融资租赁企业使用大模型安全指引（1.0版）

GDFLA
广东省融资租赁协会
GUANGDONG FINANCIAL LEASING ASSOCIATION

引 言

2025 年政府工作报告提出，要持续推进“人工智能+”行动，将数字技术与制造优势、市场优势更好结合起来，支持大模型广泛应用，大力发展智能网联新能源汽车、人工智能手机和电脑、智能机器人等新一代智能终端以及智能制造装备。

随着人工智能技术的快速发展，大模型在融资租赁行业的应用日益广泛，其在数据处理与分析、图像识别、文本生成、信息搜集等方面展现出卓越的能力，显著提升了企业的运营效率。然而，大模型的使用也带来了数据安全、合规性等方面的风险。为确保融资租赁企业在大模型应用中能够遵守相关法律法规以及金融监管总局对金融机构的数据安全要求，特制定本安全指引，希望能为广大融资租赁企业在使用大模型之路上提供有价值的参考。

感谢在本指引编写过程中来自行业相关部门、融资租赁公司及相关专家的指导和支持。

编撰委员会

主编单位 广东省融资租赁协会

编撰委员 周建余　何　凌　周俊宝　叶　舒
黄　敏　黄恩霖　蔡　晨

执行编辑 王　惠　赵国屹　程　达
王仲威　刘　鹏　张　芳
刘国健　黄　超　郑惠馨

参编单位 广州越秀融资租赁有限公司

南航国际融资租赁有限公司

南网融资租赁有限公司

深圳市融资租赁（集团）有限公司

北京市隆安（深圳）律师事务所

北京九思金信科技有限公司

目 录

第一章 总则

第一条 为规范融资租赁企业在业务流程中使用大模型技术的行为，保障个人信息和重要业务数据安全，依据《中华人民共和国个人信息保护法》、《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》（简称：数据二十条）等法律法规及政策要求，结合融资租赁行业特点，制定本指引。

第二条 本指引适用于融资租赁企业在业务经营、算法研发及数据处理活动中，涉及个人信息处理、重要数据管理和大模型技术应用进行业务数据加工、处理、分析、存储、传输等活动，包括但不限于项目尽调、合同审查、风险监控、客户服务等行业交易流程的各环节。

第二章 数据安全管理要求

第三条 数据合规采集与处理

（一）确保数据来源合规：用于训练或推理的数据应通过合规渠道采集，并确保数据的存储、传输、处理符合公司信息安全管理要求。

（二）在获取项目主体（承租人、保证人等）的基本信息（如姓名、证件号码、手机号码）、财务报表、征信等数据时，需严格、明确通过显著方式明示告知项目主体信息的使用目的、范围及处理规则，并分别取得项目主体的明示书面同意，并留存授权记录。

（三）数据采集应遵循最小必要原则，仅采集与业务直接相关的数据，禁止超范围采集个人信息或敏感数据。

第四条 数据脱敏与保护

企业征信数据获取需验证数据源合法性，通过持牌征信机构或取得数据主体书面授权。

融资租赁各项环节中使用大模型时，需对证件号码、手机号、征信信息等敏感信息（字段）在录入大模型系统

前进行去标识化或匿名化处理(如部分字段加密或替换),确保原始数据不直接暴露于大模型训练或推理流程中;个人敏感数据不得用于大模型训练、推理。

避免上传敏感数据:在使用云端大模型 API 接口进行推理服务时,员工不得上传公司个人客户的姓名、身份证号、手机号、征信情况等敏感数据,也不得上传公司内部敏感数据。企业应提前对员工进行合规培训,避免数据泄露风险。

第五条 数据存储、管理、传输

(一) 确保使用国内服务器和大模型:融资租赁企业应使用国内服务器和大模型进行训练或推理服务,避免敏感数据的跨境传输。企业可自行购买 GPU 服务器部署算力,或租用阿里云、腾讯云、华为云、国内通信运营商等国内厂商的算力服务。国内大模型品牌包括 Deepseek、通义千问、智谱 AI、文心一言、豆包、月之暗面等。

(二) 所有涉及个人信息和业务核心数据的大模型训练与推理服务,应使用国内服务器(如阿里云、腾讯云等国内知名服务商)或本地化部署 GPU 算力资源,确保数

据不出境。

（三） 对融资租赁各环节中采集的涉及财务报表、审计报告、资产评估报告等数据进行分类分级（如核心业务数据、一般数据、敏感个人信息），并实施差异化保护措施：

1. 核心数据（如征信信息、金融机构凭证等）：需加密存储，访问权限仅限授权人员；授权访问人员需进行双人双岗授权设置；

2. 一般数据（如公开工商信息）：可开放至业务部门，但需记录操作日志；操作记录应保存至本笔业务结束后的六个月；

3. 敏感个人信息(如个人生物识别信息、信用信息)：需全程脱敏，禁止用于大模型训练。

（四） 在数据传输过程中，需采用不低于 SSL/TLS 等级的加密协议，防止数据在传输过程中被截取或篡改。

（五） 使用或向第三方共享数据、云端大模型 API 接口服务的需签订数据安全协议，明确数据使用范围与责任，建立 API 接口访问日志（保留期限不少于 6 个月）并

定期进行安全评估。

（六） 严禁将包含个人信息或重要业务数据的大模型服务非法部署于境外服务器，或通过境外接口进行数据传输；

相关业务数据必须出境的，须依法通过国家网信部门的安全评估等法律规定的程序。

第三章 大模型业务场景应用

第六条 大模型应用体系建设

（一）综合能力体系建设

本地化部署与云端结合：在确保数据安全的前提下，融资租赁企业可结合本地化部署的大模型、自有知识库和云端大模型 API 接口服务，构建大模型综合能力体系，以提高海量数据处理、文本检查与生成、图文转换、风险识别与建议等业务处理效率。

方案	部署模式	大模型		方案特点				备注
		类型	部署模式	性能	成本	复杂度	上线速度	
方案一	SaaS	商业大模型	SaaS API	高	低	低	快	文档存储在本地服务器，向量化数据发给大模型，存在数据隐私顾虑

方案二	本地私有化	商业大模型	SaaS API	高	中	较低	较快	文档存储在本地服务器，向量化数据发给大模型，有一定的数据隐私顾虑
方案三	本地私有化	商业大模型	云上私有化	高	较高	较低	较快	向量化数据仍会需要发到外网， 仍有一定的数据隐私顾虑
方案四	本地私有化	“中型”开源大模型	本地私有化	中	中	中	中	所有数据完全不外发，完全没有数据隐私顾虑，但“中型”大模型的问答效果较为一般
方案五	本地私有化	“中型”开源大模型微调	本地私有化	较高	较高	较高	较慢	所有数据完全不外发，完全没有数据隐私顾虑，“中型”大模型的问答效果需要微调，因此复杂度较高
方案六	本地私有化	训练行业专属大模型	本地私有化	极高	极高	极高	极慢	所有数据完全不外发，完全没有数据隐私顾虑 理论上效果最好，但从头训练行业模型需要资深 AI 专家团队，以及海量通用数据，外加行业专有数据，因此复杂度高，成本高，且时间长

多种部署方式的优劣势比较如下：

（二）自有知识库建设

确保数据准确与合规：企业应高度重视自有知识库的建设，自有知识库是各家企业用好大模型、利用大模型做出差异化竞争力的关键要素。企业在建设自有知识库时，应确保数据的准确性和合规性，避免大模型输出错误结果和建议。

（三）大模型综合能力总结

大模型在业务场景中的应用可以归纳为五大核心应用能力：

1. **转换**：采用多模态解析（图像/语音/视频转文本）技术，将各类原始数据转化为结构化文本，为后续处理提供标准化输入，提升数据的可用性和处理效率；

2. **识别**：通过大模型语义解析与逻辑推理能力，提取文本中核心业务字段，同时依据预设规则进行不同程度的校验和筛选，保证数据的准确性和完整性；

3. **分析**：基于预设规则要求，大模型对内容进行规则性判断，同时深入挖掘数据背后的潜在信息和趋势，为决

策提供有力支持；

4. 生成：结合多样化的模板，大模型自动整合多源数据生成格式规范、内容完整的可编辑报告，通过便捷的人工复核和修订功能，确保报告的质量和准确性；

5. 问答：通过语义理解与向量检索，从不同类型知识库中高效匹配相关信息，通过多轮对话与上下文关联推理，快速提供连贯、满足要求的知识结果。

（四）具体业务场景应用

1. 业务准入判断

场景描述：业务部门工作人员自行获取或通过业务渠道资源，初步掌握项目相关主体（承租人、保证人等）、租赁物的基本信息，以及项目相关主体的财务报表、审计报告、评级报告、资产信息等财务类信息后，将前述信息加以分析，完成对项目的初步筛选和判断。

大模型方案：准入评估阶段，利用多模态、大语言模型，解析各类结构化、非结构化文件，例如企业基本介绍、评级报告、租赁物清单等资料，提取关键信息，转化为结构化数据；通过大模型快速解析前期掌握的这些资料内容；

根据公司准入要求、预设规则提示词，大模型实现内容逻辑分析、文件交叉互检，自动识别或“挖掘”潜在风险点，如描述矛盾、财务异常等，辅助业务人员判断是否继续跟进该项目。

2.辅助信息收集

场景描述：相关部门组织人员对项目的相关情况进行尽职调查，具体包括实地拜访、远程沟通、资料收集、行业分析、同类型客户业务分析等内容；通过不同方式收集到各类信息，并在过程中不断补充、调整内容要求，为后续分析奠定基础；格式各异、数量繁多的各类资料，对业务人员在解读、分析判断时带来较多工作量。

大模型方案：非结构化文档资料收集汇总并作结构化识别，识别对象主要包括：

（1）尽职调查中收集的材料与信息：现场考察/尽职调查中所采集的照片/录像/文件；客户、供应商和其他关联方的信息；客户及关联方的业务合同；审计报告、法律意见书等专业机构出具的意见/报告；租赁物的清单及现场照片及相关部门/平台登记信息；客户及关联方的公司

章程、股权结构图；

（2）通过与征信、三方数据接口对接，获取客户及其关联方的综合信用信息，包括：失信被执行、被执行、涉诉、行政处罚、股权关系、征信逾期等；

（3）基于尽调访谈、会议沟通等过程中的录音或对话记录所形成/转载的文字信息；

（4）实时抓取行业政策、发展趋势分析、客户新闻舆情等信息，抓取并分析行业龙头企业关键财报指标数据等。

同时，大模型可以综合上述各类信息，基于其语义理解和逻辑推理，辅助完善资料信息的同时，对其中的关联关系、潜在风险进行进一步分析提示，还可以形成结构化数据资产，辅助进行信息交叉互检。

3.辅助业务录入

场景描述：业务开展过程中需处理大量纸质文档、图片、语音等非结构化资料，相关业务人员需要将关键信息摘取出来，录入到系统中，并确保数据录入的准确性，后续业务评审及统计分析基于录入信息开展，批量上传的不

同附件，由大模型根据内容进行自动归类，传输到指定位置；当业务人员对业务系统、数据结构内容了解有限时，会造成录入过程效率低、录入内容易出错等问题。

大模型方案：利用多模态大模型、语音转文字、大语言模型，快速准确地对各类非标资料进行识别；例如：身份证、营业执照、发票信息、租赁清单、报价参数、押品清单等；基于大模型自然语言处理能力，深入分析识别后的文本内容，精准定位并提取关键信息，如承租人名称、关联方信息、资产信息、上下游信息等核心字段；将提取的关键字段与业务系统的结构化字段进行匹配映射，调用业务系统接口，完成结构化数据填写，同时，批量上传的附件，大模型可根据内容进行自动归类，减少人工干预、提供录单质量和效率。

4.业务辅助问答

场景描述：业务人员开展业务时需快速确认新业务模式准入条件、业务流程规则等信息，当公司推出新业务模式，或业务流程制度上有变革调整时，业务人员或存在对新业务模式、准入要求、关键流程等熟悉度较低等问题。

大模型方案：将新业务模式的准入要求、业务流程、特点等信息整理成结构化的知识库，作为问答系统的知识基础；利用大模型的语言理解和生成能力，基于新业务模式知识库信息，与业务人员或客户进行直接对话，准确理解问题并提供相关答案和信息；实时匹配和校验问题信息与准入要求，及时发现并指出不符合项，辅助相关业务人员和客户判断；收集问答过程中的用户反馈和实际业务数据，形成数据闭环，不断优化知识库和问答模型，提高处理效率。

5.尽调报告编写

场景描述：相关业务人员在起草项目尽职调查报告过程中需要重复翻阅各类信息、收集整理不同资料，耗时耗力。

大模型方案：大模型从 PDF、图片等多种格式文件，识别和提取文本、图表、数据和元素格式等关键信息，转换成进一步可处理的格式；通过搜索引擎针对特定查询进行深度搜索，整理、过滤和提炼结果；大模型将不同来源的信息进行融合形成统一、全面的视角或报告，基于预定

义好的文档模版，自动在文档中的特定位置填充特定格式内容，自动生成详细的行业分析、财报分析指标等报告内容；通过直观展示生成内容的原始来源、分析过程帮助用户了解数据准确性、分析合理性；已生成的文档可以继续编辑操作，与大模型进行二次交互，针对特定段落或内容重新生成，大大缩短尽调报表编写周期。

6. 辅助评审决策

场景描述：风险评审人员对项目资料进行审核、项目主体进行评估，判断是否符合公司内部制度及投放标准，内部决策机构根据所提交的项目材料，根据公司内部的规定，对项目是否能够进行投放以及最终的决策。过程中，评审人员或需要查看大量非结构化数据，存在信息处理效率低、主观偏差风险高、动态更新滞后等局限性。

大模型方案：在项目评审过程中，大模型可通过自然语言处理快速解析不同类型文本资料，包括通过不同方式处理后的企业资料、财报数据、行业政策信息、新闻舆情资料等；根据不同审批环节、审批部门的关注重点，设置不同类型的风险关注规则，大模型根据数据进行逻辑推理

分析，根据不同环节要求识别潜在风险点；针对不同部门、不同环节，将历史审批意见、批复意见，形成历史案例知识库，大模型识别不同尽调项目的异同，基于历史评审经验，辅助评审人员提升决策效率与客观性。

7. 审批报告处理

场景描述：项目审批过程中，由于项目信息各异，可能会存在评审批复按照非标准格式给出具体审批意见，相关部门人员需要基于非标格式文档逐条阅读，并人工提取关键结论信息、录入系统，易因疏忽导致数据偏差。

大模型方案：大模型通过信息识别解析不同格式的审批文档，提取批复结果、批复额度、利率要求、放款条件、增信措施要求等核心结果；识别结果与系统历史记录自动比对、标记异常值，也可通过与系统接口对接实现审批结果快速录入，确保审批流程的高效流转。

8. 合同内容审查

场景描述：人工对（拟）签署合同的完整性、合同关键签署内容进行逐项核对，传统方式耗时、耗力且容易信息遗漏。

大模型方案：大模型通过对合同内容的语义理解、关键信息识别，提取文件中的重点审阅内容，例如租赁利率、违约责任、租赁物信息、所有权属关系、地址等关键文字信息；同时提取（拟）签章位置、签章信息等内容；基于识别、提取后的关键信息，分别与预设合同合规规则进行比对校验，判断合同是否存在条款冲突、矛盾的问题；并与项目评审相关批复信息、结构化业务信息等内容进行比对，自动标记差异并生成审查建议，全面提升文件审查质量与效率。

9.运营智能外呼

场景描述：外呼人员在日常工作中需实时与客户沟通多种复杂业务问题，包括客户咨询、投诉问题、租后催收等多种场景，传统话术库一般支持固定问答场景，面对客户突发问题或灵活沟通方式时，会出现难以应对动态需求的问题。

大模型方案：大模型实时解析客户语音转文本内容，识别客户关键诉求，通过知识库问答调取业务流程知识生成动态话术，辅助外呼人员能自动获取问题结果、动态调

整话术策略；同时，大模型基于通话过程进行记录，辅助生成外呼小结，并结合规则及推理分析，辅助标记客户运营等级，为后续精准跟进提供帮助，提升运营效率。

10. 租后风险监控

场景描述：租后管理需持续监控承租人经营健康度，传统方式依赖人工定期爬取公开数据及内部还款记录，再进行交叉分析。因数据源分散、预警规则静态等问题比较耗时耗力，且容易漏判动态风险，在监控时效性和全面性上存在不足。

大模型方案：通过系统对接、多模态格式转换、互联网搜索等多种方式，获取最新工商信息、新闻舆情、行业政策、最新财报等多源结构化数据，大模型实时分析承租人经营动态，结合行业风险特征库构建动态风险阈值；根据预设的风险监控规则，大模型基于语义理解自动识别负面信号，辅助标识风险等级、风险类型，可通过大模型“挖掘”更多风险视角和潜在风险；同时生成预警报告并推送给管理人员；历史风险数据及风险应对、跟进措施亦可形成历史风险监控知识库，大模型识别并联动历史数据，预

测风险后续演化路径，辅助生成风险应对及处置建议，整体提升风险覆盖率和时效性。

11. 内部制度问答

场景描述：公司内部制度往往数量较多，且定时更新不同版本，制度文件也可能分散在不同的系统或存储路径；员工在日常工作中查询内部管理制度时，需回忆文件路径或手动翻查纸质文档以及求助行政、财务等后台部门帮助；其过程往往耗时耗力、容易遗漏关键信息，同时也会导致相关部门重复答疑、效率低下。

大模型方案：将公司全量、各历史版本的制度文档，形成本地制度知识库；大模型通过智能分析用户问题，快速匹配制度知识库中的相关条款，整合多条款内容生成结构化回答；并返回制度原文摘要及示例，自动标注条款的最新版本及生效日期，辅助员工了解具体引用条款信息；对于模糊问题，模型通过多轮对话逐步明确需求，确保获取完整信息，提升自助服务能力与管理效率；同时记录高频问题，优化搜索逻辑，减少重复咨询，提升自助服务效率。

12.智能客户服务

场景描述：终端客户在业务办理过程中，常常高频咨询产品信息、业务进度等问题，传统客服模式依赖人工坐席，人力成本高且需要通过手动查询多个系统获取信息，过程耗时耗力；夜间、节假日等非工作时段，人工坐席资源有限，客户可能面临服务响应滞后或无人处理的问题。大模型方案：整合产品库、业务规则库、实时数据接口，通过向量化存储与语义索引实现快速检索；大模型通过解析客户问题，结合上下文理解区分问题类型，并识别潜在需求，基于知识库、接口数据等进行综合处理，并生成准确回复，实现 7×24 小时在线服务，提高客户问题解决效率、提升客户体验。

13.快速数据问答

场景描述：领导、业务部门相关人员在一些情况下需要及时了解业务相关数据；非技术人员查询业务数据时，通常需依赖 IT 部门编写 SQL 语句或生成报表支持，整体过程需要耗费一定的时间，且存在因需求描述不清导致响应延迟严重、影响业务决策效率等风险。

大模型方案：基于完善的数据治理基础，将常用数据统计维度、数据指标形成应用层宽表成果，同时将宽表元数据建立知识库，并对专业术语、数据别名等进行智能映射；大模型通过自然语言处理技术理解用户需求的核心，将用户提出的口语化问题自动转化为数据库可执行的查询语句（即 Text2SQL 能力），直接连接业务数据库，提取相关数据并生成可视化图表；使业务人员可独立完成数据分析，从而显著降低技术门槛，提升数据驱动决策效率。

第四章 业务流程场景安全规范

第七条 所有客户交互数据留存时间不得超过业务必要期限，到期后应采用不可逆方式销毁。

第八条 项目尽职调查阶段，通过大模型整合工商信息、舆情数据等公开信息时，需验证外部数据接口的合法性与安全性，确保数据来源合规。

第九条 大模型生成的尽调报告需经人工复核，避免因模型“幻觉”导致关键风险点遗漏或错误结论。

第十条 大模型用于合同、数据比对或推理时，需将敏感信息进行脱敏处理后方可输入模型，防止敏感信息泄露。

第十一条 大模型整合还款记录、财务数据等开展风险预警时，需对输入数据进行实时脱敏，并限制访问权限至必要核心人员。

第十二条 模型输出的风险信号需与人工审核联动，确保预警结果准确性、及时性。

第十三条 在智能外呼、在线客服等场景中，客户语

音转文本内容需在本地完成处理，禁止将原始语音数据上传至云端。

第十四条 在数据问答场景中，需针对不同级别和角色人员根据管理要求设置不同的数据权限。

第五章 数据的监督管理与应急管理

第十四条 在大模型应用初期，企业应重视人工干预与审核，避免大模型因“幻觉”问题输出误导性结果。

第十五条 优化知识库与模型：企业应持续优化自有知识库和模型能力，确保大模型输出结果逐渐趋于成熟和稳定。

第十六条 加强网络安全防护：企业在部署和使用大模型时，应做好必要的网络安全防护，防止大模型被攻击者操控输出错误结果。

第十七条 每季度开展数据安全内部审计，重点检查用户授权文件、API 调用记录及模型训练日志。

第十八条 审计结果应留存备查,保存期限不得少于 3 年。

第十九条 每年至少开展两次数据安全与合规培训，重点涵盖业务流程中的敏感数据处理、大模型使用规范及法律风险案例。

第二十条 发生数据泄露事件时，应立即启动应急预案，采取断网、封存数据等措施，应立即向网信、工信及行业监管部门报告，并向受影响客户提供溯源支持。

第二十一条 建立大模型失效备用方案（如切换至本地知识库检索），保障关键业务的连续性。

第六章 技术合作与建设

第二十二条 技术伙伴选择

选择合适的技术伙伴：企业应选择熟悉租赁行业、掌握模型调参优化方法、有金融行业大模型建设经验的技术伙伴，共同建设企业自有的大模型服务能力体系。

第二十三条 项目规划与调研

充分调研与规划：大模型的部署和运维、综合能力体系的建设存在一定的技术门槛，企业应做好充分的调研和规划，确保项目的成功以及高可用性。

第七章 附则

第二十四条 本指引由广东省融资租赁协会负责解释及修订。

第二十五条 本指引与国家法律、法规和监管部门规章不一致的，依有关法律、法规和监管部门规章执行。

第二十六条 本指引于 2025 年 3 月 27 日发布。

后 记

在人工智能技术加速渗透金融领域的当下，大模型为融资租赁行业带来效率跃升的同时，亦伴生数据安全、算法偏差、合规适配等潜在挑战。而今年随着 DeepSeek 大模型突破性进展的出现，开源模式带来 AI 领域的“多快好省”，也给我们带来了前所未有的信心。

“让我们的企业能放心地使用大模型”是编撰此《指引》的初心，撰稿之初我们通过拜访、电话沟通等多种调研方式，寻找业内拥有一线业务经验的专家。来自北京、浙江、广州、深圳等地的企业家和专家们，从合规、技术、实操等不同角度对《本指引》提出了宝贵意见。经过多次的修改完善，最终形成了《融资租赁企业使用大模型安全指引 1.0》。

由于时间仓促及考虑到技术迭代快速等原因，我们也将会持续迭代完善此《指引》，为行业提供最新、最具参考价值的指导性文件。

最后，编委会再次对专家们为融资租赁业的辛勤付出表示衷心感谢！

广东省融资租赁协会

2025 年 3 月

广东省融资租赁协会
办公地址：广州市越秀区德政北路538号达信大厦2307-08室
联系电话：020-38820703
邮箱地址：gdfla@rzzlxh.org.cn
网站地址：http://www.rzzlxh.org.cn