月; (四)采取数据分类、重要数据备份和加密等措施; (五)法律、行政法规规定的其他义务。
《数据安全法》第二十七条	开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。 重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。
《个人信息保护法》第五十一条	个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失: (一)制定内部管理制度和操作规程; (二)对个人信息实行分类管理;

	(三)采取相应的加密、去标识化等安全技术措施; (四)合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训; (五)制定并组织实施个人信息安全事件应急预案; (六)法律、行政法规规定的其他措施。

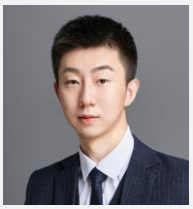
如上表所示，三部法律均要求企业在组织和技术两个方面加强安全保护措施。因此，为了确保企业对数据资源的“合法控制”，有效预防数据泄露和滥用，数据资产入表过程中，律师应当从组织和技术两个层面评估企业的数据安全管理能力。根据行业实践，采取的措施通常如下:

1. 数据安全组织措施
   - 制定全面的数据安全管理制度，明确企业数据安全的管理目标、标准，建立健全内部数据处理操作规程
   - 按照法律规定，设置网络安全、数据安全、个人信息保护负责人
   - 制定数据安全事件应急预案，包括应急响应的人员职责、处置流程、事件报告机制等，确保在数据安全事件发生时能够及时应对
   - 根据数据的敏感性和重要性对数据进行分类分级管理，并依据不同数据类别、级别采取相应的安全措施
   - 建立涉数据处理第三方管理机制，包括入库评审、数据处理协议签署、监督和定期审计等
   - 定期开展数据安全教育和培训，增强员工数据保护意识

2. 数据安全技术措施
   - 数据加密技术: 在数据存储和传输的各个环节，通过算法(如 AES 等)将原始数据转换为密文，确保数据在整个生命周期中的安全性
   - 访问控制技术: 根据员工的权限确定对数据的访问权限，并定期审查和更新访问权限
   - 数据泄露防护技术: 通过自动化 DLP 解决方案对数据泄露风险进行实时监控，识别和拦截潜在的数据泄露事件
   - 数据安全溯源技术: 记录数据的处理过程(如日志记录和审计系统)，实现数据在全生命周期的可追溯性
   - 隐私保护技术: 在个人信息处理过程中采取匿名化、去标识化等技术措施(如掩码、泛化等)，以减少对个人身份的识别

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com



朱晓阳
+86 21 3135 8683
nigel.zhu@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