ICS

CCS

# T/GXDSL

# 团　　体　　标　　准

T/GXDSL　— 2026

# 小微企业数字供应链金融业务数据交互与风控指引

Guidelines for Data Interaction and Risk Control in Digital Supply Chain Finance for Small and Micro Enterprises

（工作组讨论稿）

（本草案完成时间：2026-01-22）

2026 - - 发布　　2026 - - 实施

广西电子商务企业联合会　发 布

# 目　　次

# 前　言

本文件依据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。

本文件由广西产学研科学研究院提出并宣贯。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

# 小微企业数字供应链金融业务数据交互与风控指引

## 1 引言

随着数字经济的发展与供应链金融的深化，小微企业数字供应链金融已成为破解小微企业融资难题、提升产业链整体竞争力的重要途径。通过运用大数据、物联网、区块链等数字技术，金融机构能够更有效地获取与分析小微企业供应链交易数据，为其提供便捷、高效、低成本的融资服务。然而，当前数字供应链金融实践面临数据交互标准不统一、数据质量参差不齐、数据安全风险突出、风险识别与管理能力不足等挑战，制约了业务的规模化、规范化发展。为规范小微企业数字供应链金融业务中的多参与方数据交互，建立健全基于数据的全面风险管理体系，保护各方合法权益，促进供应链金融生态健康有序发展，特制定本指引。本指引立足于我国供应链金融发展现状，参照金融科技监管框架，对数据采集与交互、风险评估与监测、信息安全与合规管理等关键环节提出系统性技术要求与操作指引，旨在为金融机构、供应链核心企业、金融科技公司、小微企业及其他相关参与方提供实践指导。本指引由广西产学研科学研究院联合金融机构、科技企业及研究机构共同研制。

## 2 范围

本指引规定了小微企业数字供应链金融业务中，各参与方之间进行数据交互的内容、格式、流程、安全要求，以及基于数据开展风险评估与管理的原则、方法与控制措施。本指引适用于商业银行、保险公司、商业保理公司、融资租赁公司等持牌金融机构，以及为数字供应链金融业务提供数据或技术服务的供应链核心企业、金融科技公司、第三方数据服务商等相关机构在开展小微企业供应链金融业务时的数据交互与风险控制活动。

## 3 规范性引用文件

下列文件对于本指引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指引。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本指引。

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 37973-2019 信息安全技术 大数据安全管理指南

JR/T 0171-2020 个人金融信息保护技术规范

JR/T 0193-2020 金融数据安全 数据安全分级指南

《中华人民共和国网络安全法》（2017 年施行）

《中华人民共和国数据安全法》（2021 年施行）

《中华人民共和国个人信息保护法》（2021 年施行）

《关于规范发展供应链金融 支持供应链产业链稳定循环和优化升级的意见》（银发〔2020〕226 号）

《金融科技发展规划（2022-2025 年）》（中国人民银行印发）

## 4 术语和定义

4.1 小微企业数字供应链金融：指金融机构依托数字技术，通过连接供应链核心企业、上下游小微企业、仓储物流企业、交易平台等多方，整合供应链交易、物流、资金流等数据，为供应链中的小微企业提供的在线化、自动化、智能化的融资、结算、保险等综合性金融服务。

4.2 数据提供方：指在数字供应链金融业务中，向金融机构或金融科技服务平台提供原始数据或加工后数据的机构，通常包括核心企业、交易平台、仓储物流企业、第三方数据服务商等。

4.3 数据使用方：指在数字供应链金融业务中，接收并使用数据提供方所提供的数据，主要用于信贷审批、风险管理、贷后监控等目的的金融机构。

4.4 数据交互：指在获得相关授权与满足安全合规要求的前提下，数据在不同参与方之间按照约定规则进行传输、交换与共享的过程。

4.5 风险控制数据集：指用于对小微企业借款人进行信用风险评估与持续监控所需的关键数据集合，包括但不限于主体信息、交易数据、物流信息、资金流水等。

4.6 数据沙箱：指一种在安全隔离环境中，使用经脱敏处理的真实数据或模拟数据，供金融机构或科技公司进行产品开发、模型训练或合规验证的技术机制。

4.7 数字风控模型：指利用机器学习、统计分析等方法，基于风险控制数据集构建的，用于评估借款人信用风险、欺诈风险、操作风险等的量化模型。

## 5 总则

小微企业数字供应链金融的数据交互与风险控制应遵循“依法合规、最小必要、授权同意、安全可控、风险为本”的原则。数据交互活动必须严格遵守国家有关网络安全、数据安全、个人信息保护及金融监管的法律法规与标准规范。数据采集范围应限于实现业务目的所必需的最小范围，不得过度采集。必须确保数据主体（尤其是小微企业主）的知情权与同意权，获取其明确授权。 应建立健全数据全生命周期安全管理体系与技术防护措施，保障数据在传输、存储、使用、销毁等环节的安全性、保密性与完整性。风险控制应贯穿业务全流程，充分利用多维度数据，构建智能、动态、前瞻的风险管理体系。

## 6 数据交互内容与标准

数据交互应以支持对小微企业进行精准风险评估为核心目标。风险控制数据集应至少涵盖以下维度：主体身份与资质数据，包括小微企业工商注册信息（统一社会信用代码、名称、注册地址、法定代表人、股东信息、注册资本、成立日期、经营范围等）、行业分类、行政许可信息、知识产权信息、主要管理人员信息等。历史信用数据，包括企业在人民银行金融信用信息基础数据库的信贷记录、在市场监管部门的行政处罚与经营异常信息、在司法部门的涉诉与被执行信息、在税务部门的纳税信用等级与欠税信息等。核心交易数据是评估供应链关系与经营稳定性的关键，应由供应链核心企业或交易平台提供，包括但不限于：与核心企业或平台的历史交易合同信息（合同编号、签订日期、交易对手方、产品/服务描述、单价、数量、总金额、付款条件、交货日期等）。历史订单与履约信息（订单编号、下单时间、商品明细、发货状态、收货确认状态、退货记录等）。历史结算与发票信息（发票号码、开票日期、金额、已付/未付金额、账期、实际付款日期等）。当前应收账款/应付账款明细（债权债务人、金额、到期日、账龄等）。

经营与行为数据，包括通过物联网设备（如仓储监控、运输轨迹追踪）采集的货物库存、流转数据；通过企业授权获取的银行账户流水摘要信息（如收支频率、对象、大额交易对手等）；在特定平台上的经营行为数据（如店铺访问量、用户评价、物流时效等）。补充数据，可根据需要和授权，在合规前提下，整合税务、海关、电力、社保、行业协会等第三方数据源信息。

数据格式应采用标准化、结构化的形式，鼓励采用 JSON 或 XML 等通用数据交换格式。数据字段定义应清晰明确，建议参照国家或行业已发布的标准数据元目录。时间戳格式统一采用 ISO 8601 标准。数据传输频率可根据业务需求设定为实时、准实时（如 T+1）或批量方式（如日终、月终）。对于用于实时授信决策的数据，传输延迟原则上不应超过 5 分钟。

## 7 数据交互流程与授权管理

数据交互应建立在合法、有效的授权基础之上。金融机构或金融科技平台作为数据使用方，在向数据提供方（如核心企业）请求数据前，必须首先直接或通过数据提供方间接获得作为数据主体的小微企业的明确授权。授权应采用电子协议等形式，内容清晰、具体，明确告知数据主体（企业及其法定代表人/实际控制人）数据收集与使用的目的、方式、范围、存储期限、数据接收方、数据主体的权利（如查询、更正、删除、撤回同意）以及法律责任等。授权过程应留有不可篡改的存证记录。数据交互流程应规范、可追溯。基本流程包括：业务触发与授权获取；数据使用方向数据提供方发起数据请求，附上必要的授权证明与业务标识；数据提供方对请求方身份、授权有效性及业务合理性进行验证；验证通过后，数据提供方按照约定范围、格式和接口规范，通过安全通道传输数据；数据使用方接收数据，并进行校验与确认；双方记录本次交互的日志，包括时间、参与方、数据类型、数据量、用途等，日志保存时间不少于 3 年。鼓励在条件成熟时，探索基于区块链等技术构建多方协同、权责清晰、全程留痕的可信数据交换网络。

## 8 数据安全与隐私保护

所有参与方必须建立与业务规模、风险等级相匹配的数据安全管理体系，并满足网络安全等级保护（至少第二级）要求。在数据采集环节，应确保数据源的真实性、合法性。在数据传输环节，必须使用加密通道（如 TLS 1.2 及以上版本的 HTTPS、VPN 等）进行传输，对敏感数据（如企业银行账号、法定

代表人身份证号)应进行加密处理。在数据存储环节,应对数据进行分类分级管理(参照 JR/T 0193-2020),采取访问控制、加密存储、数据脱敏、安全审计等措施。原则上，原始敏感数据不应长期保存在业务系统之外的非必要环境中。个人信息保护应格外严格。处理小微企业法定代表人、股东、实际控制人等的个人信息时，必须严格遵守《个人信息保护法》及 GB/T 35273-2020、JR/T 0171-2020 的要求。除法律法规另有规定外，共享、转让个人信息必须获得个人的单独同意。在使用数据进行用户画像、自动化决策时，应保证决策的透明度和结果的公平公正，并应提供不针对个人特征的选项或便捷的拒绝方式。建立数据安全事件应急响应预案，发生或可能发生数据泄露、篡改、丢失时，应立即采取补救措施，并按规定及时向监管部门和受影响的数据主体报告。

## 9 风险评估与数据应用

金融机构应构建基于多维度供应链数据的小微企业信用风险评估体系。风险控制数据集应被有效整合，用于构建和优化数字风控模型，包括但不限于：信用评分模型，用于量化评估借款人的违约概率。反欺诈模型，用于识别虚假交易、虚构贸易背景、关联交易欺诈等风险。额度定价模型，用于基于风险评估结果确定授信额度与利率。预警监控模型，用于贷后对经营异常、交易异动、资金挪用等风险进行实时或准实时监测。数据应用应贯穿贷前、贷中、贷后全流程。贷前调查阶段，利用数据验证企业身份真实性、评估经营稳定性、分析供应链交易背景的真实性与连续性。授信审批阶段，将数据驱动的模型评分结果与专家经验相结合，作为授信决策的重要依据。合同签订与放款阶段，可利用区块链等技术支持电子合同签署与存证，并尝试将融资支付与贸易合同的关键履约节点（如发货、验收）进行有条件绑定。贷后监控阶段，持续接收和分析交易、物流、资金回流等动态数据，设定风险预警指标（如交易额连续三个月下降超过 30%、应收账款账龄显著延长、资金回流路径异常等），实现风险的早期识别与干预。当触发预警规则时，系统应自动提示风险管理人员。 模型风险管理至关重要。应建立数字风控模型的开发、验证、部署、监控与更新全生命周期管理制度。模型上线前需经过严格的验证，确保其准确性、稳定性与公平性。应定期（至少每年一次）对模型进行重检与优化，特别是在经济周期、行业政策或数据结构发生显著变化时。应避免模型过度依赖单一数据源或少数特征，防范模型风险。

## 10 合规管理与持续改进

各参与方，尤其是金融机构，应建立覆盖数字供应链金融业务全流程的合规管理体系。业务模式、

数据交互流程、风控模型的设计与运用均应符合金融监管要求。应建立清晰的客户投诉处理机制，妥善处理数据与风控相关纠纷。 应定期开展内部审计与合规检查，评估数据交互与风控活动的有效性、安全性与合规性。 鼓励在监管认可的框架内开展创新。探索利用隐私计算（如联邦学习、安全多方计算）技术在数据“可用不可见”的前提下进行联合建模与风险分析，平衡数据应用与隐私保护。探索利用数据沙箱机制，在安全可控的环境下测试新的数据源、新的分析技术与新的风控策略。行业组织可牵头制定更细化的数据交互接口标准与风控指引，促进生态协同。

## 11 附则

11.1 本指引自发布之日起实施。

11.2 各相关机构在开展小微企业数字供应链金融业务时，可参照本指引建立健全数据交互与风控机制。

11.3 本指引所引用的国家标准、行业标准及法律法规，其最新版本（包括所有的修改单）适用于本指引。

11.4 随着数字技术与金融业务的发展，本指引将适时进行修订和完善。