ICS ×××××
CCS ×××

可信数据空间发展联盟团体标准

T/××× ××××—202×
代替 T/××× ××××—××××

可信数据空间 能力要求

Trusted data space capability requirements

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

××××-××-××发布　　××××-××-××实施

目 次

前　　言 1
引　　言 3
1 范围 4
2 规范性引用文件 4
3 术语和定义 4
4 缩略语 6
5 可信数据空间整体能力要求 7
5.1 能力框架模型 7
5.2 能力类别与功能视角映射 8
6 可信数据空间运营要求 9
6.1 概述 9
6.2 战略规划与目标管理 9
6.3 组织机构与治理机制 9
6.4 长效运营与持续改进 10
6.5 安全管理体系 10
6.6 核心能力评估与监测 10
6.7 人才与资源保障 11
6.8 其他支撑能力 11
6.8.1 财务与预算管理 11
6.8.2 客户服务与运维支持 11
6.8.3 市场与生态推广 11
6.8.4 法律合规与政策协调 11
6.8.5 创新与研发管理 12
7 场景应用 12
7.1 概述 12
7.2 场景发现与价值规划 12
7.3 多主体协同与职责分配 13
7.4 数据供给侧匹配 13
7.5 数据交易与合约管理 13
7.6 数据产品化与服务化 14
7.7 场景数据产品与服务运营 14
7.8 价值衡量与收益清算 15
7.9 反馈改进与能力迭代 16
7.10 跨场景经验沉淀与推广 16
8 数据资源 16
8.1 数据资源概述 16
8.2 数据接入与登记 17
8.2.1 数据接入 17
8.2.2 数据登记与审核 17
8.2.3 数据标识与分配 17
8.3 数据处理 18
8.3.1 数据清洗与标准化 18
8.3.2 数据分类与分级 18
8.3.3 元数据治理 18
8.3.4 数据质量管理 18

8.3.5 数据脱敏处理 . . . 18
8.4 数据发布发现 . . . 18
8.4.1 数据资源目录描述信息 . . . 18
8.4.2 数据产品目录描述信息 . . . 19
8.4.3 目录发布与上架流程 . . . 19
8.4.4 供需匹配与撮合 . . . 19
8.5 数据产品研发与封装 . . . 19
8.5.1 数据产品研发流程 . . . 19
8.5.2 数据产品封装技术 . . . 20
8.5.3 数据产品质量保障 . . . 20
8.5.4 数据产品安全检测 . . . 21
8.6 数据服务与交付 . . . 21
8.6.1 服务接口标准化封装 . . . 21
8.6.2 可信交付协议与机制 . . . 21
8.6.3 服务化质量控制 . . . 22
8.7 数据价值评估与生命周期管理 . . . 22
8.7.1 数据资源价值评估模型 . . . 22
8.7.2 数据资源用后质量评价 . . . 22
8.7.3 数据资源生命周期管理 . . . 22
8.8 数据资源体系构建 . . . 23
8.8.1 基础科学数据集管理 . . . 23
8.8.2 高质量语料库构建 . . . 23
8.8.3 城市数据资源体系构建 . . . 23
9 生态主体 . . . 23
9.1 生态主体的分类与定义 . . . 23
9.1.1 数据提供方 . . . 23
9.1.2 数据使用方 . . . 23
9.1.3 数据开发方 . . . 24
9.1.4 数据中介方 . . . 24
9.1.5 数据托管方 . . . 24
9.1.6 空间运营方 . . . 24
9.1.7 监管方 . . . 24
9.2 生态主体和业务要求 . . . 24
9.2.1 主体接入 . . . 24
9.2.2 数据接入与治理 . . . 25
9.2.3 数据发布与目录管理 . . . 25
9.2.4 数据需求匹配 . . . 25
9.2.5 供需撮合 . . . 26
9.2.6 数据转换与处理 . . . 26
9.2.7 数据传输与存储 . . . 26
9.2.8 数据使用 . . . 26
9.2.9 数据销毁 . . . 27
9.2.10 后服务 . . . 27
10 规则机制 . . . 27
10.1 概述 . . . 27
10.2 接入审核规范 . . . 27

10.2.1 身份审核规则 27
10.2.2 数据审核规则 28
10.2.3 产品服务审核规则 28
10.2.4 技术组件审核规则 28
10.3 互联互通规范 29
10.3.1 数据目录管理规范 29
10.3.2 数据互操作规则 29
10.3.3 技术系统互联互通规则 29
10.4 共享使用规范 29
10.4.1 数字合约要素模型要求 29
10.4.2 数字合约协商机制 30
10.4.3 数字合约全生命周期管理规则 30
10.4.4 清算审计机制 30
10.4.5 纠纷解决机制 31
10.4.6 跨境数据流通机制 31
10.5 收益分配机制 31
10.5.1 数据价值评估模型 31
10.5.2 数据收益分配机制 32
10.5.3 结算机制 32
11 技术系统 32
11.1 可信数据空间系统功能 32
11.1.1 功能概述 32
11.1.2 中间服务平台功能 34
11.1.3 节点功能 35
11.2 可信数据空间系统技术 37
11.2.1 资源交互技术 37
11.2.2 可信管控技术 38
11.2.3 价值共创技术 40
11.3 功能与技术的映射 42
（规范性） XX 45
（资料性） YY 46
参 考 文 献 49

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由可信数据空间发展联盟提出。

本文件由可信数据空间发展联盟归口。

本文件起草单位：中国信息通信研究院、国家数据发展研究院、中国电子信息产业发展研究院、国家工业信息安全发展研究中心、国家信息中心、中国南方电网有限责任公司、国家发展改革委创新驱动发展中心、数据空间技术与系统全国重点实验室、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、蚂蚁科技集团股份有限公司、亚信科技（中国）有限公司、华为技术有限公司、数篷科技（深圳）有限公司、四川数通智汇数据科技有限公司、南方电网能源发展研究院有限责任公司、广州广电运通信息科技有限公司、中节能数字科技有限公司、中电科大数据研究院有限公司、中电数据产业集团有限公司、中国电信股份有限公司、中国铁塔股份有限公司、中国移动通信有限公司研究院、北京新材道数智科技有限公司、北京数安行科技有限公司、福建新世通律师事务所、江苏省数据集团有限公司、华控清交信息科技（北京）有限公司、鹏城实验室、杭州安恒信息技术股份有限公司、软通智慧科技有限公司、建筑材料工业信息中心、南京大数据集团有限公司、南京钢铁集团有限公司、温州市数据集团有限公司、格尔软件股份有限公司、浙江蚂蚁密算科技有限公司、浪潮云信息技术股份公司、浪潮云洲工业互联网有限公司、联通数据智能有限公司、普元信息技术股份有限公司、广州数据集团有限公司、广州数据交易所有限公司、飞友科技有限公司、广域铭岛数字科技有限公司、马上消费金融股份有限公司、中节能大数据有限公司、中电信数字城市科技有限公司、中电信数智科技有限公司、中电信数智科技有限公司、中兴通讯股份有限公司、中汽创智科技有限公司、中国汽车工业协会、中国移动通信集团有限公司、中国移动紫金（江苏）创新研究院有限公司、北京大学上海临港国际科技创新中心、北京电子数智科技有限责任公司、北京百度网讯科技有限公司 、北京易华录信息技术股份有限公司、北京信联数安科技有限公司、三未信安科技股份有限公司、上海信投智能科技股份有限公司、杭州趣链科技有限公司 、上海富数科技有限公司、上海零数众合信息科技有限公司、广东领信数科信息技术有限公司、北京阅律数字科技有限公司、北京熠智科技有限公司、西安电子科技大学、江苏中塑数据技术有限公司、国机数字科技有限公司、国网经济技术研究院有限公司、国科量子通信网络有限公司、国信中健科技有限公司、科大讯飞股份有限公司、高颂数科（厦门）智能技术有限公司、常州数据科技有限公司、深圳市洞见智慧科技有限公司、深圳吉阳智能科技有限公司、数族科技（南京）股份有限公司等。

本文件文本可登录可信数据空间发展联盟官网（www.××××.×××.cn）下载。

引　言

本文件的发布机构提请注意，声明符合本文件时，可能涉及到××××××条款与专利号为××××××名称为××××××相关的专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构承诺，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得：

专利持有人姓名：××××××××××

地址：××××××××××××

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

可信数据空间 能力要求

1 范围

本标准规定了可信数据空间的整体能力要求框架，可信数据空间运营要求、场景应用、数据资源、生态主体、规则机制和技术系统的能力要求。

本标准适用于企业、行业、城市、个人和跨境可信数据空间的规划、建设及评估参考。

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。

3 术语和定义

下列术语和定义适用于本文件。

3.1

可信数据空间

基于共识规则，联接多方主体，实现数据资源共享共用的一种数据流通利用基础设施，是数据要素价值共创的应用生态，是支撑构建全国一体化数据市场的重要载体。可信数据空间须具备数据可信管控、资源交互、价值共创三类核心能力。

3.2

数据

信息的可再解释的形式化表示，以适用于通信、解释或处理。

[来源：GB/T 25069-2022，2.2.1]

3.3

数据资源

具有价值创造潜力的数据的总称，通常指以电子化形式记录和保存、可机器读取、可供社会化再利用的数据集合。

3.4

数据要素

投入到生产经营活动、参与价值创造的数据资源。

3.5

数据产品和服务

基于数据加工形成的，可满足特定需求的数据加工品和数据服务。

3.6

数据资产

特定主体合法拥有或者控制的，能进行货币计量的，且能带来经济利益或社会效益的数据资源。

3.7

数据处理

数据操作的系统执行。

[来源：GB/T 25069-2022，2.2.2]

3.8

数据流通

指数据在不同主体之间流动的过程，包括数据开放、共享、交易、交换等。

3.9

数据交易

是指数据供方和需方之间进行的，以特定形态数据为标的，以货币或者其他等价物作为对价的交易行为。

3.10

数据治理

对数据资源管理形式权力和控制的活动集合（计划、监督和执行）。

[来源：GB/T 44109-2024，3.1]

3.11

数据安全

是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.12

元数据

关于数据或数据元素的数据（可能包括其数据描述），以及关于数据拥有权、存取路径、访问权和数据易变性的数据。

[来源：GB/T 25069-2022，2.2.7]

3.13

数据分析

是指通过特定的技术和方法，对数据进行整理、研究、推理和概括总结，从数据中提取有用信息、发现规律、形成结论的过程。

3.14

隐私保护计算

是指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一类信息技术，保障数据在产生、存储、计算、应用、销毁等数据流转全过程的各个环节中“可用不可见”。隐私保护计算的常用技术方案有安全多方计算、联邦学习、可信执行环境、密态计算等。常用的底层技术有混淆电路、不经意传输、秘密分享、同态加密等。

3.15

安全多方计算

是指在一个分布式网络中，多个参与实体各自持有秘密数据，各方希望以这些数据为输入共同完成对某函数的计算，而要求每个参与实体除计算结果、预期可公开的信息外均不能得到其他参与实体的任何输入信息。主要研究针对无可信第三方情况下，安全地进行多方协同的计算问题。

3.16

联邦学习

是指一种多个参与方在保证各自原始私有数据不出数据方定义的可信域的前提下，以保护隐私数据的方式交换中间计算结果，从而协作完成某项机器学习任务的模式。

3.17

可信执行环境

是指基于硬件级隔离及安全启动机制，为确保安全敏感应用相关数据和代码的机密性、完整性、真实性和不可否认性目标构建的一种软件运行环境。

3.18

密态计算

是指通过综合利用密码学、可信硬件和系统安全相关技术，实现计算过程数据可用不可见，计算结果能够保持密态化，以支持构建复杂组合计算，实现计算全链路保障，防止数据泄漏和滥用。

3.19

区块链

是分布式网络、加密技术、智能合约等多种技术集成的新型数据库软件，具有多中心化、共识可信、不可篡改、可追溯等特性，主要用于解决数据流通过程中的信任和安全问题。

3.20

使用控制

是指在数据的传输、存储、使用和销毁环节采用技术手段进行控制，如通过智能合约技术，将数据权益主体的数据使用控制意愿转化为可机读处理的智能合约条款，解决数据可控的前置性问题，实现对数据资产使用的时间、地点、主体、行为和客体等因素的控制。

4 缩略语

下列缩略语适用于本文件。

ABAC：属性访问控制（Attribute - Based Access Control）
AI：人工智能（Artificial Intelligence）
API：应用程序编程接口（Application Programming Interface）
CD：持续交付（Continuous Delivery）
CI：持续集成（Continuous Integration）
CPU：中央处理器（Central Processing Unit）
DCAT：数据目录词汇表（Data Catalog Vocabulary）
ETL：抽取-转换-装载（Extract-Transform-Load）
GB/T：中国国家标准推荐标准（Guobiao Recommended Standard）
GDPR：通用数据保护条例（General Data Protection Regulation）
GS1：全球统一标识系统（Global Standards 1）
GUID：全球唯一标识（Global Unique Identifier）
IdP：身份提供者（Identity Provider）
IO：输入/输出（Input/Output）
IP：网络协议（Internet Protocol）
ISO：国际标准化组织（International Organization for Standardization）
IT：信息技术（Information Technology）
JSON：JavaScript 对象表示法（JavaScript Object Notation）
JSON-LD：关联数据 JavaScript 对象表示法（JavaScript Object Notation for Linked Data）
KPI：关键绩效指标（Key Performance Indicator）
MPC：安全多方计算（Secure Multi-Party Computation）
MFA：多因素认证（Multi-Factor Authentication）
NLP：自然语言处理（Natural Language Processing）
OID：对象标识符（Object Identifier）
PDCA：计划-执行-检查-处置（Plan-Do-Check-Act）
RBAC：基于角色的访问控制（Role-Based Access Control）
RDF：资源描述框架（Resource Description Framework）
ROI：投资回报率（Return on Investment）
SDK：软件开发工具包（Software Development Kit）
SDN：软件定义网络（Software Defined Network）
SLA：服务等级协议（Service Level Agreement）
SM：国密算法（Shang Mi）
SOC：安全运营中心（Security Operations Center）
SOP：标准作业流程（Standard Operating Procedure）
TEE：可信执行环境（Trusted Execution Environment）
ZTA：零信任架构（Zero Trust Architecture）

5 可信数据空间整体能力要求

5.1 能力框架模型

本标准的能力框架旨在全面指导可信数据空间高效、安全、合规地发挥其作用。可信数据空间以场景应用为牵引，吸引数据提供方、使用方共享共用数据资源，推动服务方等生态主体联合开发数据产品，以共识规则机制和技术系统为支撑保障，推动数据可信流通与高效利用，最终以可持续运营机制为驱动，实现可信数据空间的长效运行与创新发展。因此，可信数据空间总体发展体系可以概括为“1+5”，其中“1是指”可信数据空间的运营要求；“5”是指可信数据空间的五大内部核心组成，包括场景应用、数据资源、生态主体、规则机制和技术系统等维度，构建起具备资源交互、可信管控、价值共创三大功能的可信数据空间体系，如图1所示。具体含义如下：

——运营要求是指可信数据空间通过对外输出共性能力、沉淀经验模式、设计激励机制、制定多方共赢的规则等方式，推动多元生态主体持续挖掘场景需求，带动数据资源开发为数据产品和服务，并对外输出完成数据价值闭环，实现可信数据空间自我造血和长效运营。展开逻辑是围绕可信数据空间全生命周期管理展开，从建设运营标准中的技术系统搭建，到运营规则里的接入审核、收益分配、合规审计等机制确立，构建起一套保障空间稳定运营、促进资源交互与价值共创的体系，确保各参与方在有序规则下开展数据活动 。

——场景应用是指在业务需求牵引下，可信数据空间构建起促进场景数据流通利用的软件应用和数据产品。可信数据空间以共性价值应用为牵引，聚集多元生态主体与丰富数据资源，打造满足多主体价值需求的场景解决方案。展开逻辑是基于不同类型可信数据空间的特点和需求进行挖掘与规划，如各行业根据自身痛点确定核心应用场景，明确参与方职责，通过跨主体协同实现场景落地，再经实践沉淀优化，形成可推广的模式，推动数据在各领域深度应用 。

——数据资源是指可信数据空间内承载的各类数据资源，涵盖高质量数据资源和数据集，为空间开发利用提供基础支撑保障。展开逻辑是从基础共性标准中的数据治理规范入手，对数据进行清洗、脱敏、分级等预处理，在资源交互标准下实现数据的注册上架、精准检索与高效流通，依托可信管控标准保障数据接入合规和使用安全，最终在价值共创环节转化为数据产品与服务，释放数据价值 。

——生态主体涵盖数据提供方、使用方、开发方、中介方、托管方、运营方和监管方等多元主体，参与空间内数据共享流通、开发利用等活动。展开逻辑是以多类型主体接入为起点，通过接入认证标准对主体资质和身份进行严格审核，在价值共创过程中依据服务方管理规范等明确各方权责，促进主体间协同合作，共同推动数据开发利用，构建互利共赢的生态体系 。

——规则机制是指可信数据空间内开展数据接入审核、流通利用、收益分配等全生命周期活动的依据，包括资源接入、互联互通、共享使用及收益分配等规则机制，保障可信数据空间安全、稳定、高效运行。展开逻辑是在基础共性标准的安全合规框架下，结合各环节业务需求制定详细规则，如资源交互中的接口协议、可信管控里的合约管理、建设运营中的接入审核规范等，为数据空间各活动提供清晰指引和约束，确保数据空间可信有序运行 。

——技术系统是指可信数据空间的技术支撑底座，包括可信数据空间客户端、中间服务平台以及内嵌的一系列自动化履约组件等，保障可信管控、资源交互、价值共创能力实现，支撑数据可信受控流通。展开逻辑是从基础共性标准的安全技术支撑，到资源交互、可信管控中的各类技术应用，如加密传输、多方安全计算等，再到建设运营标准里的中间服务平台、用户节点和网络架构规范，打造一个安全可靠、互联互通、高效运行的技术环境，支撑数据空间各项功能实现 。

以“1+5”的可信数据空间发展体系为指导，对数据空间功能需求进行深入分析并设计能力要求框架，从场景应用、数据资源、生态主体、规则机制、技术系统五大核心要素以及可持续运营方面提出相关的能力要求。

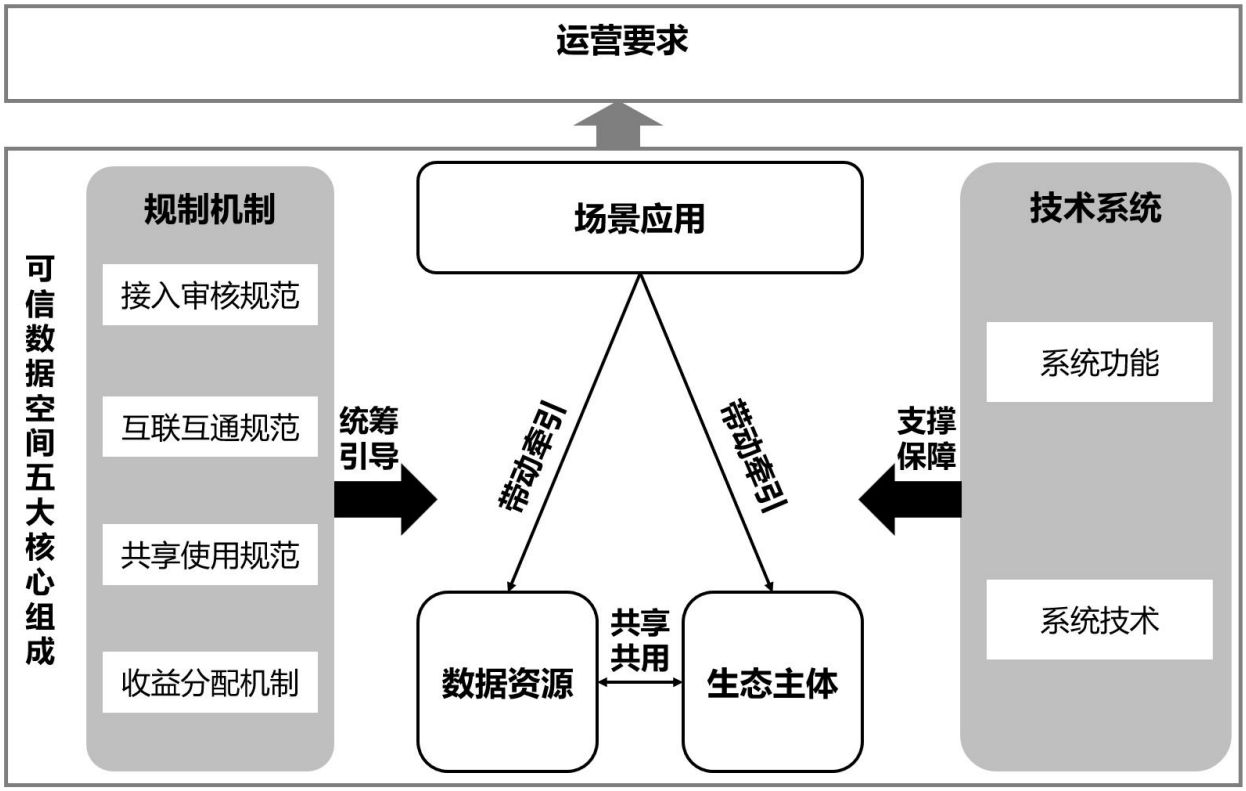

图 1 可信数据空间能力框架模型

5.2 能力类别与功能视角映射

从应用场景、数据资源、生态主体、规则机制、技术系统五大核心要素，提出可信数据空间的细分能力要求。

可信数据空间维度	可信数据空间细分功能	与三大核心能力的映射关系
场景应用	场景发现与价值规划	价值共创能力
	多主体协同与职责分配	资源交互能力
	数据供给侧匹配	资源交互能力
	数据交易与合约管理	资源交互能力
	数据产品化与服务化	价值共创能力
	场景数据产品与服务运营	价值共创能力
	价值衡量与收益清算	价值共创能力
	反馈改进与能力迭代	价值共创能力
	跨场景经验沉淀与推广	价值共创能力
数据资源	数据采集与登记	资源交互能力
	数据处理	资源交互能力
	数据发布发现	资源交互能力
	数据产品研发与封装	资源交互能力
	数据服务与交付	价值共创能力
	数据价值评估与生命周期管理	价值共创能力
	数据资源体系构建	资源交互能力

生态主体	生态主体的分类与定义	价值共创能力
	主体接入	可信管控能力
	数据接入与治理	资源交互能力
	数据发布与目录管理	资源交互能力
	数据需求匹配	资源交互能力
	供需撮合	价值共创能力
	数据转换与处理	资源交互能力
	数据传输与存储	资源交互能力
	数据使用	资源交互能力
	数据销毁	可信管控能力
	后服务	价值共创能力
规则机制	接入审核规范	可信管控能力
	互联互通规范	资源交互能力
	共享使用规范	价值共创能力
	收益分配机制	价值共创能力
技术系统	系统功能	可信管控、资源交互、价值共创能力
	系统技术	可信管控、资源交互、价值共创能力

表 1 可信数据空间能力要求与细分功能

6 可信数据空间运营要求

6.1 概述

本章立足于“1+5”能力框架中的“1”可持续运营要求，对可信数据空间的战略规划、组织治理、运营管理、安全保障、能力评估与人才资源等方面提出具体能力要求，确保可信数据空间在长效运行中不断释放数据价值，推动生态繁荣与创新发展。

6.2 战略规划与目标管理

——空间运营方宜结合国家战略规划要求、区域发展特色和行业数字化转型需求，编制可信数据空间中长期发展战略规划，明确建设愿景、重点领域、阶段性目标和风险管控要求，并在规划中对标“可持续运营”目标。

——空间运营方应依据战略规划制定年度与季度运营目标，并设置可量化的关键绩效指标（KPIs），包括生态主体接入数量、场景沉淀数量、数据产品和服务数量、数据资源交易规模、用户节点接入数量、规则机制完备性、合规审计通过率、安全事件处置时效等，以支撑闭环决策与考核。

——空间运营方宜在目标制定和评估过程中引入利益相关方协商机制，定期组织政府监管方、数据提供方、使用方、服务方及社会代表参与目标评审与修订，确保目标的可操作性、广泛认同度和动态调整能力。

6.3 组织机构与治理机制

——空间运营方宜建立与战略目标相匹配的组织架构，明确决策层、日常管理层、合规风控部、技术运维部、产品运营部和客户支持部等职能部门及其职责分工，并形成完整的组织职责说明书。

——空间运营方宜设立数据委员会或生态治理委员会，覆盖平台自治与联合治理职能，负责审议平

台规则、合约模板、定价策略、价值评估模型、风险事件与重大纠纷，确保治理决策的合法性、公正性与透明度。

——空间运营方宜推行扁平化管理和跨部门协作机制，通过虚拟团队、项目小组等方式提高决策和执行效率，定期组织跨部门例会和主题研讨，促进信息流动与快速响应。

6.4 长效运营与持续改进

——空间运营方应制定并固化日常运营流程及标准作业流程（SOP），涵盖主体接入、数据资源管理、撮合交易、合约履约、收益清算、客户服务和投诉处理等全过程，并通过流程图、操作手册与培训确保各角色准确执行。

——空间运营方应实施“计划-执行-检查-处置”（PDCA）闭环管理，定期对运营流程、服务模式与组织架构进行审视，识别瓶颈与改进点，形成改进计划并跟踪实施效果，确保运营机制持续优化。

——空间运营方宜采用运维自动化与智能化工具，监测系统性能、业务指标与合规事件，利用可视化运营大屏实时展现核心指标，辅以预警机制确保异常情况能够及时响应与处置。

6.5 安全管理体系

——空间运营方应依据《网络安全法》《数据安全法》和《个人信息保护法》，构建覆盖策略规划、安全组织、技术防护和应急响应的全方位安全管理体系，并形成完善的安全管理手册与制度文件。

——空间运营方应设置首席安全官或安全委员会，负责制定并监督执行信息安全策略、风险评估及应急演练计划，确保安全治理与业务决策紧密联动。

——空间运营方宜引入 ISO 27001、等保 2.0 等国际或国家成熟的安全框架 ，定期开展漏洞扫描、渗透测试和合规审计，并对发现的安全隐患按优先级分批次修复，形成闭环整改报告。

——空间运营方可部署安全运营中心（SOC）或安全大数据平台，通过安全事件监测、威胁情报分析和响应编排，实现 7×24 小时安全巡检与应急响应，并将处置日志纳入审计与知识库，用于持续提升防御能力。

6.6 核心能力评估与监测

——空间运营方应建立可信数据空间核心能力评估体系，从场景应用、数据资源、生态主体、规则机制和技术系统等维度开展评估，涵盖资源交互能力、可信管控能力、价值共创能力等维度，并制定对应的评估指标与权重。

——空间运营方应对照评估体系定期开展自评和第三方评估，评估结果应形成报告并向生态主体公示，形成“能力现状-差距分析-改进优化”的闭环管理。

—— 空间运营方宜建设在线监测平台，实时采集访问量、撮合量、交易额、安全事件、合规审计结果等各类运营数据，并结合大数据与 AI 技术对指标走势与风险趋势进行动态分析，为治理决策提供数据支撑。

——应具备精准用户画像与行业调研能力，能够针对不同行业用户制定差异化运营策略，通过持续的拉新促活、定向激励等手段，提升平台用户规模与活跃度。

—— 应具备基于用户需求和行为数据分析的精准营销能力，能够通过个性化推荐和定制化推广等手段，提高产品的相关性与用户参与度，从而提升产品购买率。

——应具备平台品牌建设与传播能力，围绕“可信、安全、合规”的平台价值定位，结合典型案例推广与多渠道宣传等策略，打造在业内具公信力与专业度的可信数据流通平台形象。

——应具备数据驱动的市场洞察与策略调整能力，能够持续跟踪行业发展趋势与平台运营指标，动态调整市场策略，确保平台在竞争环境中保持灵活应变与持续增长的能力。

—— 宜构建开放的商业生态体系，通过与地方政府、产业园区、行业协会等多方协作，打造以数据为核心的商业联盟，促进平台的长远发展与商业合作的深度融合。

6.7 人才与资源保障

——空间运营方应制定人才发展战略，明确核心岗位能力模型和招聘计划，重点覆盖数据科学、安全合规、产品运营、技术运维、市场推广与客户支持等领域，并建立定期考核与激励机制。

——空间运营方宜与高校、科研院所、行业协会及专业机构建立合作，开展联合培训、实习实训和人才交流，形成“产学研用”协同的人才培养链条。

——空间运营方应构建多元化经费保障与激励体系，通过政府专项资助、生态合作分润、平台服务收费、生态基金等方式筹措运营经费，在合约或股权层面设计合理的收益分配与股权激励机制，吸引并留住优质生态主体与核心人才

6.8 其他支撑能力

除了已覆盖的六大板块之外，为了更全面支撑可信数据空间的可持续运营，还可考虑以下支撑能力建设：

6.8.1 财务与预算管理

——预算编制与成本控制：空间运营方应建立基于项目和部门的年度预算编制流程，落实成本中心管控，并定期对预算执行情况进行对比分析，及时调整资金投放策略。

——收益与投资回报分析：应设计数据产品及服务的收益模型，定期开展投资回报率（ROI）评估，为后续资源配置和定价调整提供依据。

——多元化融资渠道：除政府专项资金与平台服务收费外，可引入风险投资、生态基金、行业合作资助等多渠道资金，确保运营弹性。

6.8.2 客户服务与运维支持

——用户接入与培训：为不同类型的生态主体提供分级培训与认证，帮助其快速理解平台功能、接口规范及合规要求。

——服务台与工单体系：应建设 7×24 小时客户支持系统，提供疑难解答、故障处理及技术咨询，并对工单响应时效、解决率设定严格 SLA。

——社区与生态活动：通过线上论坛、技术沙龙、黑客马拉松等形式，促进开发者与用户社区的互动，激发创新案例和二次开发。

6.8.3 市场与生态推广

——品牌建设与宣传：制定统一的品牌视觉与传播策略，通过白皮书、行业峰会、媒体合作等渠道扩大影响力，吸引更多优质生态主体。

——合作伙伴管理：应建立合作伙伴准入与评估体系，对技术厂商、行业联盟、科研院所等合作方进行资质与效能评估，并设立合作激励或认证计划。

——生态激励机制：可通过联盟积分、星级资质、联合创新基金等奖励方式，鼓励生态主体持续贡献高质量数据资源、产品和服务。

6.8.4 法律合规与政策协调

——动态法律监测：应设立专门团队或外包机构，持续关注国家及地方数据安全、隐私保护、跨境流动等政策法规，及时更新内部规范。

——合规培训与审计：定期对平台及生态主体开展合规教育，并组织内部或第三方合规审计，确保政策落地执行。

——政策协同：与政府主管部门保持定期沟通，参与相关标准与指导文件的制定，争取更多政策支持和先行先试机会。

6.8.5 创新与研发管理

——技术预研与试点：应规划技术预研项目，如可信执行环境、密态计算、数据标签与溯源新技术，并在小范围场景试点验证。

——产品迭代与版本管理：建立产品迭代节奏与质量闸门，平衡稳定性与创新速度。

知识产权与标准输出：对平台及生态创新成果进行专利或著作权保护，并将可复用的规则、模板或接口上升为行业或国家标准。

7 场景应用

7.1 概述

本章规定了可信数据空间在场景应用层面的能力要求，包括场景发现与价值规划、多主体协同与职责分配、数据供给侧匹配、数据交易与合约管理、数据产品化和服务化、场景数据产品与服务运营、价值衡量与收益清算、反馈改进与能力迭代和跨场景经验沉淀与推广等方面。

7.2 场景发现与价值规划

——空间运营方应构建多元化场景发现机制，综合运用政策研判、行业调研、自主申报、数据使用行为洞察与 AI 辅助分析等方法，持续挖掘企业级、行业级、城市级、个人级及跨境等不同维度的高潜价值应用。空间运营方应将识别结果纳入场景备选池，并基于数据禀赋、业务紧迫度与公共价值等因素，对候选场景进行系统分类与分级，形成包含场景名称、所属领域、预期价值及优先级的书面场景目录。

——对于纳入场景备选池的用例，空间运营方应在立项前开展“需求—痛点—价值链”三维分析：首先应梳理场景主体的业务或公共需求、现有困境及协同方式；其次应明确数据获取、加工、流通与应用各环节的参与方和增值节点；最后应量化评估场景用例的经济收益、社会效益与数据安全成本，并形成场景用例的商业模式蓝图与风险画像，为场景启动和优先级排序提供科学依据。

——在完成三维分析后，空间运营方宜编制场景价值规划书，对场景目标、关键里程碑、KPI 指标、所需资源、合规边界及退出条件等进行详细规划。规划书应经数据提供方、数据使用方、监管方及其他主要利益相关方联合评审后方可生效，并在项目推进过程中根据实际进展和风险变化，定期组织评审会对规划书进行复核与更新。

——空间运营方应在场景立项阶段同步开展合规审查，对涉及公共数据、个人信息或跨境流转的场景，必须依照网络安全法、数据安全法、个人信息保护法及关键信息基础设施安全保护条例、跨境数据管理规定等对数据来源、使用目的、处理方式、存储期限等关键环节完成合法性和安全性评估，特别关注涉及敏感信息（如个人隐私、商业秘密或国家重要数据）的场景；并将合规审查报告、发现的问题清单、整改措施及最终批准记录完整存档；情形复杂或影响范围较大时，宜委托具有资质的第三方机构开展专项合规评估。

——空间运营方应采用“计划—执行—检查—处置”（PDCA）闭环方法制定场景实施路线图，明确每一阶段的目标、关键里程碑、资源投入、责任主体和评估节点，并将阶段性成果与风险控制要求集成至管理体系，确保在执行中能够及时发现偏差并采取纠正措施。

——空间运营方应对场景全生命周期内的技术风险、运营风险和合规风险进行识别、定量评估与分级管理，针对高风险环节制定详细应急预案，明确触发条件、处置流程和责任人；对于判定为高风险的场景，应定期组织应急演练，并建立事故溯源与责任追责通道，保障在突发事件中能够快速响应与恢复。

——为促进多方高效协作，空间运营方宜建立常态化沟通与决策协同机制，包括定期协调例会、问

题受理与跟踪流程以及争议调解渠道，并对沟通记录、决策过程及共识结果进行系统归档，以便后续审计与绩效评价。空间运营方应通过该机制及时汇集各方需求与反馈，为场景优化与扩展提供持续动力。

7.3 多主体协同与职责分配

——空间运营方宜发布多主体协同指南，对场景中各生态主体的职责边界、沟通流程、冲突预警与解决路径做出操作性规定，并明确以下事项：各角色的名称、定位、权限与责任清单；协同决策的流程节点、决策投票机制与记录归档要求；冲突或异议触发条件、升级路径与仲裁流程；协同效率评估指标（如决策时效、事项闭环率、满意度）及评估周期等。

——空间运营方应建立协同机制。聚焦技术运维、身份认证、合约执行与审计等基础能力，空间运营方应通过自动化运维平台、统一身份管理系统和智能合约引擎，实现对各方接入、调用与行为的实时监控与自动化合规检查；聚焦数据策略、定价模型、合规规则与争议仲裁等治理能力。

——空间运营方应维护协同角色名录，并与身份管理系统联动，将角色与权限、合约模板和审计要求映射，实现“人—职能—系统—合约—审计”一体化治理。

——空间运营方宜组织定期跨域联席会议或工作组，邀请数据域负责人、技术运维、法务合规及监管代表参与，联合评审协同效果和风险事件；对于会议形成的重要决策和行动项，空间运营方应在会议后一定时间内下发执行通知，并跟踪闭环。

——空间运营方可借助协同治理平台或专用工具，对协同流程、任务分配、事件工单和决策结果进行在线化管理，并通过数据驱动的方式对协同效率、合规执行和风险趋势进行量化分析，不断优化多主体协同模式。

——空间运营方可以业务域为边界划分数据域，明确各域内的数据产品责任制，并指定域内数据产品负责人，对本域数据资产的质量、可发现性、可复用性以及持续演进负责。数据产品负责人应具备跨学科沟通能力，定期组织域内利益相关方评审数据产品路标和变更需求。

7.4 数据供给侧匹配

——在完成场景需求分析后，空间运营方应建立数据供给侧匹配清单，通过统一的资质审核流程对潜在数据提供方进行审查。资质审核至少包括法人及资信信息、数据合法来源声明、数据安全管理体系、技术交付能力以及历史合规记录等内容。未通过核验的主体不得纳入参与名单，审核结果应留档备查。

——数据提供方应按照空间运营方发布的数据分类分级规则，对其拟供给的数据资源进行类别标识和敏感等级评定，并完成权属确认、使用授权范围说明及元数据登记。元数据登记至少应覆盖数据标识符、来源与生成时间、数据格式、更新频率、质量状态、合规限制及联系方式等字段，以支撑后续自动检索与精准匹配。

——空间运营方应建设统一的数据资源目录服务平台，通过标准化接口与可视化工具实现多维检索、过滤、预览与订阅功能。目录条目应保持与数据提供方元数据的实时或准实时同步更新，并支持基于 API 的跨空间对接能力，提升资源发现效率与互联互通水平。

——当场景涉及跨行业、跨区域或跨境数据供给时，空间运营方应在供需撮合之前完成数据出境安全评估、数据权属与属地监管要求梳理，并制定风险缓解措施和数据流转管理预案。预案应明确数据流转路径、加密与存证策略、合规审批流程及各方责任划分，确保数据跨域流动合法、可控和可追溯。

——在数据供给侧匹配完成后，空间运营方宜与数据提供方签署框架合约或合作意向书，明确数据提供范围、质量基线、更新周期、价格区间、保密义务及违约责任等条款，为后续供需撮合与数据流通奠定制度和法律基础。

——空间运营方应针对不同的应用场景构建覆盖场景内数据的全生命周期的安全框架，包括数据分类分级、加密传输存储、访问控制、脱敏处理、安全审计等能力，并与国家及行业安全标准对齐。

7.5 数据交易与合约管理

——空间运营方应建立统一的身份认证与授权机制，对数据提供方、数据使用方、数据服务方以及监管主体进行多因素身份验证，并结合数字证书、密钥管理和访问控制策略，实现分级授权和动态权限调整。认证与授权日志应全程留存，任何主体身份变更或权限撤销均需同步至撮合系统，确保各方接入的可信性与可追溯性。

——空间运营方应配置可扩展的供需匹配引擎，在数据类型、数据质量等级、时效要求、价格区间、合规标签、使用场景等多维度条件下实现自动撮合。匹配引擎的算法规则应保证公开、可解释与可验证，算法更新需记录版本信息并向相关方通报；对匹配失败的请求，系统宜提供可操作的改进建议或备选方案。

——撮合达成后，空间运营方应基于可追溯的数字合约（如智能合约或链上合约）生成交易协议，明确数据使用范围、时限、地域限制、再分发权限、数据安全责任、收益分配机制以及违约处理流程。数字合约元数据应写入不可篡改的存证系统，并与实时监控策略联动，在检测到超范围调用、未授权派生或数据泄露风险时自动触发告警和处置流程。

——当场景涉及高度敏感数据或需求频繁变动、算法难以短时适应的情况时，空间运营方可启用人工协同撮合或混合撮合模式。该模式下，系统应先进行初步自动匹配，再由具备相应资质的业务与合规专家进行复核、风险评估与人工确认，最终生成复核报告和合约补充条款，实现机审与人审的有效互补。

——空间运营方应建立撮合过程全链路的审计与统计功能，对匹配请求、算法决策、合约生成、履约状态以及异常事件进行实时记录和周期性分析。审计结果宜用于优化匹配算法、调整数据价格策略、改进合约模板，并为生态主体提供决策支持和风险预警。

7.6 数据产品化与服务化

——数据开发方应支持将已处理的数据资源封装为数据产品或服务，形成标准化的交付单元。封装方式应至少覆盖批量文件、数据流接口、查询型 API、模型即服务（Model-as-a-Service）和复合服务等形态，满足不同业务场景的对接需求，并提供统一认证、鉴权与调用控制机制。

——每一种数据产品应随附完整的机读元数据和产品信息说明，包括但不限于唯一标识符、产品名称、数据来源与加工链路、适用范围、版本号、依赖关系、质量等级、合规标签、服务等级协议（SLA）范围以及定价策略。空间运营方宜采用开放数据描述语言（如 DCAT、OpenAPI 或自定义 JSON-Schema）进行元数据建模，以便跨系统自动解析与联邦检索。

——数据开发方应协同空间运营方建立数据产品与服务接口规范，明确通信协议、参数格式、分页与过滤规则、错误码、速率限制、认证方式以及安全加密要求。接口规范更新时，空间运营方应同时发布迁移指南和兼容性说明，保证现有调用方在过渡期内的业务连续性。

——空间运营方应实施数据产品生命周期管理机制，覆盖产品发布、灰度上线、版本迭代、下线与存档等阶段。管理机制需规定产品维护责任、更新频率、兼容策略、变更通告时限和退役流程。下线或重大版本升级前，空间运营方宜至少提前一个完整计费周期向所有使用方发出通知，并提供存量数据迁移与备份方案。

——空间运营方宜为数据产品和服务提供可配置的运行监控与计量计费功能，实时记录调用量、延迟、错误率、合约限额使用情况及费用明细；监控数据应与合约和收益分配系统联动，支持异常调用告警和按需扩容。

——针对机器学习模型、算法组件或其他复合型产品，空间运营方可提供隔离的在线测试环境或沙箱，允许数据使用方在真实或合成数据上验证效果、性能和兼容性。测试环境应复制生产级安全与合规策略，防止未授权数据泄露，并在测试结束后自动清除临时数据。

——为了促进产品复用与生态繁荣，空间运营方宜建设数据产品与服务目录门户，支持搜索、分类浏览、数据产品详情展示、标签过滤、订阅通知、用户评价、示例代码和快速接入向导。目录门户应与身份认证、计费结算及技术支持工单系统无缝对接，为生态主体提供一站式集成体验。

7.7 场景数据产品与服务运营

——空间运营方应将供需撮合达成的数据交付结果沉淀为场景专属的数据产品或复合服务，并为每个产品或服务应设立专门的产品运营团队，明确团队职责包括产品版本发布管理、灰度发布与回滚策略、下线与退役流程，以及对外用户沟通与教程更新。

——空间运营方应为每项场景数据产品搭建运行监控与自助服务仪表板，至少公开调用量、错误率、平均延迟、并发连接数与合规告警等关键运行指标，并支持域内用户自助订阅、告警阈值配置与报告导出。对于出现性能或合规异常的产品，运维团队应在指定时间内启动应急处置流程，并在仪表板中实时显示事件状态与恢复进度。

——当场景数据产品需跨域调用或被多业务域共享时，空间运营方应实现统一身份管理与跨域细粒度权限控制；对涉及多域协同计算的场景，空间运营方宜提供联邦学习、可信执行环境（TEE）或安全多方计算（MPC）能力，使各参与方在数据不出域的前提下实现模型训练与推理。

——空间运营方可为场景数据产品提供自动化测试脚本库、领域 SDK、CI/CD 流水线模版及质量闸门插件，使领域团队能够在提交更改时自动完成功能验收、性能基准与安全扫描，确保持续交付过程的高效性与可靠性。

——空间运营方应与产品使用方签订明确的服务等级协议（SLA），包括可用性、最大容忍响应延迟、数据准确率以及合规性审查通过率等指标，并在仪表板及电子邮件中周期性发布 SLA 达成情况，对未达标事件应执行信用扣减或补偿机制。

——空间运营方应建立完善的产品事故管理与用户支持流程，当用户通过工单、在线反馈或监控告警报告问题时，运维团队应在预案要求时间内提交解决方案和恢复业务可用，并开展根因分析与渠道通报。

——空间运营方宜定期（建议至少半年一次）基于用户使用数据与反馈，对场景数据产品与服务进行迭代评审，识别功能优化需求、安全隐患与性能改进点，并将优先级高的改进事项纳入下一个版本发布计划，以持续提升产品价值与用户体验。

7.8 价值衡量与收益清算

——空间运营方应建立统一的数据价值评估模型，对进入流通环节的每项数据资源、数据产品或数据服务进行定量估值。价值评估模型应综合数据质量等级、完整性、稀缺性、时效性、覆盖范围、需求强度、潜在衍生能力以及历史交易表现等因素，并结合行业基准及宏观市场波动进行动态校正。模型的算法逻辑、参数来源及更新频率应形成文档并向生态主体披露，以保证评估过程的可解释性和可验证性。

——空间运营方宜将价值评估模型划分为“交易前估值”和“交易后溢价”两个阶段：交易前估值用于指导价格谈判、供需撮合和保证金计算；交易后溢价用于衡量数据实际使用效果并回溯调整收益。对于算法驱动的动态定价场景，空间运营方应保留估值输入数据、运行日志与版本号，支持事后审计溯源。

——收益分配规则应遵循“贡献决定报酬”的原则，结合数据提供量、质量贡献度、加工增值比例、模型效果增益以及风险承担情况等维度，确定各参与方的收益系数；空间运营方应在数字合约中明示计算公式、分配比例、结算周期与违约金条款。合约生效后，任何收益分配参数的调整应获得受影响方明确同意并记录补充协议。

——空间运营方宜建立与协同角色强关联的激励体系，针对不同主体特征（数据提供方、使用方、服务方、监管方等）不同的动机和贡献点，差异化设计激励机制。设计阶梯式奖励、持续贡献奖励和惩罚机制，动态调整积分系数或新增奖励类别。通过将正向激励与职责约束相结合，形成“贡献可量化、权益可预期、违规必追责”的闭环体系，确保多主体在明确权责边界的基础上，持续获得协同价值创造的内生动力。

——中间服务平台应具备清算功能，实现收益结算、成本与手续费扣除、税费计提、跨币种结算与资金兑付等功能。清算系统需支持与区块链或金融机构网关对接，确保资金流与数据流、合约状态保持一致；清算周期不宜超过一个自然月，特殊情况需在合约中约定延时清算机制。

——在清算执行过程中，空间运营方应对收益分配明细、资金流向、税费扣缴记录及外汇管理凭证进行加密存证；当合约金额达到监管阈值或触发风控策略时，系统应自动生成合规报告并向指定监管节点推送。

——为保证收益透明，空间运营方宜为各参与方提供实时或准实时的收益仪表板，并按月生成正式收益报表。报表应至少包含结算区间内的调用量、单位价格、应收收入、费用与税费扣减、最终分配金额及账户余额变化等字段；报表接口应支持第三方审计机构或监管部门基于 API 获取。

——当收益分配或清算结果出现重大争议，各参与方申请运营者介入处理时，运营者应按照合约约定以及所制定的纠纷解决机制的争议解决流程受理申请；如协商未果，提请外部仲裁/诉讼机构处理的，仲裁/诉讼期间，运营者应对争议金额进行资金冻结，直至仲裁/诉讼结论生效后再行拨付。

——空间运营方宜定期（至少每年度一次）对价值评估模型、收益分配策略和清算流程开展绩效评估和风险复盘，结合市场变化、监管政策及生态主体反馈持续优化；对复盘中发现的模型偏差、分配不公或清算失误应制定整改计划并在一个清算周期内完成修正。

7.9 反馈改进与能力迭代

——空间运营方应建立多渠道反馈收集机制，通过定期问卷调查、在线工单、用户访谈、日志分析和自动化监控等方式，全面收集数据提供方、使用方、服务方及监管方对场景实施效果、合约履约、技术稳定性和风险事件的反馈，确保各类运营数据与用户体验信息及时汇总。

——空间运营方应定期召开反馈评审会议，基于收集的反馈信息对照场景预设的关键绩效指标（KPI）和风险管理指标开展综合分析，形成评估报告，明确改进需求与优先级，为流程优化、合约修订和技术升级提供决策依据。

——在评估报告基础上，空间运营方应对业务流程、撮合规则、数据预处理策略、价值评估模型、收益分配机制和清算流程等进行条款化修订，并同步更新系统配置与技术文档，确保改进措施通过版本管理系统发布后能够被快速采纳与执行。

——空间运营方宜建设统一的知识库和在线协作平台，对典型问题案例、改进方案、最佳实践以及版本迭代记录进行分类沉淀，并通过内部培训、操作手册和示例演练等方式，促进生态主体对新能力与新规范的理解与应用。

——空间运营方可设立能力迭代指标，对改进措施的执行效果和运营风险趋势进行跟踪，对效果显著或风险降低的改进项目予以重点推广，并在必要时将成功实践纳入标准化提案或行业白皮书，形成持续优化与价值提升的良性循环。

7.10 跨场景经验沉淀与推广

——空间运营方应对已验证成功的应用场景开展系统化复盘，形成涵盖需求识别、供给匹配、撮合流程、预处理策略、产品化方案、价值评估与清算等环节的通用化模板与标准化组件，并编制成可机读的场景实施指南与脚本库，为后续类似项目提供“一键化”启动能力。

——空间运营方应建设集中化的跨场景经验推广平台，支持对场景模板、数据产品、服务接口和技术组件的多维度检索、订阅、版本管理和兼容性标注，确保不同生态主体在新业务环境中能够快速集成并保持功能与合规一致性。

——各类生态主体，包括数据提供方、数据使用方和数据服务方宜在推广平台中登记其可复用的资产或方案，并为每项资产提供完整的元数据说明、质量报告、合规凭证和案例演示；当资产发生更新或修订时，主体应及时同步变更记录，保障平台信息的时效性与准确性。

——空间运营方宜制定跨场景复用评估指南，明确场景适配度、开发成本与收益预期、技术兼容性和合规风险等评估指标，并提供标准化评估工具或流程，帮助生态主体在启动新场景时快速判断所选资产或方案的可行性与潜在改造成本。

——跨场景推广过程中产生的反馈信息，包括合约执行偏差、收益分配争议、风控事件、接口兼容异常、性能瓶颈等，空间运营方应纳入规则机制与技术系统迭代的闭环之中，及时更新身份认证策略、合约模板、撮合算法、接口规范及语义模型，确保推广资产在多场景下持续可靠运行。

——空间运营方应结合跨场景推广需求定期组织技术沙龙、研讨会或在线培训，邀请各生态主体共享复用经验、碰撞创新思路，并将优选成果纳入标准化提案或行业规范，逐步推动形成行业共识与生态合规标准。

——空间运营方宜为核心复用资产配套发布 API 和 SDK、示例代码、测试工具或沙箱环境，降低新场景接入与功能验证的技术门槛；对接入效果良好且推广广泛的高价值资产，空间运营方可提供标识认证或优先支持，进一步激励生态主体贡献优质方案。

——空间运营方可协同标准化组织和行业联盟，将跨场景推广中的成熟模板、组件和最佳实践上升至国家或行业标准，同时为参与方提供标准化培训与认证服务，以提升全行业对可信数据空间能力要求的理解与执行一致性。

8 数据资源

8.1 数据资源概述

在可信数据空间中，数据资源应当按照“接入—处理—使用—沉淀”四阶段构建全生命周期价值链，并贯穿动态治理机制，以保障数据要素的合规流通与价值释放。接入阶段先行开展标准化清洗与合规校验，验证数据合法性和质量后，依约签署数字合约并将数据接入底层架构；处理阶段对接入数据进行发布登记、元数据标注与分类分级，采用分析、建模等技术手段生成可调用的数据产品和服务；使用阶段允许数据直接驱动业务决策或作为数据产品与服务开发的输入，实施访问控制与使用审计，确保与合约约定一致；沉淀阶段在使用期满后，根据合同条款安全销毁或归档数据，并通过结算与核算形成交易闭环，同时将经验证的高价值模型、算法、指标等成果纳入共享目录，形成可复用的数据产品或服务。在全流程中，需嵌入机器可读合约管理（包括权责边界、合规规则与动态更新机制）、端到端溯源审计、价值评估与经济贡献量化，以支持“可管控、可追溯、可评估、可审计”的数据资源可信流通和价值创造的目标。

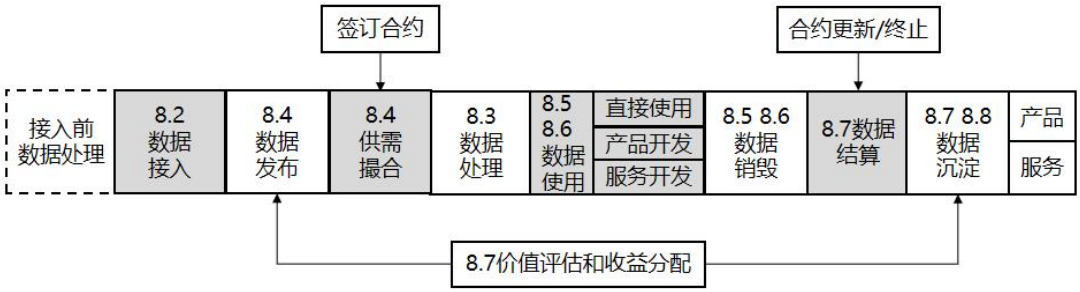

图 2 可信数据空间全生命周期价值链流程图

8.2 数据接入与登记

8.2.1 数据接入

——应支持不同类型数据接入，包含但不限于数据资源、数据产品和服务等，且应覆盖文件上传、API 拉取、流式推送和数据库直连等多种方式。

——宜定期评估并扩充接入类型、格式与转换范式。

8.2.2 数据登记与审核

——应在数据接入后开展登记流程，将数据提供方信息（主体名称、资质证书编号）、数据来源说明（采集方式、时间、地点）、数据类型与格式、元数据清单、权属与使用许可、数字合约编号等信息完整记录，并存入数据资源目录。

——应建立数据负面清单管理机制，并在接入登记环节采用自动化规则和人工校验相结合的审核流程，以确保接入数据不含负面清单所定义的敏感或违规内容，以及不违反国家法律法规（包括但不限于危害国家安全、主权、领土完整、民族团结、社会稳定、公序良俗等规定）。

——应在数据接入前利用自动和人工相结合的手段进行审核，一旦审核不通过，系统应自动阻断数据接入并生成整改工单。

——宜对复杂或高风险场景委托资质机构开展专项合规评估。

8.2.3 数据标识与分配

——应为每条通过审核的原始数据分配全球唯一标识（GUID），标识应基于统一的标识体系（如 Handle、OID、GS1 等），并具备多级解析与校验能力。

——标识映射的解析节点和模式应支持递归查找与容灾切换。

——所有标识分配与解析操作应记录审计日志，并纳入平台统一监控与追溯体系。

8.3 数据处理

8.3.1 数据清洗与标准化

——应结合业务语义与场景需求，制定清洗与标准化规则，明确数据字段含义、结构约束和格式要求。

——在处理接入数据前，可信数据空间运营方应先行进行全量或增量备份并完成备份验证。

——在清洗过程中，系统应自动执行去重、格式转换、空值处理、异常值检测与语义对齐等操作，并在关键步骤生成、存储相应审计日志与变更记录，以支持断点检查与回溯。

——清洗与标准化完成后，可信数据空间运营方应对数据的完整性、准确性、一致性和标准化程度开展自动化验证。

8.3.2 数据分类与分级

——应定期开展全量数据资源盘点，识别敏感数据并输出数据资源目录。

——应建立统一的数据分类与分级规范，明确分类方法、分级清单与保护措施，并为各数据项添加标准化标签，纳入元数据管理索引。

——针对不同安全等级的数据，可信数据空间运营方应实施差异化的加密、脱敏与访问控制策略，并依据预定周期对分级结果进行复评与调整。

8.3.3 元数据治理

——应实现元数据的自动化提取与结构化管理，支持结构化抽取数据资源的描述信息（包括数据结构、标签、来源、格式等）。

——应确保元数据在不同相关方、不同系统、不同数据源或不同业务场景间定义一致，并通过完整性校验与逻辑一致性检测保障元数据与实体数据的精确关联。

——元数据的披露范围与留存期限应符合法律法规要求。

——系统应支持基于血缘追踪技术回溯数据的来源、流转路径、加工过程及最终使用场景。

8.3.4 数据质量管理

——应依据相关标准（如 GB/T 36344-2018《信息技术 数据质量评价指标》）定义数据质量维度（完整性、准确性、一致性、及时性等）并制定校验规则。

——中间服务平台或用户节点应对数据自动执行相关检测，如合规检测、质量检测、安全检测等。

——对不满足质量标准的数据，可信数据空间运营方应预设修复策略（标准化转换、去重、缺失值插补等）并自动执行，随后对修复结果重新进行质量检测。

——对高频质量问题，系统应反馈给数据提供方并跟踪整改。

8.3.5 数据脱敏处理

——应根据数据类型与敏感度等级，选择替换、屏蔽、加密、泛化或抑制等脱敏技术，并为不同脱敏策略制定强度标准。

——在脱敏过程中，系统应实时记录关键信息并存储脱敏日志，以支持隐私保护验证与审计。

——脱敏后数据宜通过隐私保护验证机制（如 k-匿名、差分隐私），确保在满足数据可用性的前提下达到不可逆的脱敏效果。对需要做匿名化处理的数据，应符合匿名化效果评估要求。

8.4 数据发布发现

8.4.1 数据资源目录描述信息

——应为所有已处理且可流通的数据资源建立统一的目录条目，每条目录应至少包括：资源名称、全局标识符、所属主体、业务描述、数据格式、采集来源、更新频率、行业分类及合规标签。

——应支持目录条目的扩展字段，包括但不限于质量等级、敏感度分级、地域范围及订阅价格区间。

——应在目录中展示资源内容的字段级描述，涵盖字段名称、数据类型、语义说明及示例值；同时应提供挂载视图，展示该资源对应的表、文件或其他数据对象与目录条目的映射关系。

——宜为关键资源或高价值资源设置标签或关键词，支持基于标签的快速检索与聚合展示；可允许生态主体自定义标签，并对标签使用情况进行动态统计。

8.4.2 数据产品目录描述信息

——应为所有场景数据产品与服务建立产品目录条目，每条产品应至少包括：产品名称、产品标识符、提供方、功能简介、产品类型、行业应用场景及合约许可信息。

——应在目录中展示产品的使用限制信息，包括更新频率、调用边界（如访问时间段、频次限额、地域限制）与可授权操作；宜提供示例调用代码或接入文档链接。

——宜展示产品的上游数据资源信息，列明生产该产品所依赖的数据资源名称、标识与版本，并支持一键跳转至资源目录查看详情。

——宜为产品目录提供质量与价值参考模块，包含质量评估报告、价值评估结果、用户评分及使用案例，帮助使用方进行决策。

8.4.3 目录发布与上架流程

——数据提供方或产品方应通过中间服务平台提交目录上架申请，提交内容应包含目录类型（资源/产品）、名称、标识、计量方式、定价策略、交付方式及合规声明等核心信息。

——空间运营方应对上架申请进行形式与实质审核，包括合规审核、技术接入审核等，并在规定期限内完成审批；对不符合要求的申请应明确驳回理由并指导整改。

——上架通过后，目录条目应自动在平台检索引擎中生效。

——应支持按名称、标识、行业、分类、标签、合约类型等多维条件进行精准或模糊检索。

——应支持数据使用方在中间服务平台发布“数据需求”或“产品需求”公告，需求内容宜包含业务背景、数据/产品要求、时效性及交付方式等。

——平台宜根据需求自动推荐匹配的资源与产品，并反馈给需求方。

8.4.4 供需匹配与撮合

——应提供标准化的供需匹配服务，通过系统化的规则引擎或智能推荐算法，对接需求方发布的需求与目录中资源、产品进行多维度匹配，并输出匹配报告。

——供需匹配应至少基于数据类型、质量等级、更新频率、价格区间、合约条款相容性及使用场景等维度进行自动化匹配，匹配结果应按优先级排序并向需求与供给双方呈现。

——对于匹配度较低或算法难以覆盖的复杂需求，可支持人工协同筛选与复核，结合专家评审或工作坊形式，生成定制化推荐方案。

8.5 数据产品研发与封装

8.5.1 数据产品研发流程

8.5.1.1 需求分析

——应组织各利益相关方共同开展需求调研，完整搜集场景需求、用户功能需求、系统非功能需求

及合规约束，明确场景边界、使用模式与性能指标。

——调研结果应整理为需求规格说明书，详细描述功能点、接口定义、数据格式、访问频次及性能目标。

8.5.1.2 方案设计

——应根据需求规格说明书进行整体架构设计，明确技术选型、模块划分、数据流转与接口协议。

——应编制安全设计方案，涵盖访问控制、加密算法与审计策略。

——设计过程应遵循行业标准和企业内设计规范，保证可维护性、可扩展性与高可用性。

8.5.1.3 产品开发

——应制定并执行统一的编码规范，包括命名规则、注释格式和提交规范。

——应使用版本控制系统管理代码、文档及配置，确保可追溯性。

——常用功能或逻辑应封装为可复用组件或库，并通过单元测试和静态代码检查验证质量。

——宜基于可信集成框架接入“数据可用不可见”技术，合理加工敏感数据并按策略对外提供脱敏或汇总结果。

8.5.1.4 验证测试

——应制定全面测试计划，覆盖功能测试、性能测试、安全测试、兼容性测试及容错测试。

——应利用自动化测试工具执行测试用例，确保覆盖率达到既定要求并修复发现的问题。

——产品发布应采用灰度发布与回滚机制，发布流程和版本变更应纳入变更管理和审计体系，确保线上环境稳定可靠。

8.5.2 数据产品封装技术

8.5.2.1 语义封装

——应支持构建顶级本体，实现最基本的类别和关系，比如时间、空间、实体、属性、事件、过程等。

——宜结合应用域规划领域本体并支持属性继承，确保数据模型在多场景下的一致性与可扩展性。

8.5.2.2 安全增强

——应支持通过加密技术保障数据传输安全，实施精准授权和精细授权访问控制策略，利用区块链技术增强数据的透明性与不可篡改性。

8.5.2.3 可信存证

——应提供插件式存证接口，支持多种第三方存证服务（包括但不限于国产可信执行环境、区块链平台），并依据场景需求自定义存证策略，以满足不同安全与合规场景的证据保全要求。

8.5.2.4 互操作接口

——应支持语义互操作模型与数据目录、数据标识等模块进行集成交互，并具备跨域互认的语义信息模型建模、描述和解析能力。

——宜支持建立统一策略、信任机制、算法协议及接口规范的互认互信体系。

8.5.3 数据产品质量保障

——应提供完备的技术文档、在线帮助与培训资源，建立客户支持工单系统，明确响应时限和处理流程，确保用户问题能够在规定时间内得到解决。

——应定期开展静态代码审查与性能基准测试，对关键路径和热点接口进行压力测试与资源监控，并针对发现的瓶颈或安全隐患及时优化和修复。

——应跟踪收集用户反馈与使用日志，结合数据分析和满意度调查，定期评估产品体验和业务价值，并将优先级高的改进需求纳入下一个迭代版本计划。

8.5.4 数据产品安全检测

——应支持数据源头安全检测，包括数据合规性验证、数据质量与完整性检测。

——应支持数据处理过程安全检测，包括隐私计算技术检测、算法安全检测、访问控制检测。

——应支持数据流通与交互安全检测，包括接口安全检测、数据共享合规性检测。

——宜支持系统与基础设施安全检测，包括平台安全评估、硬件与环境安全检测。

——宜支持合规性与法律风险检测，包括法律法规适配性检测、伦理风险评估。

8.6 数据服务与交付

8.6.1 服务接口标准化封装

——应采用统一的接口标准进行封装，确保不同数据服务接口在结构、参数格式、调用方式等方面的一致性。

——应具备清晰明确的接口文档说明，涵盖接口功能描述、输入输出参数定义、调用示例等内容，方便第三方快速理解与使用。

——应支持身份认证和访问控制，只有经过授权的第三方才能调用数据服务接口，且访问权限应根据第三方的角色和业务需求进行精细化配置。

——应支持多种数据传输协议，以适应不同第三方的技术架构和网络环境。

——应具备接口版本管理能力，对接口的更新和变更进行版本标识，确保第三方在接口升级时能够平滑过渡，不影响正常业务使用。

——接口应具备数据格式转换功能，能将内部数据格式转换为符合第三方需求的数据格式，实现数据的无缝对接。

8.6.2 可信交付协议与机制

——应采用符合国家相关标准和行业最佳实践的加密协议，对传输给第三方的数据进行加密处理，防止数据被窃取或篡改。

——应建立数据完整性校验机制，在数据传输前后对数据进行校验，保证第三方接收的数据与发送方的数据一致。

——应具备不可抵赖机制，利用数字签名等技术，确保数据服务交互过程中各方行为可追溯，任何一方无法否认其操作行为。

——应制定明确的服务级别协议（SLA），规定数据服务的可用性、响应时间、数据准确性等关键指标，并提供相应的监控和报告机制。

——应支持隐私保护计算协议（包括多方安全计算、可信执行环境、密态计算等），在涉及数据联合计算、开发场景下，保障参与方不能在非授权的情况下获得数据，按照约定范围、用法来使用数据，防止数据泄露和不当使用。

——应建立异常处理与应急响应机制，当数据服务交付过程中出现网络故障、数据错误等异常情况时，能及时通知第三方并采取相应措施。

8.6.3 服务化质量控制

——应建立服务质量指标体系，涵盖数据准确性、数据完整性、服务响应时间、服务可用性等关键指标，明确各指标的量化标准。

——应对数据服务进行实时监测，收集服务运行数据，根据指标体系评估服务质量，及时发现潜在的质量问题。

——应具备服务质量预警功能，当服务质量指标接近或超出设定阈值时，自动发出预警信息，通知相关人员及时处理。

——应建立服务质量问题处理流程，针对出现的质量问题，迅速定位原因并采取有效措施进行整改，记录处理过程和结果。

——应定期对数据服务质量进行评估总结，分析质量趋势，为服务优化提供依据，持续提升服务质量，满足第三方的业务需求。

8.7 数据价值评估与生命周期管理

8.7.1 数据资源价值评估模型

——应基于成本法、收益法、市场法等多种评价方法，结合数据质量、稀缺性、使用频次、衍生能力和市场需求，构建数据资源价值评估模型，并对模型的输入因子、算法逻辑和输出结果形成完整文档。

——评估模型应采用回归分析、因子分析、层次分析法或机器学习方法等数理统计与智能算法，支持对不同类型数据资源价值进行定量或半定量分析，并能按需灵活组合多种模型。

——运营者应定期对评估模型进行校准和回溯验证，分析模型误差与偏差，并依据市场反馈与生态贡献度动态调整模型参数，确保评估结果的客观性与准确性。

8.7.2 数据资源用后质量评价

——应建立数据资源使用后质量评价机制，从准确性、完整性、一致性、时效性、可用性等维度，对已提供的数据资源进行回溯评估，并形成数据质量分析报告、数据画像等。

——在质量回溯机制中宜增加数据沉淀准入规则，确保只沉淀高质量、合规的数据。

——应实时监控数据使用过程中产生的质量指标和异常事件，利用监控工具自动发现并记录质量偏离，生成质量告警并触发预设的处置流程。

——宜将用后质量评价结果和使用方反馈纳入定期评审，形成改进建议和优化措施，及时反馈数据提供方，并跟踪改进结果，推动数据质量的持续提升。

8.7.3 数据资源生命周期管理

——应为每类数据资源制定生命周期策略，明确从采集、登记、使用、更新、归档到销毁的各阶段管理要求和触发条件，并在数字合约中固化。

——对于超出使用期限或价值评估低于阈值的数据资源，应按合约约定或管理策略执行归档或安全销毁，并将销毁日志或归档记录写入审计系统。

——应在生命周期管理系统中记录每一次资源状态变更，并提供查询接口，以支撑端到端可追溯与合规审计。

——宜依据生命周期管理数据，开展定期盘点与报告，评估资源存量、使用效能和价值贡献，为后续资源整合与优化提供决策依据。

——应在数据生命周期末期（如使用期满、归档、销毁、结算），对数据资源或数据产品和服务进行沉淀管理，包括成果转化与共享等。

8.8 数据资源体系构建

8.8.1 基础科学数据集管理

——应按照国际或国家元数据标准统一定义科学数据集的元数据模式，涵盖数据集名称、版本、作者、采集方法、质量控制流程、许可证及引用方式等要素。

——应建立动态更新与长期维护机制，通过自动化采集接口和人工审核流程，保证科学数据集元数据和内容的时效性与完整性，所有更新记录和维护日志应纳入审计存证。

——宜通过脱敏技术和隐私计算手段满足合规共享需求，并结合数字合约与激励机制鼓励科研机构和企业开放高质量科学数据集。

——宜与 AI 大模型研发平台及隐私计算环境对接，支持科学数据集在安全可控的条件下用于模型训练与创新应用。

8.8.2 高质量语料库构建

——应建设覆盖文本、图像、音频等多模态并结合行业专业知识的语料库，明确语料来源、领域标签和质量评估标准。

——应实施多轮清洗与标注流程，包括自动化预处理、人工校对与交叉验证，确保语料噪声率低于设定阈值，并对标注质量定期抽样复检并发布质量报告。

——应支持在边界隔离或隐私计算环境中进行模型训练，确保原始语料不出域而模型参数可用于下游服务。

——宜提供语料库 API 接口，支持按场景分发、计量计费与版本管理，可结合市场化交易平台探索定价与激励机制，激活语料价值。

8.8.3 城市数据资源体系构建

——应整合政务、交通、医疗、环境等公共及企业数据，基于统一的行政区划与地理坐标体系构建城市级数据目录与数据图谱，保障数据格式与语义模型的一致性。

——应制定数据标识、接口协议与权限管理标准，支持数据实时更新与资源池化管理，对跨部门调用应实施统一身份认证与细粒度授权。

——应聚焦典型城市治理与民生场景，搭建开放平台吸引企业和研究机构协作开发应用，形成“政府+市场+社会”多元共治生态。

宜依托数字合约机制对公共数据进行授权运营，明确使用规则、收益分配与合规审计流程，推动城市数据资源的持续开放与价值回馈。

9 生态主体

9.1 生态主体的分类与定义

9.1.1 数据提供方

提供数据资源的主体，有权决定其他参与方对其数据的访问、共享和使用权限，并有责任在数据创造价值后，根据约定分享相应权益。

9.1.2 数据使用方

使用数据资源的主体，根据与可信数据空间运营方、数据提供方等签订的协议，按约定使用数据资源、数据产品和服务。

9.1.3 数据开发方

提供数据接入、数据治理、数据处理、数据分析、数据挖掘等数据相关技术服务的主体。数据开发方与数据提供方、数据使用方签订协议，根据协议提供技术服务，按约定分享相应的权益。

9.1.4 数据中介方

为数据提供方和数据需求方之间，提供数据对接、数据交易、数据流通等撮合服务的主体。数据中介方为数据提供方和数据使用方提供撮合服务，按约定分享相应的权益。

9.1.5 数据托管方

提供数据存储、运营、安全管理等运维运营服务的主体。数据托管服务方通过专业化的数据中心和运维团队，确保数据提供方数据的安全性和可靠性。

9.1.6 空间运营方

负责可信数据空间日常运维运营管理的主体，制定并执行可信数据空间运营规则与管理规范，促进参与各方共建、共享、共用可信数据空间，保障可信数据空间的稳定运行与安全合规。可信数据空间运营方可以是独立的第三方，也可以由数据提供方、数据服务方等主体承担。

9.1.7 监管方

履行可信数据空间监管责任的政府主管部门或授权监管的第三方主体，负责对可信数据空间的各项活动进行指导、监督和规范，确保可信数据空间运营的合规性和公平性。

9.2 生态主体和业务要求

可信数据空间的参与方活动生命周期涵盖了从主体接入到数据销毁的完整过程，确保各参与方在可信数据空间中的行为合规、透明、可追溯。在主体接入、数据接入、数据发布、使用、销毁等全生命周期中，应始终贯彻合规与安全要求，包括（但不限于）法律法规遵循、最小化收集与使用、隐私计算技术应用、安全审计与监管等。若涉及跨境数据流转，需要在生命周期的各环节执行额外的跨境合规审查、国际标准对接以及数据主权保护等流程。

9.2.1 主体接入

参与方首次进入可信数据空间时需进行主体接入，退出可信数据空间后清理相关的各类信息，包括如下业务活动：

——注册申请：参与方向可信数据空间提交主体的基本信息，通过可信数据空间中间服务平台申请注册，获得接入资格。

——身份验证：自然人主体需验证实名身份信息、法定范围内的数据处理权限；法人主体需提交工商信息、行业资质、法人授权、数据安全保障能力证明等。结合身份核验机制，空间运营方校对注册主体提交的核验材料真实性，确保参与方的身份合法、合规、真实，避免恶意主体的接入。宜建立参与主体黑名单与信用评分机制，若发现主体存在严重违规或失信记录，可暂停或禁止其接入可信数据空间。

——协议签署：可信数据空间运营方验证参与方的真实身份与提交基本信息符合可信数据空间主体接入规则要求后，与参与方签署协议，明确运营方与接入主体的责权利。

——分配主体标识：通过验证的参与方，由可信数据空间运营方分配可信的主体身份标识，确保后续可辨识、可追溯。

——主体退出：参与方向可信数据空间提交主体退出的申请，可信数据空间运营方审核通过后回收该主体的权限。

——主体身份清理：参与方退出可信数据空间后，空间运营方对主体的相关身份数据执行清理，避免数据误用。对于退出的主体，空间运营方应保留其关键操作日志与合约记录一定期限（如法律法规要

求的最短时限）以便后续审计与争议处理。

——授权托管：数据提供方授权合规的主体作为数据托管方，签署授权协议后，数据托管方协助数据提供方开展数据运营。

——接入认证：节点在首次接入可信数据空间时进行初始化静态认证及注册，完成注册后每次接入可信数据空间需要进行动态认证校验。

9.2.2 数据接入与治理

数据提供方将预处理后的数据正式接入可信数据空间，确保数据可用，包括如下业务活动：

——数据接入：数据提供方对于可由可信数据空间纳管的数据资源，通过数据接口、数据文件、数据表等方式，接入至可信数据空间节点内进行统一管理及维护。

——数据治理：数据提供方对原始数据进行清洗，应通过脱敏技术去除个人信息和敏感字段，构建数据质量报告，保证数据质量和数据安全要求。

——数据合规检查：可信数据空间运营方对数据资源进行合规检查，如数据权属关系、数据是否涉及敏感数据，确保数据接入符合法律法规和规范。应依据 GB/T 38636《数据安全能力成熟度模型》、GB/T 22239《信息系统安全等级保护》等国家标准对数据进行分级保护与动态风险评估。

9.2.3 数据发布与目录管理

数据提供方将数据资源发布至可信数据空间数据资源目录中，包括如下业务活动：

——数据上传：数据提供方将数据资源的元数据上传至可信数据空间中间服务平台数据目录，元数据格式需符合统一标准。并在元数据中标明数据的敏感等级、授权范围、可共享范围等信息，便于后续合规监管与审计。在数据资源元数据上传到数据资源目录之后，由可信数据空间中间服务平台发起数据资源质量检验，标记不满足质量要求的数据。

——分类分级：可信数据空间运营方对数据按照业务、技术等维度进行分类（如实时数据、月度数据）和分级（如普通数据、敏感数据）。

——数据权限控制：数据提供方对数据资源目录和数据资源进行权限控制，如向所有主体公开、向指定主体公开等。可根据用户角色、业务场景、行业监管要求等，采用差异化的授权策略；并可基于风险监控结果实施动态权限调整（如临时冻结高风险数据使用权限）。

——数据审查：可信数据空间运营方对申请发布的数据资源信息进行业务及合规性审查，如元数据是否符合要求，数据权属关系、数据是否涉及敏感数据，确保数据接入符合法律法规和规范。

——目录生成：数据提供方把由节点接入的数据，按照可信数据空间的数据标识、语义规范和格式要求，发布至可信数据空间并生成统一格式的数据资源目录，可信数据空间其他主体可检索、查看数据资源。

——数据资源目录管理：空间运营方根据可信数据空间数据资源目录规范，对数据资源目录进行管理。为了保障对数据资源的高效查询检索，数据资源目录维护应包括数据资源目录的层次设定，审核数据资源说明的真实准确等，宜支持多平台或多数据空间的目录协同机制，推动跨平台数据互认与检索。

9.2.4 数据需求匹配

数据开发方、数据中介方、数据使用方在可信数据空间中查找所需数据资源，包括如下业务活动：

——权限确认：根据数据使用方账号匹配访问权限，确保其仅能查询授权范围内的数据资源。可集成前置合规过滤与自动审批流程，对于包含个人敏感数据、国防安全、重要公共数据等需二次审批或高级别权限才可检索。

——数据查询：通过对数据资源目录的过滤、查询、排序等，检索符合条件的数据资源。

——数据预览：通过预览数据样本，了解数据资源的结构和内容。应采用可控预览方式（如局部样本、脱敏样本、结构化元数据信息等），避免过度暴露原始敏感数据。

——跨主体互认：可信数据空间运营方提供跨参与方的数据识别与互认服务，确保数据的可发现性和一致性。鼓励采用统一的元数据标准、数据标识和互操作协议，以便在不同行业或区域的主体间实现高效互认和协同。

9.2.5 供需撮合

数据中介方负责撮合数据需求和数据供应，可信数据空间运营方负责审核，促进数据高效流通，包括如下业务活动：

——需求发布：数据使用方根据对数据资源、数据产品或数据服务（如数据开发服务、数据中介服务、审计清算等）的需求，通过可信数据空间向所有主体发布。

——需求匹配：根据数据使用方的需求，可信数据空间运营方撮合合适的数据资源、数据产品或数据服务，保障供需双方有效对接。在撮合过程中，应自动检测数据需求方是否具备相应资质与权限，包括对数据类型、用途、跨境风险等进行自动化合规审查；若发现潜在风险，需人工复核或第三方介入。

——供需协商：供需双方对数据资源、数据产品进行沟通和协商，确定数字合约。

——合约签订：供需双方完成数字合约确认后，由可信数据空间运营方进行数字合约审核，审核通过后供需双方进行数字合约签订。签订完成后，可信数据空间中间服务平台部署数字合约，并存证记录。

——数据使用授权：通过数字合约实现数据需求与数据提供方的匹配，确保数据的合法共享。数字合约中应包含数据生命周期管理及销毁条款，对使用期限、存储方式、销毁时间等进行明确约定，避免数据被滥用或超期留存。宜优先采用多方安全计算、联邦学习等技术，以降低原始数据集中化带来的合规风险。

9.2.6 数据转换与处理

在可信数据空间中，数据使用方和数据开发方根据业务需求，对获取的数据资源进行必要的转换和处理，以支持数据的互操作性和价值提升，包括如下业务活动：

——数据转换：通过对数据格式、结构或语义的转换，确保来自不同来源的数据能够在可信数据空间中实现无缝集成。这一过程需要确保转换结果符合空间内的标准化要求，同时保持数据的完整性和一致性。在转换或合并数据时，可嵌入合规水印或可追溯标识，确保后续发生数据泄露或违规扩散时能够快速定位来源和责任方。

——数据处理：数据处理是基于业务需求对数据进行加工的过程。通过数据分析工具和算法，挖掘数据的潜在价值，生成可供后续开发使用的高质量数据产品。若使用人工智能或大数据挖掘算法，应进行算法合规与伦理审查，避免算法歧视、隐私侵害或越权分析，必要时需对算法模型进行可解释性与公平性评估。

9.2.7 数据传输与存储

数据传输与存储是可信数据空间中数据资源交付和管理的关键阶段，旨在保证数据在流转和存储过程中的安全性和可控性，包括如下业务活动：

——数据传输：数据提供方根据合约条款，将数据压缩、加密、签名处理后传输给经过身份验证的数据使用方或数据开发方。应依据《数据出境安全评估办法》等规定进行跨境传输安全评估或备案，确保境外接收方满足相关的安全保护水平。

——数据存储：数据使用方根据合约要求对数据进行加密存储，并采用分级分类的方式进行管理。优先采用符合国家商用密码管理规定或安全等级保护要求（如 SM 系列算法）的加密技术，满足数据在传输和存储过程中防篡改、防泄露的需求。存储过程还需符合可信数据空间的治理规则，包括数据保留时限、访问审计、定期归档或清理等机制，确保数据在生命周期内安全合规并可被追溯。

9.2.8 数据使用

数据使用业务标准旨在确保数据在可信框架下合规、安全、高效使用，实现可追溯的价值转化，同时满足监管要求并构建信任体系，包括如下业务活动：

——数据使用：数据使用方根据合约授权范围，通过合规技术对数据进行清洗、建模、开发或人工智能训练，采用隐私计算、数据沙箱等，保障原始数据可用不可见、安全不泄露，全程记录操作日志并支持追溯，确保在授权场景下实现价值转化。对于自动化决策过程涉及个人权益时，需提供可解释性输出与申诉渠道，确保合乎个人信息保护要求。

——合约执行：数据使用方和数据开发方需严格遵循数字合约，实现数据使用管控，实现操作指令

与结果的双向验证，保障数据在使用过程中的合规性。当出现合约违规，可信数据空间中间服务平台应采取相应控制策略，及时终止数据使用。

——存证记录：数据使用方、数据开发方及空间运营方对数据使用过程中的行为进行记录存证，确保数据使用行为可追溯、可验证、可监管审计，合规举证提供支撑。

9.2.9 数据销毁

数据使用方在完成数据使用后，需对数据进行销毁，确保数据不被滥用或非法保存，确保数据资产在生命周期结束后实现安全闭环管理，包括如下业务活动：

——合约履约：数据销毁行为需符合数字合约的规定，基于合约自动识别销毁事件，确保数据在使用结束后被安全销毁。销毁过程宜采用符合国家标准的安全擦除算法，对数据副本、缓存、日志等进行彻底清理并存证。可通过区块链或第三方审计机构见证销毁过程，出具销毁凭证，并向监管方备案。

——审计记录：可信数据空间运营方负责对数据销毁全流程进行审计跟踪和记录数据销毁过程关键信息，支持监管机构实时调取销毁日志，以满足合规核验监管要求。

——残留数据处理：可信数据空间运营方针对数据销毁后可能存在的残留风险，制定专项清理策略。应评估模型中是否残留可反向还原的敏感信息，必要时对模型进行去识别化处理，防止再识别风险。

9.2.10 后服务

数据使用后，对数据资源、产品进行评价、清算、审计等服务，包括如下业务活动：

——评价：由数据使用方对数据资源、产品进行评价，反映数据的价值评估。宜包含对数据使用方信用、数据开发方能力、数据中介方满意度等多维度评价。

——清算：由节点负责对数据使用次数、使用时长等指标计量。在清算环节，由可信数据空间服务平台对各方贡献、收益比例等进行透明公示，并支持合规审计，形成可追溯、可核查的收益分配记录。

——审计：由可信数据空间运营方对数据资源、数据产品的使用进行记录，明确各参与方的贡献，并定期对数据进行审计。定期征求数据使用方与提供方对平台服务、规则及数据质量的反馈，将其纳入改进机制，优化后续版本的运营策略与技术方案。

10 规则机制

10.1 概述

可信数据空间应构建覆盖接入审核规范、互联互通规范、共享利用机制和收益分配机制 4 个部分的规则机制体系。接入审核规范需对接入主体、数据资源、数据产品和服务、技术工具的注册信息模型、资质证据格式、审核业务流程进行标准化，确保接入审核有统一的操作流程。互联互通规范应聚焦数据目录、数据标识、数据语义、技术系统互联互通方面，制定形成数据目录管理规范、数据互操作规范、技术系统互联互通规范文件等规则机制，确保不同主体间的数据资源能够互相理解并互联互通；共享利用机制主要对数字合约创建、数字合约协商机制、数字合约的全生命周期管理、清算审计、纠纷解决、跨境数据流通的业务流程进行标准化，确保数据按照合同约定进行流通使用；收益分配机制则应围绕数据价值计量评估、数据收益分配、数据收益结算方面规范建立计量标准、分配规则与结算流程，保证数据价值评估与收益分配过程和行为公开透明、自动执行。四部分共同构成规则机制体系，为可信数据空间内的接入、流通、利用与收益分配全生命周期提供可执行、可验证、可持续的规范依据。

10.2 接入审核规范

10.2.1 身份审核规则

——应明确身份审核的主要对象，覆盖对数据提供方、数据使用方、数据开发方、数据中介方、数据托管方、空间运营方、监管方等参与方的身份或资质审核和相关审核要求。

——应明确身份审核的内容，参与方的身份证明文件审核和服务方的资质证明文件（包括但不限于身份证明、资质证书、数据共享使用合同等文件）的审核，确认真实性和准确性。

——应明确身份注册、认证、信息更新、权限变更和注销等身份审核各业务环节的流程和操作规范，明确当参与方身份或资质信息发生变化时的再次审核流程和操作规范。

——应根据相关法律要求制定身份或资质审核协议，对被审核方信息的收集、记录、存储、使用等行为应获得授权同意，确保身份审核规则制定和业务流程合规性。

——应包含违规处理机制，如对身份信息造假、账号冒用等违规行为采取相关处理措施。

10.2.2 数据审核规则

——应明确数据审核的主要对象涵盖对原始数据、衍生数据和数据资源的接入审核。

——应明确数据审核的维度，包括但不限于合法合规性（数据所有权或授权证明、数据合规性声明或证明等）、数据目录内容完整性（如数据来源、数据名称、数据格式、数据描述、业务层级、业务类别、共享方式、共享条件、开放方式、开放条件、样例数据等）、数据真实性、数据描述的准确性与一致性等。

——应明确数据在准入、变更和退出环节等业务的流程和操作规范，当数据或其描述信息发生变化时，应再次审核

——应根据相关法律要求制定数据审核协议，对被审核数据信息的收集、记录、存储、使用等行为应获得授权同意，对审批过程及结果数据进行记录，确保数据审核规则制定和业务流程合规性。

——应包含违规处理机制，如对不符合要求的数据审核申请，如未按要求提交完整数据资料或属于禁止流通的数据审核申请予以驳回，对于提供虚假信息或隐瞒重要事实的行为，采取取消数据接入、账号封禁或情节严重者移交法律程序等措施。

——宜对数据审批流程进行审计，定期复核并检查审核规则的执行情况，发现问题及时进行改进，确保审核过程的合规性和可追溯性。

10.2.3 产品服务审核规则

——应涵盖数据产品、数据应用及数据服务等要素的接入审核。

——应审核数据产品的内容以及数据产品来源、业务层级、业务类别、共享方式、共享条件等描述信息；审核数据服务的内容以及内涵、范围、类型、用户和方式、访问权限和实施方法等描述信息，确认真实性及合规性。

——应明确数据产品及服务在准入、变更和退出环节等业务的流程和操作规范，当产品或服务或其描述信息发生变化时，应再次审核。

——应制定并签署产品或服务审核协议，对产品或服务信息的记录、存储与使用，应获得产品或服务提供方同意，并符合相关法律法规要求。

——应明确违规处理机制，对产品或服务信息造假等违规行为采取处理措施。

10.2.4 技术组件审核规则

——应审核技术组件的服务范围和服务内容，技术组件应以产品文档、说明手册等形式明确标注技术组件的服务对象、服务形式、服务方式、覆盖范围等服务范围和内容。

——应审核技术组件的功能和技术指标，技术组件应该以演示、测试报告、认证报告等方式说明其功能和具体技术指标。

——应审核技术组件的部署方式，技术组件应可独立部署。

——应审核技术组件的使用方式，技术组件应完成封装，通过标准接口与外部交互。

——宜审核技术组件的安全防护范围和责任边界，明确技术组件提供方和使用方的安全责任。

——应审核技术组件的权限索取，技术组件且仅应在服务范围内获取相应权限，获取的操作权限应与其服务范围和服务内容相适应。

——可审核技术组件的协同性，技术组件之间可以协同的方式形成功能体系。

10.3 互联互通规范

10.3.1 数据目录管理规范

——应制定数据目录管理基础流程规范，通过流程规范明确数据目录管理过程中的关键活动、责任范围以及遵循的规则和要求，确保数据资源目录发布、查询、订阅、更新等过程的及时、准确、合规。应且仅应在服务范围内获取相应权限。

——宜制定数据资源、数据产品、数据服务分类规范，便于可信数据空间对数据认识的一致性，更好地服务于供需匹配。

——应制定数据目录中统一标识规范，以实现数据空间内部、跨数据空间互联互通，保障资源共享、服务共用。

——应制定数据目录接口协议标准规范，以保证数据空间服务平台与节点之间，节点与节点之间数据目录操作互通。

10.3.2 数据互操作规则

——应对参与互操作的数据进行标识，确定数据标识的相关规则。

——应制定数据语义相关的规则，确保不同主体间的数据语义能够互通。

——宜对跨空间语义互认情况进行分类管理，可设置语义等同、语义等效等语义互认类型。

——应对参与互操作的数据制定分级分类管理办法，同一数据在不同的数据空间中采用的安全级别或安全类型应当等同或等效。

——宜对参与互操作等数据制定共享范围等级管理办法，根据共享范围等级辅助数据互操作自动化。

——应制定互操作数据安全应急响应机制，及时处理数据互操作安全事件。

10.3.3 技术系统互联互通规则

——应对技术系统互联互通所需的通信框架、通信接口、数据格式、传输机制等内容进行规范化要求。

——应建立流程支持节点技术系统的互联互通，参与互联互通的节点应可相互发现、合作授权、建立连接。

——应建立技术系统的互联互通协同机制，在节点和资源互通的基础上，通过执行协同机制实现具体任务的协同。

——应建立技术系统互联互通身份认证规则，采用技术手段对可参与互联互通的技术系统进行标识，技术系统间建立互联互通时应进行身份互认。

——应建立互联互通技术系统的日志互认规则，互联互通的技术系统可在授权范围内回溯相关日志，可包括对各类数据、算法、模型等资源的认证、发布、发现、授权、状态同步等操作。

——应制定合理的技术系统互联互通应急响应机制，防止危险通过互联互通渠道扩散。

——宜对可采用的互联互通技术进行分类管理，并针对节点之间互通、跨空间互通等不同场景做出适配。

10.4 共享使用规范

10.4.1 数字合约要素模型要求

——应包含唯一标识符、版本编号信息。

——应包含合约创建时间戳、最后更新时间戳、关联合约链式标识等。

——应包含目标数据的描述范围，包括数据标识和元数据、数据来源、数据分类、数据完整性、是否包含个人信息等描述。

——应包含参与方信息，包含数据提供方、数据使用方、数据开发方、数据中介方、数据托管方、空间运营方，数据开发方、数据中介方和数据托管方为可选参与方。

——应明确数据授权的具体范围，包括授权使用的数据集、可访问的时间周期、使用次数、使用方式、可操作的地域范围和使用目的等。

——应界定数据授权行为，涵盖数据的查看、下载、修改、共享、再授权等操作权限。

10.4.2 数字合约协商机制

合约协商流程应当在合约草稿生成之后发起，应满足以下要求：

——应支持要约方将初版合约草稿发送给指定受要约方。

——应支持受要约方修订合约后将修订版本发送给要约方。

——应支持多轮协商直至合约当事方对合约内容达成一致。

——应支持合约当事方分别对合约进行确认操作，形成合约文件（含使用控制文件附件）。

——应支持保留协商记录，用于审计或回溯。

10.4.3 数字合约全生命周期管理规则

10.4.3.1 数字合约管理

——应支持数字合约的全生命周期管理，包括创建、签署、执行、履约管理、存证审计和废止。

——应支持通过模板化工具快速生成合约条款，明确合约方主体、数据范围、应用场景、使用方式、使用期限、结算规则、收益分配机制等，确保条款的标准化与合规性。

——应提供多方数字签名功能，确保合约的有效性和抗抵赖性。

——应支持数据提供方按需加入提前终止合约的相关合约条款。

——应确保所有签署的合约被安全存储、备份，并提供相应措施防止合约被破坏或篡改。

——应提供相应机制控制用户对合约的操作，包括但不限于创建、访问、修改等权限，确保合约的安全。

——宜支持多语言和多地域合约模板，满足国际化和本地化需求。

10.4.3.2 数字合约执行与监控规范

——应支持数字合约自动执行，并在执行完成后通知相关方。

——应监控合约的履约情况，确保各方严格按照条款执行。

——应提供合约状态查询与反馈功能，供各方实时了解履约进度。

——应支持相关参与方查看合约信息，包括但不限于合约的签订方、资源文件信息、使用控制策略、合约执行情况等。

——应支持记录合约的执行日志，便于审计和问题排查。

——应具备合约执行过程的安全性能力，包括防篡改、抗攻击、容错与异常处理等。

——宜支持履约异常告警机制，能够在合约执行异常或其他违约情况下及时发出警告通知并建议处理方案。

10.4.4 清算审计机制

——应清算数据资源、数据产品、数据应用、数据服务等交易内容，包括来源与内容合规性检查、应收应付内容核对、内容交付。

——应清算交易资金，包括计算和核对应收应付资金、资金划拨。

——应审计存证数据完整性与合规性，包括对交易数据与资金流水的核对、检查、复算，并提供审计报告。

——应包含违规处理与风险控制机制，如拦截不合规交易、风险提示等。

10.4.5 纠纷解决机制

——内部应设立统一的纠纷受理平台（如官方网站、专用邮箱、客服热线等），并公开相关联系方式，确保各方能够便捷地提交争议问题。

——应规定清晰的内部纠纷处理程序，如应在收到申请后 24 小时内予以回应，并在 5 个工作日内核实申请人主体情况，作出正式受理或不予受理的认定。受理后通知双方收集相关证据材料，包括但不限于合同文本、交易记录、日志文件等，对双方提交材料进行初步研判，组织双方进行友好沟通协商，如协商未果，由内部纠纷平台作出责任认定并出具书面意见。

——应对纠纷受理平台作出的责任认定设立反馈渠道，允许各方对纠纷解决过程和结果提出意见或申诉。

——应明确具体的外部纠纷管辖机构，对于内部途径无法解决的纠纷，应约定由某仲裁委员会仲裁或向有管辖权的人民法院提起诉讼。

——应对违规一方的行为，明确规定相应的处罚措施，对于拒不配合调查或隐瞒重要事实的行为，应取消其参与资格；对于违反合同约定或法律法规的行为，根据情节严重程度采取经济处罚、限制交易权限等措施。

——宜在面对较为复杂的内部纠纷时，引入第三方调解机构，如律所等，为复杂纠纷提供专业化的调解服务以及法律援助服务。

10.4.6 跨境数据流通机制

——应制定数据跨境负面清单，明确需要重点开展数据出境安全评估的数据清单。

——应制定数据出境安全评估规则，明确需要申报数据出境安全评估的主体、需要提交的评估材料、重点评估的事项、评估的流程及整改要求等内容。

——应制定数据出境监管和安全应急机制，明确数据出境后的风险监测机制、预警机制、以及安全事件发生后的应急措施。

10.5 收益分配机制

10.5.1 数据价值评估模型

——应明确价值评估对象，涵盖数据集、数据接口、数据报告等，以及不同对象价值评估的侧重点和原则。

——应提供动态数据价值评估模型，应综合考虑成本因素、场景因素、市场因素、质量因素等多维度因素。

a）成本因素，包含前期成本、直接成本、间接成本、管理成本、其他成本等指标

b）场景因素，包含使用范围、应用场景、商业模式、市场前景、财务预测、应用风险等指标

c）市场因素，包含交易市场、数据稀缺性、供求关系等指标

d）质量因素，包含规范性、完整性、准确性、一致性、时效性、可访问性等指标

——应明确提供多种评估方法，包含成本法、收益法、市场法及多种方法相结合的复合估值方法。

——应建立数据价值评估定价的业务流程和操作规范，形成估价、报价、议价、定价的流程和规范流程。

——应支持数据提供方自行评估，宜支持第三方服务机构进行评估。

10.5.2 数据收益分配机制

——应明确数据收益分配的主体及不同主体收益分配的相关比例。

——应明确数据收益分配的方法，如固定比例分配法、动态收益分配法等。

——应制定收益分配流程，形成明确收益主体、通过数字合约或协议约定收益比例、支付结算的流程和规范。

——应建立监督约束机制和信息披露规则。

——宜构建生态主体激励机制，明确数据供给、应用场景创新、数据产品和服务开发等方面的激励举措。

10.5.3 结算机制

——应明确结算模式和周期，可支持多种模式，不限于预付款、后付款、一次性、分阶段结算模式。

——应明确结算流程，包含交易支付、结算处理、凭证生成、对账等环节。

——应明确退款规则及流程、凭证管理规则、交易对账机制。

——应建立资金安全保障机制，包含支付与账户安全、异常处理责任等，宜引入第三方存管机制、冻结解冻规则、保证金制度。

11 技术系统

11.1 可信数据空间系统功能

11.1.1 功能概述

可信数据空间的功能概述基于可信数据空间参考架构框架，对数据提供方与数据使用方节点、数据服务方节点、中间服务平台以及监管与合规所需的功能进行了系统性规范，可支持中心化模式和联邦模式。各个功能模块协同工作，支撑可信数据空间全生命周期的业务活动。

可信数据空间参考架构框架由数据提供方节点、数据使用方节点、数据服务方节点和中间服务平台构成，如图 3 所示。中间服务平台与数据提供方节点、数据服务方节点、数据使用方节点之间进行管控流信息交互。中间服务平台与数据提供方节点之间的管控流包含元数据、合约、日志存证与溯源、数据标识等信息。中间服务平台与数据使用节点/数据服务节点之间的管控流包含数据产品和服务、合约、日志存证与溯源等信息。数据提供方节点可以直接和数据使用方节点进行数据流交互，也可以借助数据服务方节点进行交互，其中数据服务方节点可以提供供需撮合、托管运营、委托/联合开发等服务。

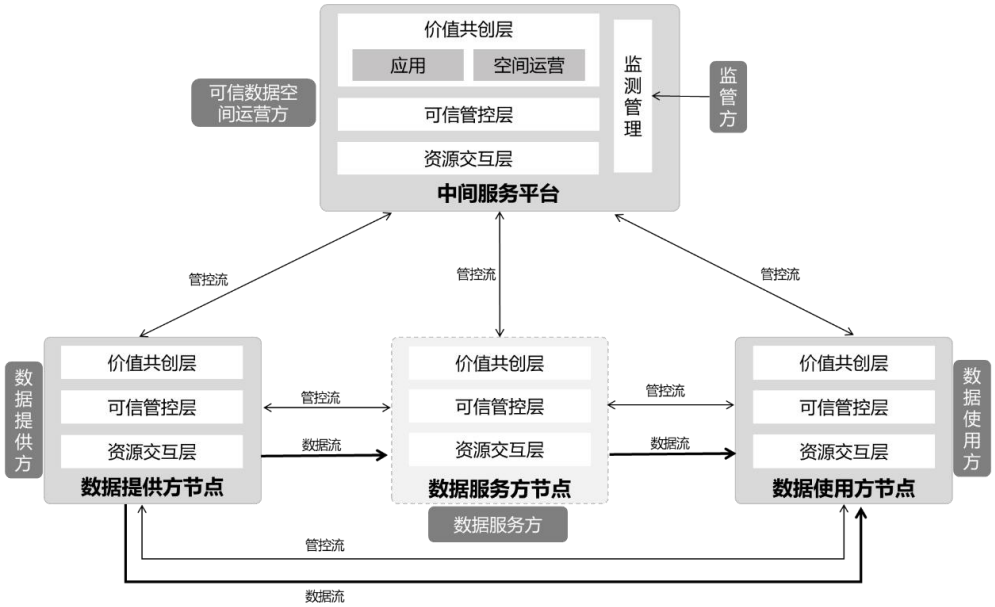

图 3 可信数据空间参考架构框架

中间服务平台由资源交互层、可信管控层和价值共创层组成，用于支持可信数据空间内不同参与方的协作与管理，促进数据资源的高效共享、可信流通和价值创造，如图4所示。三层包含的功能模块如下：

——资源交互层：提供数据目录管理、数据标识和语义管理、连接支持的功能，达成数据资源的统一发布、高效查询和跨主体互认，实现可信数据空间内外的数据互通和资源共享。

——可信管控层：提供平台级的可信管理和控制能力，包括身份认证与管理、使用管控、数字合约管理、存证溯源等，确保可信数据空间内的数据流通和操作行为安全、可控和可追溯。

——价值共创层：提供服务管理、数据产品管理、应用场景支持、空间运营等功能。

图 4 中间服务平台架构

数据提供方、使用方、服务方等节点三层包含的功能模块如图 5 所示：

——资源交互层：要提供数据的采集、预处理接入、存储、管理、使用和销毁等功能，支持数据提供方和数据使用方在可信数据空间中对数据资源的有效管理和使用。

——可信管控层：提供身份认证与管理、数字合约与履约管理、使用管控、存证溯源等功能，确保

数据在可信数据空间内的安全合规流通和使用。

——价值共创层：为可信数据空间的参与方提供数据开发、分析和应用的环境和工具，支持参与方开发数据产品和服务，促进价值共创。主要功能包括：提供节点运营、服务协同、数据产品开发、应用场景支持等。

图 5 节点架构

11.1.2 中间服务平台功能

11.1.2.1 资源交互层

11.1.2.1.1 数据目录管理

数据目录管理直接支撑“数据接入”阶段的元数据登记与更新、“数据发布”阶段的目录生成与上架，以及“数据发现”阶段的查询、检索与订阅。应提供统一的数据资源目录服务，支持数据资源的发布、分类、检索和订阅，提升数据资源的可发现性和可获取性。

11.1.2.1.2 数据标识和语义管理

应建立统一的标识体系和语义管理机制，确保不同主体间的数据资源和服务能够互认互通，提升数据互操作性。具体要求包括数据标识、元数据标准化、语义管理、数据互操作协议等。

11.1.2.1.3 连接支持

应支持中间服务平台、数据提供方节点、数据使用方节点、数据服务方节点与其他可信数据空间的连接，实现资源的跨主体和跨空间共享。具体要求包括节点接入支持、跨空间协同、兼容性与扩展性等。

11.1.2.2 可信管控层

11.1.2.2.1 身份认证与管理

应提供统一的接入认证和管理服务，确保参与方和节点的身份可信，为数据访问和操作提供基础保障。具体要求包括统一接入认证、身份管理与维护、身份可信度评估等功能。

11.1.2.2.2 数字合约管理

应支持管理可信数据空间内的数字合约，包括合约的创建、签署、执行和维护，确保数据交易和合作的权责明确和自动履约。具体要求包括数字合约创建与签署、合约执行与监控、合约存储与管理、争议解决与仲裁支持等功能。

11.1.2.2.3 使用管控

基于数据提供方、数据使用方和/或数据开发方协商一致的数字合约和控制策略，对数据的访问和使用进行实时控制，确保数据的合规使用和安全流通。具体要求包括使用控制管理、沙箱功能、隐私保护计算、实时监控等功能。

11.1.2.2.4 存证溯源

应支持对可信数据空间内的操作行为进行全面的日志记录和存证，为合规审查、争议解决和责任追溯提供可靠的依据。具体要求包括日志记录、日志存储、日志查询、日志分析等功能。

11.1.2.3 价值共创层

11.1.2.3.1 服务管理

应支持数据交换共享的相关服务，帮助数据提供方和使用方高效匹配，促进数据资源的流通和价值实现。具体要求包括服务发布、供需撮合、数据经纪服务、数据托管服务、审计清算服务、评价反馈等功能。

11.1.2.3.2 数据产品管理

应支持参与方发布、管理和分享数据产品和服务，促进数据资源的增值和广泛应用。具体要求包括应用开发环境、数据产品开发与发布、产品维护等功能。

11.1.2.3.3 应用场景支持

可提供面向特定应用场景的支持，如供应链优化、金融风控、智能制造、医疗健康等，满足行业数据应用需求。具体要求包括解决方案库、可定制的应用模块、知识集成等功能。

11.1.2.3.4 空间运营

应制定收益分配规则等空间生态主体服务机制，促进数据资源的价值共创和生态繁荣。具体要求包括规则规范、价值评估与分配机制、生态构建等功能。

11.1.2.4 安全

应从数据合规、过程合规、安全防护等方面保障空间的基础安全。

11.1.2.5 监测管理

应实现合规审查功能、审计功能、违规处理功能等，保障空间运行合规化。

11.1.3 节点功能

11.1.3.1 资源交互层

11.1.3.1.1 数据接入

应支持数据提供方采集多种格式和来源的数据，包括结构化、半结构化和非结构化数据，以及为满足数据使用方需求所需要进行的数据预处理功能。具体要求包括接入方式、数据预处理、数据脱敏、数据源管理等方面的功能。

11.1.3.1.2 数据存储

应提供安全、高效的数据存储、索引和管理功能，支持数据的快速访问、维护和高效调用。具体要求包括多格式存储、分类分级存储、容灾备份等方面的功能。

11.1.3.1.3 数据目录管理

节点的数据目录管理应遵从中心服务平台的目录要求，同时实现数据发布、数据分类、数据检索、语义管理等方面的功能。

11.1.3.1.4 数据传输

应支持数据在数据提供方节点与数据使用方节点和或数据开发方节点之间的安全传输功能，保障数据传输过程中的机密性和完整性。具体要求包括：安全传输协议、身份验证、完整性校验、错误检测、重传机制等方面的要求。

11.1.3.1.5 数据使用

应支持数据使用方、数据开发方按照数字合约的规定，合法使用数据资源，实现数据的价值利用。具体要求包括数据访问、分析工具、缓存和临时存储、性能优化、数据销毁等方面的功能。

11.1.3.2 可信管控层

11.1.3.2.1 身份认证与管理

应提供参与主体的身份验证和访问控制机制，确保参与方身份可信，管理其对数据资源和服务的访问权限。具体要求包括身份认证、权限管理、访问控制等方面的功能。

11.1.3.2.2 数字合约与履约管理

管理参与方之间的数据使用协议，确保数据使用行为符合约定和法规要求。并应对数字合约履约过程中的关键操作进行存证，为纠纷处理提供可靠的电子证据。在联邦模式下，合约签署与履约主要由各节点自管，但仍需与平台或第三方审计机构进行日志上报与合约备份。具体要求包括数字合约创建与签署、合约执行与监控、合约存储与管理、争议解决与仲裁支持等方面的功能。

11.1.3.2.3 使用管控

应采用使用控制技术或隐私计算、数据沙箱等其他技术，保护数据在流通和使用过程中的安全和隐私，防止数据泄露和滥用。具体要求包括使用控制、隐私保护计算、沙箱功能等功能。

11.1.3.2.4 存证溯源

记录数据操作的全生命周期行为，确保数据流通和使用过程的可追溯性和可审计性。具体要求包括日志记录、日志上报、日志存储、日志查询等功能。

11.1.3.3 价值共创层

11.1.3.3.1 节点运营

应和中心服务平台具备相同的收益分配、审计清算等功能，促进数据资源的价值共创和生态繁荣。具体要求包括规则规范、价值评估与分配机制、评价反馈等功能。

11.1.3.3.2 服务协同

应支持数据提供方、数据使用方和数据服务方之间的实时数据交互和协同，优化数据利用效率，促进价值共创。具体要求包括接口协同、服务集成、权限管理等功能。

11.1.3.3.3 数据产品开发

宜支持数据开发方和数据使用方基于可信数据空间内提供的数据资源，进行数据分析、处理和加工，以及数据价值评估。具体要求包括：开发环境、数据处理与分析工具、模型部署与服务、模型治理等功能。

11.1.3.3.4 应用场景支持

可提供面向特定行业和应用场景的支持，如供应链优化、金融风控、智能制造、医疗健康等，满足行业数据应用需求。具体要求包括解决方案库、可定制的应用模块、知识集成等功能。

11.1.3.4 安全

安全方面应符合如下要求：

——提供方提供的数据应保障数据来源合规合法。

——应确保数据使用过程中的合规性，符合相关法律法规和数字合约的要求。

——可支持国密 SM2/SM3/SM4 等国产密码算法，并根据数据敏感度进行分层存储和访问控制。

11.2 可信数据空间系统技术

可信数据空间技术体系包含资源交互、可信管控、价值共创三大类技术。资源交互技术实现数据的标准化连接与互通，包括资源识别、数据目录等；可信管控技术确保全流程安全合规，涵盖身份管理、访问控制等；价值共创技术支撑数据要素的价值度量与协同创新，涉及产品认证、收益分配等。三类技术协同构建安全、可控、合规的数据流通基础设施。本部分围绕可信数据空间的突出功能特性，选择更重要、更具代表性的技术，并不以全面性覆盖为规范目的。

11.2.1 资源交互技术

主要包含数据资源识别、数据资源目录、数据资源处理、数据资源交互等数据的标准化互通技术，确保异构数据资源的可信识别与高效交互。

11.2.1.1 数据资源识别

——数据认证技术：通过数字签名、哈希校验或权威机构核验等手段，确保数据来源真实、内容完整且未被篡改的技术，为数据可信流通提供身份和完整性证明。

——数据标识技术：采用统一的标识体系，为各类数据资源赋予唯一标识，实现快速准确的索引和定位，确保数据全生命周期的可追溯性和可访问性。

——语义发现技术：融合自然语言处理、多模态数据处理技术，通过语义规范体系实现数据内涵解构与上下文建模，实现智能搜索和关联发现。

——语义转换技术：通过映射规则、标准化协议，将异构数据转换为目标格式或结构，并保持语义一致性、数据完整性和上下文关联，实现不同来源和不同类型数据的智能索引、关联和发现。

11.2.1.2 数据资源目录

——数据资源索引技术：通过构建多维度索引体系（如标签、关键词、数据类型、业务领域），对数据资源进行结构化编目，支持快速检索与定位。采用分布式索引架构实现海量数据的高效查询，兼容模糊搜索、语义检索等功能，提升数据资源的发现效率。

——元数据智能识别技术：基于自然语言处理（NLP）、机器学习算法，自动解析数据文件（文本、数据库、API 接口）的元数据信息（数据字段、格式、业务含义、更新频率）。支持非结构化数据的元数据抽取（如从文档中识别业务实体、数据血缘关系），实现元数据采集的自动化与精准化。

——数据分类分级技术：依据数据业务属性（如客户数据、交易数据）、敏感程度（公开数据、隐私数据、机密数据）及合规要求（GDPR、数据安全法），建立多层级分类分级体系。通过预设规则引擎或机器学习模型，自动匹配数据标签并生成分类分级结果，为数据访问控制、共享授权提供基础支撑。

——跨境数据资源目录互操作技术：遵循国际数据目录标准与跨境数据治理规则，实现不同国家或地区数据资源目录的语义互认与服务对接。支持跨境目录的动态映射（如数据分类体系转换、权限规则适配），结合区块链技术记录跨境数据共享日志，确保跨境数据流通的合规性与可追溯性。

11.2.1.3 数据资源处理

——数据接入集成技术：通过 ETL 工具、数据虚拟化或流式处理等技术，将分散在不同系统、格式和协议中的数据进行抽取、转换和加载，实现多源异构数据的统一访问与分析，提升数据利用效率。

——数据存储技术：利用分布式文件系统、云存储或时序数据库等方案，对结构化、半结构化和非结构化数据进行高效存储与管理，确保数据高可用、可扩展和安全持久化，满足不同业务场景需求。

——数据质量管理技术：通过数据标准化、异常检测、规则引擎和血缘追踪等手段，识别并修复数据中的错误、冗余和不一致问题，保障数据的准确性、完整性和时效性，为业务分析提供可靠依据。

——数据销毁技术：采用物理粉碎、多次覆写或加密擦除等方法，确保存储介质中的敏感数据被不可逆地彻底清除，防止数据泄露和恶意恢复，满足 GDPR 等数据安全合规要求。

11.2.1.4 数据资源交互

——数据封装技术：通过标准化元数据描述和加密手段，将原始数据及其上下文信息打包为可独立传输和解析的单元，确保数据在流转过程中保持完整性和可追溯性，同时支持权限控制和分级披露。

——数据互操作协议技术：基于开放标准（如 JSON-LD、RDF）设计跨系统数据交换接口和语义解析规则，解决异构系统间的语法与语义差异，实现不同平台数据的无缝交互与协同计算。

——数据传输技术：高速数据网是指面向数据流通利用场景，依托网络虚拟化、软件定义网络（SDN）等技术，提供弹性带宽、安全可靠、传输高效的数据传输服务。支持差异化网络传输能力、多种网络接入等。

11.2.2 可信管控技术

主要包含身份管理、访问控制、数字合约、使用控制、数据沙箱、隐私保护计算、实时监控、跨境数据流动控制、存证溯源等核心技术，构建全流程合规管控体系。

11.2.2.1 身份管理技术

——身份标识技术：为主体（自然人、法人、设备、系统等）分配唯一且可解析的标识符，实现身份唯一识别、映射与引用的技术手段。它包括标识符生成机制、命名规范、标识解析协议、与主数据的绑定关系，并支持在空间中进行身份映射与统一识别。应在身份注册时为空间主体提供全局唯一身份标识，并建立其与真实身份信息的关联。

——多因素认证技术：通过整合知识因素（密码）、所有权因素（硬件令牌）和生物特征（指纹、虹膜）等验证要素，结合零信任安全框架的动态风险评估机制，实现高安全级别的身份核验与实时授权决策，抵御伪造身份和越权访问风险。

——分布式身份认证技术：基于标准化协议构建跨组织身份联盟，允许用户通过单一身份提供者（IdP）完成多服务方的无缝认证，减少身份信息重复存储风险，支持大规模异构系统间的信任传递。

——集中式身份认证技术：通过会话期内实时监测用户行为特征、设备指纹与环境上下文（如 IP 地址、地理位置），结合机器学习模型动态评估身份可信度，实现从"单次认证"到"持续验证"的安全升级，防范会话劫持与身份冒用。

——资质评估技术：通过自动化规则引擎和可信凭证验证，对数据提供方的技术能力、合规水平及信用等级进行动态评估，确保参与数据流通的主体持续满足预设资质要求，降低协作风险。

——身份吊销技术：基于实时黑名单机制，对失效或高风险主体（如违规组织）的访问权限进行即时撤销与全网同步，阻断其后续数据交互，保障生态安全性。

11.2.2.2 访问控制技术

——基于角色的访问控制技术：基于角色访问控制（RBAC）和属性访问控制（ABAC）模型，通过策略引擎解析用户属性、资源标签和环境上下文，动态生成访问决策，确保数据与服务资源的按需授权，满足最小化权限分配原则。

——动态权限管控技术：结合实时风险评估和行为分析，通过上下文感知引擎动态调整用户权限范围，例如根据设备安全状态、地理位置或访问频率触发权限升级或降级，实现自适应安全防护与风险缓解。

——基于风险的动态访问控制技术：整合实时威胁情报与用户行为分析，通过风险评分引擎动态调整访问权限阈值，例如在检测到异常操作时自动触发访问阻断或二次认证，实现安全防护与业务灵活性的平衡。

——跨域联合策略执行技术：采用策略联邦机制，在多个信任域间同步访问控制策略语义与执行上下文，通过分布式策略决策点协同工作，实现跨组织边界的统一权限管控。

11.2.2.3 数字合约技术

一种协商一致后基于可编程逻辑和自动化执行机制的数字化协议技术，通过计算机代码而非自然语言定义合约条款，并在满足预设条件时自动触发执行，确保合约执行的确定性、透明性、不可篡改性、可追溯性和可验证性。

11.2.2.4 使用控制技术

——基于策略的使用控制技术：一种规则驱动机制，预设数据使用策略，对访问主体、用途、时间、频次等进行精细限制。确保数据在授权范围内合规使用，防止越权与滥用。

——动态使用控制技术：一种实时决策机制，结合行为分析与环境上下文动态评估使用权限。可根据风险级别自动调整或中止数据操作。

11.2.2.5 数据沙箱技术

通过构建隔离环境，允许数据使用方在安全和受控的区域内对数据进行分析处理，防止数据的未授权使用、篡改或泄露。

——通过虚拟化技术构建隔离环境，确保沙箱内的运行环境和数据与其他环境、数据的隔离。

——通过细粒度的权限控制沙箱的访问，并控制数据的输入和输出。

——通过对沙箱内的应用的运行、数据的操作等进行记录，监测沙箱内的运行环境和数据处理。

11.2.2.6 隐私保护计算

——多方安全计算：一种密码学协议体系，允许多个参与方在不暴露各自私有数据的前提下，协同合作完成特定计算任务，仅输出计算结果。确保各方数据的隐私性与计算结果的准确性。

——联邦学习：一种分布式机器学习框架，允许多个参与方在不共享原始数据的前提下，通过协作共同训练出共享的全局机器学习模型，保障数据权益与隐私合规性。

——密态计算：通过综合利用密码学、可信硬件和系统安全的可信隐私计算技术，其计算过程实现数据可用不可见，计算结果能够保持密态化，以支持构建复杂组合计算，实现计算全链路保障，防止数据泄漏和滥用。

——可信执行环境：一种基于硬件安全机制构建的隔离执行环境，通过与设备主操作系统并行运行但硬件隔离的方式，确保敏感数据与代码在处理过程中的机密性、完整性和抗篡改性。

11.2.2.7 实时监控技术

通过持续采集、分析和预警系统运行状态或数据动态变化的技术，确保异常行为或风险能被即时发现和响应，保障业务连续性与数据安全。

11.2.2.8 跨境数据流动控制

一种基于策略驱动与自动化执行的跨域数据管控技术，通过实时监控数据流动意图，自动触发合规审批流程，动态匹配目标司法管辖区的法规要求，对不符合合规策略的数据传输行为执行阻断、限流或标记。

11.2.2.9 存证溯源技术

——可信存证技术：利用区块链分布式账本特性，将数据哈希值、操作时间、参与方信息等上链存证，通过智能合约自动执行存证流程。支持跨系统数据存证接口适配，结合数字签名技术实现存证主体身份认证，为数据权属证明、交易记录存证提供去中心化信任支撑。

——可信追溯技术：通过区块链、数字水印等技术手段，完整记录数据全生命周期操作轨迹，确保数据来源可查、流向可追、责任可究的核心技术体系。

11.2.3 价值共创技术

主要包含数据产品与服务认证、数据加工、数据开发、价值评估模型、优化增强、模型治理、供需管理、服务协同、收益分配、场景应用等增值服务技术，支撑数据要素的价值转化与生态协同。

11.2.3.1 数据产品与服务认证技术

——产品溯源追踪技术：基于区块链、数字水印等技术手段，完整记录数据产品从制作、加工、流转到使用的全生命周期轨迹。该技术能够精确追踪数据来源、操作记录和流转路径，同时支持数据真实性验证，防止篡改和伪造，为数据产品的可信度提供坚实基础。

——产品质量认证技术：采用规则引擎、统计分析、异常检测等方法，对数据的完整性、准确性、一致性进行多维度评估。通过自动化检测数据中的缺失值、重复值、异常值等问题，生成标准化质量评分报告，帮助判断数据产品的可靠性。

——服务性能评估技术：通过压力测试、负载测试和实时监控，对数据服务的响应时间、吞吐量、稳定性等关键指标进行量化分析。基于测试结果生成服务等级协议（SLA）认证，帮助了解服务的可靠性。该技术可优化数据服务架构，提升高并发场景下的性能表现，确保体验流畅。

11.2.3.2 数据加工技术

——数据清洗技术：利用规则引擎、异常检测和模式匹配等方法，识别并处理数据中的缺失值、重复值、异常值和格式错误等问题，确保数据的一致性和准确性。该技术可自动化修复或标记问题数据，减少人工干预，为后续分析提供高质量数据基础。

——数据脱敏技术：利用掩码、泛化、加密等手段对敏感信息（如身份证号、手机号）进行变形或替换，确保数据在共享测试环节不泄露隐私。该技术平衡了数据可用性与安全性，支持静态脱敏（批量处理）和动态脱敏（实时查询）。

——数据合并与拆分技术：数据合并通过主键关联、时间序列对齐等方式，将多表或多文件数据整合为统一视图；而数据拆分则按业务规则将大数据集分解为更小单元。两者均依赖高效的索引和查询优化算法，解决数据冗余或碎片化问题，优化存储与计算性能。

11.2.3.3 数据开发技术

——数据可视化技术：通过图表、仪表盘及交互式图形（如折线图、热力图、地理信息映射）将复杂数据转化为直观视觉呈现，帮助用户快速识别趋势、异常和关联规律。该技术结合前端框架和动态渲染能力，支持多维度数据探索。

——嵌入式分析技术：将数据分析功能集成到第三方应用中，无需切换系统即可获得数据洞察。通过嵌入方式，结合权限隔离和白标定制，提升数据应用的智能化水平。

11.2.3.4 价值评估模型技术

一种用于评估数据价值的模型算法和大数据分析体系，综合考虑数据的质量状况、稀缺程度以及市场供需态势等多维度因素，结合基于供需撮合机制的市场行情监控历史数据分析，对数据的经济效益、业务效用、风险成本及潜在衍生价值进行动态量化评估，为数据产品管理、数据交易和资产化管理提供科学依据。

11.2.3.5 优化增强技术

——缓存优化技术：缓存优化技术通过将高频访问数据存储在高速缓存层，减少数据库查询负载，显著提升系统响应速度，适用于读多写少的高并发场景，同时采用合理的缓存失效策略保证数据一致性。

——代码级性能优化技术：代码级性能优化技术通过算法改进、数据结构选择、减少系统调用等技术手段，从微观层面提升程序执行效率，特别适用于计算密集型任务的关键路径优化。

——并发编程技术：并发编程技术采用多线程、协程、异步 IO 等编程范式，充分利用多核 CPU 资源提高程序吞吐量，通过锁优化、任务分解等技术解决竞态条件，实现高并发场景下的性能提升。

——资源预加载技术：资源预加载技术通过分析用户行为模式，提前将可能需要的计算资源或数据加载到内存，减少等待延迟，特别适用于需要快速响应的交互式系统，通过预测性加载实现性能的平滑过渡。

11.2.3.6 模型治理技术

建立全生命周期管理框架，涵盖开发规范、版本控制、性能监控和伦理审查等环节，确保 AI 模型的可靠性、公平性和可追溯性，实现模型资产的规范化管理与风险控制。

11.2.3.7 供需管理技术

通过需求分类、智能匹配及动态推荐等技术手段，结合多维度标签体系、智能算法和实时数据分析，实现数据供需双方的精准对接、推荐排序，并保障隐私安全与监管合规的智能化管理技术。

11.2.3.8 服务协同技术

——服务编排技术：一种基于自动化流程引擎、智能决策算法和安全协作框架的技术体系，通过动态发现、组合、调度和监控多个异构数据服务，实现跨组织、跨平台的数据协同任务，同时保障数据安全、隐私保护、合规性及服务质量。

——实时通信技术：一种基于低延迟、高可靠性和安全加密的通信协议与架构，通过实时传输、处理和分发跨组织、跨平台的数据或服务请求，支持多方协同任务的动态交互与响应，确保数据隐私、身份认证、访问控制和通信内容的完整性。

11.2.3.9 收益分配技术

通过数字合约、收益分配算法和区块链等技术，基于共识的公平条款，实现数据交易中各方利益的自动化分配，确保数据交易过程中的公平性与透明度，促进各方的协同与利益共享。

——权益量化建模技术：基于各利益相关方在数据交易链条中的实际贡献，构建可度量的权益表达模型，明确各方在交易中的权益归属与分配权重，为收益分配提供量化基础。

——共识分配规则技术：采用多方协商、平台设定或行业模板等方式，形成公开透明、可验证的收益分配规则体系。该体系以“共识公平”为核心理念，支持比例设定、场景定制和动态调整，确保收益分配的公平性及各利益相关方对分配制度的认同。

——数字合约分账技术：通过数字合约自动执行，实现收益拆分、定向分账与多轮分润流程，确保分账过程无需人工介入、全程可验证和结果不可篡改，提升收益分配的执行效率与可信度。

——收益分配溯源技术：通过对收益相关的交易记录、数据使用行为及分账流程进行全链条记录，结合区块链不可篡改特性，构建可追溯、可审计的收益分配行为日志体系，保障事中监管与事后审计的合规性与透明性。

11.2.3.10 场景应用技术

通过场景建模、跨境数据管理、数字孪生与边缘计算等核心技术，结合行业知识框架与合规治理手段，面向特定领域，如供应链、金融、制造、医疗等，的定向数据应用技术体系。

——场景建模技术：基于领域知识，利用标准化建模语言、语义技术或行业框架，通过集中式或分布式建模方法对数据空间中的多角色协作流程、数据共享规则、信任锚点及合规要求进行结构化表达的技术。

——跨境数据管理技术：通过整合法律合规、数据安全、隐私保护与治理框架，在遵守不同司法管辖区法律法规的前提下，实现数据在跨国或跨地区场景下的安全流动、合规存储、可控使用，确保数据主权与数据全球化需求，以及隐私保护与数据价值释放之间的平衡。

——跨境合规审查技术：通过自动化、智能化的手段，对数据跨境流动的全流程进行合规性验证、风险评估和动态监控，确保数据全生命周期符合目标国家/地区及国际间的法律法规要求。

11.3 功能与技术的映射

功能分层	功能模块	具体技术	功能与技术映射关系
资源交互层	数据目录管理	数据资源索引技术	提高数据检索速度，实现快速精准的数据资源定位。
		元数据智能识别技术	自动化提取和处理元数据，提高元数据管理的效率和准确性。
		数据分类分级技术	提供结构化标签，支撑权限控制与元数据检索。
		跨境数据资源目录互操作技术	通过统一元数据标准，实现跨域目录对接与权限同步。
	数据标识与语义管理	数据标识技术	为数据资源分配唯一标识符，实现快速准确的数据检索和定位。
		语义发现技术	理解数据的含义和上下文，实现智能搜索和关联发现，将异构数据转换为目标格式或结构。
		语义转换技术	统一异构数据语义，关联标识并消歧，支撑跨域互操作。
	连接支持	数据封装技术	构建独立、自描述和可控的数据单元，提升数据交互效率与兼容性。
		数据互操作协议技术	提供标准化接口与协议，实现跨系统、跨领域、跨空间数据高效连接与交互。
	数据接入	数据接入认证技术	通过验证身份与权限，保障数据安全准入与合规传输。
		数据集成技术	将接入的异构数据整合为符合统一标准的数据视图。
	数据存储	数据存储技术	为各类数据提供合适的存储架构，保障数据完整性、可用性和可扩展性。
	数据传输	数据传输技术	支持数据高效、安全的规模化传输。
	数据使用	数据质量管理技术	持续评估与修复数据，确保所管理数据符合业务需求与标准规

			范。
		优化增强技术	通过加速处理与资源调度，提升数据调用效率与实时性。
		数据销毁技术	通过安全擦除机制，确保数据使用后不可恢复，防泄露。
可信管控层	身份认证与管理	身份认证技术	验证主体合法性，动态管控权限并保障可信访问。
		身份标识技术	定义唯一身份凭证，绑定权限并实现全周期管理。
		资质评估技术	审核主体资质等级，动态分配权限并确保合规准入。
		身份吊销技术	通过撤销权限实现身份动态管理与安全控制。
	使用管控	使用控制技术	支持使用控制规则化配置，以限制对数据资源的使用，防止数据的违规使用与滥用。
		数据沙箱技术	在安全隔离的环境中处理数据，确保数据使用过程受控、安全、合规。
		隐私保护计算	在不泄露原始数据的前提下进行数据分析和计算，实现数据全过程可用不可见。
		实时监控技术	通过动态追踪数据使用过程实现风险即时管控。
	数字合约与履约管理	数字合约技术	承载合约条款，建立互信机制，确保合约的自动执行。
	存证溯源	可信存证技术	保存数据流通全过程的信息记录，为溯源提供有效、可靠的电子证据。
		可信追溯技术	通过全链路操作记录实现数据存证与来源追溯。
价值共创层	服务管理	供需管理技术	通过动态匹配供需资源实现服务高效调度与管理。
		数据产品与服务认证技术	通过验证服务合规性保障服务质量与规范管理。
	服务协同	服务协同技术	通过跨系统集成与流程协作实现服务高效协同。
	数据产品管理	产品溯源追踪技术	通过合规性核验实现数据产品可信流通与价值确认。
	数据产品开发	数据加工技术 数据开发技术	通过清洗、转换等处理实现数据产品开发与价值构建。
		模型治理技术	通过规范模型全周期管控与优化，支撑数据产品的可信开发与持续迭代。
	应用场景支持	场景应用技术	通过适配场景需求实现功能落地

			与价值转化，驱动场景化应用创新。
		跨境数据管理技术	为跨境数据流通提供合规的技术工具与服务。
		跨境数据流动控制	通过合规性校验与安全技术，支撑跨境贸易、金融等场景安全应用。
		数据应用技术	通过分析、建模与场景适配，实现数据价值释放并支撑多元场景落地应用。
	空间运营	收益分配技术	通过智能合约自动化执行与权益量化，实现参与方收益公平分配，保障空间生态可持续运营。
		价值评估模型技术	综合考虑数据的质量、稀缺性、市场需求等因素，对数据价值给出对应评估方式和量化结果。

表 2 功能与技术的映射表

（规范性）

XX

详细列出针对不同主体（企业、行业、城市、个人、跨境）的具体能力要求：

A 企业可信数据空间能力要求

——企业级数据管理、共享和协同机制。

B 行业可信数据空间能力要求

——针对特定行业的数据共享标准和应用支持。

C 城市可信数据空间能力要求

——城市公共数据资源管理及服务集成能力。

D 个人可信数据空间能力要求

——个人数据的授权和隐私保护能力。

E 跨境可信数据空间能力要求

——支持跨境数据流动和合规管理的标准和机制。

（资料性）
YY

涉及的法律法规和规范主要有《数据安全法》《个人信息保护法》《网络安全法》以及相关行业的数据管理规定等。具体表格如下：

类别	法律法规及规范	核心要点	标准立项建议
数据安全基础法律	《中华人民共和国数据安全法》	全面规范数据安全保护义务、管理职责及监管，贯穿数据产品全流程合规要求。	/
个人信息保护法律	《中华人民共和国个人信息保护法》	明确个人信息处理规则、主体权利及处理者义务，规范数据产品中个人数据操作。	/
网络安全法律	《中华人民共和国网络安全法》	保障网络安全，维护网络空间主权及各方权益，为数据产品运营网络环境提供依据。	/
行业特定规范 - 医疗	《健康医疗大数据管理办法（试行）》	规范医疗数据收集、存储、应用，确保医疗数据安全与患者隐私保护。	/
行业特定规范 - 金融	《金融数据安全 数据安全分级指南》《个人金融信息保护技术规范》等	对金融数据安全管理、个人金融信息保护作出详细规定。	/
行业特定规范 - 能源	能源领域数据管理相关规定	保障能源数据在生产、传输、消费等环节的安全与合理利用。	/
电商交易法律	《中华人民共和国电子商务法》（若数据产品通过电商平台交易）	规范电商经营者义务、电子合同订立履行及争议解决，适用于数据产品交易场景。	/
消费者权益保护法律	《中华人民共和国消费者权益保护法》	在数据产品交易中保护消费者知情权、选择权、公平交易权等。	/
市场竞争法律	《中华人民共和国	防止数据产品市场垄断，保障公平竞争，规范企业数据相关市场行	/

	反垄断法》	为。	
知识产权法律	《中华人民共和国著作权法》	保护数据产品中原创数据内容、算法模型、软件程序等知识产权。	/
标准规范 - 数据格式	国际通用数据格式标准	确保不同系统间数据兼容性与可交换性，利于数据产品在不同环境使用。	/
标准规范 - 数据质量评估	已有行业或国际数据质量评估标准	衡量数据产品的数据准确性、完整性、一致性等质量指标。	/
数据产品发布环节	/	/	制定数据产品内容审核标准，涵盖准确性抽样、完整性评估、时效性判定等方法及审核流程和责任主体。 建立数据产品质量评估指标体系标准，明确一致性、可靠性、可用性等指标定义、测量方法及评估等级
数据产品订阅、交易环节	/	/	制定基于成本核算、市场需求调研、数据价值评估等多因素的数据产品定价标准，规范定价流程。 制定包含合同基本信息、产品描述、交易金额与支付、交付方式、权利义务、违约责任等内容的数据产品交易合同标准模板
数据产品及活动运营环节	/	/	制定针对各类数据产品更新频率、更新内容验证方法、更新通知方式的数据产品更新规范标准。 明确客户服务响应时间、问题解决率、服务态度等考核指标量化标准的数据产品客户服务质量标准。 制定涵盖活动策划流程、

			风险评估方法、活动审批标准、活动执行规范以及活动效果评估指标的数据产品活动策划与执行标准

参 考 文 献

[1] GB/T ×-×××× ××××××××××××

[2] FZ/T ×-×××× ××××××××××××

[3] T/CNTAC ×-×××× ××××××××××××