ICS
CCS 点击此处添加 CCS 号
登记号：

T/ACCEM

团　　体　　标　　准

T/ACCEM XXXXX—XXXX

数据资产安全合规有序交易流通指南

Guide for data asset security compliance and orderly trading circulation

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国商业企业管理协会　发布

目　　次

前　　言

本文件按照GB/T 1.1-2020《标准化工作导则 第一部分：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xxxx提出。

本文件由中国商业企业管理协会归口。

本文件起草单位：xxxxxx。

本文件主要起草人：xxxxxx。

数据资产安全合规有序交易流通指南

1 范围

本文件提供了数据资产交易的基本原则，提出了数据交易原则、交易流程、交易参与方和交易安全等各环节的合规要求。

本文件适用于组织、参与数据交易的组织，包括数据交易双方、数据交易服务商等。本指南旨在规范数据资产交易过程中所遵循的合规及安全要求。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

3.1

数据资产交易 data trading

以数据产品作为交易对象，进行的以货币或货币等价物交换数据商品的行为。

3.2

合规管理 compliance management

确保业务活动遵守相关法律法规、行业标准，采取的一系列管理措施和活动。

4 数据资产交易原则

4.1 合法合规

数据资产交易行为应遵守国家、地方相关法律法规，建立适用于数据资产交易服务平台的交易制度，规范数据资产交易参与方的各项行为。

4.2 公平公正

数据资产交易过程中不应存在不合理条件限制或排斥性条款，以及针对潜在数据资产交易参与方的歧视性待遇。

4.3 安全可控

应采用相关安全标准、安全技术，强化数据资产交易安全保护措施与应急响应措施，防止数据被窃取、损毁、泄露或篡改，确保数据资产交易全流程可供审计、溯源、调查，保证数据资产交易安全可控。

4.4 权益保护

应建立投诉处理与争议解决机制，对数据资产交易过程中合法权益受到损害的数据资产交易参与方及第三方机构提供法律保障。

5 数据资产交易流程合规要求

5.1 数据资产登记

数据产品提供方应在数据交易所进行产品登记，并提供：

a）数据产品持有者主体的基本信息；

b）数据产品的基本信息、物理信息、内容说明、来源描述；

c）数据产品说明书；

d）由第三方服务机构出具的数据产品合规评估报告；

e）由数据产品提供方或第三方服务机构出具的数据产品质量评估报告；

f）由数据产品提供方或第三方服务机构出具的数据产品资产评估报告。

5.2 发起交易

5.2.1

数据产品提供方通过数据交易所下属交易平台选择已登记的数据产品开放交易，应提供报价信息、交付方式、应用场景和使用限制、数据项示例、用户指南等。数据产品需求方可在交易平台选择数据产品发起交易流程。

5.2.2

数据交易所应对数据产品提供方所提供产品信息进行线上公开展示，可提供公开挂牌、定向交易等可选交易模式供数据产品提供方选择。

5.2.3

数据交易所应定期分析市场成交情况和已交易数据产品的应用价值，为数据交易双方提供各类数据产品的报价的区间参考值。

5.3 交易测试及协议签订

5.3.1

数据产品需求方可选择是否对数据产品进行交易测试。数据产品需求方可以在正式购买之前，对数据产品进行的有限期或有条件的测试使用，以评估其性能和适用性。

5.3.2

数据产品提供方与数据交易所应配合数据产品需求方进行数据产品的交易测试，提供相应的测试接

口或数据集测试样本等。

5.3.3

数据产品通过数据需求方的交易测试后数据交易所确认相关交易信息，并签订交易协议。交易协议应包括数据产品信息、价格、交付方式、使用场景及限制、违约责任、争议解决机制、数据使用期限以及适用法律等关键要素。

5.3.4

数据产品未通过数据需求方的交易测试的，数据需求方应向数据交易所提交未通过交易测试原因说明。如未通过数据测试原因为数据质量相关问题，数据提供方应及时对数据产品进行改进并更新，并配合数据交易所再次进行交易测试。

5.3.5

数据需求方由于交易测试未通过而提出中止交易的，数据交易所应中止相关交易流程，并对相关数据产品记录备案。

5.4 产品交付

5.4.1

数据交易双方可以协商选择数据产品交付方式。交付方式可包括物理媒介交付或电子方式交付，具体包括但不限于直接下载、通过云服务提供、API 接口调用、数据流传输、物理媒介如 CD/DVD 或 USB 驱动器的邮寄、以及通过专用的数据交易平台进行的加密和安全传输。交付方式旨在确保数据产品的安全性、完整性和可用性，同时满足不同用户的需求和偏好。

5.4.2

数据交易所可提供线上交付生态，供数据交易双方进行数据产品交付使用。线上交付生态应包含数据产品的展示、交易、支付以及售后服务等功能。

5.4.3

数据交易双方之间也可选择直接交付，交付明细数据和关联的账单信息需上传至相关数据交易所进行备案。

5.5 交易结算

5.5.1

交易双方应该按照协议约定的付款方式进行付款。

5.5.2

数据需求方转账至供方指定同名账户完成付款，并在数据交易所处上传交易凭证进行备案，由数据提供方确认并完成结算。

5.5.3

数据交易所应在交易结算完成后，为数据交易双方开具数据交易凭证。数据交易凭证一般包含以下信息：交易凭证编号、数据产品名称、数据产品代码、需方名称、供方名称、交易金额、使用目的、使用主体、时间限制、不得转让规则、发证日期等。

6 数据资产交易参与方合规要求

6.1 数据资产交易双方合规要求

6.1.1 主体资质

数据交易双方主体资质相关合规要求包括但不限于：

a. 依法成立、有效存续；
b. 具有良好商业信誉；
c. 法定代表人、董事、监事不存在重大数据类违法违规行为等情形；
d. 不存在重大财务风险；
e. 不存在影响持续经营的担保、诉讼、仲裁；
f. 过去三年无数据交易、隐私保护相关的行政处罚与行业处分。

6.1.2 数据来源

数据交易提供方应对其数据来源开展合规管理，具体要求包括：

a. 收集公开数据时，不得以不正当竞争目的收集信息，不得采取违法侵入，非法获取内部访问、操作权限，技术破解等违法违规方式获取数据；
b. 自行生产数据时，应确保数据的生产和处理行为合法协议获取数据时，应保存相关交易文件，依法取得特殊资质、许可、认证或备案，作出数据获取渠道合法、权利清无争议的承诺；
c. 收集个人信息时，应满足个人信息处理的相关法定要求。

6.2 数据资产交易服务商合规要求

6.2.2 主体资质

数据交易服务商主体资质相关合规要求包括：

a. 在中国境内依法设立并有效存续，数据依法存储在中国境内；
b. 组织治理结构完善，具备与从事数据交易相关服务相匹配的风险控制和数据保护能力；
c. 过去三年无数据相关行政处罚和行业处分以及其他重大违法违规行为。

6.2.3 其他要求

a. 数据交付服务商应提供安全可信的交付环境，并建立安全事件应急响应机制，发生交易数据泄露或其他安全事件时，应向数据交易平台报告并及时启动应急预案；
b. 数据专业评估服务商应严格依据法律规定和专业的审慎原则，出具评估报告、鉴定意见或者专家结论；
c. 数据专业中介和咨询服务商应确保其服务活动符合法律法规要求、保障数据交易安全、适应数据交易实际；
d. 清结算服务商应遵守相关的数据交易规则和标准，确保交易清结算流程的合法性、安全性和透明度，同时保障交易各方的权益。

7 数据资产交易安全要求

7.1 管理制度

数据交易参与方应积极履行数据安全保护义务，建立健全全流程数据安全管理制度，采取相应的技术措施和其他必要措施，确保数据在安全的基础上有序流通。

7.2 管理部门

数据交易参与方应设立数据安全管理部门，承担以下职责：

a) 在全面梳理业务和现有资源的基础上，应充分评估各相关部门在日常处理数据活动中的主要风险明确数据全生命周期的安全要求；

b) 应结合业务需求、监管要求、自身能力，确定企业数据安全目标，制定数据安全战略；

c) 应指定人员实施内部数据安全管理工作，明确工作职责与任务；

d) 应制定与完善数据安全管理规范体系并推动其有效实施；

e) 应统筹实施数据安全管理工作，监督落实数据安全管理制度及技术防护措施执行情况，对数据处理活动定期开展数据安全风险评估；

f) 应建立安全风险监测体系，采取措施监控内部数据处理活动和外部访问活动，防范不正当的数据访问和处理行为；

g) 应建立数据安全事件应急管理制度，制定数据安全事件应急预案并定期进行演练，及时处置数据安全风险和事件；

h) 应定期对员工进行数据安全宣传教育培训并考察员工能力与岗位职责的匹配程度；

i) 建立数据安全投诉受理、调查与督导机制，督促企业落实数据安全保护义务。

7.3 数据分类分级保护

数据交易参与方在对数据进行全面梳理时，可参照国家标准和行业标准，结合自身业务对数据进行分类分级，形成目录清单并采取相匹配的保护和管理措施。

7.4 数据安全管理

数据交易参与方应当建立数据安全管理制度针对不同类型和级别数据，实施数据收集、存储、使用、加工、传输、提供、销毁等环节的保护与管理，保障数据的保密性、完整性、可用性和合规性。

7.5 数据安全技术保护体系

数据交易参与方应当结合数据应用场景以及数据分类分级情况，可建立覆盖数据全生命周期的安全防护机制，采取数据加密、数据脱敏、身份认证、入侵防护、安全监测等技术保护措施，提高数据安全保障能力。

7.6 安全人员

数据交易参与方需明确关键岗位人员及员工数据安全问责规范，可通过制定可行的管理制度和操作规程、数据安全培训及考核等方式提升企业员工的数据安全意识。

7.7 安全事件应急响应机制

数据交易参与方应当制定数据安全事件应急预案，积极开展数据安全应急演练，提高对数据安全事件的预防和应对能力。