ICS 35.040
L 80

中华人民共和国国家标准

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

2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:阿里云计算有限公司、中国电子技术标准化研究院、北京赛西科技发展有限责任公司、北京软件和信息服务交易所有限公司、贵阳大数据交易所有限责任公司、上海数据交易中心有限公司、阿里巴巴(北京)软件服务有限公司、中国科学院信息工程研究所、中国移动通信集团公司、陕西省信息化工程研究院、北京奇安信科技有限公司、中国网络安全审查技术与认证中心、清华大学、西北大学、陕西省网络与信息安全测评中心、中国科学院软件研究所、启明星辰信息技术集团股份有限公司、北京天融信科技有限公司、联想(北京)有限公司、西安电子科技大学。

本标准主要起草人:叶润国、张大江、孙彦、沈锡镛、刘贤刚、陈雪秀、胡媛媛、孙爱梅、于铁强、胡影、张敏翀、谢安明、刘玉岭、赵蓓、张群、叶晓俊、吴迪、蔡磊、李怡、金涛、张勇、李克鹏、陈驰、郑新华、张锐卿、常玲、刘嘉林、任兰芳、裴庆祺、孙骞。

引　言

数据正日益对全球生产、流通、分配、消费活动以及经济运行机制、社会生活方式和国家治理能力产生重要影响。数据交易可以促进数据资源流通，破除数据孤岛，有效支撑数据应用的快速发展，发挥数据资源的经济价值。然而，数据交易面临诸多安全问题和挑战，影响了数据应用的进一步健康发展。

为规范数据资源交易行为，建立良好的数据交易秩序，促进数据交易服务参与者安全保障能力提升，本标准将对数据交易服务进行安全规范，增强对数据交易服务的安全管控能力，在确保数据安全的前提下，促进数据资源自由流通，从而带动整个数据产业的安全、健康、快速发展。

信息安全技术
数据交易服务安全要求

1 范围

本标准规定了通过数据交易服务机构进行数据交易服务的安全要求，包括数据交易参与方、交易对象和交易过程的安全要求。

本标准适用于数据交易服务机构进行安全自评估，也可供第三方测评机构对数据交易服务机构进行安全评估时参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2010 信息安全技术 术语

GB/T 35273—2017 信息安全技术 个人信息安全规范

GB/T 35274—2017 信息安全技术 大数据服务安全能力要求

GB/T 36343—2018 信息技术 数据交易服务平台 交易数据描述

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

3 术语和定义

GB/T 25069—2010 和 GB/T 36343—2018 界定的以及下列术语和定义适用于本文件。

3.1

数据交易 data transaction

数据供方和需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。

注 1：数据商品包括用于交易的原始数据或加工处理后的数据衍生产品。

注 2：数据交易包括以大数据或其衍生品作为数据商品的数据交易，也包括以传统数据或其衍生品作为数据商品的数据交易。

3.2

数据供方 data supplier

数据交易中提供数据的组织机构。

3.3

数据需方 data acquirer

数据交易中购买和使用数据的组织机构。

3.4

数据交易服务 data transaction service

帮助数据供方和需方完成数据交易的活动。

3.5

数据交易服务机构　data transaction service provider

为数据供需双方提供数据交易服务的组织机构。

3.6

数据交易服务平台　data transaction service platform

为数据交易提供各项服务的信息化平台。

3.7

在线数据交付　online data delivery

数据供方通过网络向数据需方交付数据的模式。

3.8

离线数据交付　offline data delivery

数据供需双方在达成数据交易协议后，由数据供方通过离线方式将数据从供方提供给需方的交付模式。

3.9

托管数据交易　custodian data delivery

数据供需双方在达成数据交易协议后，由供方将数据拷贝到数据交易服务机构指定的数据托管服务平台，需方在数据托管服务平台内使用数据，数据不发生转移的交付模式。

3.10

数据交易过程　data exchanging process

数据供需双方依托数据交易服务平台针对具体的数据交易对象，进行的一次完整和具体的数据交易行为。

注：数据交易过程一般分为交易申请、交易磋商、交易实施和交易结束等环节。

3.11

重要数据　important data

我国机构和个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据。

注：重要数据通常指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的各类机构在开展业务活动中收集和产生的，不涉及国家秘密，但一旦泄露、篡改或滥用将会对国家安全、经济发展和社会公共利益造成不利影响的数据（包括原始数据和衍生数据）。

[GB/T 35274—2017，定义 3.13]

4　安全概述

4.1　参考框架

数据交易是供需双方对原始数据或加工处理后的数据依照交易过程进行的活动。通过数据交易服务机构进行的数据交易服务参考框架如图 1 所示。数据交易涉及数据供方、数据需方和数据交易服务机构。数据交易服务机构依托数据交易服务平台，为数据供需双方提供数据交易服务。从数据交易服务机构角度出发，数据交易过程一般包括交易申请、交易磋商、交易实施和交易结束四个环节。常见的数据交付模式包括在线模式、离线模式和托管模式。

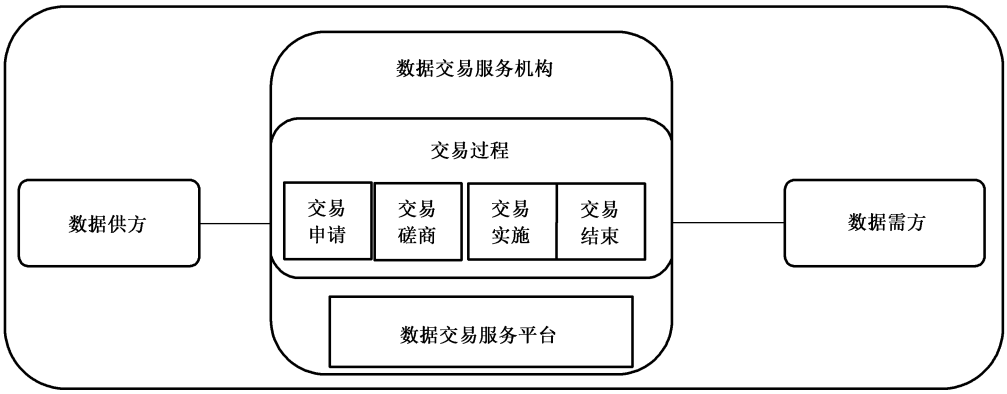

图 1　数据交易服务参考框架

4.2　数据交易安全原则

数据交易应遵循以下原则：

a）　合法合规原则：数据交易应遵守我国关于数据安全管理的相关法律法规，尊重社会公德，不得损害国家利益、社会公共利益和他人合法权益。

b）　主体责任共担原则：数据供需双方及数据交易服务机构对数据交易后果负责，共同确保数据交易的安全。

c）　数据安全防护原则：数据交易服务机构应采取数据安全保护、检测和响应等措施，防止数据丢失、损毁、泄露和篡改，确保数据安全。

d）　个人信息保护原则：数据供需双方和数据交易服务机构应采取个人信息安全保护技术和管理措施，避免个人信息的非法收集、非法获取、非法出售、滥用、泄露等安全风险，切实保护个人权益。

e）　交易过程可控原则：应确保数据交易参与方的真实可信、交易对象合法、数据交付过程可控和交易的非否认性，做到安全事件可追溯、安全风险可防范。

5　数据交易参与方安全要求

5.1　数据供方安全要求

数据交易服务机构应确保数据供方满足以下要求：

a）　为一年内无重大数据类违法违规记录的合法组织机构。

b）　完成在数据交易服务机构的注册，并经数据交易服务机构审核通过，才允许参与数据交易业务。

c）　数据供方应证明其具备向数据需方安全交付数据的能力。

d）　向数据交易服务机构提供书面的安全承诺，内容包括但不限于：交易数据来源合法性证明材料、交易数据满足法律法规和政策要求、对交易数据质量评估说明、遵守数据交易安全原则、愿意接受数据交易服务机构安全监督、愿意对数据流通后果负责等。

e）　遵守数据交易服务机构的安全管理制度和流程。

5.2　数据需方安全要求

数据交易服务机构应确保数据需方满足以下要求：

a) 为一年内无重大数据类违法违规记录的合法组织机构。
b) 完成在数据交易服务机构的注册，并经数据交易服务机构审核通过，才允许参与数据交易业务。
c) 证明具备对交易数据实施安全保护的能力。
d) 提供书面的数据交易和使用安全承诺，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、愿意接受数据交易服务机构安全监督、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。
e) 按照供需双方约定的使用目的、范围、方式和期限使用数据，禁止进行个人信息的重新识别。
f) 在按照数据交易约定方式完成数据使用后，应及时销毁交易数据。
g) 遵守数据交易服务机构的安全管理制度和流程。

5.3 数据交易服务机构安全要求

5.3.1 基本要求

数据交易服务机构应满足以下基本要求：

a) 得到我国行政或主管部门的授权或许可。
b) 为一年内无重大数据类违法违规记录的境内合法组织机构。
c) 具备承担数据交易服务相对应的安全保障能力。
d) 将从事境内数据交易服务的数据交易服务平台部署在我国境内。
e) 对数据供方提供的数据来源合法性证明材料声明进行审核。
f) 对数据违规使用行为进行监测。
g) 制定并执行交易违规处罚规则。
h) 未经授权不擅自使用数据供方或需方的数据或数据衍生品。
i) 至少满足 GB/T 37988—2019 中的三级要求。

5.3.2 组织安全管理要求

5.3.2.1 安全管理制度和规程

数据交易服务机构应满足以下要求：

a) 制定数据交易服务安全管理策略，说明数据交易安全总体目标、范围、原则和安全框架等。
b) 建立数据交易服务安全管理制度，包括但不限于：交易参与方安全管理制度、数据安全管理制度、个人信息安全保护制度等。
c) 为数据交易管理人员或操作人员执行的管理或业务操作建立操作规程。
d) 定期对数据交易服务安全管理策略、制度和规程进行评审，并及时进行更新。
e) 建立和执行针对数据供方和需方的安全管理制度和流程。
f) 建立供需方的信用管理机制。

5.3.2.2 安全相关组织机构和人员

数据交易服务机构应满足以下要求：

a) 建立数据交易安全领导小组，由机构最高管理者或授权代表担任组长。
b) 建立数据交易安全管理职能部门，设立安全管理负责人岗位，明确安全责任。
c) 设立数据交易安全管理员、个人信息安全管理员等岗位，定义各个岗位的安全职责，并配备一定数量的岗位人员。
d) 对数据交易重要岗位人员进行安全审查和技术考核，确保无违法违规记录。

e) 与数据交易重要岗位人员签署安全保密协议，与重要岗位人员签署岗位责任协议。
f) 对数据交易各类岗位人员制定和实施培训计划，培训内容包括安全意识、专项技能等，具备与岗位要求相适应的安全管理知识和专业技术水平。
g) 对第三方人员进行安全管理，对于可能接触交易数据的第三方人员，签署安全保密协议。

5.3.3 数据交易服务平台安全要求

5.3.3.1 基本要求

数据交易服务平台应满足以下要求：
a) 符合 GB/T 22239—2019 中第 3 级的相关安全要求。
b) 提供对数据泄露进行处置的紧急预案。
c) 采用的密码技术遵循相关国家标准和行业标准。

5.3.3.2 扩展要求

5.3.3.2.1 交易数据安全保护

数据交易服务平台应满足以下要求：
a) 分别为数据供方、需方提供安全的上传或下载接口，强身份认证机制，传输链路加密等保护措施，确保数据传输的安全。
b) 对交易数据实施加密存储、访问控制等安全措施，防止数据泄露或非法使用。
c) 实现数据源和数据操作的可追溯性，以及交易的非否认性。
d) 在托管数据交付模式下，为数据需方提供隔离安全环境，对数据需方在数据使用环境中运行的相关程序和产生的数据结果进行审核。
e) 在托管数据交付模式下，对交易数据进行安全存储和备份，确保数据的保密性、完整性和可用性。
f) 当数据供方撤销托管数据时，清除剩余信息，并且不可恢复。

5.3.3.2.2 交易过程安全控制

数据交易服务平台应满足以下要求：
a) 允许对数据交易的参与方、对象、关键过程设置人工干涉功能。
b) 人工干涉的内容中至少应包括：交易参与方审核、交易审核、交易暂停、交易撤销、交易恢复。
c) 处理数据供方或数据需方的仲裁要求，并要求被诉方提供应对证据。

5.3.3.2.3 数据交易安全审计

数据交易服务平台应满足以下要求：
a) 对每笔数据交易操作进行记录，生成数据交易日志。
b) 数据交易日志至少包括以下信息：交易唯一标识、交易时间、交易供方、交易需方、交易数据标识、敏感数据标签、交易价格、交易模式、交易结果等。
c) 安全保存数据交易日志、数据来源合法性等文件至少 6 个月。
d) 只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) 允许数据供方和数据需方查询与自己数据交易相关的日志信息，并允许导出。
f) 提供数据交易日志访问接口给国家监管部门或第三方审计机构。

5.3.3.2.4 数据托管服务平台安全

对于提供托管数据交付模式的数据交易服务机构，应遵循 GB/T 35274—2017 来建设和运维数据

安全托管服务平台。

6 交易对象安全

6.1 禁止交易数据

数据交易服务机构应根据我国相关法律法规，制定禁止交易的数据目录，目录至少应包括：

a) 受法律保护的数据。
b) 涉及个人信息的数据，除非获得了全部个人数据主体或未成年人的监护人的明示同意，或者进行了必要的去标识化处理以达到无法识别出个体的程度。
c) 涉及他人知识产权和商业秘密等权利的数据，除非取得权利人明确许可。
d) 从非法或违规渠道获取的数据。
e) 与原供方所签订的合约要求禁止转售或公开的数据。
f) 其他法律法规明确禁止交易的数据。

6.2 数据质量要求

数据交易服务机构应确保交易数据满足以下质量要求：

a) 数据供方应向数据交易服务机构提供交易数据获取渠道合法，权利清晰无争议的承诺或证明材料。
b) 数据供方应向数据交易服务机构提供拥有交易数据完整相关权益的明确声明。
c) 数据供方应向数据交易服务机构提供数据真实性的明确声明。
d) 数据供方应对交易数据进行分类，并对交易数据进行安全风险评估，出具安全风险评估报告。
e) 数据供方应明确交易数据的限定用途、使用范围、交易方式和使用期限。
f) 数据供方应按照 GB/T 36343—2018 的要求对交易数据进行准确描述，明确数据类别等内容，描述内容满足准确性、真实性要求。
g) 数据交易服务机构应对交易数据描述和样本的准确性、真实性进行审核。
h) 数据交易服务机构应对交易数据的安全风险评估报告进行审核，确保数据可交易。
i) 数据交易服务机构应对交易数据分类结果进行审核。

6.3 个人信息安全保护

数据交易服务机构应确保数据交易在个人信息安全保护方面满足以下要求：

a) 满足 GB/T 35273—2017 中第 8 章关于个人信息的委托处理、共享、转让、公开披露安全要求。
b) 要求数据供方对交易数据进行个人信息安全风险评估，提供个人信息安全风险评估报告。
c) 数据对个人信息安全风险评估报告进行审核，确保数据可交易。

6.4 重要数据安全保护

数据交易服务机构应确保交易数据在重要数据安全保护方面满足以下要求：

a) 满足 GB/T 35274—2017 中 5.6.2 的增强要求。
b) 要求数据供方对交易数据进行重要数据安全风险评估，提供重要数据安全风险评估报告。
c) 对重要数据安全风险评估报告进行审核，确保数据可交易。

7 数据交易过程安全

7.1 交易申请

数据交易服务机构应确保交易申请环节满足以下要求：

a) 数据供方应明确界定交易数据的内容范围、使用范围，以确保符合国家相关法律法规的要求。
b) 数据供方应按数据交易服务机构要求，提供对交易数据的概要描述，并提供样本数据。
c) 数据交易服务机构对数据供方提供的样本数据进行内容审核，确认数据合法合规。对于不符合要求的，数据交易服务机构应要求数据供方重新提交样本数据进行审核。
d) 数据需方应披露数据需求内容、数据用途，以确保符合国家法律法规的要求。
e) 数据交易服务机构对数据需方的数据需求进行审核通过后方可发布。

7.2 交易磋商

数据交易服务机构应确保交易磋商环节满足以下要求：

a) 供需双方应对交易数据的用途、使用范围、交易方式、使用期限和交易价格等协商和约定，形成交易订单。
b) 数据交易服务机构应遵循国家法律，对交易订单从数据出境安全、个人信息保护安全等方面进行审核，确保符合相关法律法规和标准等合规性要求，撤销不符合要求的交易订单。
c) 数据交易服务机构应对审核通过的订单进行登记备案，并对供需双方发出交易确认通知。

7.3 交易实施

数据交易服务机构应确保交易实施环节满足以下要求：

a) 数据交易服务机构应审核数据需方的数据安全能力成熟度，确保不低于数据供方的数据安全能力成熟度。
b) 数据交易服务机构应为数据交易与数据供方和数据需方签订三方合同，明确数据内容、数据用途、交付质量、交付方式、交易金额、交易参与方安全责任、保密条款等内容。
c) 数据交易服务机构应对交付数据内容进行监测和核验，如发现违法违规事件，应及时中断数据交易行为，同时依法依规进行处理。
d) 数据交易服务机构应对交易过程中的违法违规数据具有追溯能力。
e) 对于在线数据交付模式，数据交易服务机构应在供需双方的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。
f) 对于托管数据交付模式，数据交易服务机构应为数据需方建立安全的数据使用环境，并分配相应的权限。
g) 数据供方在数据需方未完全获取数据内容前，有义务保证交易数据质量和数量符合数据成交时的相关描述。
h) 在托管数据交付模式下，数据需方在数据使用完成后，应向数据交易服务平台提供提取结果数据请求，核准后由数据交易服务平台发放给数据需方。

7.4 交易结束

数据交易服务机构应确保交易结束环节满足以下要求：

a) 数据交付完成后，数据供方应立即关闭数据访问接口，数据供方发出数据交付完成确认。
b) 数据交付完成后，数据需方发出数据接收完成确认。
c) 在托管数据交付模式下，数据交易服务机构应在交易结束后立即销毁残余数据。
d) 数据交易服务机构应为交易过程形成完整的交易日志并安全保存。