

《数据要素价值形成规范》研究

Research on specification for data factor value formation

2025-08-29

2025 中国国际大数据产业博览会

数据要素价格形成与认定创新实验室 发布

版权声明

本规范研究于 2025 年 8 月 29 日在国家数据局主办、贵州省人民政府承办的 2025 中国国际大数据博览会上发布,版权归国家发展和改革委员会价格成本和认证中心所有,由数据要素价格形成与认定创新实验室组织实施,并受法律保护,转载、摘编或利用其他方式使用本规范研究内容的,应注明“来源:国家发展和改革委员会价格成本和认证中心”。违反上述声明者,将追究其相关法律责任。

如对本规范研究的内容有任何意见或建议,请联系数据要素价格形成与认定创新实验室(联系邮箱:dplab@datapricing.cn)。

目录

前 言	3
1. 范围	4
2. 规范性引用文件	4
3. 术语和定义	4
4. 概述	6
5. 数据盘点与治理	6
5.1 数据资源盘点	6
5.2 数据分类分级	10
5.3 数据质量评价	13
5.4 数据产品的设计与规划	17
5.5 数据资产的识别	18
5.6 数据要素目录建立	21
6. 数据合规与确权	23
6.1 数据确权的原则	23
6.2 数据要素权属认定	24
6.3 数据合规审查	26
6.4 数据安全	31
7. 数据产品定价	33
7.1 数据产品的分类与特征	33
7.2 数据产品价值形成机制	35
7.3 数据产品定价方法模型	38
7.4 数据产品定价流程	41
7.5 公共数据的定价模型	43
8. 数据资产价值评估	45
8.1 数据资产的属性	45
8.2 数据资产价值形成机制	46
8.3 数据资产价值评估方法模型	47
8.4 数据资产价值评估流程	51
9. 数据资产入表	52
9.1 入表原则与要求	52
9.2 入表流程与核算方法	53
9.3 数据资产计量	56
10. 数据交易与流通	57
10.1 交易机制设计	57

10.2 交易主体与客体管理	59
10.3 交易监管与安全保障	62
10.4 收益分配和成本分摊机制设计	65
11. 数据资本化	69
11.1 数据要素经营与管理	69
11.2 数据资本化的形态	70
11.3 数据资本化的流程	71
11.4 通过资本化实现数据要素增值	72
12. 数据要素授权运营	73
12.1 运营模式与机构选择	73
12.2 授权协议与管理	75
12.3 运营效果评估与优化	75
12.4 数据安全合规审计	76
参考文献	81

前 言

本文件由国家发展和改革委员会价格成本和认证中心提出并归口。

组织单位：国家发展和改革委员会价格成本和认证中心、数据要素价格形成与认定创新实验室。

主编单位：中国检验认证集团、中国航天标准化与产品保证研究院、北京大成律师事务所。

副主编单位：北京国际大数据交易所、湖北大数据集团、中国交通建设集团、中国二十二冶集团、深圳数据交易所、贵阳大数据交易所、安徽高端智能机器创新研究院。

参编单位：新晨科技股份有限公司、安徽云信达科技有限公司、北京市百伦律师事务所、惠州雷士光电科技有限公司、北京分贝通科技有限公司、中国电子数据产业集团、德勤中国、北京数据要素科技有限公司、北京易华录信息技术股份有限公司、中德高路科技（云南）股份有限公司、公安部第一研究所、昆明国际数据交易所、郑州数据交易中心、浙江大数据交易中心、上海数据交易所、天津武清区数据局、中国信息通信研究院、中电信数政科技有限公司、广东跑合中药材电子商务有限公司、北京市市政工程设计研究总院有限公司、中国移动通信集团、中国国际经济咨询有限公司、北京数字认证股份有限公司、北京神州数码云计算有限公司。

指导委员会：卢延纯、杨东、姜怀浩、蔡红宇、李晓鹏、杨杰。

专家委员会：王东明院士、任福继院士、杨善林院士、方明院士、王立梅、孙毅、张涛、李志杰、吴沈括、邢会强、赵精武、谢丹夏。

编写委员会：王安、陈福、王瑞锋、郭翔、袁丽、杨丽、赵慧、代健、李振军、栾明月、湛宏东、安华杰、王忠浩、彭聪、安明石、刘业政、孙见山、王冠、李颖、李伟良、吴荣彬、焦建玲、古伟、杨志立、翟静、刘龙生、赵朴花、左建芬、张俊鹏、杨帆、张兵、李帆、路兴、李峰、硕天鸾、孙承乾、豆思涵、羊琰琰、刘炜、王端阳、李盛、熊婷、谢琴超、李春江、秦美虎、覃校红、邹锋、林微、王蓉、卢丹、刘茜、牛一锋、孔俊、陈钰炜、张宇春、王凯伟、曹国钧、袁振辉、章恒靖、邓晨、国伟、高历红、吕正英、崔瑞媛、武振国、傅毅明、田力、王隆泰。

1. 范围

本文件为我国数据要素价格形成机制提供依据,为数据要素的价值实现提供一套明确的路径指引和操作方法,助力各行业各领域充分挖掘数据要素的潜力,实现数据要素价值的最大化,推动数字经济的高质量发展。

本文件适用于企业、公共机构开展数据要素价格形成、交易与流通、管理增值等活动。

2. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 36344-2018 信息技术 数据质量评价指标

GB/T 37932-2019 信息安全技术 数据交易服务安全要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 40685-2021 信息技术服务 数据资产 管理要求

GB/T 42450-2023 信息技术 大数据 数据资源规划

GB/T 43697-2024 数据安全技术 数据分类分级规则

3. 术语和定义

3.1

数据资源 data resource

作为资源看待的用于支持实现组织业务目标的数据。

[来源: GB/T 42450-2023, 3.1]

3.2

数据资产 data asset

特定主体合法拥有或控制的，能进行货币计量的，能够带来经济利益或社会价值的数据资源。

3.3

数据产品 data product

数据产品是指基于数据资源，经过采集、清洗、分析、可视化、加工、包装等处理后形成的、能够满足特定用户需求并提供价值的数据集合或数据服务。

3.4

数据价格形成 data price formation

指在数据要素市场活动中，通过静态的数据要素价值确认和动态的数据要素价值实现等多种因素相互作用最终确定数据价格的过程。

3.5

数据资产入表 data assets incorporating into the balance sheet

企业依据会计准则等相关规定，将符合确认条件的数据资源确认为无形资产或存货等资产类别，或就未满足资产确认条件但符合其他列报要求的数据资源进行财务处理并在会计报表中反映的行为。

3.6

数据交易 data transaction

数据提供方和需求方之间以数据商品作为交易对象，进行的以货币或货币等价物交换数据商品的行为。

[来源：GB/T 37932-2019, 3.1]

3.7

数据安全合规审计 data security compliance audit

针对数据处理者的数据处理活动是否遵守法律、行政法规的情况进行审查和评价的活动。

4. 概述

本文件旨在打通数据要素流通市场，规范数据资源、数据产品、数据资产等数据要素价值的形成机制，包括静态的数据要素价值确认和动态的数据要素价值实现，其中静态的数据要素价值确认的流程节点包括数据盘点与治理、数据合规与确权、数据产品定价、数据资产价值评估等环节，动态的数据要素价值实现的流程节点包括数据资产入表、数据交易与流通、数据资本化、数据要素授权运营等环节。通过构建和规范数据要素价值的形成机制，充分释放数据要素价值，繁荣数据要素市场，更好地推动数据资产化和数据要素市场的高质量发展。

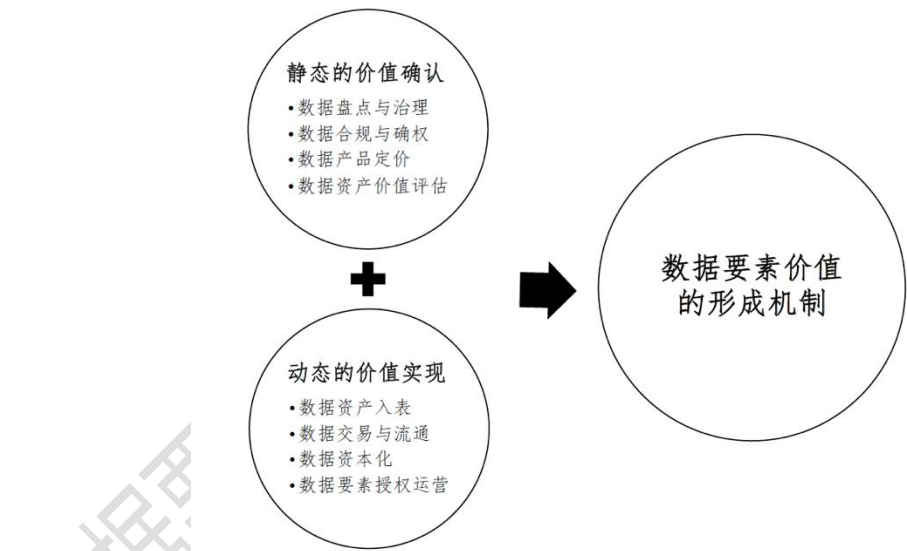


图1 数据要素价值形成机制架构

5. 数据盘点与治理

5.1 数据资源盘点

数据资源盘点是指从全局出发对企业业务系统、数据平台、数据仓库、数据湖等数据资源进行全面摸底，采集元数据、发现企业数据字典、识别数据之间的

关系，从业务流程和数据应用的视角出发梳理数据资源的技术属性、业务属性、管理属性，掌握数据资源全貌，形成数据资源清单。

5.1.1 数据资源盘点目标

通过数据资源盘点，明确每类数据资源的业务归属和责任人，有助于在后续数据治理过程中更好地管控和维护数据，帮助企业了解数据资源情况，理解、识别、使用和管理数据，有效推进数据资源对内应用和对外交易。

5.1.2 数据资源盘点范围

5.1.2.1 组织范围

明确盘点需要覆盖的组织和部门，包括公司本级、子分公司等。

5.1.2.2 业务范围

明确盘点需要覆盖的业务领域，包括生产业务、采购业务、营销业务、财务业务、人力资源业务、数据运营业务等。

5.1.2.3 系统范围

明确盘点需要覆盖的信息系统，包括ERP系统、MES系统、SCM系统、CRM系统、HR系统等。

5.1.3 数据资源盘点内容

5.1.3.1 数据来源

明确数据资源的来源方式，包括自行产生收集、公开渠道爬取和基于协议获取。对于数据的不同来源进行描述：

a) 自行产生收集，描述要素包括：

- 1) 产生方式分为人工采集、信息系统产生或感知设备采集；
- 2) 收集细节，人工采集方式涉及的收集细节包括时间、地点、对象特征、响应率；信息系统产生方式涉及的收集细节包括系统名称、版本、业务场景；感知设备采集方式涉及的收集细节包括设备型号、部署位置、采集频率、环境参数；

- 3) 工具与方法，人工采集方式依赖调查问卷，涉及的方法包括问卷设计、访谈提纲确定、记录观察等；依赖数据进行运转的汇总系统、清洗系统和加工系统等信息系统，涉及的方法包括数据汇总结构的确定、数据清洗过程设计、数据加工方法的选择等；感知设备采集方式依赖各类型数据传感器，涉及的方法包括传感器的分布布置、数据传输协议的选择、数据存储节点的设置等。
- b) 公开渠道爬取，描述要素包括：
 - 1) 数据来源，即平台名称、URL、数据范围、使用许可协议等；
 - 2) 爬取细节，即爬虫工具名称、版本、爬取时间、遵守的规则等；
 - 3) 数据范围，即爬取的数据主题类型、行业归属、主要字段、时间范围等；
 - 4) 变量说明，即爬取数据的字段名称、计量单位、业务含义等；
 - 5) 数据质量评估，参考本文5.3节的内容确定。
- c) 基于协议获取的，描述要素包括：
 - 1) 协议信息，即合作机构名称、协议编号、授权范围等；
 - 2) 数据内容，即数据授权的范围、数据规模、数据表头、更新频率等；
 - 3) 交付方式，即API接口交付、文件传输交付和数据库同步等；
 - 4) 数据质量评估，参考本文件第5.3节的内容确定。

5.1.3.2 数据类型

明确数据资源的类型，包括结构化数据、半结构化数据、非结构化数据。

5.1.3.3 数据规模与更新频率

明确数据资源的规模与更新频率，包括数据量、数据存储形式、数据更新周期类型、数据更新频率。

5.1.3.4 数据质量

评估数据的完整性、准确性、一致性和可靠性等方面，发现数据中的潜在问题，并制定相应的数据清洗和验证策略，参考本文件第5.3节。

5.1.3.5 数据用途与价值定义

定义数据的用途和价值，明确数据在组织运营、决策支持和业务发展中的作用。

5.1.4 数据资源盘点实施路径

5.1.4.1 元数据摸排

通过定义技术元数据、业务元数据和管理元数据，帮助业务人员和管理人员理解、识别、管理和使用数据，包括元数据管理（明确元数据管理相关参与方，确定元数据类型、范围、属性，设计元数据的元模型规范，包括技术元数据、业务元数据、管理元数据，确定元数据新增、变更、废止等管理流程）、元数据采集（对不同类型、不同来源的元数据进行采集和存储，形成对数据结构、数据描述的统一视图及清单）、元数据变更管理（根据元数据摸查结果，监控公司数据资源变化，评估数据变更影响范围）。

5.1.4.2 构建数据标准

制定数据格式标准、数据编码标准、数据接口标准等，确保数据的一致性和互操作性，提高数据管理的效率和质量。

5.1.4.3 数据定义

对企业所持有的数据资源进行识别、定义、深度剖析、标记数据内容，补充业务含义，明确数据组织、结构、关系，形成更完整、有效的数据架构的过程。

5.1.4.4 明确数据血缘

建立数据血缘图谱，清晰展示数据在各个系统和业务环节中的流转路径。建立字段级可视化血缘关系图，明确数据的来源权属、合法性和相关业务归属和责任人，追溯数据的操作和流向。

具体工作包括识别数据资源源头、分析数据资源的加工过程、明确数据资源的输出结果。

5.1.4.5 构建数据资源目录

对数据资源按照数据来源、业务主题等进行分类、编码、描述，提供完整的数据定义、数据说明、数据特征、标签、数据责任人等技术、业务、管理信息，建立可共享、可复用的多层级数据资源目录。

5.1.5 数据属性标注

包括数据基础属性和状态属性，状态属性包括：原始数据、中间数据和结果数据。

5.1.6 数据规模计量

5.1.6.1 数据计量单位标准化

在对数据规模进行计量前，应先对数据规模的计量单位进行统一。

5.1.6.2 数据的增量计量

数据的增量计量是指在特定的时间段对数据的增长情况进行计量。

5.1.6.3 数据的存量计量

数据的存量计量是指在某一个时间节点对现有数据的规模进行计量。

5.1.7 数据存储信息

数据资源盘点还包括对数据存储信息的描述，具体涉及以下方面：

- a) 存储位置与路径：物理位置、逻辑路径、跨地域存储情况等；
- b) 存储方式与介质：存储技术、存储介质、数据格式等；
- c) 访问控制与权限管理：认证机制、授权策略、审计日志等；
- d) 备份与恢复策略：备份频率、备份类型、恢复流程等；
- e) 存储期限与销毁策略：存储期限、销毁方法、销毁验证等；
- f) 安全与合规性：数据加密、隐私保护、合规性声明等；
- g) 技术细节：数据库版本、存储架构、性能参数等。

5.2 数据分类分级

根据数据在经济社会发展中的重要程度和可能造成的危害程度，将数据划分为不同类别和安全级别，可以提高数据管理效率和安全保障能力，有利于数据规

范化管理和价值实现。在实施分类分级时，应当坚持科学实用、边界清晰、就高从严、点面结合、动态更新的原则。

5.2.1 业务场景分类

根据业务流程和应用场景对数据进行分类，是确保数据处理符合业务需求和监管要求的重要手段。常见的业务场景分类方式包括：

5.2.1.1 行业领域分类

按照数据所属产业或行业进行分类，例如将数据划分为金融数据、制造数据、能源数据、交通运输数据、卫生健康数据、教育数据、科学数据等。

5.2.1.2 业务流程分类

依据业务流程或功能场景对数据进行细分，如生产管理数据、销售服务数据、客户管理数据、运营监控数据等。不同业务条线的数据可根据其产生环节和使用场景进行归类。

5.2.1.3 数据主体分类

按照数据涉及的主体或归属进行分类，将数据划分为公共数据、企业数据和个人信息等类别。其中，公共数据指政府及公共组织履行公共事务职责或提供公共服务过程中产生的数据；组织数据指企业、机构在自身生产经营中产生的非个人信息数据；个人信息应依照个人信息保护相关法律、法规、标准进行识别和分类。

5.2.1.4 其他维度分类

根据数据的内容主题、用途、来源、数据处理方式等特征对数据进行细化分类，以满足不同业务系统和分析需求。

通过上述分类维度的综合应用，可以形成多维度的数据分类标签，为后续的分级和管理提供依据。特别是涉及法律法规有专门管理要求的数据类别（如个人信息、重要数据等），应当参照相关规定和标准进行识别和分类。

5.2.2 敏感等级划分

数据分级是按照数据的重要程度和敏感度实施差异化保护的关键环节，应当根据数据对国家安全、公共利益、企业运营和个人隐私等影响程度进行划分。一般可将数据分为以下安全级别：

5.2.2.1 核心数据

关系国家安全、国民经济命脉、重要民生或重大公共利益的数据，一旦泄露、篡改或损毁将造成极大危害的类别。此类数据应实行最严格的保护制度，设置更高级别的管理和技术措施。

5.2.2.2 重要数据

重要数据是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。此类数据需要重点保护，可采用分级备案、分类加密和访问审计等措施。

5.2.2.3 一般数据

核心数据、重要数据之外的其他数据。此类数据影响程度较低，可按照一般管理要求进行保护，但也应避免泄露和篡改风险。

以上分级结果应当参照国家和行业标准，以及组织自身业务特点综合确定。对于个人信息，应当按照《中华人民共和国个人信息保护法》和《信息安全技术 个人信息安全规范》（GB/T 35273）等要求，将个人信息分为一般个人信息和敏感个人信息，对敏感个人信息实施更高保护级别。总体上，应建立分级目录和清单制度，将确定的核心数据和重要数据列入数据分类分级目录，落实相应的重点保护措施。

5.2.3 动态分级调整规则

数据分类分级并非静态过程，应根据业务变化、风险评估结果和法律法规更新情况进行动态调整。为保持分类分级结果的准确性，应建立常态化的评估和调整机制。

5.2.3.1 定期评审

应定期或在业务重大调整后对现有的数据分类分级方案进行复核,判断是否需要更新分级级别或增加新的分类维度。

5.2.3.2 触发事件调整

当出现新业务场景、合规要求变更、安全事件或风险水平明显升高等情况时,应及时启动专项评审,对相关数据重新评估分类分级并调整保护策略。

5.2.3.3 记录与备案

对每次分类分级的调整结果应形成书面记录,更新数据分类分级文档,并向数据安全负责人或监管部门备案,以保证可追溯性和合规性。

所有调整工作应遵循“动态更新原则”,即根据数据属性、重要性和潜在危害程度的变化,对数据分类分级和重要数据目录进行定期审核和更新。

5.3 数据质量评价

5.3.1 数据质量评价维度

数据质量评价是衡量数据规范性、完整性、准确性、一致性、时效性、可访问性等特性是否满足业务和管理需求的过程。高质量的数据是数据要素价值实现的重要前提,为此,应当建立科学的数据质量评价体系,按照国家标准和企业自身需求确定评价指标和方法。

5.3.1.1 规范性

数据符合既定标准、数据模型、业务规则或权威参考的程度。规范性确保数据格式和内容符合业务约定。

5.3.1.2 完整性

数据集或记录中各字段值齐全、无缺失的程度。完整性反映了数据是否存在漏值或缺项。

5.3.1.3 准确性

数据真实反映其所描述对象事实的程度。准确性要求数据错误率低,能够正确表达业务事实。

5.3.1.4 一致性

数据在不同记录、不同系统或不同时间之间保持一致、无矛盾的程度。一致性确保各系统间数据的同步性和逻辑协调性。

5.3.1.5 时效性

数据能够及时更新并反映最新状态的程度。时效性要求数据在业务要求的时间窗口内完成采集和更新。

5.3.1.6 可访问性

数据资源可以按需访问和获取的程度。可访问性关注数据是否处于可用状态，并能被授权用户正常读取。

以上指标可结合企业业务特点进行扩展。数据质量评价工作应采用定量与定性相结合的方法，通过计算率、差异率等指标进行评分，设定阈值进行监控。

建立完善的数据质量评价流程，明确质量评价的周期、方法和责任。质量评价结果应当作为改进数据处理流程、优化系统接口和加强人员培训的依据，形成“发现问题—评估指标—整改治理—持续监控”的闭环管理。定期的评价报告应提交给管理层和相关职能部门，以督促各方落实整改措施，持续提升数据质量水平。

5.3.2 数据质量评价维度指标

可采用两级编码体系（一级指标2位数字+二级指标2位顺序码），具体指标如表1-6所示。

表1 规范性评价指标

指标编号	指标名称	评价要点
0101	数据标准符合性	遵循国际/国家/行业数据命名、定义、结构规范（如值域约束）
0102	数据模型一致性	符合组织数据模型的结构与关系定义
0103	元数据完备性	元数据文档完整度（如数据字典、血缘描述）
0104	业务规则遵从性	满足业务流程定义的逻辑约束（如风控规则）

指标编号	指标名称	评价要点
0105	参考数据有效性	参考数据（如分类编码）与权威源的一致性
0106	安全合规性	符合数据权限管理、隐私保护等安全规范

表2 完整性评价指标

指标编号	指标名称	计算方法
0201	数据元素完整性	$\lambda = \text{应赋值元素数} / \text{已赋值元素数}$
0202	数据记录完整性	$\lambda = \text{预期记录数} / \text{有效记录数}$

表3 准确性评价指标

指标编号	指标名称	示例
0301	内容正确性	地址信息与实际地理位置匹配
0302	格式合规性	身份证号无非数字字符、性别字段无非“男/女”值
0303	数据重复率	重复客户 ID 数占比
0304	数据唯一性	主键冲突记录占比
0305	数据异常率	交易金额为负值的记录占比

表4 一致性评价指标

指标编号	指标名称	评价场景
0401	同源数据一致性	同一用户信息在 CRM 系统与订单系统的差异率
0402	关联数据一致性	订单金额与支付流水金额的逻辑一致性

表5 时效性评价指标

指标编号	指标名称	价值关联
0501	时间范围正确性	历史数据时间戳符合业务周期(如季度报表数据完整性)
0502	数据交付及时性	实时数据流延迟 ≤ 1 秒(高频交易场景)
0503	时序逻辑合理性	用户注册时间早于首次购买时间

表6 可访问性评价指标

指标编号	指标名称	度量方式
0601	数据可获取性	API 接口平均响应时间 $\leq 500\text{ms}$
0602	系统可用性	数据服务平台年可用率 $\geq 99.9\%$

5.3.3 数据质量评价实施流程

5.3.3.1 数据质量评价按如下流程闭环运行：

构建评价组织 → 制定数据规范 → 选定评价指标 → 实施质量检测 → 优化数据质量 → 交付价值应用

5.3.3.2 数据质量评价关键要求

动态评价：在数据采集、加工、服务等环节嵌入质量检查点；

量化管理：各级指标需输出数值化评分，阈值按业务场景设定；

价值关联：质量评分纳入数据资产估值模型。

5.4 数据产品的设计与规划

5.4.1 数据产品形态

数据产品形态是对数据产品呈现方式的分类描述，涵盖多种不同类型。

5.4.1.1 数据集

数据集是指具有一定主题，可以标识并可以被计算机化处理的数据集合。

5.4.1.2 数据报告

数据报告是指以文档形式呈现数据分析结果与结论。

5.4.1.3 数据接口

数据接口是不同系统或组件间数据交互的通道。

5.4.1.4 数据应用

数据应用是指基于数据构建的可直接服务于用户的软件或服务。

5.4.2 数据产品研发流程

5.4.2.1 需求分析

调研用户需求和市场情况，梳理使用场景并明确数据产品功能。确认构成数据产品的数据来源，以及权属与权益分配规则。判断构成数据产品的数据来源是否具备标准化、脱敏、结构化等可产品化条件。

5.4.2.2 产品设计

根据需求分析结果，对数据产品的技术架构、功能模块、定价模式、产品形态进行设计，编制设计方案，确保设计方案的可行性与合理性。

5.4.2.3 开发测试

按照设计方案开展数据产品开发工作，定期进行开发进度跟踪与阶段性成果评审。进行功能测试、性能测试、安全测试等多维度测试，修复测试中发现的问题。

5.4.2.4 上线推广

通过企业官网、数据交易所备案等渠道推动数据产品部署上线，开展用户培训与技术支持工作，收集用户反馈，确保产品顺利投入使用。

5.4.2.5 运营维护

对产品进行持续运营管理，包括用户服务、市场推广、数据更新、功能优化等，提升产品市场竞争力和用户满意度。当产品市场需求下降、功能无法满足新的业务需求或出现更优替代产品时，评估产品下线的必要性，制定下线计划，妥善处理用户数据和相关服务。

5.5 数据资产的识别

5.5.1 数据资产识别条件

数据资产识别需满足以下条件：

5.5.1.1 权属清晰性

- a) 持有合法的数据权属证明文件；
- b) 完成全链路数据来源合规审查。

5.5.1.2 价值可量化

- a) 具备明确的经济价值实现路径(如直接交易、质押融资或内部降本增效)；
- b) 支持至少一种标准化估值方法(成本法、收益法或市场法)的应用基础。

5.5.1.3 技术可管控

- a) 拥有独立的物理/逻辑存储标识；
- b) 提供标准化访问接口(如API、SDK或文件传输协议)。

5.5.1.4 生命周期完整

- a) 数据记录时间戳的创建，应严格根据应用数据产生的频率进行，以确保数据及时间戳的完整性；
- b) 全生命周期记录清晰，至少包括创建时间戳和流转时间戳。

5.5.2 数据资产目录构建

数据资产目录构建可以采用三级架构体系，自上至下可以包括业务域层、主题集层和资产单元层。各层构建依据及典型应用说明如下：

5.5.2.1 业务域层

构建依据：严格遵循国民经济行业分类标准（GB/T 4754）。

典型应用：金融数据域、医疗健康数据域。

5.5.2.2 主题集层

构建依据：按业务流程切割各功能模块。

典型应用：以医疗健康数据为例包括：临床诊断主题集、药房管理主题集等。

5.5.2.3 资产单元层

构建依据：定义最小可独立管理实体。

典型应用：以临床诊断主题集为例，包括电子病历库、主治医生归档库等。

5.5.3 数据资产状态动态监控

数据资产状态的动态监控旨在实现资产全生命周期的可视化管理，需建立多维度监控机制。

5.5.3.1 监控对象覆盖

- a) 完整性监控：实时追踪数据资产的存储状态、副本分布及备份完整性，确保关键资产无缺失；
- b) 合规性状态：持续扫描数据资产的授权协议有效期、使用范围限制及敏感字段脱敏状态，触发超范围使用预警；
- c) 价值波动评估：通过市场交易数据、应用场景反馈等指标，动态修正资产价值系数，反映其经济效用变化。

5.5.3.2 技术实现路径

- a) 部署元数据采集代理，自动捕获资产访问日志、修改记录及权限变更事件；
- b) 基于API接口集成业务系统，实时同步资产调用频次与业务关联性数据；
- c) 应用区块链技术建立审计溯源链，确保状态变更记录不可篡改。

5.5.3.3 管理流程设计

- a) 设置多级状态阈值（如闲置、活跃、高风险），触发自动化处置流程；

- b) 生成周期性监控报告，涵盖资产利用率、合规偏离度及价值趋势分析，支持管理决策；
- c) 建立闭环处置机制，对异常状态（如授权过期、非法跨境传输）执行系统自动冻结并通知责任人。

5.5.4 跨系统数据资产的识别

识别分散跨系统的数据资产需解决系统壁垒问题，具体实施包括：

5.5.4.1 识别框架构建

- a) 统一标识体系：为每个资产分配全局唯一ID，关联其在各系统的物理存储位置与逻辑映射关系；
- b) 分布式元数据注册：通过标准化接口汇聚多系统元数据，构建跨系统资产目录索引库。

5.5.4.2 关联规则定义

- a) 业务关联性：识别跨系统流转的核心业务对象，建立以业务实体为中心的资产聚合视图；
- b) 技术特征映射：根据数据模式（Schema）、存储格式及处理引擎分类技术同构资产。

5.5.4.3 实现路径

- a) 部署中间件层，自动发现并注册新增系统的资产元数据；
- b) 构建领域模型，实现语义级资产关联（如“用户画像资产”在CRM与BI系统的映射）；
- c) 设立冲突消解机制，对多系统重复资产采用权属优先级规则或人工仲裁。

5.5.5 数据资产入表入卡

企业数据资产入表：按照《企业数据资源相关会计处理暂行规定》《企业会计准则第6号——无形资产》《企业会计准则第1号——存货》等会计准则要求，企业进行数据资产入表。

政府事业单位数据资产入卡：按照《关于加强数据资产管理的指导意见》（财政部2023年12月发布）要求，明确数据持有权、数据使用权、数据经营权，建立数据资产卡片，获得数据资产编号。

5.6 数据要素目录建立

5.6.1 数据要素目录结构设计

数据要素目录可采用分层逻辑架构实现资源统一管控，需满足以下基本要求：

5.6.1.1 分层架构设计

- a) 资源层：按数据资源（原始数据集）、数据产品（加工后服务）、数据资产（确权可估值实体）建立基础分区，每类实体设置唯一标识符；
- b) 业务域映射层：根据企业核心业务线划分主题域，建立业务术语与数据实体的映射关系（如“客户画像”映射至客户域资产目录）；
- c) 管理属性层：嵌入安全分级标签、生命周期状态及合规标识。

5.6.1.2 元数据规范

- a) 强制字段定义：名称、标识符、数据类型、格式标准、更新频率、责任主体；
- b) 扩展字段支持：血缘关系指针（溯源至原始数据源）、关联业务场景、质量评估分值。

5.6.1.3 多维度索引机制

- a) 主索引：按业务主题域纵向聚合数据实体；
- b) 辅助索引：通过技术特征、安全等级、地域属性建立跨域检索路径；
- c) 动态标签索引：自动提取高频访问标签生成热点导航树。

5.6.2 数据要素目录动态更新机制

通过建立闭环的数据要素目录动态更新机制以确保数据要素目录的时效性：

5.6.2.1 变更触发规则

- a) 事件驱动更新：对数据资源结构变更、数据产品版本迭代、数据资产状态迁移自动触发目录元数据刷新；
- b) 周期性核验：每日批量扫描底层系统，校验目录项与物理资产的映射一致性。

5.6.2.2 版本控制策略

- a) 主版本迭代：重大业务重组或技术架构升级时生成V2.0等主版本，保留历史版本追溯；
- b) 增量更新日志：记录每次变更的操作用户、时间戳、修改内容。

5.6.2.3 异常处理机制

- a) 冲突消解：多系统同步修改时采用时间戳优先原则，对目录项加锁防止并发覆盖；
- b) 失效项清理：对超过180天无访问记录的目录项自动标记“待归档”，经责任人确认后移入历史库。

5.6.3 不同系统间的互操作性要求

不同系统间的互操作性需满足以下互操作基准：

5.6.3.1 接口规范

- a) 标准接入协议：强制采用特定的接入格式，响应时间<500ms；
- b) 元数据交换规范：遵循统一的标准元模型，在数据跨系统流转过程中制定统一的元数据交换记录规范。

5.6.3.2 语义一致性

- a) 业务术语对齐：建立企业级数据字典（如“客户ID”在CRM/ERP中统一为CUST_ID）；
- b) 度量单位转换：内置单位换算引擎。

5.6.3.3 安全互信机制

- a) 跨域认证：采用认证授权协议等实现系统间双向鉴权，敏感目录项查询需申请临时令牌；

- b) 策略联动：当源系统启用数据脱敏时，目录自动同步更新访问策略标签。

5.6.4 分级开放管理

表7 开放分类层级设计（公开、受限、敏感、机密）

级别	定义	开放策略
公开	非敏感、可无条件开放	注册即可访问，如人口普查数据
受限	需授权或脱敏后开放	申请审批制，如企业信用数据
敏感	涉及隐私或商业秘密	协议约束+加密传输，如患者医疗记录
机密	影响国家安全或公共安全	禁止开放，如军事数据

5.6.5 数据要素目录的价值挖掘

数据要素目录构建后，可以基于以下维度对数据要素目录的价值进行挖掘：

5.6.5.1 业务赋能维度

- a) 精准资产发现：支持多条件组合检索；
- b) 智能推荐引擎：基于用户角色推荐高相关度目录项。

5.6.5.2 管理决策维度

- a) 资源健康度看板：可视化展示资产覆盖率、闲置资产预警；
- b) 成本效益分析：关联目录访问频次与存储计算成本，识别高ROI资产（如高频访问的营销数据产品）。

5.6.5.3 创新驱动维度

- a) 开放目录API：允许开发者查询目录元数据开发新应用（如自动生成数据合规报告）；
- b) 知识图谱构建：将目录实体与外部知识库（行业标准/法规）链接，支撑智能决策。

6. 数据合规与确权

6.1 数据确权的原则

数据确权的目的在于明确数据的归属、使用权限以及责任范围，确保数据的安全流通。促进数据的价值释放，数据确权应该遵循如下原则：

- (1) 合法性原则；
- (2) 透明可追溯性原则；
- (3) 权责明确原则；
- (4) 公平合理原则；
- (5) 安全可控原则。

6.2 数据要素权属认定

6.2.1 制定数据要素确权策略

根据数据的特点、性质、用途和使用场景等，制定具体的数据确权策略。数据确权的核心在于界定清晰的数据产权结构，构建数据持有权、数据使用权和数据经营权三权分置的产权运行机制。

6.2.1.1 数据持有权

数据持有权是指权利人自行持有或委托他人代为持有合法获取的数据的权利，重点聚焦数据的依法取得和合规持有，旨在防范他人非法违规窃取、篡改、泄露或者破坏持有人持有的数据。

6.2.1.2 数据使用权

数据使用权是指权利人通过加工、聚合、分析等方式，将数据用于优化生产经营、提供社会服务、形成衍生数据等的权利，强调对数据进行聚合、清洗、分析等处理后进行应用的权能。

6.2.1.3 数据经营权

数据经营权是指权利人通过转让、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，强调数据价值链中由数据资源到数据产品再到数据商品的价值创造和价值实现的过程。

6.2.2 按照数据主体确认权属

数据要素的创造是多方主体共同参与的结果,为保障数据要素的交易流通与利益分配,应该对各方主体的权属予以明确。

6.2.2.1 公共数据的权利归属

公共数据是指各级党政机关、企事业单位依法履职或提供公共服务过程中产生的数据。在确认公共数据的权属时,应从以下几个方面进行考虑:

- a) 收集个人信息、企业信息、自然信息、事件信息等的批文、批复或指示等公文或政策性文件;
- b) 向自然人收集个人信息的个人信息保护政策、隐私保护政策、个人信息处理政策文件;
- c) 个人信息、企业信息的处理过程,如数据的产生、收集方式、使用历史、当前状态等。

6.2.2.2 企业数据的权利归属

在确认企业数据的权属时,应从以下几个方面进行考虑:

- a) 明确数据的来源,企业在自行合法经营过程中产生的数据,包括但不限于生产数据、日志数据、销售数据、采购数据、维护数据等;企业购买或授权使用的数据,包括但不限于从第三方购买以及由第三方授权使用的数据等;应严格排查通过爬虫技术爬取的公开数据甚至通过其他技术手段获取的非公开数据;
- b) 合同与文件的核实与梳理,按照不同的数据来源,梳理其权利链条是否完整;
- c) 权属证书核查,对于已经取得数据权属证书的企业数据,核实证书的真实性,包括颁发主体、颁发依据等。

6.2.2.3 个人数据的权利归属

在确认个人数据的权属时,应从以下几个方面进行考虑:

- a) 企业在收集个人信息之前，获得个人的同意或有其他的合法基础，向数据主体明确告知数据收集的目的、方式、范围、使用期限以及个人信息安全保护措施，审查用户协议、隐私政策以及其他个人信息保护相关政策；
- b) 数据处理者将个人信息匿名化处理后形成的信息，不属于个人信息，个人信息主体对匿名化处理后的信息不享有权属；但是，匿名化处理应该满足经过处理无法识别特定自然人且不能复原的要求；
- c) 数据处理者应该保障个人信息主体的权益，包括行使查阅、更正、撤回个人信息、申请删除非必要个人信息等权利。

6.2.3 按照数据处理过程确认权属

6.2.3.1 原始数据的权利归属

对于未经加工的原始数据，一般情况下原始数据的权益归属于合法拥有或控制数据的主体，但有相反证据证明的除外。在原始数据的确权过程中，应梳理主体合法拥有或控制的证据，同时应保障原始数据来源方的收益权。

6.2.3.2 衍生数据的权利归属

衍生数据是在原始数据的基础上，经过数据加工等创造性劳动而产生的数据。对于衍生数据权利的归属，应该基于各参与方付出的创造性劳动的贡献予以确权。数据加工方对衍生数据享有优先运营权。

6.3 数据合规审查

6.3.1 数据来源制度合规审查

6.3.1.1 自行收集数据制度合规审查

企业应合法合规收集数据。如所收集的数据涉及个人信息，企业在数据收集过程中需要遵守获得用户授权同意规则，基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。在取得用户同意时，应当遵守：

- a) 不得在征得用户同意前就开始收集个人信息或打开可收集个人信息的权限,在APP首次运行时应通过弹窗等明显方式提示用户阅读个人信息保护政策等收集使用规则;
- b) 用户明确表示不同意后,不得收集个人信息或打开可收集个人信息的权限,不得频繁征求同意、干扰正常使用服务;
- c) 实际收集的个人信息或打开的可收集个人信息权限,应与声明并经用户同意的收集规则保持一致;
- d) 不得以默认选择同意个人信息保护政策等非明示方式征求用户同意;
- e) 不得未经用户同意更改其设置的可收集个人信息权限状态,如APP更新时自动将用户设置的权限恢复到默认状态;
- f) 按照服务类型分别向用户申请处理个人信息的同意,不会使用概括性条款取得同意;
- g) 不会以改善服务质量、提升用户体验、研发新产品等为由,强迫用户同意处理其个人信息;
- h) 不会通过误导、欺诈、胁迫等方式获得用户的同意;
- i) 不会通过捆绑不同类型服务、批量申请同意等方式诱导、强迫用户进行批量个人信息同意;
- j) 不会超出个人授权同意的范围处理个人信息。

企业应保障用户的同意撤回权,并提供便捷的撤回同意的方式。基于用户同意处理个人信息的,用户有权撤回其同意。用户撤回同意,不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

在一些特殊情形下,应单独取得用户的同意:例如向第三方提供个人信息、公开其处理的个人信息、处理敏感个人信息、跨境转移个人信息等。

6.3.1.2 采购数据制度合规审查

从外部采购数据时,应对数据供应商进行尽职调查,核实其经营资质、信誉状况、数据来源情况,并通过合同明确要求其提供数据来源的合法性证明、约定数据质量、安全责任和违约责任。

6.3.1.3 数据授权制度合规审查

从第三方获得数据授权使用时，应审查授权链条的完整性，核对授权使用的范围。如授权使用的数据涉及个人信息时，应核实数据提供方获得个人信息主体授权的范围。如超出原始的授权范围，必须在处理前获得个人信息主体的单独同意。

6.3.2 数据存储制度合规审查

6.3.2.1 数据存储原则

一般情况下，数据存储地点为中华人民共和国境内。存储个人信息的期限应符合最小化原则，即：

- a) 个人信息存储期限应为实现用户授权使用目的所必须的最短时间，法律法规另有规定或者用户另行授权同意的除外；
- b) 超出个人信息的存储期限后，应当对个人信息进行删除或者匿名化处理。

6.3.2.2 数据存储要求

按照数据分类分级的情况，对不同类型、不同级别的数据采取差异化的安全存储措施。对于敏感个人信息、重要数据、核心数据，应采取更高级别的安全保障措施。

关键信息基础设施运营者和处理100万人以上个人信息的数据处理者的数据应储存在中华人民共和国境内，确需存储至境外的，需办理数据出境手续。

6.3.3 数据加工制度合规审查

数据加工过程中，通常涉及数据清洗、脱敏、匿名化、去标识化处理。对所有数据加工操作，应保留详细的日志记录，以备审计和溯源。

6.3.3.1 匿名化处理

未经用户同意，不得向他人提供用户信息。但是，经过匿名化处理的除外。匿名化处理是指通过对个人信息的技术处理，使得个人信息主体无法被识别或者

关联，且处理后的信息不能被复原的过程。匿名化处理的应用场景有：超出个人信息存储期限、授权期限；个人信息主体注销账户后；停止运营其产品或服务。

6.3.3.2 去标识化处理

去标识化处理是指通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体的过程，去除标识符与个人信息主体之间关联性。

6.3.4 数据使用制度合规审查

6.3.4.1 数据使用原则

在使用个人信息时，不应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。因业务需要，确需超出上述范围使用个人信息的，应再次征得用户的明示同意。

6.3.4.2 数据使用限制

涉及通过界面展示个人信息的，需要对展示的个人信息的采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。

6.3.4.3 自动化决策

利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对用户进行交易价格等交易条件上实行不合理的差别待遇。

6.3.5 数据提供制度合规审查

6.3.5.1 对外提供数据的要求

将数据提供给第三方是数据流通的关键形式，对外提供个人信息时，应获得个人信息主体的单独同意。

6.3.5.2 对外提供数据的记录与监督

对外提供个人信息的，应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，以及数据接收方的基本情况等。应对数据接收

方采取持续监督措施,在得知或发现数据接收方未按照委托要求或违反法律法规要求或双方约定处理个人信息的,应立即要求数据接收方停止相关行为,且采取或要求数据接收方采取有效补救措施控制或消除个人信息面临的安全风险。

6.3.5.3 第三方产品或服务的管理义务

对于接入的具备收集个人信息功能的第三方产品或服务(例如小程序、SDK等)具有监督和管理义务。

6.3.5.4 数据传输要求

在传输数据(尤其是敏感个人信息、重要数据、核心数据)时,应采用加密等安全措施,采用密码技术时宜遵循密码管理相关国家标准。

6.3.6 数据出境制度合规审查

6.3.6.1 数据出境行为的界定

数据出境行为主要包括以下情形:

- a) 出于日常办公或企业管理需要向海外传输在境内运营中收集和产生的数据;
- b) 数据处理者收集和产生的数据存储在境内,境外的机构、组织或者个人可以查询、调取、下载、导出;
- c) 将存储境内数据的便携设备(如电脑、移动硬盘)携带至境外。

6.3.6.2 数据出境前的通用合规义务

在数据出境前,数据处理者应当开展如下合规审查工作:

- a) 识别重要数据:重要数据需通过安全评估后方可出境;
- b) 识别个人信息:如出境的数据包括个人信息,需进行个人信息保护影响评估,并履行告知义务,获得个人主体的单独同意;
- c) 识别数据出境特定主体:识别数据出境主体是否为关键信息基础设施运营者或为处理100万人以上个人信息的数据处理者。

6.3.6.3 数据出境路径

满足如下数据出境路径条件的,数据处理者根据实际情况选择具体的数据出境路径:

a) 安全评估,满足下列任一条件,将数据传输至中国境外的实体必须向相关主管部门申请数据出境安全评估:

1) 数据处理者向境外提供重要数据;

2) 关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息;

3) 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。

b) 标准合同备案,根据相关法律法规的要求,数据处理通过签订标准合同并向相关主管部门备案后,可向境外提供个人信息;

c) 保护认证:根据相关法律法规的要求,专业认证机构对个人信息处理者个人信息出境活动开展个人信息保护认证;数据处理者获得个人信息出境个人信息保护认证的,可以进行个人信息出境活动。

d) 自贸区负面清单制度:自由贸易试验区内数据处理者向境外提供负面清单外的数据,可以免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

6.3.6.4 数据出境后的合规管理

数据出境后,应建立持续合规与风险管理机制:

a) 对境外接收方的持续监督,包括对合同履行情况进行监督与审查评估,对境外接收方再转移数据进行管控;

b) 法律法规变化与合同更新机制,包括境内外法律政策变化的监测与应对,重新评估、续签合同与备案的触发监控;

c) 数据安全事件的应急响应与报告,包括制定跨境数据安全事件的应急预案,当发生数据安全事件时应向监管机构和个人主体的报告。

6.4 数据安全

6.4.1 数据安全治理系统

根据数据分类分级管理制度，对不同类型、不同级别的数据采取差异化的安全保障措施。

6.4.1.1 核心数据的安全要求

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，应该实行更加严格的管理制度。

6.4.1.2 重要数据的安全要求

企业应建立重要数据识别机制，形成并动态更新自身的重要数据目录，明确责任部门和负责人，并作为重要数据处理者定期开展风险评估，向有关主管部门报送风险评估报告。

6.4.1.3 数据治理组织与人员管理

应设立权责明确的数据安全管理机构，并任命数据安全负责人。处理个人信息达到国家网信部门规定数量的企业还必须指定个人信息保护负责人。

对数据处理关键岗位人员进行背景调查和能力考核；与所有接触数据的员工签订保密协议；建立人员转岗与离岗的数据权限管理流程；定期对全体员工进行数据安全意识和专项技能培训。

6.4.2 网络安全合规审查

6.4.2.1 网络安全等级保护

国家对企业应按照法律、法规、相关标准的要求开展网络安全定级备案、安全建设整改、等级测评和自查等工作，采取管理和技术措施，保障数据安全和信息安全，有效应对安全事件。

6.4.2.2 关键信息基础设施的特殊要求

国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，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、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

关键信息基础设施运营者必须履行特殊的安全保护义务，包括对重要系统和数据库进行容灾备份，以及在数据出境时履行更严格的法律程序。

6.4.2.3 技术安全措施与风险评估

通过访问控制、加密技术、脱敏技术等手段保障技术安全措施的有效性。建立常态化的数据安全风险评估机制，依法开展个人信息保护影响评估。

6.4.2.4 网络安全人员管理

企业应明确网络安全负责人和管理机构，建立工作责任制，落实责任追究制度。建立安全管理和技术保护制度。落实监测、记录网络运行状态、网络安全事件、违法犯罪活动的管理和技术措施，制定安全事件应急响应制度，评估企业是否具备数据安全突发事件的应急响应预案和演练机制。

7. 数据产品定价

7.1 数据产品的分类与特征

7.1.1 数据产品的分类

与原始数据相比，数据产品具有明确的使用场景、标准化的格式和可衡量的价值。根据产品形态可将数据产品划分为数据集产品（如脱敏后的区域流动人员手机信令数据集，具备结构化、标准化特征）、数据展现品（如数字地图、台风云图，通过可视化技术呈现数据价值）、数据分析产品（如市场趋势报告、行业发展指数，基于统计模型生成决策支持）、数据服务产品（如企业信用查询、身份验证服务，提供实时数据交互接口）。

从应用场景角度，数据产品可以分为商业数据产品、政务数据产品和科研数据产品三大类。商业数据产品主要服务于企业决策、市场营销、风险控制等商业场景；政务数据产品主要服务于政府治理、公共服务、政策制定等公共管理场景；

科研数据产品主要服务于学术研究、技术创新、知识发现等科研场景。从数据形态角度，数据产品可以分为结构化、非结构化和半结构化数据产品。从价值密度角度，可以分为高价值密度、中价值密度和低价值密度三类。高价值密度数据产品通常包含稀缺性信息或深度洞察，如专利数据、金融交易数据等。

7.1.2 数据产品的核心构成要素

数据产品的核心构成要素具体包括：

- a) 数据资源：原始数据经过合规采集与预处理后的集合；
- b) 算法模型：如机器学习模型、统计分析方法，赋予数据解释力；
- c) 应用载体：软件平台、API接口或可视化工具，实现用户交互；
- d) 质量指标：准确性、完整性、时效性等维度保障数据可信度。

7.1.3 数据产品的特征分析

7.1.3.1 基本特征

- a) 非竞争性：同一数据产品可被多用户同时使用且互不影响；
- b) 可复制性：边际成本趋零，复制与分发成本极低，但前期研发成本高；
- c) 价值不确定性：价值往往取决于应用场景和用户能力，从而促使定价需用灵活方法。

7.1.3.2 独特性特征

- a) 技术驱动性：依赖大数据、AI等技术实现价值挖掘；
- b) 时效性：需持续更新以适应业务需求，许多数据产品的价值会随时间推移而衰减；
- c) 合规敏感性：涉及隐私保护与数据安全。

7.1.3.3 价值创造特征

- a) 决策赋能：通过数据分析降低企业决策不确定性；
- b) 流程优化：自动化数据流提升效率；
- c) 生态构建：数据产品作为基础设施支撑新业态。

7.1.4 数据产品的价值属性

数据产品的价值属性包括使用价值、交换价值、直接价值、间接价值、当前价值和潜在价值。使用价值是基础，通常可以通过效率提升、成本节约、收入增长等指标衡量。交换价值反映市场认可，是供需关系、竞争状况、市场预期等因素综合作用的结果。直接价值易于量化，如通过数据分析获得的市场洞察。间接价值具有战略意义，如提升品牌形象、增强竞争优势。当前价值相对稳定，潜在价值具有不确定性，需要在定价中适当考虑。

7.2 数据产品价值形成机制

7.2.1 价值形成基础

从劳动价值论视角，数据产品价值来源于采集、处理、分析等劳动投入，但价值往往与劳动投入不成正比。从效用价值论视角，价值取决于为用户创造的效用，强调用户主观评价和需求满足程度。从稀缺性价值论视角，价值主要来源于稀缺性，稀缺性越高的数据产品价值越大。从网络效应价值论视角，价值随用户数量增加而提升，体现了数据产品的规模效应。

7.2.2 影响数据产品定价的因素

影响数据产品定价的因素包括内部因素和外部因素。

7.2.2.1 内部因素

a) 成本结构

- 1) 开发成本：数据采集、清洗、建模、维护；
- 2) 合规成本：确权、安全审计、跨境评估；
- 3) 维护成本：元数据更新、接口运维。

b) 质量维度

数据质量是决定数据价值的核心要素，其影响贯穿数据交易的全流程；从本质上看，数据通常具有规范性、完整性、准确性、一致性、时效性、可访问性等特征，这些属性直接决定了数据的基础价值；高质量数据能够降低决策风险、提升运营效率，而低质量数据可能导致错误判断，甚至造成经济损失。

c) 稀缺性

- 1) 数据产品的可替代性程度直接影响其定价能力；
- 2) 由企业自身业务活动产生的、外界无法获取的专有数据具有较高的价值；
- 3) 稀缺的数据可能来自于特定的领域、特定的时间段或特定的采集方法，可分为天然稀缺与人为稀缺两类；天然稀缺数据通常具有不可复制的特性，人为稀缺则源于技术壁垒或独家授权。

d) 数据规模

数据规模也是定价的重要考量因素。一般来说，大规模的数据集合能提供更全面的信息，有助于发现更深入的模式和趋势，从而具有更高的分析价值。在大数据时代，数据量的增加往往能提升数据的预测能力和决策支持效果。

e) 可复制性

数据的可复制性指同一数据在相同条件下，经过多次采集、处理或分析后，能够得到一致结果的特性。它体现了数据生成和处理过程的稳定性，确保数据在不同时间、不同操作环节中保持一致的表现，是验证数据可靠性的重要指标，也是影响数据价格的重要因素。但是，当数据规模增长到一定程度后，可能会出现边际效益递减的情况，即增加相同规模的数据所带来的价值提升幅度逐渐减小。

f) 时效性衰减

数据的时效性衰减是指数据的价值随着时间的推移而逐渐降低的现象。不同类型的数据受时间影响程度不同，部分数据会因环境变化、信息更新等因素，其对决策或分析的参考作用随时间延长而减弱，导致其在市场交易中的价格或应用价值出现下降。

g) 数据权属与合规性

数据权属与合规是数据定价中应考虑的因素。清晰的权属关系能够明确数据交易的主体和权益，减少交易纠纷。如果数据的权属存在争议，其交易

价值将受到严重影响。数据合规、数据安全和隐私保护，是数据产生价值的前提条件。

7.2.2.2 外部因素

a) 数据应用场景

不同的数据应用场景对数据的价值有不同的体现，从而影响定价。其定价会根据其能够为特定应用场景带来效益、解决的问题的重要性的紧迫性进行调整。数据价值的场景依赖性体现在三个维度：行业特性、业务环节、决策权重。

例如，在金融行业数据运用场景广泛，涵盖信贷业务、投资管理、反欺诈、客户服务与营销、风险管理，助力提升效率与安全性。

又如，在医疗领域，患者的基因数据若用于罕见病的研究和药物研发，其价值极高，因为可能对攻克疑难病症产生重大影响。而同样的基因数据若仅用于一般的健康科普或非关键的医学统计分析，其价值相对较低。

再如，在智能交通领域，实时的交通流量数据对于优化交通信号灯控制、缓解拥堵具有重要意义，其在该场景下的价值远高于用于历史交通模式研究的场景。

b) 数据供需关系

数据供需关系指数据市场中数据供给量与数据需求量之间的相互作用状态。数据供给量即市场中可用于交易和使用的数据总量，涵盖各类数据提供者所拥有的数据规模、类型及可交易数量等；数据需求量则是市场中各类主体对数据的需求总和，包括企业、机构、个人等为实现自身目标而需要的数据规模和类型。

当供给量大于需求量时，市场呈现供过于求的状态，数据可能面临降价压力；当需求量大于供给量时，市场处于供不应求的局面，数据价格往往会上升；而供需平衡时，数据价格相对稳定。数据供需关系是动态变化的，受数据生成速度、市场需求变化、技术发展等多种因素影响，直接反映了数据在市场上的稀缺程度和交易活跃度。

c) 市场成熟度

市场成熟度指数据交易市场在发展过程中所达到的完善程度和规范化水平。包括市场交易规则的健全性；市场参与主体的多样性与专业性；数据交易产品的丰富性与标准化程度；以及市场监管的有效性。

市场成熟度高的表现为交易有序、效率高、风险低；成熟度低则可能出现交易混乱、效率低下、风险频发等情况。

d) 技术成熟度

技术成熟度指支撑数据采集、存储、处理、分析、传输等环节的技术所达到的发展水平和完善程度。在数据采集环节，技术成熟度体现在采集工具的先进性、采集方法的科学性以及采集过程的稳定性，能否精准、高效地获取所需数据；存储技术的成熟度表现为存储容量的大小、存储速度的快慢、数据安全性和可靠性的高低；处理和分析技术的成熟度则反映在对海量、复杂数据的处理能力，能否快速完成数据清洗、转换、建模等操作，并从中提取有价值的信息；传输技术的成熟度关乎数据传输的速度、稳定性和安全性，能否实现数据的实时、准确传输。

技术成熟度高意味着数据相关操作的效率高、成本低、效果好，能更好地挖掘数据价值；成熟度低则可能限制数据的处理和应用，影响数据价值的实现。

7.3 数据产品定价方法模型

7.3.1 成本导向定价方法

数据采集成本法基于数据采集、处理、存储的直接成本确定价格，适用于基础数据产品。数据获取成本包括数据购买费用、API调用费用、爬虫开发费用等。数据处理成本包括数据清洗费用、数据转换费用、数据质量检查费用等。数据存储成本包括硬件成本、软件成本、维护成本等。

开发成本法考虑全部投入，计算公式为： $P = (C + M) \times (1 + R)$ ，其中C是直接成本，M是间接成本，R是利润率。直接成本包括数据采集、处理、存储等直

接相关的费用。间接成本包括管理成本、营销成本、财务成本等间接相关的费用。利润率根据行业标准、市场状况、竞争程度等因素确定。

7.3.2 市场导向定价方法

市场比较法通过参考同类数据产品价格确定定价,关键在选择比较对象和确定调整因素。质量差异调整根据准确性、完整性、一致性、时效性等维度进行评估。规模差异调整根据数据量、覆盖范围、更新频率等维度进行评估。时效差异调整考虑时间价值,实时数据产品价格调整系数较大。

竞争定价法基于市场竞争状况确定策略,包括渗透定价、撇脂定价、跟随定价等。渗透定价适用于新进入市场的数据产品,以较低价格快速占领市场。撇脂定价适用于具有独特优势的数据产品,以较高价格获取高利润。跟随定价适用于市场竞争相对稳定的数据产品。

7.3.3 价值导向定价方法

收益分成法基于数据产品使用产生的收益进行分成,收益贡献评估包括直接收益贡献和间接收益贡献。直接收益贡献是指数据产品直接带来的收入增长,如通过精准营销提升的销售额。间接收益贡献是指数据产品通过提升效率、降低成本等方式产生的收益。

价值评估法通过评估对用户业务的价值贡献确定价格,包括效率提升、成本节约、收入增长、风险降低等维度。效率提升价值通过时间节约、错误减少、决策质量提升等指标衡量。成本节约价值通过人力成本节约、运营成本节约、风险成本节约等指标衡量。收入增长价值通过新客户获取、老客户价值提升、产品优化等指标衡量。

7.3.4 博弈论与动态定价方法

博弈论与动态定价模型是近年来在数据定价领域逐渐兴起的方法,这些方法能够更好地适应数据市场的动态变化和复杂的交易环境。

7.3.4.1 基于Stackelberg博弈的定价方法

Stackelberg博弈是一种领导者-追随者模型,适用于数据交易市场中交易所作为价格领导者引导市场均衡的场景。

交易所作为价格引领者，根据市场情况和数据的供需关系，设定一个基础价格或价格区间。数据商作为追随者根据交易所设定的价格，结合自身的成本和收益预期，调整自己的报价。最后通过交易所和数据商的互动，形成一个市场均衡价格。

Stackelberg博弈适用于数据交易市场中存在一个或多个具有较强市场影响力的交易所的场景。例如，在一些大型数据交易所中，交易所可以通过设定价格区间来引导市场交易。Stackelberg博弈能够充分发挥交易所的市场引导作用，促进市场的稳定和高效运行。同时该模型依赖于交易所的市场影响力和信息透明度，如果交易所的决策不准确或信息不透明，可能导致市场失衡。

7.3.4.2 讨价还价模型

讨价还价模型是一种基于买卖双方协商定价的模型，适用于数据交易中双方直接协商价格的场景。

卖方根据数据的成本和预期收益，提出一个初始报价。买方根据数据的价值评估和预算，提出一个还价。双方通过多轮讨价还价，最终达成一个双方都能接受的价格。

讨价还价模型适用于数据交易中买卖双方直接沟通和协商的场景。例如，在一些场外交易中，买卖双方可以根据自身的实际情况进行灵活地协商。讨价还价模型能够充分考虑买卖双方的实际需求和利益，达成一个双方都满意的交易价格。同时该模型的效率较低，协商过程可能较长，且存在一定的不确定性。

7.3.5 新技术驱动的智能定价

随着大数据、人工智能和区块链等新技术的快速发展，智能定价方法逐渐成为数据定价领域的重要发展方向。这些方法能够利用新技术的优势，提高数据定价的效率和准确性。

7.3.5.1 基于联邦学习与多方安全计算的价格形成机制

联邦学习和多方安全计算是一种在保护数据隐私的前提下，实现多主体数据共享和收益分配的方法。

多个数据所有者通过联邦学习和多方安全计算技术，共享数据的特征和模型，而不直接共享数据本身。根据各方的贡献和数据价值，通过智能合约等方式进行收益分配。

联邦学习和多方安全计算适用于多个数据所有者需要共享数据，但又担心数据隐私泄露的场景。例如，在医疗数据共享和金融风险评估等领域，这些技术可以有效保护数据隐私，同时实现数据的价值最大化。联邦学习和多方安全计算能够在保护数据隐私的前提下，实现数据的共享和价值最大化。同时这些技术的实现需要较高的技术门槛和计算资源，且在实际应用中可能存在一定的复杂性。

7.3.5.2 机器学习动态定价

机器学习动态定价是一种基于机器学习算法，根据市场供需变化实时调整数据价格的方法。机器学习技术被广泛引入各个研究领域：在版权金融化价值评估中优化定价模型，在股票市场中预测价格走势与波动率，为二手房和专利的价值评估提供精准参考等。相较于传统分析方法，机器学习在预测准确性上展现出明显优势。

这种定价方法需要收集市场上的数据交易记录、供需关系、用户行为等数据。然后利用机器学习算法，如强化学习、深度学习等，训练一个动态定价模型。根据实时市场数据，动态调整数据价格，以实现最优的交易效果。

机器学习动态定价适用于数据交易市场较为活跃，且市场供需关系变化较快的场景。例如，在实时数据交易市场中，机器学习动态定价可以实时调整价格，提高交易效率。机器学习动态定价能够实时反映市场供需变化，提高交易效率和收益。同时该方法需要大量的数据和复杂的算法支持，且模型的训练和优化需要较高的技术能力和计算资源。

7.4 数据产品定价流程

7.4.1 定价前准备阶段

数据产品分析包括产品特征识别、价值属性评估、目标用户分析、竞争环境调研。产品特征识别对数据产品的基本特征进行全面分析，包括数据类型、数据规模、数据质量、应用场景等。价值属性评估对数据产品的价值属性进行深入分

析，包括使用价值、交换价值、直接价值、间接价值、当前价值、潜在价值等。目标用户分析对目标用户群体进行详细分析，包括用户特征、需求特点、购买能力、使用习惯等。竞争环境调研对市场竞争状况进行全面调研，包括竞争对手分析、市场格局分析、竞争策略分析等。

定价策略制定包括定价目标确定、定价方法选择、定价模型构建、定价参数设定。定价目标包括利润最大化、市场份额最大化、品牌价值提升等。定价方法选择根据数据产品特征和市场环境选择合适的定价方法。定价模型构建根据选择的定价方法构建具体的定价模型。定价参数设定确定定价模型中的具体参数值。

7.4.2 定价实施阶段

基础价格计算包括成本核算、价值评估、市场调研、价格测算。成本核算对数据产品的各项成本进行详细核算，包括直接成本和间接成本。价值评估对数据产品的价值进行科学评估，包括使用价值评估、市场价值评估、战略价值评估等。市场调研对数据产品市场进行全面调研，包括市场需求调研、竞争状况调研、用户反馈调研等。价格测算根据定价模型和参数进行具体的价格计算。

价格调整优化包括影响因素分析、价格敏感性测试、竞争策略考虑、最终价格确定。影响因素分析对影响价格的各种因素进行深入分析，包括内部因素和外部因素。价格敏感性测试分析价格变化对需求的影响程度，包括价格弹性分析、需求曲线分析、收益最大化分析等。竞争策略考虑分析竞争对手的价格策略和反应，制定相应的竞争策略。最终价格确定在综合考虑各种因素的基础上确定最终的价格方案。

7.4.3 定价后管理阶段

价格监控包括市场反应跟踪、销售数据分析、用户反馈收集、竞争价格监测。市场反应跟踪对市场对价格变化的反应进行持续跟踪，包括销售数据变化、用户反馈变化、竞争反应变化等。销售数据分析对销售数据进行深入分析，包括销售趋势分析、销售结构分析、销售效果分析等。用户反馈收集系统性地收集和分析用户对价格的反馈意见，包括用户满意度调查、用户需求调研、用户建议收集等。竞争价格监测对竞争对手的价格变化进行持续监测，包括价格水平监测、价格策

略监测、价格趋势监测等。

价格调整包括定期价格评估、动态价格调整、价格策略优化、长期价格规划。定期价格评估是定期对价格策略进行评估，包括价格合理性评估、价格竞争力评估、价格效果评估等。动态价格调整根据市场变化动态调整价格，包括需求变化调整、竞争变化调整、成本变化调整等。价格策略优化根据市场反馈和业务发展的需要优化价格策略，包括定价方法优化、定价模型优化、定价参数优化等。长期价格规划制定长期的价格发展规划，包括价格战略规划、价格体系规划、价格管理规划等。

7.5 公共数据的定价模型

7.5.1 基于边际成本与社会效益的定价模型

公共数据通常由政府或公共机构采集和维护，其目的不仅在于回收成本，更重要的是促进社会整体效益的提升。在这个模型中，首先计算公共数据的边际成本 MC，即每增加一个单位的数据使用所增加的成本，包括数据存储容量扩展的成本、数据访问权限管理的边际成本等。

假设增加一定量的数据存储容量需要投入成本 C_{extra} ，而由此可增加的数据使用量为 Q_{extra} ，则边际成本 $MC = C_{extra}/Q_{extra}$ 。

然后，评估公共数据使用所带来的社会效益 BS。社会效益可以从多个方面衡量，如促进产业发展带来的就业增长、经济增长，提升公共服务效率带来的社会福利提升等。通过建立社会效益评估指标体系，运用定性和定量相结合的方法确定社会效益的量化值。

最后，设定一个社会效益分配系数 β ($0 < \beta < 1$)；

公共数据价格 P 的计算公式为 $P = MC + \beta BS$ 。

这种定价模型在考虑成本的基础上，充分体现了公共数据对社会的价值贡献，有助于实现公共数据的合理利用和社会效益的最大化。

7.5.2 基于应用场景分类的差别定价模型

公共数据在不同的应用场景下具有不同的价值和影响。此模型将公共数据的应用场景分为多个类别，包括民生服务类、产业促进类、科研创新类等。

对于每一类应用场景，分别评估其对公共数据的需求程度、数据使用的频率和强度以及数据使用后可能产生的效益。根据这些评估结果确定每类应用场景下公共数据的价格。

对于民生服务类应用场景，由于其涉及广大民众的基本权益，需求广泛且具有一定的公益性，数据价格相对较低。假设设定为基础价格 P_0 。

而对于产业促进类应用场景，企业使用公共数据可能带来较大的经济效益，根据对企业潜在收益的预估和市场情况，价格可以设定为 $P_0 \times (1+k_1)$ ，其中 k_1 为根据产业类型和预期效益确定的价格调整系数。

对于高附加值产业， k_1 可能取值为 0.5，即价格为基础价格的 1.5 倍。

对于科研创新类应用场景，考虑到科研项目的长期价值和不确定性，价格可以根据科研项目的资助情况、预期成果的潜在影响力等因素确定，如采用协商定价的方式在基础价格上进行适当调整。通过这种基于应用场景分类的差别定价模型，能够使公共数据的定价更加贴合不同场景的实际需求和价值，提高公共数据的配置效率。

7.5.3 基于增值服务定价模型

增值服务定价模型是公共数据定价中聚焦数据衍生价值的模式，核心逻辑是将原始公共数据与增值服务分离定价。原始公共数据通常免费或极低价格开放，保障公共属性和基础可用性；基于原始数据的深度加工、分析、定制化开发等增值服务，则依据服务成本与价值单独定价，通过增值服务收益维持数据生态可持续运转。

定价构成要素包括服务成本与服务价值。在服务总成本（人力+技术+时间）的基础上，叠加一定比例的利润率（通常根据行业平均水平设定），服务价值是定价上限的核心，价值越高，定价空间越大。

该模型优势显著，能兼顾公益性与市场性，保障原始数据普惠性，同时让增值服务体现市场价值；促进数据深度应用，降低企业使用门槛，推动公共数据从“可用”向“好用”升级；形成“数据开放-服务增值-收益反哺”的良性循环，缓解公共部门资金压力。但其存在定价透明度风险，垄断性风险，边界模糊风险。

8. 数据资产价值评估

8.1 数据资产的属性

8.1.1 数据资产的形态与价值密度

与数据产品不同，数据资产更强调其作为企业资产的价值属性和管理属性，是数据要素价值实现的重要载体。数据资产经采集、挖掘、清洗、标注、分析等处理而形成，一般应用于特定的使用场景。

从资产形态角度，数据资产可以分为结构化、非结构化和半结构化数据资产。从业务价值角度，可以分为核心数据资产、支持数据资产和辅助数据资产。核心数据资产是支撑企业核心业务的关键数据，如客户数据、交易数据、产品数据等。支持数据资产是支持企业运营管理的数据，如财务数据、人力资源数据、供应链数据等。辅助数据资产是辅助企业决策和创新的数据，如市场数据、竞争数据、趋势数据等。

从价值密度角度，数据资产可以分为高价值密度、中价值密度和低价值密度资产。高价值密度资产通常包含稀缺性信息或深度洞察，如专利数据、商业秘密、客户洞察等。

8.1.2 数据资产的特征分析

数据资产具有无形性、可复制性、价值不确定性、时效性和网络效应等特征。无形性使价值评估复杂化，需要采用专门的方法和技术。可复制性带来价值维护和知识产权保护的挑战，需要在价值评估中充分考虑。价值不确定性使价值评估需要采用更加灵活和动态的方法。时效性影响价值衰减，需要在价值评估中体现时间价值。网络效应使数据资产具有规模经济特征，价值会随着使用规模的扩大而提升。

8.1.3 数据资产的价值属性

应用场景和使用者的不同，数据资产价值也有所不同，其价值具有不确定性，而且反复使用不会导致其内在价值降低。数据资产的价值属性包括使用价值、交换价值、账面价值、市场价值和战略价值。使用价值是基础，通常可以通过效率

提升、成本节约、收入增长等指标衡量。交换价值反映市场认可，是供需关系、竞争状况、市场预期等因素综合作用的结果。账面价值相对稳定，基于历史成本或公允价值确定。市场价值具有动态性，会随着市场环境的变化而变化。战略价值包括竞争优势、战略布局、长期发展等方面，在企业战略决策中具有重要参考意义。

8.2 数据资产价值形成机制

8.2.1 价值形成理论基础

从资产价值论视角，数据资产的价值来源于其作为企业资产的经济价值，主要由其能够为企业创造的经济利益决定。从资源基础论视角，数据资产的价值来源于其作为企业核心资源的战略价值，强调数据资产的稀缺性、不可替代性和价值性。从能力理论视角，数据资产的价值来源于其支撑企业核心能力的作用，不仅体现在数据本身，还体现在企业利用数据的能力上。从动态能力论视角，数据资产的价值来源于其支撑企业动态能力的作用，在帮助企业适应环境变化、实现持续发展方面具有重要价值。

8.2.2 价值影响因素分析

数据质量因素包括规范性、完整性、准确性、一致性、时效性、可访问性。准确性越高的数据资产价值越大，完整性越高的数据资产越能满足企业需求，一致性越高的数据资产越便于使用，时效性越强的数据资产价值越高。

数据规模因素包括数据量、覆盖范围、更新频率。数据量越大，能够支持的分析越深入，价值越高。覆盖范围越广，能够服务的业务范围越大，价值越大。更新频率越高，数据的时效性越强，价值越高。

应用能力因素包括技术能力、分析能力、创新能力。技术能力越强，能够从数据资产中提取的价值越多。分析能力越强，能够提供的洞察越深入。创新能力越强，数据资产的战略价值越高。

市场环境因素包括市场需求、竞争状况、政策环境。市场需求越旺盛，数据资产的价值越大。竞争状况越激烈，数据资产的差异化价值越重要。政策环境越有利，数据资产的发展空间越大。

8.2.3 价值评估维度

经济价值维度包括直接经济收益、成本节约、效率提升。直接经济收益是指通过使用数据资产直接获得的收入增长。成本节约是指通过使用数据资产减少的运营成本。效率提升是指通过使用数据资产提高的工作效率。

战略价值维度包括竞争优势、战略布局、长期发展。竞争优势是指数据资产在市场竞争中的独特价值。战略布局是指数据资产在长期发展战略中的地位和作用。长期发展是指数据资产对未来发展的支撑价值。

风险价值维度包括风险识别、风险控制、风险转移。风险识别是指数据资产在风险识别方面的价值。风险控制是指数据资产在风险控制方面的价值。风险转移是指数据资产在风险转移方面的价值。

8.3 数据资产价值评估方法模型

8.3.1 成本法评估

成本法是一种以数据资产形成过程中所投入的各项成本费用为基础,来衡量和评估其价值的方法。在采用成本法进行评估时,应满足以下前提条件:

- (1) 评估对象处于可正常使用或正在使用的状态;
- (2) 评估对象可以通过重新建设或重置的方式获得;
- (3) 能够合理估算评估对象的重置成本及相关折旧、贬值;
- (4) 数据质量达到特定应用场景下的可接受标准。

数据资产的价值评估主要依据其重置成本,即在评估时点重新获取该资产所需的全部成本,同时需综合考虑税费、利润等相关因素。成本构成要素为重置成本的计算提供了全面的视角,其基本计算公式如下:

$$P = \sum_{i=1}^n (C_{i1} + C_{i2} + C_{i3} + C_{i4} + t_i + p_i)$$

其中, P——待评估数据资产的价值;

C_{i1} ——每个数据集重置规划成本;

C_{i2} ——每个数据集重置建设成本；

C_{i3} ——每个数据集重置维护成本；

C_{i4} ——每个数据集其他重置成本；

n ——数据集的个数。

t_i ——每个数据集流通的税费；

p_i ——每个数据集流通的利润。

8.3.2 收益法评估

收益法是一种通过预测评估对象的未来收益、确定适当的折现率，并将这些预期收益折现到现值来评估价值的方法。该方法基于数据资产未来能够带来经济收益、具备内在价值的假设。采用收益法需注意的前提条件：

- (1) 评估对象未来能够产生可预期且可用货币计量的收益；
- (2) 与预期收益相关的风险（即折现率）可以被合理衡量；
- (3) 评估对象的预期寿命可以确定或合理估算。

因此，收益法的应用需同时具备预期收益、折现率和预期寿命这三个核心参数。

确定预期收益时应重点关注：

- (1) 明确预期收益类型（如收入、利润、现金流等），无法用经济收益衡量的数据资产可参考社会价值；
- (2) 分析用于收益预测的财务及相关信息、假设和评估目的的适用性；
- (3) 预期获利年限应结合自然和合规收益期，综合考虑寿命、法规、合同等因素；
- (4) 折现率需反映时间价值和相关风险，并与收益类型匹配，可参考风险报酬率和无风险报酬率；
- (5) 预期经济收益为数据资产带来的额外收益，现金流可用增量收益、分成或超额收益法确定，需剔除无关收益，并关注行业市场情况。

公式如下：

$$P = \sum_{i=1}^m \left(\sum_{t=1}^{n_i} \frac{R_{it}}{(1+r_i)^t} \right)$$

其中，P——待评估数据资产的价值；

R_{it} ——第 i 种应用第 t 年的预期收益；

n_i ——第 i 种应用的预期寿命，指待评估数据资产还能产生价值的剩余时间，取自然收益期和合规收益期的最小值；

r_i ——折现率，将预计未来收益折算成现值的比率，体现数据资产的财务成本。

8.3.3 市场法评估

市场法是一种基于公开且活跃的交易市场，通过参考近期或历史上类似资产的成交价格，并对具有特殊性或个性化的因素进行调整，从而确定估值的方法。

采用市场法时需满足以下前提条件：

(1) 评估对象存在可比的参照物，并且这些参照物在公开市场中有活跃的交易；

(2) 能够获取相关交易的关键信息，如成交价格、交易时间、交易条件等。

市场法一般包括两个主要环节：筛选和调整。

在筛选阶段，需要在市场中寻找与待评估数据资产具有相同或相似特征的参考对象或可比交易案例。评估要素为筛选提供了对比的基础和标准。评估人员应结合评估对象的具体特性，选取与其相同或具备可比性的维度，如交易市场、数量、价值影响因素、交易时间（尽量接近评估基准日）、交易类型（与评估目的相符）等，并选择正常或可通过修正达到正常状态的交易价格作为参照。

调整阶段则是通过对比评估对象与参考数据资产或可比交易案例之间的差异，合理设定调整系数，对价值影响因素和交易条件的不同进行修正，从而获得

更为准确的评估结果。数据市场越成熟、可参考对象越多、交易类型越丰富，越有助于实现对数据资产的精准估值。

公式如下：

$$P = \sum_{i=1}^n (\hat{P}_i \times f(X_{i1}) \times g(X_{i2}) \times X_{i3} \times X_{i4}) / n$$

其中，P——待评估数据资产的价值；

$\hat{P}_i$ ——每个参照数据集的价格；

n——数据集的个数；

$f(X_{i1})$ ——每个数据集的质量调整系数的经验函数，包括行业经验、应用场景经验等；

$g(X_{i2})$ ——每个数据集的供求调整系数的经验函数，包括行业经验、应用场景经验等；

X_{i3} ——每个数据集的时点调整系数；

X_{i4} ——每个数据集的数量调整系数。

8.3.4 综合评估法

综合评估法是指将成本法、市场法和收益法三种评估方法所得的数据资产价值，按照一定权重进行加权计算，从而得出数据资产最终价值的评估方法。

在确定成本法、市场法和收益法的权重系数时，应充分结合市场环境、行业特性、数据资产属性等多方面因素，科学合理地分配各方法的权重，以确保评估结果的客观性和准确性。

公式如下：

$$P = \alpha_1 P_1 + \alpha_2 P_2 + \alpha_3 P_3$$

其中，P——待评估数据资产的价值；

P_1 ——用成本法计量的数据资产价值；

P_2 ——用市场法计量的数据资产价值；

P_3 ——用收益法计量的数据资产价值；

α_1 ——用成本法计量数据资产价值的权重系数；

α_2 ——用市场法计量数据资产价值的权重系数；

α_3 ——用收益法计量数据资产价值的权重系数。

8.4 数据资产价值评估流程

8.4.1 评估准备阶段

数据资产分析包括资产特征识别、价值属性评估、业务应用分析、技术支撑分析。资产特征识别对数据资产的基本特征进行全面分析，包括数据类型、数据规模、数据质量、应用场景等。价值属性评估对数据资产的价值属性进行深入分析，包括使用价值、交换价值、账面价值、市场价值、战略价值等。业务应用分析对数据资产的业务应用情况进行详细分析，包括应用范围、应用深度、应用效果等。技术支撑分析对数据资产的技术支撑情况进行全面分析，包括技术架构、技术能力、技术发展等。

评估策略制定包括评估目标确定、评估方法选择、评估模型构建、评估参数设定。评估目标包括投资决策、资产交易、财务报告、战略规划等。评估方法选择根据数据资产特征和评估目标选择合适的评估方法。评估模型构建根据选择的评估方法构建具体的评估模型。评估参数设定确定评估模型中的具体参数值。

8.4.2 评估实施阶段

基础价值计算包括成本核算、收益评估、市场调研、价值测算。成本核算对数据资产的各项成本进行详细核算，包括历史成本和重置成本。收益评估对数据资产能够创造的收益进行科学评估，包括直接收益评估和间接收益评估。市场调研对数据资产市场进行全面调研，包括市场需求调研、竞争状况调研、交易案例调研等。价值测算根据评估模型和参数进行具体的价值计算。

价值调整优化包括影响因素分析、敏感性分析、市场验证、最终价值确定。影响因素分析对影响价值评估的各种因素进行深入分析,包括内部因素和外部因素。敏感性分析关键参数变化对评估结果的影响程度,包括参数敏感性分析、情景敏感性分析、风险敏感性分析等。市场验证通过市场调研和专家咨询验证评估结果的合理性,包括市场比较验证、专家咨询验证、历史数据验证等。最终价值确定在综合考虑各种因素的基础上确定最终的评估价值。

8.4.3 评估后续管理

价值监控包括市场变化跟踪、业务应用跟踪、价值表现跟踪、技术发展跟踪。市场变化跟踪对市场环境变化进行持续跟踪,包括市场需求变化、竞争状况变化、技术发展变化等。业务应用跟踪对数据资产的业务应用情况进行持续跟踪,包括应用范围变化、应用深度变化、应用效果变化等。价值表现跟踪对数据资产的价值表现进行持续跟踪,包括账面价值变化、市场价值变化、战略价值变化等。技术发展跟踪对数据资产的技术发展情况进行持续跟踪,包括技术架构变化、技术能力变化、技术投资变化等。

价值调整包括定期价值评估、动态价值调整、评估方法优化、长期价值规划。定期价值评估定期对数据资产价值进行评估,包括年度评估、季度评估、专项评估等。动态价值调整根据市场变化和业务发展动态调整数据资产价值,包括市场变化调整、业务变化调整、技术变化调整等。评估方法优化根据实际应用情况优化评估方法,包括方法选择优化、模型构建优化、参数设定优化等。长期价值规划制定长期的价值发展规划,包括价值战略规划、价值体系规划、价值管理规划等。

9. 数据资产入表

9.1 入表原则与要求

9.1.1 入表原则

数据资产入表应当遵循客观性、可靠性、重要性和合法合规原则，且符合会计准则的基本要求。

9.1.1.1 客观性

数据资产的计量和入表应基于可验证的客观事实，避免主观臆断和不合理的估计。

9.1.1.2 可靠性

数据资产的信息应真实、准确、完整，能够为使用者提供可靠的决策依据。

9.1.1.3 重要性

数据资产的重要性需结合资产价值、业务影响等因素综合评估。对于重要的数据资产，应进行详细的计量和披露，对于不重要的资产，可以适当的简化处理。

9.1.1.4 合法合规性

应遵守相关法律法规和企业会计准则等相关法律法规规定，保证数据合法性、合规性和安全性。

9.1.2 入表要求

对于数据资产的确认及入表，应该符合《企业数据资源相关会计处理暂行规定》《企业会计准则第6号——无形资产》《企业会计准则第6号——存货》的要求。

9.2 入表流程与核算方法

9.2.1 数据资产入表流程

数据资产合规入表，应该包含以下工作：对数据资源进行治理、数据资产的识别与分类、数据资产合规确权、数据资产质量评价、数据资产价值评估、数据资产成本归集、数据资产入表。

9.2.1.1 数据资源治理

企业应通过建立数据质量管理、数据资产目录、数据管理组织、数据安全管理体系多维度完成数据资源治理工作。

9.2.1.2 数据资产识别

企业应该从“特定主体合法拥有或控制”“能进行货币计量”“能带来直接或间接经济利益”三个方面来识别数据资产。

9.2.1.3 数据资产合规与确权

a) 数据资产合规审查

企业应该从数据来源合法性、数据内容准确性与完整性、数据存储安全性、数据使用合规性、隐私保护、跨境数据传输合规性等维度进行合规性审查。

b) 数据资产确权

数据资产确权登记，应该从登记目的、登记对象、登记申请过程、审核及颁发凭证过程进行审查。

9.2.1.4 数据资产质量评价

数据资产质量评价的维度包括规范性、完整性、准确性、一致性、时效性和可访问性六个方面。

9.2.1.5 数据资产价值评估

数据资产价值评估由评估机构按照数据资产的成本、预期收益等，选择合适的评估模型进行评估。

9.2.1.6 数据资产成本归集

数据资产成本归集的处理方式分为确认为无形资产的会计处理、确认为存货的会计处理和未确认为资产的数据资源的会计处理三种形式。

9.2.1.7 数据资产入表

数据资产入表的过程包括设计会计科目、确定初始计量金额、编制会计凭证、登记会计账簿、确定摊销方式、数据资产披露。

9.2.2 核算原则、内容及科目

9.2.2.1 核算原则

数据入表核算应当遵循真实性原则、分期核算原则、成本效益原则；

- a) 真实性原则，数据资产核算应与客观经济事项相一致，以实际发生的金额计价，不得人为降低或提高成本。
- b) 分期核算原则，各期分别计算数据资产初始核算的成本，并遵循一贯性进行后续计量，后续计量按月进行。
- c) 成本效益原则，数据资产核算应为公司决策提供有用信息。

9.2.2.2 核算内容

数据入表核算应当包括数据资产构成及其初始计量、后续计量、处置和报废。

9.2.2.3 核算范围

数据资产核算应就核算区间和核算成本构成分别定义。核算区间应包括数据加工的完整链路、并包括该区间确保资产达到预计可使用状态的全部直接支出，但不包括可直接形成其他资产的相关支出。核算区间中满足条件的相关支出可作为数据资产的初始计量成本。

9.2.2.4 核算科目

核算应在“无形资产”或“存货”下，设立“数据资源”二级科目，根据使用需要下设“基础数据”“加工数据”“应用数据”三级科目。“基础数据”可下设明细科目，如：“XX数据”等科目，“应用数据”下可按需自行下设。

9.2.3 核算方法与要求

在成本核算中，应满足如下要求：

- a) 保证核算成本的真实与可靠，依据真实的交易记录，不能随意估计或虚构成本；

- b) 遵循一贯性原则，成本的核算方式和分摊方式，企业一旦确定，就应该在一定时期内保持一贯性，不得随意变更；
- c) 合理分摊共担成本，对于一些共同成本（如存储成本、运营成本等），需要采用合理的比例进行分摊，不能因为追求入表金额而故意增加分摊比例。

9.3 数据资产计量

9.3.1 数据资产的构成

数据资产初始核算应至少包含数据采购成本、人工成本、运维成本、安全管理成本和其他分摊费用。

9.3.2 初始计量

初始计量确认的期间，当月入账当月摊销，应按一定期限进行摊销。摊销时应注意：

- a) 采购成本应根据签署的数据采购合同的不含税合同金额作为数据采购成本的入账金额；
- b) 应按员工岗位职责说明进行分摊的人工成本金额作为人工成本的入账金额；
- c) 应按服务器使用对象区分后的存储成本作为运维成本的入账金额；
- d) 安全管理成本应包括与安全相关的软件及硬件的相关支出与安全认证费等；
- e) 房租、水电等间接成本可分摊部分可纳入数据资产入表范围。

9.3.3 后续计量

- a) 按照能够为公司带来经济利益的周期，判断数据资产在预计场景下的收益期；
- b) 摊销计算采用年限平均法，按年限摊销；摊销金额，是数据资产的成本扣除残值后的金额；

- c) 数据资源是使用寿命有限的无形资产，期末若出现减值，应进行减值测试，应在资产负债表日将当期数据资产的账面价值和可变现净值的大小进行对比。

10. 数据交易与流通

10.1 交易机制设计

10.1.1 数据要素场内交易机制

数据要素场内交易，是数据销售方基于数据交易场所的数据交易平台上架数据产品，采购方在数据交易平台发起订单、并与销售方开展交易、交付和资金结算的行为，具有全流程线上化、标准化的特征，同时数据交易场所对交易标的在登记、上架、交易、交付、资金结算等各个环节进行全程指导、审核和监督，确保其符合相关法律法规及数据交易场所的业务规则和管理办法。

10.1.1.1 登记上架

数据销售方进行身份注册，登记数据产品相关基础信息和价格信息，提交数据来源、合规等有关材料，数据交易场所对注册、登记信息进行审核。

10.1.1.2 上架审核

数据交易场所对数据产品上架申请进行审核，审核通过后在数据交易平台正式上架展示。

10.1.1.3 订购和签约

数据购买方可在平台直接下单，并选择与数据销售方签约，购买方和销售方先后上传签字盖章后的合同，然后订单流转到数据交易场所或平台运营主体进行审核。

10.1.1.4 支付、交付和资金结算

订单审核通过后数据购买方进行在线网银支付，支付完成后，购买方可直接下载数据集、数据报告，或获得数据API和数据应用的使用方式，订单完成、在线自动资金结算。

10.1.1.5 交易后管理

数据购买方可对数据销售方数据产品进行用后评价，在产生交易纠纷时也可申请数据交易场所进行调解仲裁。

10.1.2 数据要素场外交易机制

数据要素场外交易，是指销售方与采购方进行点对点交易和交付的行为，具有局域化、定制化的特征，交易前和交易中无需登记和审查、交易后向数据交易场所存档备查，能够在降低审查成本、提升交易效率的同时，鼓励各类市场主体的主动改革创新。

数据要素场外交易并不等于无序、无监管交易，需要进行合理引导。场外交易应逐步落实备案制度。

10.1.3 数据要素的跨境交易机制

建立安全可控的数据要素跨境交易机制需满足以下核心要求：

10.1.3.1 合规框架构建

- a) 监管沙盒机制：在自贸区等试点区域设立跨境数据流通沙盒，允许经审批的主体在封闭环境测试交易模型，输出风险评估报告作为正式监管规则依据。
- b) 双轨制流通过程：年出境数据量超特定数量用户的个人信息或重要数据时，强制申报数据出境安全评估；小规模非敏感数据采用网信部门备案的标准合同模板（含数据接收方义务、再转移限制等条款）。

10.1.3.2 技术保障措施

- a) 可信传输通道：部署国际加密专线，实施端到端加密及量子密钥分发技术。
- b) 实时审计追踪：区块链存证跨境传输全链路日志（数据包哈希值、接收方数字身份、传输时间戳），支持监管机构穿透式查询。

10.1.3.3 动态风险管控

- a) 地缘政治预警：实时监测数据接收国政策变动，触发交易熔断或数据回迁机制。
- b) 敏感数据拦截：基于AI的内容识别引擎自动拦截含国家核心数据字段的出境请求。

10.2 交易主体与客体管理

10.2.1 交易主体的资质审查

数据交易流通中的交易主体主要包括数据提供方、数据需求方、数据交易平台运营方和第三方服务商等。

数据交易场所一般实施会员制。申请数据交易场所会员资格，一般应当符合相关条件，并根据申请的会员类型，向数据交易场所提交相关资料，包括营业执照、法人身份证复印件、国家信息中心“信用中国”出具的信用报告等。

10.2.2 交易客体的合规标签

数据交易客体的合规标签核心主要包括六个方面，分别是数据类型、数据分类分级、合法来源证明、处理状态、数据权属以及数据质量。具体标签内容如下表8所示：

表8 标签内容

类型	合规标签
数据类型标签	个人信息
	敏感个人信息
	非个人信息
	企业数据
	公共数据

类型	合规标签
数据分类分级标签	核心数据
	重要数据
	一般数据
合法来源证明	个人信息授权书
	数据使用许可协议
处理状态标签	匿名化数据
	去标识化数据
数据权属标签	数据持有权
	数据使用权
	数据经营权
数据质量标签	规范性
	完整性
	准确性
	一致性
	时效性
	可访问性

10.2.3 交易客体合规验证机制

为验证交易客体的合规性，数据交易场所一般通过自证承诺+第三方专业评估+平台合规审核三重防线，确保数据在安全合规的基础上实现高效流通与创新应用。

10.2.3.1 自证承诺

交易主体对自身数据来源、安全性、合规性等进行承诺，确保不存在违反法律法规或规章制度的情况。

10.2.3.2 第三方评估

专业律师事务所等合规机构对企业数据进行调查，出具法律意见书。

10.2.3.3 平台合规审核

数据交易场所对提供信息和资料进行核查，确保形式合规，并在必要条件下开展现场核查。

10.2.4 交易客体的全生命周期可追溯

数据交易所建设或联合建设数据流通存证平台，利用区块链不可伪造、不可篡改、去中心化和可追溯等特性建设数据流通存证平台，将数据要素交易客体以及与客体相关的核心业务流程上链存证。数据交易过程中，客体的全生命周期可划分为6个核心阶段，每个阶段需针对性记录关键追溯信息：

10.2.4.1 数据产生与采集阶段

需明确数据“从哪来”，确保源头合规。核心追溯信息包括：

- a) 数据来源主体：个人、企业或者公共数据；
- b) 采集合规性：采集是否获得合法授权，例如个人信息需明确告知并获得同意、是否符合数据采集的法定范围；
- c) 数据原始特征：记录数据初始状态、数据类型、敏感等级，如原始格式、字段含义等。

10.2.4.2 数据处理与加工阶段

数据在交易前可能经过清洗、脱敏、聚合、标注等加工，需追溯如何被处理，避免未经授权的加工导致数据合规性受损。核心追溯信息包括：

- a) 处理主体：加工机构或人员的身份、资质；
- b) 处理行为：加工方法、处理目的、处理前后的数据映射关系等；
- c) 合规性证明：加工过程是否符合数据安全要求。

10.2.4.3 交易前准备阶段

交易前需明确数据客体的当前状态，为后续交易流转追溯提供基准，避免数据被替换。核心追溯信息包括：

- a) 数据客体标识：为待交易数据生成唯一交易编码，明确数据范围；
- b) 合规性标签：标注数据是否可交易，是否属于禁止交易的敏感数据、交易限制是否仅限特定场景使用、禁止二次流转等；
- c) 权属与授权：明确数据权属人、交易方是否具备交易权限。

10.2.4.4 交易流转阶段

交易过程是追溯的核心环节，需明确“谁交易了什么数据、如何交易、交易条件是什么”，确保流转路径透明。核心追溯信息包括：

- a) 交易主体：买卖双方身份信息、经办人信息；
- b) 交易标的：关联交易前的唯一编码，明确交易数据的具体版本，避免后续被篡改后追溯失效；
- c) 交易约定：交易时间、价格、用途范围、适用场景、授权期限、是否允许二次交易等；
- d) 交付方式：数据交付渠道、接收确认记录等。

10.2.4.5 交易后使用阶段

需追溯“数据被如何使用、是否符合约定”。核心追溯信息包括：

- a) 使用行为记录：数据接收方的使用场景、使用时间、使用人员等信息；
- b) 流转范围：是否发生二次流转，如转售给第三方，需记录二次流转的接收方、授权依据、是否需要获得原权属人同意等；
- c) 合规性验证：是否存在超约定用途使用。

10.2.4.6 销毁、归档阶段

数据使用完毕后，需记录最终去向，避免数据被不当留存或泄露，确保生命周期有始有终。核心追溯信息包括：

- a) 销毁或删除记录：若约定“使用后销毁或删除”，需记录销毁方式或删除方式、时间、执行人、销毁验证结果等；
- b) 归档记录：如合规要求若需长期留存，记录归档存储位置、访问权限、保管责任人等；
- c) 终止标志：对生命周期结束的数据，标注终止状态，关联全生命周期记录，停止交易和使用授权。

10.3 交易监管与安全保障

10.3.1 数据交易的全链路可审计追踪

为确保数据交易安全，数据交易场所应建立数据“可用不可见、可控可计量、可信可追溯”的交易范式，构建包含存储、传输、审计、计算、平台等安全要素在内的可信执行环境，使用包括密文查询、多方安全融合计算、联邦学习、同态加密、区块链审计在内的数据密态计算技术，保障数据不被数据使用方再次拷贝、过度使用甚至再次贩卖。

10.3.2 数据交易的安全传输控制

依据法律法规对专有信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置；根据全国信息安全标准化技术委员会发布的《网络安全标准实践指南——网络数据分类分级指引》等标准，构建多套分类分级规则和体系配套不同等级安全策略、满足不同的合规性要求，确保有效地管理、保护、存储和使用数据资产。

10.3.3 数据交易的应急熔断机制

导致或可能导致数据交易场所数据交易全部或者部分不能正常进行(以下简称“交易不能进行”)的情形称为交易异常情况，引发交易异常情况的原因包括不可抗力、意外事件、技术故障等。

10.3.3.1 引发交易异常情况的不可抗力

数据交易场所市场所在地或全国其他部分区域出现或据灾情预警可能出现严重自然灾害、出现重大公共卫生事件或社会安全事件等情形。

10.3.3.2 引发交易异常情况的意外事件

数据交易场所市场交易地发生火灾或电力供应出现故障等情形。

10.3.3.3 引发交易异常情况的技术故障

数据交易场所交易、通信系统中的网络、硬件设备、应用软件等无法正常运行；数据交易场所交易、通信系统在运行、主备系统切换、软硬件系统及相关程序升级、上线时出现意外；数据交易场所交易、通信系统被非法侵入或遭受其他人为破坏等情形。

10.3.3.4 交易不能进行

无法正常开始交易、无法连续交易、交易结果异常、交易无法正常结束等情形。

10.3.3.5 无法正常开始交易

数据交易场所交易、通信系统在开市前无法正常启动；数据交易查询、计算、调用、交付、支付、结算等重要操作在开市前未及时、准确处理完毕；前一交易日的日终清算处理未按时完成或虽已完成但清算数据出现重大差错而导致无法正确交易；10%以上的交易因系统故障无法正常接入数据交易场所交易系统等形式。

10.3.3.6 无法连续交易

数据交易场所交易、通信系统出现10分钟以上中断；数据交易场所行情发布系统出现10分钟以上中断；10%以上会员无法正常发送交易申报、接收实时行情或交付结果；10%以上的中断交易等情形。

10.3.3.7 交易结果异常

交易结果出现严重错误或数据交易场所认定的其他指数计算出现重大偏差等可能严重影响整个市场正常交易的情形。

10.3.3.8 交易无法正常结束

交易异常、可能导致无法正常完成等可能对市场造成重大影响的情形。

10.3.4 数据交易的监管试点

出现下列情形之一的,数据交易场所可以向指定的数据中介方、技术提供方、数据交易方等交易相关方提示风险,或者要求其报告相关情况:

- a) 数据交易价格出现异常波动,相对基期或均价出现大幅溢价或折扣;
- b) 会员账户交易异常、资金异常、访问异常等;
- c) 会员涉嫌违法、违规、违约,涉及执法调查;
- d) 数据交易场所接到涉及会员及交易相关方的投诉、举报;
- e) 数据交易场所收到会员关于平台使用、管理的系统漏洞报告、功能异常报告、系统功能建议等;
- f) 数据交易场所认定的其他情况。

10.4 收益分配和成本分摊机制设计

10.4.1 多主体的贡献度计量

数据交易场所应遵循“贡献导向、风险匹配、动态调整”原则,按各方在数据交易中的价值贡献分配收益,同时考虑风险承担比例,提供数据交易各方收益分配的基准比例,并根据市场变化动态优化分配比例,在确定分配比例时需要考虑数据的稀缺性、使用频率等因素。

10.4.1.1 数据供给方收益分配

数据提供方获得的收益应结合数据资源产生价值的确定程度、规模、是否涉及数商参与等因素综合确定数据提供方的分配。

10.4.1.2 数据商收益分配

与数据提供方获得收益的因素相关。

10.4.1.3 生态参与方收益分配

为数据确权、合规审核、技术支持的律师事务所、会计师事务所、技术服务机构等第三方机构预留收益份额,激励其提供专业服务,保障交易安全合规。生态参与方一般通过固定费用模式获得收益。

10.4.1.4 平台运营方收益分配

数据交易场所从每笔交易中抽取固定比例佣金，覆盖基础运营成本。

10.4.2 成本分摊机制

10.4.2.1 成本构成要素

按照数据产品的保存、增值与使用过程，可将数据产品成本分为三种类型：

- a) 数据资源成本，是指持有数据产品所付出的成本，包括数据存储、数据安全、数据加密等成本；
- b) 增值成本，指对原始数据价值进行增值的过程中所付出的成本，包括数据加工、建模、应用功能开发等成本；
- c) 实施成本，指将数据产品提供给客户并为客户带来价值过程中所付出的成本，包括提供数据接口、数据部署测试、数据合规确权、数据登记结算、运营等成本。

10.4.2.2 成本追溯

通过血缘分析工具，梳理数据产品形成的物理链路，并分析每个节点、环节发生的增值活动和成本类型，如数据产品经历数据采集、数据存储、数据传输、数据开发、数据共享、数据合规确权等环节，需要将各环节相关成本进行归集，为成本分摊做准备。

10.4.2.3 分摊比例模型设计

对于上述成本，可进一步细分为直接成本和间接成本。直接成本是指与交易客体直接相关的成本，如数据采购成本、税费、数据合规确权成本、登记结算成本等；间接成本是指交易客体与其他数据资源共享而又难以直接区分开的成本，需要结合成本类型选择适合的分配因素，如数据采集成本、分析成本可按照采集工作量占比分摊，存储成本可按照数据量占比分摊，加工成本可按照数据记录数占比分摊。

10.4.3 跨境交易的收益分配规则

在构建数据要素跨境交易分配规则时需兼顾公平与效率,为实现收益分配结算的公平与高效,可满足以下要求实现:

10.4.3.1 主体贡献度计量

- a) 数据提供方:按数据资产估值权重(成本法/收益法)分配基础收益;
- b) 数据处理方:可根据增值处理复杂度(如脱敏算法研发、多语言适配)获取增值分成;
- c) 平台运营方:固定佣金比例($\leq X\%$)+跨境通道使用费(按数据传输量阶梯计价)。

10.4.3.2 汇率波动及争议解决

- a) 汇率波动补偿:建立收益币种对冲池,当汇率波动超过一定比例时自动触发再平衡结算;
- b) 预置智能合约仲裁模块:当多方对贡献权重争议时,可通过调用链上预设的行业贡献度系数表自动裁决;
- c) 跨境司法协同:支持通过国际公约、协定等向接收方所在国申请收益追偿。

10.4.4 公共数据的收益分成

在公共数据的价值释放过程中需同时考量公益性与市场化之间平衡,可以通过以下途径实现:

10.4.4.1 基础公益分成

强制提取交易额的一定比例注入公共数据运营基金,用于数据基础设施升级。

10.4.4.2 市场化调节分成

- a) 初次交易:政府授权运营机构享一定比例收益,原始数据生产部门获一定比例收益;

- b) 二次增值交易：政府分成比例采用阶梯递减，激励市场主体深度开发。

10.4.4.3 特殊场景规则

- a) 民生领域优惠：教育、医疗等民生类数据产品交易，政府分成比例下限可适当降低；
- b) 小微主体扶持：对符合条件的中小企业返还一定比例的分成收益作为数据开发补贴。

10.4.4.4 透明度保障

- a) 链上公示收益流向：通过政府区块链浏览器公开资金拨付记录；
- b) 第三方审计：年度聘请第三方审计机构核查分成比例执行合规性。

10.4.5 基于智能合约的自动化结算

在收益分配和成本分摊过程中，可通过基于智能合约的自动化结算，实现全流程无人值守结算，可供参考的实现路径如下：

10.4.5.1 智能合约的标准化条款设计

- c) 支付条件：当数据交付量达到约定阈值时自动触发付款；
- d) 分账规则：采用公式化计算（示例：结算金额 = 基础价格 × 实际交付数据量 × 汇率调整系数）；
- e) 违约处理：设置阶梯式罚则；
- f) 法律效力保障：合约代码需经司法鉴定机构备案，生成具有法律效力的电子凭证。

10.4.5.2 技术实现方案

- a) 跨币种清算：通过央行数字货币转换通道支持多币种结算，实时汇率对接国家外汇管理局公示牌价。
- b) 高效验证技术：采用先进数据验证算法将结算确认时间压缩至3秒内，建立结算失败重试机制。

10.4.5.3 异常处理与安全保障

a) 智能熔断机制：连续3次结算失败暂时冻结账户，触发人工核查流程，需手动解冻。

b) 争议解决通道：通过设置监管机构干预接口、司法机构接入接口，供监管机构线上干预或司法机构线上裁判。

11. 数据资本化

11.1 数据要素经营与管理

数据要素资本化的核心在于将数据要素资产赋予资本属性，使其能够实现保值、增值和流通。数据要素经营与管理是数据要素资本化的前提条件。

11.1.1 数据要素经营的核心内容

11.1.1.1 数据采集整合

建立应采尽采、按需采集、合规采集机制，使用自动化、实时化、可溯源技术，把内部系统、外部渠道、公共接口等多源数据汇聚、清洗、去重、标准化，形成统一目录和资源池。

11.1.1.2 数据价值评估

用成本法、收益法、市场法综合打分，量化稀缺、完整、时效、收益、风险，输出可复核的评估报告。

11.1.1.3 数据权属确认

实现来源可确认、用途可追溯、责任可追究，用区块链存证、数字水印、智能合约分置登记数据持有权、数据使用权、数据经营权以及收益分配约定，明确主体、边界、期限。

11.1.1.4 市场化应用

以场景需求为导向，搭“数据产品-数据服务-数据解决方案”梯次体系，经数据交易所、行业空间、API市场挂牌、撮合、交付、结算。

11.1.2 数据要素管理的关键机制

11.1.2.1 数据分类分级

建立数据分类分级制度，同步建立敏感清单、豁免清单，实现差异化管理。

11.1.2.2 数据安全保护

按照事前风险评估—事中监测预警—事后应急处置的程序，实现数据安全保护的闭环，加密脱敏、零信任、多方计算守护全生命周期机密、完整、可用。

11.1.2.3 数据生命周期管理

对数据的收集、加工、存储、应用、提供、出境、删除等全周期进行合规管理，明确保存期限、更新频率、归档条件、销毁方式。

11.1.2.4 合规审查机制

法务、合规、审计、业务、技术多部门联合审查，对外共享、跨境流动、资本化操作事前评估并留痕。

11.2 数据资本化的形态

11.2.1 数据资产出资

企业将数据资产直接作为股权或出资投入公司，经确权、评估、审计后的数据资产才能开展数据资产出资活动。为了防止虚假出资和估值不准确，在实践中应对数据资产的合规性、合法性、安全性和真实性进行严谨的审查。

11.2.2 数据资产质押融资

企业以数据资产作为质押物获取银行贷款。为防范风险，金融机构仅接受来源合法、权属清晰、高质量的数据资产进行质押，开展贷款业务。经实践，数据资产质押融资是最普遍的数据资产化形态。

11.2.3 数据资产信托融资

通过信托公司设立信托计划，将数据资产作为信托财产进行融资。这种方式有助于实现数据资产的长期价值最大化，同时也为投资者提供了新的投资选择。其利用信托公司的专业能力和资源优势，将数据资产转化为可融资的信托财产，从而帮助企业实现资金筹措和资产增值。企业就能够通过数据资产信托融资获得所需的资金，用于扩大生产、研发创新或偿还债务等方面。同时，数据资产信托融资也为投资者提供了新的投资选择。

11.2.4 数据资产证券化

将数据资产通过证券化手段转化为可在市场上流通的证券，实现了数据资产价值的挖掘和释放。数据资产证券化不仅有助于提升数据资产的流动性，拓宽融资渠道，还能为投资者提供更多的投资选择。在数据资产证券化的过程中，企业会将其拥有的数据资产进行评估和包装，形成具有一定价值的资产池。然后，通过证券化手段，将这些资产池转化为可在市场上流通的证券产品。这些证券产品可以在证券交易所或其他交易平台进行买卖交易，从而实现了数据资产的流动性和市场化。

11.3 数据资本化的流程

数据资本化的实现将遵循从“数据资源化”到“数据资产化”再到“数据资本化”的数据价值释放过程，在这过程中需经数据资产登记与评估、资本化路径与实施、风险防控与合规管理等流程。

11.3.1 数据资产登记与评估

在数据资产化过程中首先对数据资源进行梳理与盘点，再开展数据合规、确权登记工作，并对数据资产进行质量评价与价值评估，实现将数据资源确认为数据资产的目标。

11.3.2 资本化路径与实施

选择数据资本化路径：根据数据资产评估结果和企业具体融资需求，选择数据资产出资、数据资产质押融资、数据资产信托融资、数据资产证券化等方式开展资本化活动。

签订数据资本化相关合同：在合同中列明数据资产清单，明确数据资产的权属，约定数据资产的用途，约定保密义务、违约条款、争议解决方式。

履行数据资本化登记公示手续：在数据资本化过程中，应向网信、工信、金融、知识产权、数据主管部门等监管机构办理登记、审批、备案手续，保障交易安全，维护善意第三人的权益。

11.3.3 风险防控与合规管理

在数据资本化过程应进行数据资产合规管理和风险防控。通过合规审查、动态监测、违规追责闭环管理来防范法律风险。

建立数据减值测试制度，触发减值测试条件时开展减值测试，而且定期开展减值测试，并披露减值测试，据此来防范财务风险。

通过设立等级保护制度、构建关键信息基础设施特殊的保护制度、依法开展个人信息保护影响评估等措施，来保障数据安全，防范数据安全风险。

11.4 通过资本化实现数据要素增值

数据要素增值包括数据本身价值的提升、基于数据服务合作的价值提升、基于金融手段的价值提升等多个维度。

11.4.1 提升数据资源配置效率

通过数据确权、定价、交易、流通环节，实现数据“资源-资产-资本”三级跳，让数据向高价值场景、高效率企业、高成长行业流动，与基于商业实践的算法和模型相结合，促进数据本身价值的提升。

通过数据服务合作，将新的数据与现有数据结合时，产生新的洞察，从而提升两者价值，形成“正外部性”，最终实现数据要素的增值。

11.4.2 拓展融资渠道与投资回报

数据具备资本属性后，其增值路径将进一步拓宽。通过数据资产质押、数据资产信托、数据资产证券化等模式拓展企业融资的新渠道。将数据资产转化为可投资的金融产品，不仅实现了数据价值的直接变现，也为数据资产的跨界流通和金融创新提供了可能。

11.4.3 推动数字经济生态建设

通过数据采集、清洗、标注、建模、交易、运营、应用全链协同管理，催生数据融资、托管、保险、审计新业态，构建以数据为核心、以流动为特征、以价值最大化为目标的新生态，推动数字经济生态建设。数据资本化是数字经济发展的关键一环，其深入推进将重塑企业价值创造模式，激发市场活力，并为经济社会发展注入强大动能。通过政策、法律、技术和市场各方的协同努力，数据要素的巨大潜力将得到充分释放。

12. 数据要素授权运营

12.1 运营模式与机构选择

12.1.1 公共数据授权运营

明确公共数据授权运营的概念、基本原则和适用范围。公共数据授权运营是指政府依法授权特定主体加工处理公共数据，形成数据产品并向社会提供服务。应遵循依法合规、公平公正、公益优先、合理收益、安全可控的原则。

12.1.1.1 整体授权模式

将公共数据的整体运营权全面赋予某一地方性平台公司（通常为国有背景，如数据集团、大数据公司、城投公司等），由其作为公共数据运营的主要载体，负责数据资源的集中管理、运营、开发利用等工作。

12.1.1.2 分层授权模式

指政府将公共数据资源授权给国资数据平台作为一级主体,由其负责公共数据平台的构建与运营,实现数据的集中汇聚、存储与管理,各类市场主体作为二级开发主体,在一级主体提供的数据库基础上进行深度开发和应用。

12.1.1.3 分场景授权模式

运营机构根据具体的市场需求和应用场景,向数据主管单位明确提出所需的数据内容及其应用场景,并进行授权的模式。

12.1.1.4 主体职责与机构选择

- a) 政府单位主导,负责确定公共数据资源授权运营的范围,全面委托国资企业作为该地区公共数据的综合运营主体;
- b) 实施者是被政府明确授权,负责具体执行公共事务管理的机构或单位,进一步授权委托运营者开发相应的信息系统;
- c) 运营者连接政府与数商,设计开发信息系统,并进行系统维护和升级,将数据转化为数据产品,后向数商出售数据产品;
- d) 数商进行数据产品再开发,形成细分领域的数据库应用并销售。

12.1.2 企业数据授权运营

介绍企业数据授权运营的常见模式,包括独立运营、与第三方合作运营等,同时阐明企业选择授权运营机构时需关注的重点,包括运营机构的市场信誉、行业经验、数据管理能力以及能否为企业带来商业价值等,以保障企业在数据授权运营过程中的权益和商业利益。

12.1.3 个人数据授权运营

个人数据授权运营中数据提供方、个人信息主体、数据使用方和数据授权平台四方的角色和责任:

- a) 数据提供方在收集数据时必须合法并取得个人信息主体的明确同意;
- b) 个人信息主体有权查阅、复制和更正自己的个人信息,同时可以撤回已同意的授权;

- c) 数据使用方在使用数据前需明确使用目的和范围，并在授权期限内合法使用数据；
- d) 数据授权平台负责接收数据使用申请，向个人信息主体发送授权请求，并监督授权过程。

12.2 授权协议与管理

12.2.1 授权协议的主要内容

核心条款需要包括授权数据的范围与目录、授权期限、数据产品和服务的类型与技术标准、收益分配机制、数据安全与个人信息保护要求、运营成效评估与退出机制、违约责任与争议解决方式等内容。

12.2.2 协议执行与监管

实施机构应建立健全协议执行的监督机制，包括定期审计、运营报告提交、数据使用合规性检查等。运营机构不得超范围使用数据，不得参与已交付数据产品的再开发。

12.3 运营效果评估与优化

12.3.1 评估机制建设

建立科学的运营效果评估体系，评估内容包括数据产品质量、市场应用效果、社会经济效益、安全合规情况等。评估方式可结合定量指标与专家评审，必要时引入第三方评估机构。

12.3.2 评估结果应用

评估结果应作为续约、退出、奖惩的重要依据。对表现优秀的运营机构可给予政策支持和资源倾斜；对存在问题的机构应提出整改要求，严重违规者应终止授权。

12.3.3 持续优化与迭代机制

根据评估结果和市场反馈，动态调整授权范围、运营模式和管理制度，推动数据要素市场的健康发展。鼓励运营机构探索新场景、新技术、新产品，提升数据价值转化能力。

12.4 数据安全合规审计

12.4.1 数据安全合规审计原则

数据安全合规审计应遵循合法性、独立性、客观性、全面性、公正性、保密性原则：

- a) 合法性原则：审计人员应了解并遵守所有适用的法律法规要求，在审计过程中始终遵守审计过程规范；审计活动的流程及人员应遵从相关法律法规；
- b) 独立性原则：审计人员应独立于审计活动，与被审计方无利益冲突。对于内部机构自行开展的审计，实施审计的人员应独立于具体被审计的个人信息处理活动；
- c) 客观性原则：审计人员收集和记录的审计证据应保证其可信性，应采取科学、透明的方式获得审计证据，应保证审计证据的真实、完整、有效；
- d) 全面性原则：审计人员针对审计对象，应进行全面、系统的审计，进行综合、全面、系统的审查，确保证据充分；
- e) 公正性原则：审计发现、审计结论和审计报告应真实和准确地反映审计活动；审计人员应报告在审计过程中遇到的重大障碍，以及审计组和被审计方之间没有解决的分歧。沟通必须真实、准确、客观、及时、清楚和完整；
- f) 保密性原则：审计人员应遵守保密协议，审慎使用并保护在审计过程获得的信息和数据。

12.4.2 数据安全合规审计范围

审计人员应根据审计目的，明确数据合规审计的范围，包括以下五个基本方面：

- a) 数据和数据资产：对特定数据对象集合的定义、属性、特征、数据形态和生存情况等方面的审计，包括数据来源、数据质量、数据资产建设等方面，数据的名称、类型、格式、来源、用途、价值、敏感性、所有权、存储位置、生命周期等，检查方法包括对被审计单位的数据目录、数据字典、数据清单、数据资产登记表等进行查阅和分析；
- b) 数据环境：对数据在生存周期内，所处组织上游、下游及组织间流转环境，包括开放、封闭（如离线数据）、线下（如打印的独立数据表）等环境的安全属性进行审计；
- c) 数据处理行为：包括但不限于对数据生存期中与数据相关活动，包括数据分类分级、流通交易、数据治理、授权和认证管理、关键人员管理等行为操作的审计；
- d) 数据合规管理：包括但不限于被审计单位数据合规管理体系的符合性诊断、数据合规审查、有效性评价、数据合规测评、数据合规认证等；
- e) 数据安全：被确定的数据和数据资产、数据环境和数据处理行为的应用系统、工具平台的安全性，包括完整性、准确性、有效性或真实性。

12.4.3 数据安全合规审计重点

数据资产价值形成与应用包括数据资产的产生、流转、消费三大过程，每个过程具有共性及各自特性的合规审计重点。

12.4.3.1 数据资产生成阶段

a) 数据资产真实性

数据资产真实性、有效性合规审计，应该从数据的 IT 属性合规性出发，审查数据的一致性：数据是否具备应用一致性从而对业务数据有效留痕；还需审查数据的时间完整性：数据是否具备时间完整性从而保全业务数据的完整时间。

b) 数据存储安全

明确存储介质类型、位置及访问权限配置；定期核查数据存储完整性与可恢复性，结合备份机制开展验证；使用 WORM、加密等防护手段等不可篡改技术保

障重要数据的长期存储审计合规性。

c) 数据可恢复性

数据是否具备可恢复性从而可以还原到任意时间的原始数据状态。审查的内容包括：是否定期备份；是否定期恢复演练与生产数据对比备份数据的一致性，检验其真实性；备份是否可还原历史状态，支撑溯源分析，版本追溯；是否可检查备份操作与恢复记录，通过日志与恢复记录提供审计能力。

12.4.3.2 数据的处理、流转、交易阶段

a) 数据处理过程控制

授权与权限：是否明确各类数据对象、操作的权限对应的责任人；

操作过程记录：是否记录各类处理行为及其责任人；

处理过程行为数据记录：数据加工、脱敏、清洗、分析等代码、操作实施日志留存与行为审计；

流程控制：变更管理控制，确保每一次处理动作有迹可循。

b) 数据脱敏

敏感数据识别与分类：

是否完成对数据资产中敏感字段的识别（如身份证、手机号、银行卡、医疗信息等）；是否有敏感数据分类分级制度，并定期更新；是否依据业务用途对敏感数据制定使用边界；

策略与技术：是否采用国家/行业认可的脱敏技术（如：掩码、加密、泛化、数据扰动等）；是否对脱敏算法进行有效性评估与测试（防止逆向还原）；

流程控制：是否建立脱敏前审批机制及记录；是否对脱敏过程进行日志留存、审计可追溯；是否明确数据脱敏责任人、操作人、审查人；

c) 数据存储

明确存储介质类型、位置及访问权限配置；定期核查数据存储完整性与可恢复性，结合备份机制开展验证。

d) 数据传输安全

数据传输路径、加密措施、协议规范是否符合国家或行业标准；按照国家法

律、法规要求留存数据传输记录、接口调用日志，确保数据未被截取或泄露；建立跨系统、跨组织传输的审批与审计机制，支持事后溯源。

e) 数据溯源

对数据血缘进行分析，审查数据生成路径、加工环节、流转节点及责任人；审查系统日志是否完整，记录时间戳、操作者身份与具体内容，要求日志防篡改；核对数据是否具备版本号、时间标签与来源标识，以保障数据标签与版本控制。

12.4.3.3 数据消费、使用阶段

数据资产生命周期中，“消费/使用”阶段的合规审计是保障数据合规性、杜绝滥用和非法使用的关键环节。

数据使用权限审计：是否只向使用者开放必要字段，是否避免敏感字段无关暴露，是否符合授权与最小权限原则；

使用人身份认定及授权：是否对使用者进行身份认证，是否对使用者进行数据使用范围、方式进行授权，防止未经授权的数据调用或访问行为；

用途范围：数据使用是否与收集目的、使用声明、用户授权相符，是否超出既定范围；

使用行为记录：是否对数据的使用行为做详细日志记录（如 IP、时间戳、API 路径、数据范围），是否建立策略识别突发调用、高频访问、越权查询等可疑行为；

使用接口行为记录：是否记录数据消费所依赖的 API/分析平台/BI 工具的使用权限与操作行为。

12.4.4 审计流程

- a) 审计准备：明确数据对象、收集字典与流程图、界定责任人；
- b) 数据真实性核查：包括原始对比、一致性校验、异常检测与备份交叉验证；
- c) 数据血缘梳理：使用工具分析数据流向，标注加工节点与责任人；
- d) 问题定位与风险评估：分类记录发现问题与风险等级；

- e) 报告与整改：形成审计报告、制定整改措施并跟踪复审。

12.4.5 职责分工

- a) 数据治理委员会：统筹审计工作与策略审批；
- b) 内部审计团队：组织开展审计任务；
- c) IT 运维部门：提供系统日志、权限记录与备份记录；
- d) 各业务数据负责人：配合提供数据来源及原始凭证；
- e) 安全与合规部门：监督审计的合规性与追责链条；
- f) 数据备份管理员：确保备份数据真实、完整、可追溯、可验证，并配合审计对比。

12.4.6 审计工具类型

数据审计工具，不同涉及不同类型的工具：

- a) 数据资产准备阶段：数据备份平台、数据血缘追踪工具；
- b) 数据资产交易阶段：数据质量检测工具；
- c) 数据资产使用阶段：日志与操作分析工具。

12.4.7 审计频次

- a) 核心数据资产每年至少开展一次审计；
- b) 出现系统上线、数据异常或外部要求时进行临时审计。

12.4.8 保密与合规

所有审计数据和结果应严格保密，遵守国家法律法规，未经授权不得披露或外传。

参考文献

- [1] 《中华人民共和国价格法》
- [2] 《中华人民共和国网络安全法》
- [3] 《中华人民共和国个人信息保护法》
- [4] 《中华人民共和国数据安全法》
- [5] GB/T 36344-2018 信息技术 数据质量评价指标
- [6] GB/T 37932-2019 信息安全技术 数据交易服务安全要求
- [7] GB/T 35273-2020 信息安全技术 个人信息安全规范
- [8] GB/T 40685-2021 信息技术服务 数据资产 管理要求
- [9] GB/T 42450-2023 信息技术 大数据 数据资源规划
- [10] GB/T 43697-2024 数据安全技术 数据分类分级规则
- [11] DB11T 2348-2024 数据交易通用指南
- [12] DB11T 2350-2024 数据交易安全评估指南