

T/JNBDA

济南市大数据协会团体标准

T/JNBDA 0005-2025

数据交易合同规范

Specifications for Data Transaction Contracts

2025 - 11 - 13 发布

2025 - 11 - 13 实施

济南市大数据协会发布

目 录

前言	1
1. 范围	1
2. 规范性引用文件	1
3. 术语和定义	1
3.1 数据产品 data production	1
3.2 数据交易 data transaction	1
3.3 数据卖方 data seller	1
3.4 数据买方 data buyer	1
3.5 数据产权 data property right	1
4. 基本原则	1
5. 交易主体资格	2
5.1 卖方资质	2
5.2 买方资质	2
5.3 禁止交易主体	2
6. 交易交易流程	2
6.1 前期准备	2
6.2 磋商与签约	2
6.3 交付	3
7. 数据产品交易协议内容	3
7.1 标准协议构成	3
7.2 非标准协议补充要求	4
8. 数据安全与隐私保护条款	4
8.1 数据分类分级	5
8.2 技术保障措施	5
8.3 数据备份条款	5
8.4 隐私保护条款	5
9. 争议解决与法律责任条款	5
9.1 协商与调解	5
9.2 仲裁与诉讼	5
9.3 赔偿标准	5
10. 附则	5
参考文献	6

前 言

本文件按照GB/T1.1-2020《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。

本文件由济南大数据协会提出并归口。

本文件起草单位：泰和泰律师事务所、济南六源数字科技有限公司。

本文件主要参与单位：山东土地数字科技集团有限公司、北京中企华资产评估有限责任公司山东分公司、国盾（山东）知识产权运营管理有限公司、山东浪潮傲林大数据科技有限公司、山东双泽信息技术有限公司、山东涛峻子淼智能科技有限公司、山东正源和信资产评估有限公司、泰山财产保险股份有限公司、易简大数据科技（山东）有限公司、正元节能科技（泰安）有限公司、中建八局第二建设有限公司、中荣国投智慧城市建设有限公司。

本文件主要起草人：尹晓东、黄怡敏、郑娟、于家欣、臧丽娟、张志红、吴博。

数据交易合同规范团体标准

1. 范围

本团体标准规定了数据产品交易合同的基本原则、术语定义、签约主体资格、交易流程、协议内容、审核机制、争议解决等要求，适用于通过数据交易平台进行的数据产品交易活动。

本标准旨在为数据交易参与方提供规范性指导，确保交易合法性、公平性与安全性，促进数据要素市场健康发展；适用于在中华人民共和国境内开展的数据交易活动中所涉及的数据交易合同的制定、签署、履行及管理。

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 38667-2020 信息技术 大数据数据分类指南

GB/T40094.1-2021 电子商务数据交易第 1 部分:准则

3. 术语和定义

下列术语和定义适用于本标准：

3.1 数据产品 data production

用于交易的原始数据和加工处理后的数据衍生产品。

注：数据产品包括但不限于数据集、数据分析报告、数据可视化产品、数据指数、API数据、加密数据等。

3.2 数据交易 data transaction

数据卖方和买方之间以交易标的作为交易对象，进行的以货币或货币等价物交换交易标的的行为。

3.3 数据卖方 data seller

在数据交易场所内或数据交易场所外由合法组织机构出售交易标的的组织或自然人。

3.4 数据买方 data buyer

在数据交易场所内购买交易标的的组织或自然人。

3.5 数据产权 data property right

包括数据所有权、数据加工使用权、数据经营权等，数据产权的具体内容和范围可由合同双方约定。

4. 基本原则

- 4.1 **合法性原则**：交易行为须符合国家法律法规及交易所规定。
- 4.2 **公平性原则**：交易双方权利义务对等，禁止垄断或恶意竞争。
- 4.3 **透明性原则**：交易流程、定价机制及协议内容应公开透明。
- 4.4 **安全性原则**：数据产品须符合数据安全与隐私保护要求。
- 4.5 **可追溯性原则**：交易全过程应留存记录，确保责任可追溯。

5. 交易主体资格

5.1 卖方资质

- a) 须具备数据产品合法权属证明；或者由数据交易所确认，并颁布数商资格。
- b) 数据产品需通过合规性审查，确保无法律风险。

5.2 买方资质

需方提供合法使用数据产品的用途说明。

5.3 禁止交易主体

涉及国家安全、公共利益或敏感个人数据的非法交易主体。

5.4 完善合同主体信息

明确数据交易合同的双方主体，包括名称（姓名）、住所、联系方式、统一社会信用代码（身份证号码）等基本信息。同时需注明双方主体具备相应的民事权利能力和民事行为能力，能够依法独立享有民事权利和承担民事义务，确保主体资格合法。

6. 交易流程

6.1 前期准备

6.1.1 数据产品审核

供方做好数据产品合规审查工作，并提交产品信息及合规证明。

6.1.2 需方测试申请

需方可申请对数据产品进行试用测试，供方须在 5 个工作日内响应。

6.1.3 数据产品描述

合同对交易的数据需进行详细描述，包括数据类型、数据来源、数据格式、数据量、数据涵盖的时间范围等信息，确保双方对交易的数据有清晰一致的理解；特别要说明数据来源的合法性，如数据是通过合法收集、加工等方式获得，不存在侵犯他人合法权益的情形。

6.2 磋商与签约

6.2.1 订单生成

供需双方通过磋商协议明确产品内容、价格、交付方式等要素。

6.2.2 协议选择

双方选择标准协议（详见7.1 标准协议构成）或拟定非标准协议，非标准协定需要满足7.2 的要求。

6.2.3 协议签署

通过电子签名或线下签章完成合同签署。

6.3 交付

6.3.1 交付流程

数据供方按照数据交易合同约定方式向数据需方进行数据交付的流程如下：

- a) 数据供方按约定向数据需方交付数据交易标的；
- b) 数据需方按约定接收、验证数据交易标的；
- c) 数据交易双方进行确认交付完成。

6.3.2 交付方式

双方确定数据交付的方式（如应用程序接口 API、数据集传输等）、交付时间、交付地点等内容，确保数据能够按照约定顺利交付给接收方。交付过程需符合相关法律法规关于数据传输的规定，保障数据传输的合法性和安全性。

7. 数据产品交易协议内容

7.1 标准协议构成

7.1.1 基础条款

交易双方名称、联系方式及资质证明。

数据产品名称、版本及内容。

7.1.2 权利义务条款

供方确保数据合法性与完整性，需方承诺合规使用。

保密义务：双方不得泄露交易内容及数据细节。

7.1.3 交付

交付时间、方式（API接口、文件传输等）。

7.1.4 数据质量标准与验收

从数据规范性、完整性、准确性、一致性、时效性、可访问性等多维度设定明确的数据质量评估标准。

约定验收方式、时间、流程等，数据接收方在约定的检验期限内完成数据验收；明确非经使用无法判断数据质量时的处理方式。

7.1.5 费用与结算

计价方式（按次、按量、订阅制等）、支付期限及发票开具要求。

7.1.6 违约责任

延迟交付、数据质量问题、未履行保密义务的赔偿标准。

7.1.7 保密条款

双方对在数据交易过程中知悉的对方商业秘密、数据内容等信息负有保密义务，保密期限、保密范围、违约责任等应详细明确。

保密条款不得违反法律关于保密义务的强制性规定。

7.1.8 争议解决

协商、调解、仲裁或诉讼等途径。

7.1.9 数据安全

7.1.9.1 数据安全基本要求

明确双方在数据安全方面的责任和义务，包括但不限于数据存储安全、数据传输安全、数据使用安全等。

7.1.9.2 重要数据和个人信息

重要数据和个人信息处理，应符合相应的技术标准，如匿名化处理并提供脱敏算法合规性证明，重要数据交付前需完成数据安全风险评估并提供《数据分类分级报告》。

7.1.9.3 数据提供方责任

在数据交付前承担主要安全责任，包括：

确保数据在存储和传输过程中采取必要的加密、访问控制等安全措施，防止数据在交付前发生泄露、篡改或丢失。

向数据接收方提供必要的数据安全使用指导和说明，包括数据的安全存储方式、适用的安全技术标准等。

7.1.9.4 数据接收方责任

在数据接收后承担主要安全责任，包括：

在数据接收后，建立健全数据安全管理制度，配备必要的技术设施，采取加密、备份、防病毒等技术措施保障数据的存储、使用和传输安全，防止数据泄露、篡改、丢失等情况发生。

不超出合同约定的使用范围使用数据，不将数据用于非法目的。

涉及数据共享或二次转让，应事先获得数据提供方的书面同意，并确保接收方同样遵守本合同的安全要求，对接收方的安全行为进行监督和管理。

7.1.9.5 双方共同责任

共同建立数据安全应急响应机制，发生数据安全事件时的通知流程、处置措施和责任分工；发生数据安全事件，及时通知对方，配合对方采取措施进行处置，防止事态扩大。

7.2 非标准协议补充要求

7.2.1 必须包含标准协议中的基础条款和核心条款（包括违约责任、数据安全）。

7.2.2 个性化条款需经双方书面确认。

8. 数据安全与隐私保护条款

8.1 数据分类分级

根据《数据安全法》对数据产品进行敏感度分级（一般数据、重要数据、核心数据），并在交易合同中载明数据等级。

8.2 技术保障措施

在条款中需涉及具体的技术保障措施，包括但不限于加密传输、访问控制、日志留存等具体要求。

8.3 数据备份条款

供需双方应当保留相关数据备份，以防止双方的系统故障或任何其他不可预见的事件导致相关数据或其任何部分丢失。

8.4 隐私保护条款

合同中涉及个人信息的，需取得个人同意或进行匿名化处理。

9. 争议解决与法律责任条款

9.1 协商与调解

争议发生后，双方应在10个工作日内协商解决。

9.2 仲裁与诉讼

约定合同争议的解决方式，可选择协商、调解、仲裁或诉讼等方式，明确仲裁机构或管辖法院等相关信息。

争议解决方式的约定应符合《民事诉讼法》《仲裁法》等相关法律法规的规定。

9.3 违约责任及赔偿标准

双方在违反合同约定时应承担的违约责任，包括但不限于支付违约金、赔偿损失、继续履行合同等方式，违约金的数额或计算方式应合理明确，违约方需承担直接损失及合理维权费用（律师费、鉴定费等）。

违约责任约定应不违反法律关于违约金的限制性规定。

10. 附则

10.1 标准修订

本标准由济南大数据协会负责解释与修订，每两年评估一次。

10.2 实施日期

自发布之日起生效，过渡期内原有协议可继续执行。

10.3 合法性审查建议

为进一步确保数据交易合同的合法性和有效性，建议合同双方在签署合同前，将合同文本提交专业法律机构或律师进行合法性审查。

审查内容包括但不限于合同主体资格、合同条款的合规性、权利义务的公平性等。

参考文献

- [1] 《中华人民共和国民法典》
- [2] 《中华人民共和国数据安全法》
- [3] 《中华人民共和国个人信息保护法》
- [4] 《中华人民共和国网络安全法》
- [5] GB/T 25069-2022 信息安全技术 术语
- [6] GB/T 35273-2020 信息安全技术 个人信息安全规范
- [7] GB/T 37964-2019 信息安全技术 个人信息去标识化指南
- [8] GB/T 38667-2020 信息技术 大数据 数据分类指南
- [9] GB/T 43697-2024 数据安全技术 数据分类分级规则
- [10] GB/T 40094.1-2021 电子商务数据交易第 1 部分:准则