ICS 25040.40
CCS L 70

DB21

辽　宁　省　地　方　标　准

DB21/T 3895—2023

工业数据流通　通用安全要求

2023—12—30 发布　　2024—01—30 实施

辽宁省市场监督管理局　发布

目　　次

前言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 数据流通前安全要求 3
4.1 采集所需流通的数据 3
4.2 数据流通安全风险评估 5
4.3 确定数据流通目录 6
4.4 数据脱敏 6
5 实施数据流通安全要求 7
5.1 数据交易安全 7
5.2 数据出境安全 12
5.3 数据传输安全 13
5.4 数据接口安全 14
6 数据流通后安全要求 14
6.1 数据存储 14
6.2 数据处理 18
6.3 数据销毁 21
附录 A（规范性） 工业数据分类分级要求 24
A.1 数据分类 24
A.2 数据分级 26
参考文献 29

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。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：沈阳华睿博信息技术有限公司、上海数据交易所、国家计算机网络应急技术处理协调中心辽宁分中心、辽宁艾特斯智能交通技术有限公司、东北大学、辽宁职业学院、辽宁省大数据管理中心、北京赛迪时代信息产业股份有限公司、辽宁省先进装备制造业基地建设工程中心等。

本文件主要起草人：邵华、 申翔宇、李凯、黄书鹏、王宇飞、宋宪辉、谭振华、王义刚、杨成实、张翔宇、魏国伟、刘洋等。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

本文件起草单位通讯地址和联系电话：通讯地址：辽宁省沈阳市和平区青年大街386号华阳国际大厦2396，联系电话：18698840986。

本文件归口部门通讯地址和联系电话：通讯地址：辽宁省沈阳市皇姑区北陵大街45—2号，联系电话：024—86893258。

工业数据流通　通用安全要求

1　范围

本文件规定了工业数据流通基本原则、数据流通参与方安全要求、数据流通前安全要求、实施数据流通安全要求以及数据流通后安全要求。

本文件适用于工业数据流通安全防护工作指导和落实。

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 5271.1-2000　信息技术　词汇　第1部分：基本术语

GB/T 22239-2019　信息安全技术　网络安全等级保护基本要求

GB/T 25069-2022　信息安全技术　术语

GB/T 35273-2020　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 37932-2019　信息安全技术　数据交易服务安全要求

GB/T 37973-2019　信息安全技术　大数据安全管理指南

GB/T 37988-2019　信息安全技术　数据安全能力成熟度模型

GB/T 42128-2022　智能制造　工业数据　分类原则

3　术语和定义

GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1

数据　data

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 5271.1-2000,01.01.02]

3.2

工业数据　industrial data

在工业领域中，涉及企业的所有生产活动和服务所产生的数据。

[来源：GB/T 42128-2022，3.1.1]

3.3

数据供方　data supp lier

数据流通中提供数据的组织机构。

[来源：GB/T 37932-2019，3.2]

3.4

数据需方　data acquirer

数据流通中购买和使用数据的组织机构。

[来源：GB/T 37932-2019，3.3]

3.5

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。

[来源:GB/T 37932-2019，3.1]

3.6

数据流通　data circulation

数据及数据产品在不同实体间流转的行为。

3.7

数据交易服务机构 data circulation service

为数据供需双方提供数据交易服务的组织机构。

[来源：GB/T 37932-2019，3.4]

3.8

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、流通信息等。

注2：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如,用户画像或特征标签,能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的,属于个人信息。

[来源：GB/T 35273-2020，3.1，有修改]

4 数据流通前安全要求

4.1 采集所需流通的数据

4.1.1 数据采集安全管理

数据供方数据采集应满足如下要求：

a） 组织开展数据采集活动的过程中应满足权责一致、目的明确、选择同意、最小必要、公开透明、确保安全、主体参与等原则；

b） 应设立数据采集安全管理团队，负责制定和推动实施整体的数据采集安全合规管理制度；

c） 应设立数据采集风险评估团队，负责对不同业务或项目场景的数据采集提供安全评估服务支持，并制定相应的改进方案，评估内容包括但不限于合规安全性、技术安全性等；

d） 定义采集数据的目的和用途，明确数据来源、采集方式、采集范围等内容，并制定标准的采集模板、数据采集方法、策略和规范；

e） 遵循合规原则，确保数据采集的合法性、正当性和必要性；

f） 设置专人负责信息生产或提供者的数据审核和采集工作；

g） 对于初次采集的数据，应采用人工与技术相结合的方式进行数据采集，并根据数据的来源、类型或重要程度进行分类；

h） 最小化采集数据，仅需要完成必须工作即可，确保不收集与提供服务无关的个人信息和重要数据；

i） 对采集的数据进行分级分类标识，并对不同类别、级别的数据实施相应的安全管理策略和保障措施，对数据采集环境、设施和技术采取必要的安全管理措施；

j） 部署数据采集系统或相关工具，制定数据采集策略（如采集周期、频率、采集内容等）对数据进行采集；

k） 在采集过程中对被采集方授权同意采集的过程和信息进行日志记录；

l） 实施数据采集过程的数据防泄漏安全技术措施：如采集数据的加密、采集链路加密、敏感信息和字段的脱敏、权限的访问控制等；

m） 应按照本文件7.1中的要求对数据进行存储。

4.1.2 数据源鉴别及记录管理

数据供方开展数据源鉴别及记录活动的过程中应遵循如下基本要求，防止数据仿冒和伪造：

a） 设立负责数据源鉴别和记录的岗位和人员，负责对数据源进行鉴别、记录和追溯，检测数据是否被仿冒、伪造，同时提供统一的数据源管理策略和方案；

b） 采取标注法、反向查询法等技术手段对外部收集的数据和数据源进行识别和记录；

c） 对关键溯源数据进行备份，并采取数据加密、访问控制及数据备份等技术手段对溯源数据进行安全保护；

d） 确保负责该项工作的人员理解数据源鉴别标准和组织内部的数据采集业务，并结合实际情况执行标准要求；

e） 通过身份鉴别、数据源认证等安全机制确保数据来源的真实性。

4.1.3 数据质量管理

数据供方应对采集的数据进行质量管理，应满足如下要求：

a） 应设立数据质量管理岗位和人员，负责制定统一的数据质量管理要求，明确对数据质量进行管理和监控的责任部门或人员；

b） 应明确数据质量管理相关的要求，包含数据格式要求、数据完整性要求、数据字典维护管理要求、数据源质量评价标准等；

c） 应明确数据采集过程中质量监控规则，明确数据质量监控范围及监控方式；

d） 应明确组织的数据清洗、转换和加载操作相关的安全管理规范，明确执行的规则和方法、相关人员权限、完整性和一致性要求等。

4.1.4 数据分类分级

数据供方应对采集到的数据进行分类分级，应满足如下要求：

a） 应按照附录A的要求对组织的数据进行分类分级标识和管理；

b） 应对不同类别级别的数据建立相应的访问控制、数据加解密、数据脱敏等安全管理和控制措施；

c） 应明确数据分类分级变更审批流程和机制，通过该流程保证对数据分类分级的变更操作及其结果符合组织的要求。

4.2 数据流通安全风险评估

4.2.1 按照GB/T 37973-2019 中的风险评估过程对数据流通操作进行风险评估和分析，包括但不限于以下内容：

a） 数据流通目的；

b） 目的实现方式，以及是否可以通过不流通数据或流通脱敏后的数据等方式达成；

c） 流通数据对国家安全、社会经济、公共秩序、企业生产运营、个人利益等造成的影响和数据安全等级改变；

d） 流通数据对个人信息主体可能造成的侵害；

e） 是否涉及数据出境；

f） 不流通数据是否会造成损害或损失；

g） 访问这些流通数据的相关方及其数据安全能力是否足够保证流通数据安全；

h） 流通数据是否已经达成目的，是否需要继续流通数据；

i） 是否有任何法定限制或其他因素对数据流通的限制。

4.2.2 根据风险评估结果，对于可能影响国家安全、经济安全、生产安全、个人信息安全等的数据，应限制进行流通，或者采取措施在保证安全的前提下进行流通。对于可以进行流通的数据，应根据风险评估结果采取相应安全措施进行流通。

4.3 确定数据流通目录

根据风险评估结果，针对可进行共享的工业数据，制定流通数据目录，目录包括但不限于以下内容：

a） 流通数据所在域，包括研发域、生产域、管理域、运维域、标识解析域、工业互联网平台域等；

b） 流通数据目的；

c） 流通数据类型、格式、级别和规模；

d） 流通数据用途、支撑的业务系统；

e） 流通数据允许使用的范围；

f） 流通数据使用期限；

g） 流通数据的方式。

4.4 数据脱敏

工业数据脱敏应满足如下要求：

a） 应设立数据脱敏部门并配置专职的技术人员和管理人员，负责制定整体的数据脱敏原则和制度，并推动相关要求确实可靠的落地执行；

b） 应根据实际业务场景，结合行业法规的要求，制定相应的数据脱敏策略；

c） 应确保经过数据脱敏处理后，原始信息中包含的敏感信息已被移除，无法通过处理后的数据得到敏感信息；

d） 脱敏后的数据应尽可能的体现原始数据的特征，且应尽可能多的保留原始数据中的有意义信息，以减小对使用该数据的系统的影响；

e） 应保证数据脱敏的过程可通过程序自动化实现，可重复执行；

f） 数据脱敏时需保证对相同的原始数据，在各输入条件一致的前提下，无论脱敏多少次，其最终结果数据是相同的；

g） 可通过配置的方式，按照输入条件不同生成不同的脱敏结果，从而可以方便的按数据使用场景等因素为不同的最终用户提供不同的脱敏数据；

h） 在数据脱敏之前，应结合数据分级分类表对敏感数据进行识别和定义，明确需要脱敏的数据信息，一般包括个人信息数据、组织敏感信息、国家重要数据等，并根据识别出的敏感数据的具体情况，确定合适的脱敏方法；

i） 在数据脱敏的各个阶段需加入安全审计机制，严格、详细记录数据处理过程中的相关信息，形成完整的数据处理记录；

j） 设置专人定期对脱敏相关的日志记录进行安全审计，发布审计报告，并跟进审计中发现的异常。

5 实施数据流通安全要求

5.1 数据交易安全

5.1.1 数据交易参与方安全要求

5.1.1.1 数据供方安全要求

数据供方应满足如下要求：

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、愿意对数据交易后果负责等；

e） 遵守数据交易服务机构的安全管理制度和流程。

5.1.1.2 数据需方安全要求

数据需方应满足如下要求：

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） 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；

d） 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；

e） 在按照数据交易约定方式完成数据使用后，应根据合同约定做好相应处理；

f） 遵守数据交易服务机构的安全管理制度和流程。

5.1.1.3 数据交易服务机构安全要求

5.1.1.3.1 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；

j） 不应对主要业务进行外包；

k） 应确保使用的云平台安全可靠。

5.1.1.3.2 组织安全管理要求

5.1.1.3.2.1 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，确保数据完整性、正确性、机密性的同时，防止数据的泄漏、篡改、伪造及相关人员的抵赖行为；

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。

5.1.1.3.2.2 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。

5.1.1.4 数据交易服务平台安全要求

5.1.1.4.1 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。

5.1.1.4.2 扩展要求

5.1.1.4.2.1 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。

5.1.1.4.2.2 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。

5.1.1.4.2.3 数据委托服务平台安全

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。

5.1.2 交易申请

数据交易申请环节应满足如下要求：

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。

5.1.3 交易磋商

数据交易磋商环节应满足如下要求：

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。

5.1.4 交易实施

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/127065022104010006