ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 37932—XXXX
代替 GB/T 37932-2019

信息安全技术　数据交易服务安全要求

Information security technology—
Security requirements for data transaction service

(征求意见稿)

(本稿完成时间：2023 年 8 月 25 日)

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

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

本文件代替GB/T 37932—2019《信息安全技术 数据交易服务安全要求》。与GB/T 37932—2019相比，除编辑性改动外，主要技术变化如下：

a) 增加了“数据交易服务平台安全要求”一章（见第 6 章）；
b) 更改了“总则”的数据交易活动参考模型（见 4.1）；
c) 增加了数据交易安全原则章节（见 5）；
d) 增加了数据交易参与方的“基本要求”（见 6.1）；
e) 增加了数据商和第三方专业服务机构安全要求（见 6.4）；
f) 更改了“禁止交易数据”的有关要求（见 8.1）；
g) 更改了“数据质量合规要求”的有关要求（见 8.2）；
h) 增加了数据交易标的中“交易数据分类分级保护”的有关要求（见 8.3）；
i) 更改了数据交易过程的“交易磋商”的有关要求（见 9.2）；
j) 增加了数据交易过程的“产品交付、交易结算”（见 9.3）；
k) 增加了数据交易过程的“纠纷处理”（见 9.4）；
l) 增加了禁止交易数据示例（见附录 A）。

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。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：中国电子技术标准化研究院、上海数据交易所有限公司、北京国际大数据交易有限公司、华控清交信息科技（北京）有限公司、浙江省数字经济发展中心、上海市信息安全测评认证中心、浙江大数据交易中心有限公司、中国网络空间安全研究院、北京市政务信息安全保障中心、华东江苏大数据交易中心股份有限公司、阿里巴巴（北京）软件服务有限公司、蚂蚁科技集团股份有限公司、国家计算机网络应急技术处理协调中心、中国网络安全审查技术与认证中心、陕西省信息化工程研究院、浙江大学等。

本文件主要起草人：上官晓丽、胡影、李海东、姚相振、苏丹、卓训方、郎佩佩、靳晨、田燕翔、金铭彦、陈钰玮、姜伟、李媛、张宇光、李世奇、白晓媛、王秉政、盛晶、王云河、谭坤、陈世翔、王晖、张勇、刘金飞、程瑜琦等。

本文件及其所替代文件的历次版本发布情况为：

——2019 年首次发布为 GB/T 37932—2019；
——本次为第一次修订。

引　言

当前，数据作为新型生产要素，数据基础制度建设事关国家发展和安全大局。2022年12月，《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》发布，提出二十条政策举措，从数据产权、流通交易、收益分配、安全治理等方面构建数据基础制度。数据流通交易作为数据基础制度之一，能够激活数据要素潜能，促进数字经济发展，但与此同时也面临数据权属、数据定价、安全合规、场内场外交易等难点问题，亟需建立健全数据交易管理制度，规范数据交易行为，保障数据要素市场高质量发展。

本文件根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》等政策法规要求，提出了统一的数据交易安全规则，规定了数据交易服务安全要求，适用于规范数据交易场所和交易服务生态的数据交易活动，为建立健全数据交易制度，保障数据要素市场高质量发展提供标准支撑。

信息安全技术　数据交易服务安全要求

1　范围

本文件规定了数据交易服务安全要求，包括数据交易参与方、交易对象、交易平台及交易过程的安全要求。

本文件适用于数据供方、数据需方、数据交易场所、数据商、第三方专业服务机构规范其数据交易活动，也适用于监管部门、评估机构对数据交易服务安全进行监督、管理、评估。

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 22239　信息安全技术　网络安全等级保护基本要求
GB/T 25069　信息安全技术　术语
GB/T 35273　信息安全技术　个人信息安全规范
GB/T 36343　信息技术　数据交易服务平台　交易数据描述
GB/T 37988　信息安全技术　数据安全能力成熟度模型
GB/T 39335　信息安全技术　个人信息安全影响评估指南
GB/T AAAAA　信息安全技术　数据分类分级规则
GB/T BBBBB　信息安全技术　数据安全风险评估方法

3　术语与定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

数据资源　data resources

由组织或个人持有的，加工后具有经济价值的数据。

3.2

数据产品　data product

数据资源经过实质性处理后，形成依法可交易、满足用户特定需求的产品。

注：数据产品，通常涉及 API 接口、数据集、数据报告等。

3.3

数据交易　data transaction

以数据产品作为交易标的，进行的以货币或货币等价物交换数据使用权和市场化流通的行为。

3.4

数据供方 data supplier

数据交易中出售和提供数据产品的组织，简称供方。

3.5

数据需方 data demander

数据交易中购买和使用数据产品的组织，简称需方。

注：数据供方和数据需方，合称为数据交易双方。

3.6

数据交易场所 data transaction place

为数据集中交易提供场所和基础设施，组织和管理数据交易活动的组织机构。简称交易所。

3.7

数据商 data provider

为数据交易双方提供数据产品开发、发布、承销和数据资产的合规化、标准化、增值化等服务，提高数据交易效率的组织机构。简称数商。

注：广义的数据商也包括数据供方，泛指将数据资源加工处理成数据产品，或者受委托提供数据产品开发、发布、承销等服务的组织。

3.8

第三方专业服务机构 third-party professional service agency

辅助数据交易活动有序开展，提供法律服务、数据资产化服务、安全质量评估服务、培训咨询服务及其他第三方服务的组织机构。

注：第三方服务包括数据集成、数据经纪、合规认证、安全审计、数据公证、数据保险、数据托管、资产评估、争议仲裁、风险评估、人才培训等服务。

3.9

数据交易服务 data transaction service

为帮助数据供方和需方完成数据流通交易全过程，实现数据资产化和数据价值变现提供的各类服务。

3.10

数据交易平台 data transaction platform

为供需双方提供数据交易服务的信息系统。

3.11

场内交易 insite transaction

数据供方和数据需方依托数据交易场所开展数据交易。

3.12

场外交易 off-site transaction

数据供方和数据需方不通过数据交易场所，直接或依托数据商、第三方专业服务机构完成数据交易。

3.13

数据交易参与方 data transaction participants

参与数据交易服务的相关方。

注：场内交易的参与方可能涉及数据交易场所、数据供方、数据需方、数据商、第三方专业服务机构，场外交易的参与方可能涉及数据供方、数据需方、数据商、第三方专业服务机构。

3.14

数据交易标的 data transaction object

数据供需双方交易的数据产品，也称数据交易对象或交易数据。

3.15

数据交易过程 data transaction process

数据交易参与方针对具体的数据交易标的，进行的一组完整和具体的数据交易活动。

3.16

交付 delivery

数据供方按照协议约定，使数据需方实际访问、调用、计算（处理）或取得交易数据产品的行为。

注：访问，是指数据供方仅给数据需方使用数据的环境或接口允许其计算、查阅数据，但不允许其下载、复制或下载原始数据到本地的交付方式。

4 总则

4.1 数据交易服务参考模型

数据交易服务分为场内交易和场外交易两种模式，场内交易是数据供方和需方依托数据交易场所进行交易，场外交易则是数据供需双方在交易场所外进行交易。实际交易中，既可能由数据供需双方直接或通过数据交易场所交易，也可能有数据商参与数据交易过程，为交易双方提供数据产品开发、发布、承销等服务，还可能有第三方专业服务机构提供法律、数据资产化、安全质量评估、培训咨询等服务，辅助数据交易活动有序开展。数据交易服务参考模型如图 1 所示。

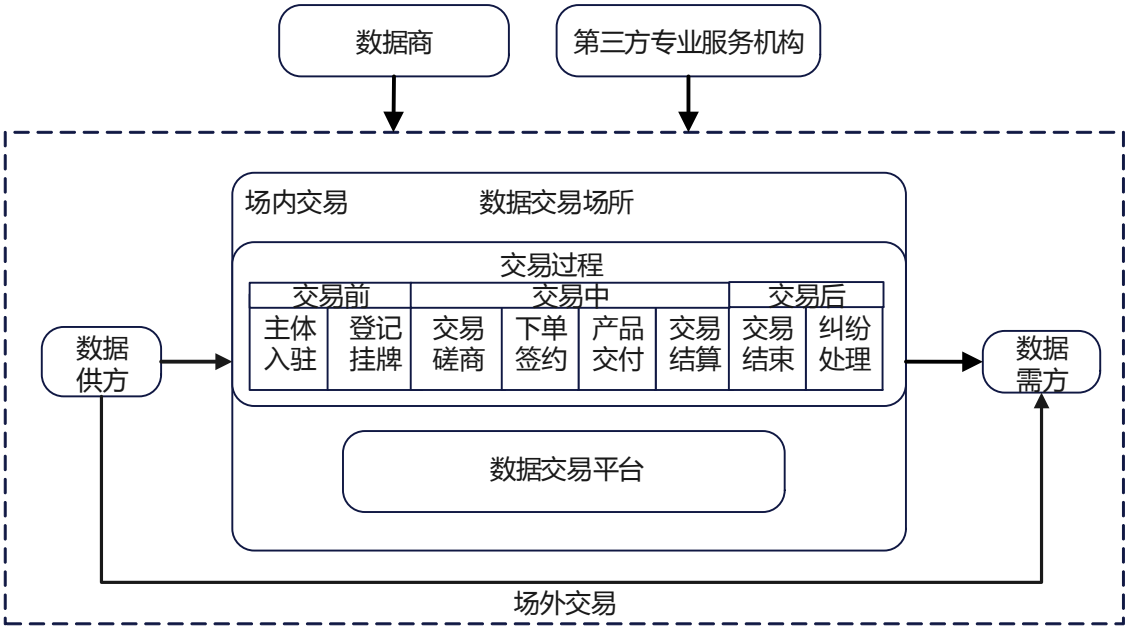

图 1　数据交易服务参考模型

4.2　数据交易过程

场内交易全过程，通常包括主体入驻、登记挂牌、交易磋商、下单签约、产品交付、交易结算、交易结束、纠纷处理等环节。其中，主体入驻、登记挂牌属于交易前的准备阶段，交易磋商、下单签约、产品交付和交易结算属于交易中的实施阶段，交易结束、纠纷处理则属于交易后的售后阶段。场外交易过程，通常涉及交易磋商、下单签约、产品交付、交易结算、交易结束等环节。

a) 主体入驻：数据供方、需方、数据商、第三方专业服务机构等入驻数据交易场所，完成用户注册、实名认证、资质审核、信息完善等。

b) 登记挂牌：对数据交易标的进行信息登记,并对数据产品合规性、质量等进行评估审核，审核通过的数据产品在数据交易场所挂牌上架。

c) 交易磋商：交易双方对接后，对交易标的的交易用途、交易金额、交付方式、安全责任等内容进行协商，需方也可申请数据产品或样本数据测试。如还需对数据产品进一步加工，需方可发布需求，由数据供方或数据商对数据进行加工。

d) 下单签约：数据需方选择数据产品下单，待供方确认订单信息后，双方签订数据交易合同协议，数据交易场所对合同进行审核和备案。

e) 产品交付：按照数据交易合同协议约定交付数据产品，通过数据交易平台、数据商或交易双方自主进行交付，数据需方对交付的数据产品进行验收。

f) 交易结算：按照合同协议约定和交易账单支付交易费用，对交易参与方的费用进行结算，并支持对超额购买的费用进行退款。

g) 交易结束：结束此次数据交易操作，并对交易相关信息进行记录、存证、审计等，同时提供数据交易售后服务。

h) 纠纷处理：建立数据交易投诉举报和争议解决机制，对数据交易的投诉、举报、争议、纠纷进行处理，支持对违法违规数据交易行为进行审查追溯，保障交易参与方权益。

4.3　数据交易标的

数据交易标的，通常涉及 API 数据、数据集、数据报告、数据应用、数据工具、数据服务、其他数据等数据产品。

a) API 数据：通过应用程序接口 API 实现调用的数据；
b) 数据集：具有一定主题，可满足用户需求的数据集合或数据文件；
c) 数据报告：对数据进行统计、建模、分析等处理，以文字、图表等可视化方式呈现的报告；
d) 数据应用：数据资源经过加工处理后，提供的数据应用服务或定制化解决方案；
e) 其他数据：其他依法可交易的数据产品，如应用账号、算法模型、数据指数、加密数据等；
f) 数据工具：提供数据采集、存储、传输、预处理、加工、可视化、删除等数据处理能力的工具；
g) 数据服务：在数据交易过程中，由数据商、第三方专业服务机构提供的数据服务，如数据采集服务、数据加工服务、安全评估服务等。

5 数据交易安全原则

数据交易应遵循以下安全原则：

a) 合法合规原则：数据交易参与方应遵守法律法规等有关规定，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，不得危害国家安全、公共利益，不得损害个人、组织的合法权益；
b) 过程可控原则：数据交易过程应确保数据来源合法可确认、使用范围可界定、交易过程可追溯、安全风险可防范；
c) 分类分级原则：数据交易标的应遵守国家和行业数据分类分级保护要求，结合数据流通范围、影响程度、潜在风险，建立公共数据、企业数据、个人信息等数据分类分级授权使用和保护机制；
d) 确保安全原则：数据交易参与方应采取必要的管理措施和技术手段，防范交易对象被篡改、破坏、泄露或者非法获取、非法利用、非法交易等风险，保障个人信息主体权益；
e) 权责一致原则：数据交易参与方在享有数据要素流通收益的同时，应当对各自的数据交易活动承担安全责任。
    1) 数据供方应对数据交易标的的质量、安全和合规负责；
    2) 数据需方应对数据交易标的使用的安全和合规负责；
    3) 数据交易场所应对数据交易平台安全、交易过程合规监管等负责；
    4) 数据商、第三方专业服务机构应对其提供的产品服务的安全性、合规性负责。

6 数据交易参与方安全要求

6.1 基本要求

数据供方、需方、数据商、第三方专业服务机构、数据交易场所等交易参与方，应满足以下要求：

a) 应遵守合法合规、过程可控、分类分级、确保安全、权责一致等数据交易安全原则；
b) 不应以欺诈、诱骗、误导、胁迫、贿赂等方式交易数据；
c) 不应从数据流通非法产业交易数据；
d) 数据交易服务需取得相关行政许可的，应取得行政许可；
e) 应谨慎对待原始数据交易；
f) 应履行数据处理者安全保护义务，建立全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全；

g) 应制定安全应急预案，发生数据安全事件时，应立即采取处置措施，按照规定及时告知相关方并向有关主管部门报告；
h) 涉及个人信息的，应依法承担个人信息处理者责任，履行个人信息保护义务；
i) 涉及跨境交易向境外提供数交易标的的，应遵守国家数据出境管理有关规定；
j) 涉及人工智能算法模型的，应遵守人工智能有关规定；
k) 涉及知识产权的，不应侵害他人依法享有的知识产权；
l) 场内交易的供方、需方、数据商和第三方专业机构应完成交易所入驻才能进行数据交易，交易时应遵守数据交易场所的制度要求。

6.2 数据供方

数据供方在符合6.1基本要求基础上，还应满足以下要求：

a) 组织作为供方进行数据交易，应满足以下条件：
   1) 依法成立并有效存续，具有承担民事责任能力；
   2) 具有良好的商业信誉，无重大财务风险；
   3) 注册成立时间应超过一年
   4) 业务经营活动需取得相关行政许可的，应当依法取得行政许可；
   5) 近一年不存在违法违规和失信记录；
   6) 近一年未发生网络和数据安全事件；
   7) 具备数据要素市场主体相应的数据安全能力；
b) 供方应确保交易标的的数据来源合法，保证对数据资源的处理活动合规；
c) 供方应有正当合法的经营目的，且挂牌交易标的在本身的业务范围内或者与自身业务直接相关；
d) 供方应保障交易标的的数据质量，加强数据的真实性、准确性、完整性；
e) 供方应采取措施保护交易标的安全，防范数据泄露、篡改、破坏或者非法获取、非法利用等风险；
f) 供方应真实、准确、完整披露交易标的信息，不应隐瞒数据来源及涉及的个人信息、重要数据；
g) 如存在数据流通限制，供方应明示数据产品使用数据产品使用或流通的目的、方式、范围进行明确说明，法律法规另有规定的除外。

6.3 数据需方

数据需方在符合6.1基本要求基础上，应满足以下要求：

a) 组织作为需方进行数据交易，应满足以下条件：
   1) 依法成立并有效存续，具有承担民事责任能力；
   2) 具有良好的商业信誉，无重大财务风险；
   3) 近一年不存在违法违规和失信记录；
   4) 近一年未发生网络和数据安全事件；
   5) 具备数据要素市场主体相应的数据安全能力；
b) 需方使用交易标的应具有明确、合理的目的，购买的交易标的应与使用目的直接相关；
c) 需方应按照数据交易双方协议约定使用数据，授权使用范围不应超出交易协议约定要求的流通范围；
d) 需方应具备与处理交易标的相适应的数据安全能力；
e) 需方不应绕过或破坏交易数据的安全保护措施，不应对去标识化的个人信息进行重新识别；

f) 需方对交易数据的使用加工，不应对国家安全、公共利益造成影响，不应损害组织或个人合法权益；
g) 需方应按照交易约定的授权范围，合理确定交易数据的访问权限，并定期对相关人员进行安全培训；
h) 需方应对供方提供的交易标的的安全性、合规性进行审核；
i) 需方在数据交易协议到期或按照约定完成交易数据使用目的后，应按照协议约定要求及时对交易数据进行处理。

6.4 数据商和第三方专业服务机构

数据商和第三方专业服务机构应满足以下要求：

a) 组织作为数据商或第三方专业服务机构参与数据交易，应满足以下条件：
   1) 在我国境内依法成立并有效存续，具有承担民事责任能力；
   2) 具有良好的商业信誉，无重大财务风险；
   3) 近两年不存在违法违规和失信记录；
   4) 近两年未发生网络和数据安全事件；
   5) 具备从事相关业务的技术能力和经验；
   6) 具备数据要素市场主体相应的数据安全能力；
   7) 如从事数据商、第三方专业服务机构服务需要专门资质的，应取得相应资质许可。
b) 未经授权不应将数据商、第三方专业服务机构身份提供给他人使用；
c) 应对数据商、第三方专业机构提供的产品服务的安全性、合规性、真实性和有效性负责。
   1) 从事专业评估服务的，应按照法律法规要求和专业审慎原则，对交易标的进行严格审查，确保交易标的来源合法、内容真实、质量可靠；
   2) 从事数据开发服务的，应保障数据开发过程安全可追溯；
   3) 从事数据发布、承销服务的，应严格审核数据来源及数据供方的身份、资质，未达到数据安全合规要求的不代理；
   4) 从事数据交付服务的，应提供安全、可信的交付环境，确保数据交付安全；
d) 第三方专业服务机构应坚持独立、客观、公正原则开展服务，出具的法律意见书、评估报告、鉴定意见、专家结论、认证证书等，应保证客观性、真实性、准确性和完整性，不应出现虚假记载、误导性陈述等违反法律法规、行业规则的情形，自觉接收数据交易场所和有关部门的监督检查；
e) 未经委托方同意，不应将数据商、第三方专业服务机构的服务外包，如确需外包应征得委托方同意，并对外包方的数据安全能力、资质进行审核，明确外包方的安全责任、保密义务和任务结束后的数据处理方式；
f) 应妥善保管供方或需方的数据资料，不应泄露、伪造、篡改、隐藏、毁损；
g) 按照约定方式完成服务后，及时删除收到的客户数据和服务过程中所产生的相关数据。

6.5 数据交易场所

6.5.1 制度机制

数据交易场所应满足以下要求：

a) 提供数据集中交易场所，建设安全稳定的数据交易环境，支持数据交易合规监管和基础服务；
b) 建立数据交易管理制度，明确数据交易主体、交易标的、交易平台、交易过程、交易安全、纠纷处理等交易规则、管理规范和服务指南；

c) 建立交易所内部数据安全制度，对交易所提供服务过程中收集和产生的数据进行安全管理，并规范数据交易相关人员的安全操作规则；
d) 建立数据交易主体入驻、交易标的上市、交易合同登记等审核机制，对数据交易主体、交易标的、交易订单、交易合同等进行审核；
e) 建立交易所信息报送和披露机制，及时披露数据交易行情、重大事项等信息，及时向市场主体提示数据交易风险，定期将数据交易情况报送相关监管部门；
f) 应真实、准确、及时披露上市交易标的信息，不应以虚构交易、编造用户评价等方式进行虚假或者引人误解的商业宣传，欺骗、误导交易主体；
g) 发现违反市场监督管理、网络安全、数据安全等有关规定的数据交易行为，应依法采取必要的处置措施，保存有关记录，并向相关监管部门报告；
h) 不应未经交易主体委托、违背交易主体意愿、假借交易主体名义开展交易活动，不应传播虚假信息诱导交易主体进行不必要的交易；
i) 应建立完善数据交易主体信用评价制度，公示信用评价规则，为消费者提供对交易所上市售的交易标的进行评价的途径，且交易所不应删除消费者评价；
j) 应建立交易所数据交易管理制度、内部数据安全制度的制定、评审、发布流程，及时对制度内容进行更新完善，定期对制度落实情况进行监督；
k) 未经授权不应私自留存及使用数据供方或需方的数据或数据衍生品，法律法规另行要求的除外；
l) 应建立数据交易合规巡检机制，定期对交易主体、交易标的的安全性、合规性进行检查；
m) 应定期开展数据安全风险评估和个人信息保护合规审计，并向有关部门报送风险评估报告和合规审计报告；
n) 建立数据交易所违规行为处罚机制，对数据交易过程中的违规行为进行处罚；
o) 建立数据交易主体入驻和退出机制，提供主体入驻交易所和主动退出的渠道和方式，如交易主体存在严重违反交易规则的行为，交易所也可要求主体退出并终止其数据交易；
p) 建立交易标的上市和退出机制，提供数据资产登记、交易标的上市和下架退出的方式。

6.5.2 机构人员

数据交易场所应满足以下要求：

a) 数据交易场所注册成立，应获得有关部门的授权或许可；
b) 应明确数据安全负责人和主要职责，负责人应由交易所最高管理者或授权代表担任；
c) 应明确数据安全管理部门，配备相应的数据安全岗位和人员，落实数据安全保护责任，并对数据交易安全和个人信息保护进行监督；
d) 应定期开展员工数据安全教育培训，鼓励数据交易主体参加数据安全培训；
e) 应明确数据交易人员关键岗位，关键岗位人员入职进行背景调查，并定期进行安全考核和行为安全审计，确保无违法违规记录；
f) 新员工入职应签署安全保密协议，建立人员转岗、离岗管理制度，及时回收人员账号权限；
g) 数据交易所的董事、监事、高级管理人员及其他工作人员，不应直接或间接入市参与本交易场所交易，也不应接受委托进行交易。

7 数据交易平台安全要求

7.1 基本要求

数据交易平台应满足以下基本要求：

a) 应对交易过程进行安全管控，确保数据来源合法可确认、使用范围可界定、交易过程可追溯、安全风险可防范；
b) 符合 GB/T 22239—2019 中第 3 级相关要求；
c) 从事境内数据交易服务的数据交易平台，应部署在我国境内；
d) 采用的密码技术应符合国家密码管理相关要求；
e) 加强安全风险监测，发现安全缺陷、漏洞等风险时，立即采取补救措施。

7.2 交易数据安全保护

数据交易平台应保护交易数据安全，满足以下要求：

a) 应提供安全的数据传输通道，保证数据在传输过程中的保密性和完整性；
b) 应为数据供方、需方提供安全的上传或下载接口，包括基于密码技术的身份认证、访问控制、传输链路加密、传输数据保密性和完整性校验等保护措施；
c) 应对数据交易平台接口的不安全输入参数进行限制和过滤，为接口提供异常处理能力；
d) 应为数据交易标的生成不可篡改的电子凭证，实现交易标的和交易操作的可追溯性及交易的不可否认性；
e) 宜提供敏感数据识别和数据分类分级管理能力，能够根据交易标的的分类分级结果，对敏感数据进行识别和标注，并采用相应安全能力的数据流通安全保障技术进行交付；
f) 如数据交易平台提供数据交付能力，应提供安全稳定的数据交付环境，如：
   1) 宜支持原始数据不出域、数据可用不可见的交付方式；
   2) 宜提供隔离安全环境，并采取数据加密、访问控制、数据防泄漏、水印溯源、安全审计等措施，防止交易过程中的数据泄露、篡改、破坏或非法获取、非法交易、非法利用等；
g) 采取隔离存储、加密存储等措施，保障交易数据在存储过程中的保密性和完整性；
h) 提供数据交易平台的热冗余，支持本地数据备份恢复、异地实时备份等功能，保证系统和数据的高可用性；
i) 数据加工所涉算法的提供者应落实主体责任，加强算法安全管理，确保算法能维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益；
j) 具备恶意代码防护能力，能够对交易数据含有的恶意代码进行检测。

7.3 交易过程安全控制

数据交易平台应对交易全过程进行安全管控，满足以下要求：

a) 对数据交易主体身份进行鉴别认证，并对用户进行权限管理和访问控制；
b) 允许对数据交易的参与方、对象、关键过程设置人工干预功能，人工干预内容至少包括交易参与方审核、交易数据和需求审核、交易暂停、交易撤销、交易恢复；
c) 宜提供交易合约的创建、上传、编辑、确认等功能，交易合约内容包括但不限于数据供方、数据需方、处理数据的算法逻辑或相关数据服务，数据的使用频次、使用期限、使用场景等；
d) 数据交易平台可提供电子化交易合约模板，各交易主体对合约条款内容进行电子签名和确认；
e) 宜采用区块链技术对交易过程主要环节进行登记存证，记录交易参与方、交易标的、交易行为等信息，并确保存证信息不可篡改、不可伪造和可追溯性；
f) 授予数据交易各参与方所需的最小必要权限，实现各参与方的权限分离；
g) 数据交易标的上架挂牌前应通过评估，数据交易平台应对评估结果进行审核和记录，确保交易标的的安全性、合规性和数据质量；
h) 对于已实现数据交易目的或授权到期等情况，应立即删除或销毁交易数据，并对删除或销毁的效果进行记录和定期审计。

7.4 交易安全审计

数据交易平台应建立安全审计机制，满足以下要求：

a) 应记录、保存平台发布的交易标的信息和交易信息，确保信息的完整性、保密性和可用性，交易标的信息和交易信息保存时间自交易完成之日起不少于三年；
b) 交易信息应记录每笔数据交易信息，至少包括交易唯一标识、交易时间、供方、需方、交易标的、交易量、交易金额、交付方式、交易结果等；
c) 应在数据交易平台运营过程中，记录急交易主体、运营人员的操作处理、权限管理、交易过程等日志，日志留存时间不少于六个月；
d) 应定期开展数据交易安全审计，仅允许授权审计员访问数据交易日志，支持对数据交易日志进行查询和分析；
e) 允许数据交易参与方查询与自己数据交易相关的日志信息，并允许导出；
f) 支持监管方访问交易日志、数据存证、电子服务合约等审计资料，开展数据交易服务的安全监管工作；
g) 采取相应技术手段，对日志记录和安全审计结果进行保护，防止未授权篡改、破坏或泄露。

8 数据交易标的安全要求

8.1 禁止交易数据

数据交易标的应遵循合法、安全和可交易原则，满足以下要求：

a) 数据交易标的应具有明确、合理的应用场景和具体用途；
b) 有下列情形之一的数据交易标的，不应进行流通交易：
    1) 涉及国家秘密的信息；
    2) 危害国家安全和社会稳定的数据；
    3) 涉及损毁他人名誉及未经授权的身份、财产和其他敏感数据等特定个人权益的；
    4) 涉及未经授权的企业数据、商业秘密等特定企业权益的；
    5) 未经自然人或其监护人同意，涉及其个人信息的数据；
    6) 侵犯他人肖像、名誉、荣誉等人格权的数据；
    7) 未经有关部门授权，涉及公共利益、公共安全的公共数据；
    8) 未依法依规公开的原始公共数据；
    9) 关系国家安全、国民经济命脉、重要民生、重大公共利益等国家核心数据；
    10) 以欺诈、诱骗、误导等方式或者从非法、违规渠道获取的数据；
    11) 其他法律、法规明确规定禁止交易的数据。
c) 数据交易场所应根据我国相关法律法规，制定禁止交易数据目录，禁止交易数据示例见附录 A。

8.2 数据质量合规要求

d) 为确保交易数据的质量和合规，应满足以下要求：
a) 数据供方应向数据交易所、数据需方提供数据交易标的合法性的证明和承诺。
    1) 针对公开收集的数据，应说明公开数据收集的目的、方式、范围，提供公开收集的数据类型、采集策略、数据来源、收集合法性证明等。
    2) 针对组织经营活动和信息系统自行产生的数据，应说明系统建设和运维情况及其数据采集的目的、方式、范围情况；
    3) 针对协议方式获取的数据，应提供完整的购买协议、合作协议或许可使用协议等；

4) 针对用户授权获取的数据，应说明数据获取的目的、方式范围，并提供用户授权证明。

b) 数据供方向数据交易场所、数据需方提供拥有交易完整相关权益的明确声明；
c) 数据供方向数据交易场所、数据需方提供交易数据真实性的明确声明；
d) 数据供方明确交易数据的限定用途、使用范围、交易方式和使用期限；
e) 数据供方按照 GB/T 36343 要求对交易数据进行准确描述，明确数据类别等信息，描述信息满足准确性、真实性要求；
f) 数据交易场所、数据需方对交易数据描述和样本的准确性、真实性进行审核。

8.3 交易数据分类分级保护

交易数据分类分级保护，应满足以下要求：

a) 交易数据应按照国家和行业有关要求进行数据分类分级，识别可能涉及的个人信息、公共数据和重要数据；
b) 结合数据流通范围、影响程度、潜在风险，建立公共数据、企业数据、个人信息等数据分类分级授权使用和保护机制；
c) 在保护个人隐私和确保公共安全的前提下，公共数据宜按照“原始数据不出域、数据可用不可见”的要求，以模型、核验等产品服务等形式向社会提供；
d) 在保护个人合法权益的前提下，涉及个人信息的数据交易应征得个人单独同意，并向个人告知数据需方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类；
e) 数据供方应在涉及个人信息的数据交易前，对涉及个人信息的交易活动开展个人信息保护影响评估，并采取相应措施控制个人信息泄露风险；
f) 原则上应采用去标识化、匿名化等技术手段，对涉及的个人信息进行去标识化处理后再进行交易；
g) 数据需方变更原先的个人信息处理目的、处理方式的，应当依照重新取得个人同意；
h) 在确保重要数据安全的前提下，重要数据对外提供或交易前应按照 GB/T BBBBB 开展数据安全风险评估，并采取相应措施控制数据安全风险；
i) 数据交易场所、数据需方应对个人信息保护影响评估报告、数据安全风险评估报告等进行审核，确保数据交易不会影响国家安全、公共利益、组织或个人合法权益；
j) 数据交易场所对交易数据分类结果进行审核；
k) 数据供方按照 GB/T BBBB 的要求开展数据交易安全风险评估，出具安全风险评估报告；
l) 数据需方应按照约定的授权范围处理个人信息或重要数据；
m) 提供对重要数据符合国家相关规定的数据脱敏方法，并具备评价重要数据脱敏有效性的评估能力。

9 数据交易过程安全要求

9.1 主体入驻、登记挂牌

主体入驻、登记挂牌环节应满足以下要求：

a) 数据供方明确界定交易数据的内容范围、使用范围、商品形态，以确保符合国家相关法律法规的要求；
b) 数据供方提供对交易数据的概要描述，并提供样本数据；
c) 数据需方披露数据需求内容、数据用途，以确保符合国家法律法规的要求；

d) 数据交易场所和数据需方对数据供方提供的敏感个人信息和重要数据进行识别，并进行数据脱敏处理；
e) 数据交易场所按照相关要求审核数据供方和数据需方的交易资质；
f) 同意并遵守交易所的各项规章制度，承担相应责任与义务；
g) 在参与数据交易业务前，完成在数据交易场所的注册，并经数据交易场所审核通过；

注：场外交易下，数据需方按照数据交易场所的审核要求审核数据供方。

h) 遵守数据交易场所的安全管理制度和流程；
i) 向数据交易场所提供书面承诺，内容包括但不限于：交易数据真实性说明、交易数据来源合法性证明、交易数据满足法律法规和政策要求说明、对交易数据质量评估说明、遵守数据交易安全原则说明、接受数据交易场所安全监督承诺、对数据流通后果负责承诺等；

注：场外交易下，书面承诺提供给数据需方。

j) 需方在参与数据交易业务前，应完成在数据交易场所的注册，并经数据交易场所审核通过，同时应遵守数据交易场所的交易管理制度要求；

注：场外交易下，数据供方按照数据交易场所的审核要求审核数据需方。

k) 保证其数据需求及使用场景的合理、真实，并向数据交易场所提供书面的数据交易和使用承诺，内容包括但不限于：满足法律法规和政策要求、遵守数据交易安全原则、接受数据交易场所安全监督、遵守与数据供方约定的数据安全要求、对所持有数据提供充分的安全保护、未经明确授权不公开或转交数据给第三方等；

注：场外交易下，书面的数据交易和使用承诺提供给数据供方。

l) 应要求申请入驻交易所的主体提交其身份、地址、联系方式、行政许可等真实信息，进行核验、登记，建立数据交易主体登记档案，并定期核验更新。

9.2 交易磋商、下单签约

交易磋商、下单签约环节应满足以下要求：

a) 数据交易场所对交易数据的类型、质量、用途、使用范围、交付方式、使用期限、交易价格和保密条款等内容与交易参与方协商和约定；
b) 数据需方参照数据交易服务平台上提供的样本数据明确交易数据的用途、使用范围、交付方式、使用期限和交易价格等；
c) 数据交易场所对审核通过的交易申请进行登记备案，并对数据交易参与方发出交易确认通知；
d) 数据交易场所就各方磋商结果进行登记并以电子服务合约或合同的形式进行规定，内容包括数据交易参与方、数据的内容描述、服务产品的算法逻辑和说明、合约有效期、定价与收益方式、交付质量、交付方式、使用范围、使用对象和使用期限等；
e) 数据交易场所具备针对交易合约的数字化存证及管理机制，保证已签署的电子服务合约或合同不可篡改、可追溯等；
f) 数据商与数据供方明确数据范围，确保加工的过程和结果数据不超出数据供方要求的使用范围；
g) 数据商对交易数据的类型、质量、用途、使用范围、交付方式、使用期限、交易价格和保密条款等内容与数据供方进行协商，加工数据；
h) 加工前，数据商根据可能产生的数据内容、所用于的目的、范围、所采用的算法逻辑等开展数据安全风险评估；
i) 数据商以合同协议等方式明确用于加工的数据内容和范围、结果的用途和知悉范围、数据保护责任和义务、数据保护要求等，并采用密码技术等手段降低数据泄露、窃取等风险；

j) 参照 GB/T 37964—2019，数据商对去标识化后的个人信息进行重识别风险评估，并采用相应技术手段对借助其他信息的重标识行为进行有效防范；
k) 数据商对数据加工过程的访问和操作进行记录，并形成审计日志，对访问和操作进行记录、风险监测与分析，对识别出的风险及时告警；
l) 数据商确保用于数据加工的算法模型具有鲁棒性以抵御恶意攻击，恶意攻击包括但不限于对抗样本、数据投毒和后门攻击；
m) 数据商具备数据加工全流程的安全防护能力，并提供相应的记录供监管管理；
n) 完成数据使用加工后，数据商不再保留原始数据内容。

9.3 产品交付、交易结算

产品交付、交易结算环节应满足以下要求：

a) 按照 GB/T 37988—2019 的要求，确保数据需方的数据安全能力成熟度，不低于数据供方的数据安全能力成熟度；
b) 约定开展数据加工过程中的电子服务合约或合同，在加工后数据的权属关系；
c) 数据交易场所对交付数据内容进行监测和核验，如发现违法违规事件，及时中断数据交易行为，同时依法依规进行处理；
d) 数据交易场所为数据参与方建立安全的数据交付环境，并分配相应的权限；
e) 数据供方和需方共同协商数据交付方式，可直接交付或选择安全可靠的机构交付；
f) 数据交易场所记录数据交付过程，所记录信息具有不可篡改性；
g) 数据交易场所在数据传输链路上部署交易数据监控工具，具有完备的数据保护机制和数据泄露检测能力；
h) 数据供方在数据需方未完全获取交易对象前，有义务保证数据质量符合数据成交时的相关描述；
i) 数据需方对所获得的数据进行评估验证，可委托第三方专业服务机构代为评估；
j) 数据需方在数据供方交付后，按电子服务合约或合同金额及时支付费用；
k) 数据交易场所在交易结算后及时进行数据交付，若存在交付周期，数据交易场所可按周期提供结算服务；
l) 数据交易场所按所签署的电子服务合约或合同分配收益。

9.4 交易结束、纠纷处理

交易结束、纠纷处理环节应满足以下要求：

a) 数据交付完成后，数据供方和数据交易场所立即关闭数据访问渠道；
b) 数据各参与方在交易结束后，清除相关数据的缓存，并对清除记录及数据清除措施的有效性进行检查；
c) 数据交易场所对数据交易过程的证据材料进行归档，如交易过程的记录、合规性评估报告等；
d) 数据交易场所建立投诉举报渠道，维护交易过程中各相关方权益；
e) 数据交易场所应提供交易过程记录材料供监督管理和纠纷处理；
f) 数据交易场所应提供投诉举报渠道来监督数据交易各环节的数据泄露、滥用等情况；
g) 数据交易场所应建立数据安全事件响应机制来应对数据交易各环节的数据泄露、滥用等情况。

附 录 A
（规范性）
禁止交易数据示例

A.1 危害国家安全和社会稳定的数据

危害国家安全和社会稳定的数据示例如下：

a) 反对宪法所确定的基本原则的；
b) 危害国家安全，泄露国家信息，颠覆国家政权，破坏国家统一的；
c) 损害国家荣誉和利益的；
d) 煽动民族仇恨、民族歧视，破坏民族团结的；
e) 破坏国家宗教政策，宣扬邪教和封建迷信的；
f) 散布谣言，扰乱社会秩序，破坏社会稳定的；
g) 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
h) 涉及枪支弹药、爆炸物品、剧毒化学品、易制爆危险化学品和其他危险化学品、放射性物品、核材料、管制器具等能够危及人身安全和财产安全的危险物品的；
i) 宣扬吸毒、销售毒品以及传播毒品制造配方的；
j) 涉及传销、非法集资和非法经营等活动的；
k) 含有法律、行政法规禁止的其他内容的。

A.2 涉及特定个人权益的数据

涉及特定个人权益的数据示例如下：

a) 侮辱或者诽谤他人的；
b) 捏造损害他人名誉的；
c) 未经个人授权的可直接识别到特定个人的身份数据，如：身份号、社保号、驾驶证、护照/台胞证等有效证件号码、电话、微信、QQ 等即时通信账号、E-mail 地址等；
d) 未经个人授权的可直接识别到特定个人的敏感数据，如：姓名、性别、民族、出生日期或年龄、本人相片、婚姻状况、工作单位、学历、履历等个人数据，常住户口所在地住址或家庭地址，指纹、健康疾病等生物数据。
e) 未经个人授权的可直接识别到特定个人的财产数据，如：收入和支付记录、银行卡账号、证券账户数据、房屋登记数据、保险单等。

A.3 涉及特定企业权益的数据

涉及特定企业权益的数据示例如下：

a) 未经企业授权的企业客户数据；
b) 未经企业授权涉及企业商业信息的，如：财务数据、产销数据、货源数据、工艺配方、技术方法、计算机程序等。

参 考 文 献

[1] GB/T 37964-2019 信息安全技术　个人信息去标识化指南

[2] GB/T 38636-2020 信息安全技术　传输层密码协议（TLCP）

[3] 中华人民共和国数据安全法（2021年6月10日中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过）

[4] 中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见（2022年6月22日中央全面深化改革委员会第二十六次会议审议通过）