ICS 35.03

|  |
| --- |
| CCS L80 |

 DB21

辽宁省地方标准

DB21/T XXXX—XXXX

|  |
| --- |
|  |

工业数据流通 数据合规性检查规范

（征求意见稿）

|  |
| --- |
| 在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。 |
|  |

XXXX - XX - XX发布

XXXX - XX - XX实施

 辽宁省市场监督管理局　发布

目　次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 数据供方合规检查 3

5.1 业务资质检查 3

5.2 网络安全等级保护检查 3

5.3 委托处理数据情形的检查 3

6 数据来源合规检查 3

7 交易数据合规检查 4

8 数据处理过程合规检查 4

8.1 数据收集 4

8.2 数据存储 4

8.3 数据使用、加工 4

8.4 数据传输、提供 5

8.5 数据公开 5

8.6 数据删除、匿名化 5

9 可追溯检查 5

9.1 文件检查 5

9.2 技术措施检查 5

9.3 数据登记 5

10 数据出境合规 6

10.1 出境安全评估要求 6

10.2 数据出境合规检查 6

11 征信场景下数据合规检查的特殊要求 7

11.1 征信机构采集数据合规检查 7

11.2 征信机构提供数据合规检查 7

12 检查过程 7

12.1 主要环节 7

12.2 检查准备 7

12.3 检查实施 9

12.4 分析 9

12.5 判定 9

参　考　文　献 10

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。

本文件由辽宁省工业和信息化厅归口。

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、北京赛迪时代信息产业股份有限公司、辽宁艾特斯智能交通技术有限公司、东北大学、辽宁省大数据管理中心、国家计算机网络应急技术处理协调中心辽宁分中心等。

本文件主要起草人：邵华、申翔宇、张翔宇、魏国伟、王宇飞、宋宪辉、谭振华、杨成实、李凯等。

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。

归口管理部门通信地址：沈阳市辽宁省沈阳市皇姑区北陵大街45-2号。

归口管理部门联系电话：024-86913384。

标准起草单位通讯地址：辽宁省沈阳市和平区青年大街386号华阳国际大厦2396。

标准起草单位联系电话：18698849086。

工业数据流通 数据合规性检查规范

1. 范围

本文件规定了数据供方合规检查、数据来源合规检查、交易数据合规检查、数据处理过程合规检查、可追溯检查、数据出境合规、征信场景下数据合规检查和检查过程等方面的内容。

本文件适用于工业数据流通中的数据合规性检查。

1. 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 22240-2020 信息安全技术 网络安全等级保护定级指南

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 37932-2019 信息安全技术 数据交易服务安全要求

GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求

GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

1. 术语和定义

下列术语和定义适用于本文件。

数据　data

任何以电子或其他方式对信息的记录。

[来源:GB/T 41479-2022，3.1]

数据供方　data supplier

数据交易中提供数据的组织机构。

[来源:GB/T 37932-2019，3.2]

数据需方　data acquirer

数据交易中购买和使用数据的组织机构。

[来源:GB/T 37932-2019，3.3]

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]

数据交易服务机构　data transaction 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]

匿名化　anonymization

个人信息经过处理无法识别特定自然人且不能复原的过程。

[来源:GB/T 41479-2022，3.13]

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、交易信息等。

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]

关键信息基础设施　critical information infrastructure

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、国防科技工业等重要行业和领域,以及其他一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

[来源:GB/T 39204-2022，3.1]

1. 缩略语

下列缩略语适用于本文件：

API：应用程序接口（Application Programming Interface）

SDK：软件开发工具包（Software Development Kit）

1. 数据供方合规检查
	1. 业务资质检查

应根据数据供方的经营范围、具体业务模式和数据产品类别等，对数据供方取得的行政许可及相关证照的完备性、运营主体的一致性、授权范围与实际数据处理相关活动的匹配性以及质量管理体系的健全性进行检查。

* 1. 网络安全等级保护检查

应对数据供方实施网络安全等级保护的情况进行检查，检查要求如下：

1. 按照GB/T 22240-2020的要求对数据提供者的网络安全保护等级定级结果进行复核；
2. 对确定为二级及以上的网络信息系统，检查定级备案情况、测评的频率；
3. 对确定为三级及以上的网络信息系统、关键信息基础设施，检查是否每年至少开展一次密码评估工作的情况；
4. 处理重要数据的网络信息系统应满足三级及以上网络安全等级保护要求，处理核心数据的网络信息系统应依据有关要求从严保护；
5. 必要时，对网络信息系统安全保护措施和测评整改符合要求的情况进行核查；
6. 如涉及关键信息基础设施，应按GB/T 39204-2022的相关要求进行检查。
	1. 委托处理数据情形的检查

数据供方委托外部机构进行数据处理时，应检查以下内容：

1. 建立数据安全风险评估、个人信息安全影响评估以及内外部数据安全检查与评估制度的情况；
2. 对外部机构业务资质检查的相关记录，外部机构业务资质检查内容包括行政许可及相关证照的完备性、运营主体的一致性、授权范围与实际数据处理相关活动的匹配性以及质量管理体系的健全性；
3. 与外部机构签订的数据处理合同或协议的效力及内容，包括合同约定的履行数据安全要求、数据处理目的、处理期限、处理方式、信息种类、保护措施、处理地点、销毁、转委托处理、分享以及双方的权利和义务等；
4. 对外部机构数据处理过程的监督记录，包括履行数据安全保护义务情况、处理方式及处理地点的正确性、是否进行超出目的处理、处理后数据的删除和销毁情况等；
5. 涉及处理个人信息的，检查委托前进行个人信息安全影响评估的实施记录和记录保存情况，个人信息安全影响评估活动应依据GB/T 39335-2020开展。
6. 数据来源合规检查

数据来源包括公开数据收集、自行生产、间接获取和直接采集，各类型的数据来源合规检查内容如下。

1. 公开数据收集：针对公开数据收集合法性，从收集数据是否会侵犯其他主体的合法权益、收集方法和使用目的等方面进行检查。
2. 自行生产：检查数据分类分级制度及落实情况，检查不同数据等级的安全机制。

注：针对不同的数据类型，检查时要求提供的证明文件也是不同的，例如，针对生产数据，可能要求企业提供其生产的控制信息、工况状态、工艺参数、系统日志等，针对运营数据及管理数据，则要求企业提供设备信息、数据库模型、客户数据及运维日志等。

1. 间接获取：检查采购协议或授权许可协议的真实性、合理性。
2. 直接采集：对于数据主体自主输入上传或同意采集的数据，应重点审查授权情况；对于以第三方组件方式采集数据的，除检查授权外，还需审查采集方是否对第三方组件具有完整的内控制度；对于采集水文、气候及地理测绘等客观世界数据，则应综合国家利益、所涉行业、采集方性质等多方因素综合检查来源合规。
3. 交易数据合规检查

交易数据合规检查内容如下：

1. 应检查交易数据是否包含GB/T 37932-2019中6.1列出的禁止交易数据；
2. 应检查交易数据的安全风险评估报告的全面性、真实性；
3. 应检查交易数据描述和样本的准确性、真实性；
4. 应检查交易数据的分类结果是否正确；
5. 交易数据为重要数据的，应检查是否已取得相关部门对于数据交易的同意或许可，应检查重要数据传输过程中是否采取校验技术、密码技术、安全传输通道或者安全传输协议等措施。
6. 数据处理过程合规检查
	1. 数据收集

数据收集情况的检查内容包括：

1. 收集信息的合法性基础，包括相关资质、行政许可、授权等；
2. 个人信息的收集是否符合GB/T 35273-2020中第5章的要求；
3. 数据收集授权的展示时机、形式（明显、非默认同意）和内容的规范性；
4. 实际收集数据与隐私政策、用户协议等内容是否一致。
	1. 数据存储

数据存储情况的检查内容包括：

1. 重要数据和个人信息的存储是否采取加密、访问控制和安全审计等安全措施；
2. 存储时间是否超过与重要数据和个人信息主体约定的存储期限或个人信息主体授权同意有效期；
3. 存储个人生物特征识别信息的,是否符合GB/T 35273-2020中6.3 b)和 c)的要求及生物特征识别信息保护相关国家标准要求；
4. 数据及其副本的存储地点是否符合数据本地化存储和数据跨境相关要求。
	1. 数据使用、加工

数据使用、加工的检查内容包括：

1. 数据的使用和加工是否获得相关方的授权；
2. 数据实际使用、加工的方式和范围符合约定；
3. 是否涉及相关规定禁止的数据使用和加工，如未获得用户授权、用户已撤回同意、歧视性的营销策略、违反道德伦理等情况。
	1. 数据传输、提供

数据传输、提供的检查内容包括：

1. 数据传输是否符合GB/T 41479-2022中5.6的要求；
2. 数据提供是否符合GB/T 41479-2022中5.7的要求；
3. 涉及第三方SDK组件或API接口的，检查是否对SDK组件或API接口进行安全检测，是否存在已知的安全漏洞和可能引起数据泄露或未授权的数据出境行为。
	1. 数据公开

数据公开的检查内容包括：

1. 数据公开是否会危害国家安全、公共安全、经济安全和社会稳定；
2. 数据公开行为和内容是否取得了相关单位的许可和授权；
3. 公开对个人权益有重大影响的个人信息，是否已取得个人同意。
	1. 数据删除、匿名化

删除、匿名化处理检查内容包括：

1. 删除、匿名化处理范围是否包括数据本身及其所有副本；
2. 检查删除、匿名化处理是否符合GB/T 41479-2022中5.13、GB/T 35273-2020中8.3和8.5的要求。
3. 可追溯检查
	1. 文件检查

应检查数据交易服务机构是否建立并留存以下文件：

1. 交易数据的来源介绍和证明文件；
2. 交易数据的处理记录、使用记录和审查记录；
3. 数据供方和数据需方的基本信息；
4. 交易过程的记录。
	1. 技术措施检查

应检查是否采用区块链技术，将数据供方、数据需方身份信息，交易合同或协议，交易数据和交易过程等信息进行登记、备案。

应检查是否将交易数据简介、来源、用途等信息上链，是否对交易数据进行了一数一码唯一标识的处理。

应检查数据交易服务平台是否具备交易过程信息，数据供方、数据需方身份信息及交易数据等信息的交易溯源功能。

* 1. 数据登记
		1. 基本原则

为保证数据交易可追溯，数据交易服务机构宜建立数据确权登记、数据权利对抗登记和数据交易存证登记等数据登记制度，但建立并落实登记制度不是数据交易的必要条件。

* + 1. 数据确权登记

数据确权登记是针对权利归属情况清晰、产权主体单一的数据进行的登记，如在不涉及数据安全问题的情况下，对企业自行收集的实验数据、测绘数据进行的初始权利登记，其目的在于通过严格审查程序明确数据初始产权。

* + 1. 数据权利对抗登记

数据权利对抗登记是对数据整体转让和排他许可使用进行的登记，登记产生对抗第三方的法律效力。数据权利对抗登记的目的在于通过对数据权利主体、使用权限和转让过程的记载，明确数据供方处理数据权限、数据需方使用数据的范围。

* + 1. 数据交易存证登记

数据交易存证登记是针对涉及普通许可使用或者数据服务场景下，数据交易历程的登记，登记对象为数据产品的普通许可使用和数据开发服务，其目的在于通过对历次交易核心内容的记录与公示，为交易溯源提供依据和证明。

1. 数据出境合规
	1. 出境安全评估要求

重要数据和个人信息在出境前，应由数据交易服务机构向数据出境安全相关主管部门提交数据出境安全评估申报，提出申报前，还需自行进行出境风险自评估。出境风险自评估应从以下几个角度进行。

1. 出境数据，包括规模、范围、种类、敏感程度和潜在风险；涉及个人数据的，向个人告知境外数据接收方的名称、联系方式、出境目的、出境方式、个人信息种类及个人向境外数据接收方行使权利的方式和程序等，并取得个人明示同意。
2. 数据出境行为，包括数据出境的目的、方式等是否合法，是否符合最小必要原则；关键信息基础设施的运营者在境内运营中收集和产生的个人信息和重要数据应当在境内存储。
3. 境外数据接收方当地的保护政策及保护水平是否满足我国相关政策、法规及标准化文件的要求。
4. 数据出境过程中及数据出境后，应检查数据安全和个人信息权益保护途径是否畅通有效；应检查使用境外的数据服务商和SDK组件可能引起的潜在的数据出境风险情况；
5. 与境外数据接收方拟订的合同、协议及相关的法律文件。合同中应至少约定数据出境的目的及方式、境外数据保存情况、境外数据再转移、不可抗力、其他违约或侵权事宜及其解决途径、方式。
	1. 数据出境合规检查

数据出境合规检查内容包括：

1. 涉及个人信息的，是否向个人告知境外接收方的名称或者姓名、联系方式、出境目的、出境方式、个人信息的种类以及个人向境外接收方行使本文件规定权利的方式和程序等事项，并取得个人的明示同意；
2. 是否具有个人信息安全影响评估的责任部门或责任人员，是否自行开展或聘请外部独立第三方进行个人信息保护影响评估，个人信息保护影响评估报告和处理情况记录是否妥善保存；

注：个人信息安全影响评估活动应依据GB/T 39335-2020开展。

1. 是否与境外接收方订立合同，约定双方的权利和义务。合同中是否约定数据出境的目的及方式、境外数据保存情况、境外数据再转移、不可抗力以及其他违约或侵权事宜及其解决途径与方式；
2. 数据出境处理活动是否需要向相关管理机构申报数据出境安全评估，如需要申报，应开展数据出境风险自评估，并向相关管理机构申报数据出境安全评估；
3. 关键信息基础设施的运营者在中国境内运营中收集和产生的个人信息和重要数据是否在中国境内存储；
4. 出境数据是否包含相关管理机构认定的不得出境的数据；
5. 是否存在使用境外的服务供应商和第三方SDK组件可能引起的潜在的数据出境风险情况；
6. 是否建立并保存跨境传输相关的管理记录，包括传输发送方、接收方及所在区域、传输机制、信息类型、处理目的、合同条款、数据主体同意的相关记录。
7. 征信场景下数据合规检查的特殊要求
	1. 征信机构采集数据合规检查

征信机构采集数据合规情况，应检查以下内容：

1. 征信机构是否对数据来源、数据质量、数据安全措施和数据主体授权等进行必要检查；
2. 采集的数据是否包含个人的宗教信仰、基因、指纹、血型、疾病和病史信息以及法律、行政法规规定禁止采集的其他个人信息；
3. 采集的数据是否包含个人的收入、存款、有价证券、商业保险,不动产的信息和纳税数额信息，如包含上述信息，是否明确告知信息主体提供该信息可能产生的不利后果，并取得其书面同意；
4. 征信机构是否与数据供方通过协议等形式明确信息采集的原则以及各自在获得数据主体同意、数据采集、加工处理、数据更正、异议处理和数据安全等方面的权利义务和责任。
	1. 征信机构提供数据合规检查

征信机构提供数据合规情况，应检查以下内容：

1. 征信机构是否取得相关行政许可、是否已依法办理相关备案；
2. 征信机构采集个人信用信息的方式、方法，是否遵循最小必要的原则，是否存在过度采集情况；
3. 征信机构是否提供相应的证据或承诺表明已采取合理措施，保障提供数据的准确性，数据采集、存储和加工等过程中不存在篡改原始信息的情形。
4. 检查过程
	1. 主要环节

数据合规性检查包括检查准备、检查实施、分析、判定等4个主要环节。

* 1. 检查准备
		1. 主要工作内容

检查准备阶段主要工作内容包括制订检查方案、调研、资料收集。

* + 1. 检查方案

检查方案应包括以下内容：

1. 检查团队的人员数量、专业组成以及沟通机制；

注：团队人员应具备可支撑检查开展的法律、技术、安全管理、业务规则等方面的专业知识和技能。

1. 根据检查对象和检查目的确定的检查范围；

注：检查范围可包括组织范围、物理地域范围、项目范围、业务流程和业务活动范围、信息系统和技术工具范围、人员范围、数据范围、时间范围等维度。

1. 应明确相关的法律法规、监管规定、行业准则、国际条约及行业标准化文件等检查依据；
2. 应明确可能使用的检查工具，包括但不限于检查表、基线检查工具、安全扫描及测试工具、安全审计工具等；
3. 对检查进度进行预期规划，包括检查准备、检查实施、分析、判定阶段的周期及时间点安排；
4. 对检查活动可能存在的风险及造成的影响进行分析，如检查活动可能造成信息泄密的风险、测试扫描活动对业务运行和数据正确性的影响、检查工作自身的局限性及约束等，检查实施应采取最小影响原则。
	* 1. 调研
			1. 应对检查对象的业务运营模式、数据处理活动、安全管理制度构建及落实、处罚及整改相关情况进行调研。
			2. 业务运营模式调研包括业务范围、内容、模式以及与外部机构合作的情况。
			3. 数据处理活动调研涉及处理数据的类型、流程、规模及数据收集、存储、使用、加工、传输、流通、删除等全生命周期的活动。
			4. 安全管理制度构建及落实调研包括安全管理组织架构、管理制度、技术措施、网络安全等级保护落实情况、培训教育制度的构建及落实。
			5. 处罚及整改调研是否存在数据合规的投诉、行政处罚、诉讼、仲裁，如存在，还应调研以往的信息安全相关测评和数据合规检查的整改措施。
		2. 资料收集

应收集的数据合规相关资料包括但不限于：

1. 数据交易主体的营业执照以及相关行业的经营许可；
2. 相关的协议、合同以及审查文件；
3. 数据交易主体的网络安全、数据安全、数据分级分类、个人信息保护等事项的管理文件，包括制度文件、程序文件、行业准则和承诺、指引文件、培训考核和监督要求以及近三年执行相关活动形成的技术和质量记录等；
4. 近年（例如三年内）与信息安全或数据安全相关的诉讼、仲裁和被执法机关调查和处罚的相关文件，包括约谈、调查通知、处罚通知、判决书等；
5. 近年（例如三年内）涉及的网络安全审查报告、等级保护的备案证明以及相关信息系统的等级保护测评报告、网络信息安全及数据安全风险评估报告等；
6. 已发生过的网络安全攻击、系统中断、信息泄露等事件的情况分析及应急响应报告。

可根据检查需求，通过对公开信息进行查询的方式获取评估对象的相关信息，以对收到的资料进行印证和补充，查询渠道包括：国家企业信用信息公示系统、信息产业主管部门网站、各地行业主管部门网站、国家及地方网信部门网站以及执行和裁判信息公开网站等。

检查实施过程中，可根据实际情况，要求被检查方补充资料。

* 1. 检查实施

检查实施主要通过文档审查、安全检测、人员访谈三种方式进行。

1. 文档审查：逐一审查收集到的相关文档，判断相关制度、文件的建立和落实情况是否符合相关要求。
2. 安全检测：对相关的网络、信息系统和数据信息实施安全检测，通过查看、分析被测系统的响应和输出结果，检查被测系统的安全技术保障措施是否有效。进行安全检测时，需要注意测试数据和检测工具可能对系统运行产生的影响，并尽可能减小这些影响。
3. 人员访谈：与相关人员进行交流、讨论、询问等形式的访谈，作为文档审查和安全检测的补充，以核实数据安全合规的情况。访谈对象包括但不限于：信息系统相关的研发人员、产品经理、业务设计人员、业务负责人、技术负责人、数据安全负责人、法律合规负责人、运维人员和信息安全管理人员。
	1. 分析

在检查过程中，记录发现的问题，并对问题可能产生的风险进行分析。问题记录内容应包括：

1. 问题事实描述（所在业务、违规事实和发生场景等）；
2. 违反的相关制度规定的名称和条款；
3. 定性问题的依据名称和条款；
4. 问题可能引起的风险和处罚后果；
5. 必要时，应记录风险等级。
	1. 判定

检查工作完成后，应编制数据合规性检查报告，明确数据是否合规的判定结论。检查报告内容包括：

1. 背景，描述检查的目的；
2. 声明，描述检查结果的适用范围、约束、假设及免责声明；
3. 依据，介绍所依据的法律法规、相关政策和标准化文件等；
4. 检查范围，对检查对象的组成、检查内容和指标进行描述；
5. 流程，整个检查活动的过程性描述；
6. 判定结论，可包括数据处理业务的合规性判定、安全管理措施及落实情况的合规性判定、技术保障措施及落实情况的合规性判定。

如在检查过程中发现问题及存在风险，宜给出整改和持续改进的建议。宜针对之前的网络和数据安全审查、测评、评估中发现问题的整改情况进行总结。

参　考　文　献

1. GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南
2. GB/T 35273-2017 信息安全技术 个人信息安全规范
3. GB/T 35274-2017 信息安全技术 大数据服务安全能力要求
4. GB/T 37932-2019 信息安全技术 数据交易服务安全要求
5. GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求
6. GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南
7. GB/T 41479-2022 信息安全技术 网络数据处理安全要求
8. T/SZBA 001-2023 数据安全合规评估方法
9. DB52/T 1468-2019 基于区块链的数据资产交易实施指南
10. 《工业和信息化领域数据安全管理办法（试行）》
11. 《数据出境安全评估办法》

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_