

吴江区 AI agent 知识产权保护手册

苏州市吴江区市场监督管理局（知识产权局）

前言

《中华人民共和国国民经济和社会发展第十五个五年规划纲要》指出，要完善新兴领域知识产权保护制度。当下，AI 技术已实现从对话交互到落地执行的跨越式升级，且个人部署门槛大幅降低，高度契合 OPC（One Person Company）“个人+AI 员工”的创新模式。AI agent 作为核心智能交互应用，其技术研发、场景落地、数据沉淀过程中产生的轨迹数据、Agent 工作流逻辑、专属模型架构等新兴领域知识产权将成为主体发展的核心竞争力。为护航 AI agent 相关主体高质量发展，明晰新兴领域知识产权权利归属、确权路径、风险防控与实操方法，依据《中华人民共和国商标法》《中华人民共和国专利法》《中华人民共和国反不正当竞争法》《江苏省数据知识产权登记管理办法》等法律法规规定，编制本手册，为 AI agent 应用全流程的知识产权创造、管理、运用、保护提供系统性规范与实操指导，助力将创新成果转化为核心竞争优势，推动吴江区 AI 产业、OPC 模式与知识产权保护深度融合、高质量发展。

目录

第一章 核心资产——AI agent 知识产权范畴	1
(一) 商业品牌标识——商标权	1
(二) 技术研发成果——专利权	1
(三) 新型数据资产——数据知识产权	1
(四) 核心工作逻辑——商业秘密	2
第二章 确权路径——AI agent 知识产权分类登记	2
(一) 商标提前布局	2
(二) 专利便捷申请	3
(三) 数据知识产权专项登记	4
(四) 商业秘密即时存证与保密管理	5
第三章 风险防控——AI agent 高频风险与防控规范	6
(一) AI agent 领域高频知识产权风险	6
(二) AI agent 知识产权保护规范	7
第四章 合作规范——跨主体协作知识产权权属与责任约定	8
(一) 联合开发场景知识产权分配	8
(二) 商业合作合同知识产权条款约定	8
第五章 实操指引——AI agent 知识产权管理自检清单	9
(一) 部署与配置阶段	9
(二) 使用与开发阶段	9
(三) 合作与交付阶段	10
(四) 固证与维权阶段	10

第一章 核心资产——AI agent 知识产权范畴

AI agent 的核心知识产权是相关市场主体的核心“无形资产”，主要围绕商业品牌、技术研发、数据资产、工作逻辑四大维度形成专属权利体系，覆盖商标权、专利权、数据知识产权、商业秘密四大类别，是 AI agent 技术落地与商业应用的核心价值载体。

（一）商业品牌标识——商标权

涵盖基于 AI agent 开发的专属产品/服务名称、中英文简称及变体、图形 LOGO、组合标识等商业标识，同时包括商业主体的企业字号、新媒体账号名称等与 AI agent 运营强关联的品牌标识，是区分 AI agent 产品与服务来源的核心标识性权利。

（二）技术研发成果——专利权

包括发明、实用新型、外观设计三类专利，覆盖 AI agent 技术研发与配套硬件设计全维度。发明专利适用于 AI agent 任务执行算法架构、轨迹数据采集处理方法、智能交互决策逻辑等创新性技术方案及配套硬件电路结构、数据传输与处理模块设计等；实用新型专利适用于 AI agent 配套智能硬件实用型结构设计、轨迹数据存储硬件模块化设计、简易交互终端的结构改进等实用性技术方案；外观设计专利适用于 AI agent 前端交互界面、配套硬件产品外观、专属品牌形象等具有美感的设计方案。

（三）新型数据资产——数据知识产权

指经清洗、标注、结构化处理的高质量数据集，是 AI agent

数据开发、模型训练的重要基础，具体包括 AI agent 运行过程中形成的操作意图记录数据集、错误纠正模型数据集、场景化训练数据集、交互反馈数据集等。此类数据资产具有智力成果属性和实用价值，可通过江苏省数据知识产权法定登记程序明确权利归属，强化法律保护与权属证明。

（四）核心工作逻辑——商业秘密

涵盖使用 AI agent 过程中产生的不为公众所知悉、具有商业价值并采取相应保密措施的专属 workflows 逻辑、知识库架构体系、专业化提示词工程等，属于商业秘密范畴，受《中华人民共和国反不正当竞争法》保护。此类内容是实现 AI agent 专属化、高效化运行的核心，相关核心文档需采取加密存储等保密措施，不得随意公开、传播。

第二章 确权路径——AI agent 知识产权分类登记

为适配 AI agent 灵活开发、快速迭代的需求，结合《商标法》《专利法》《反不正当竞争法》《江苏省数据知识产权登记管理办法》等相关法律法规规定，构建“精准布局、专项登记、即时存证”的高效确权体系。

（一）商标提前布局

针对 AI agent 名称、产品标识、服务品牌等商业标识，可在产品上线第一时间，通过国家知识产权局商标局中国商标网（<https://pub.sbj.cnipa.gov.cn/toas-pub-prod/portalui-p>

ub-prod/systemJumpPage) 开展商标查询与在线申请, 提前完成商标检索, 规避近似风险, 对重要品牌可进行防御性注册, 重点布局第 9 类 (软件、APP 等智能产品)、第 35 类 (广告、营销服务)、第 42 类 (技术服务、SaaS 服务等) 等与 AI agent 产品及服务相关的商标类别, 防范商标抢注与侵权风险。



(二) 专利便捷申请

针对 AI agent 相关技术研发成果, 依托线上平台实现专利高效申请。可通过国家知识产权局专利业务办理系统 (<https://ggfw.cnipa.gov.cn/home>) 在线提交申请材料, 实现专利高效申请。建议提前整理技术交底材料, 包含技术方案的核心细节、实施方式、有益效果等内容, 可依托知识产权服务机构优化, 提升专利授权率并优化保护范围。如有快速确权需求, 可通过专利预审通道缩短授权周期。同时, 专利申请需确保数据来源合法合规, 不得包含非法爬取、未经授权使用数据的设计, 不

得存在歧视性、违背公序良俗的技术逻辑，明确自然人为唯一发明人主体，AI 仅作为研发工具不得列为发明人。



（三）数据知识产权专项登记

针对 AI agent 任务轨迹数据、行业专业化数据集等数据资产，可通过江苏省数据知识产权登记平台（<https://dataip.jsipp.cn/#/home>）在线办理登记手续，通过专项登记明确权属。需提交数据采集、加工、处理的合规证明，确保数据来源合法、权属清晰，杜绝使用未经授权的第三方数据进行登记，避免后续权属纠纷。完成登记后获取数据知识产权登记证书，作为数据资产权属、许可、转让、质押融资、作价入股的法定证明文件。



（四）商业秘密即时存证与保密管理

针对 AI agent 工作流逻辑、提示词工程等商业秘密，建议

采取“存证+管理”双重确权保护模式。通过中国版权保护中心DCI系统、微版权等合法区块链平台进行即时电子存证，对商业秘密相关资料进行即时上传存证，生成唯一哈希值与电子存证证书，依据《人民法院在线诉讼规则》，经核验的区块链存证可作为司法证据。同时，对商业秘密采取加密存储、分级访问措施，实行物理隔离与电子加密双重保护，与研发、运营、合作等相关主体签订保密协议，明确保护范围、保密期限与违约责任，实现商业秘密的全流程管控。

第三章 风险防控——AI agent 高频风险与防控规范

结合AI agent研发、部署、使用、协作全流程应用场景，梳理商标权、专利权、数据知识产权、商业秘密四大领域的高频知识产权风险，通过针对性、可落地的规避方法与保护规范，构建全流程风险防控体系，防范知识产权侵权与泄漏风险。

（一）AI agent 领域高频知识产权风险

1. 商标侵权风险：使用与他人注册商标近似的AI agent产品/服务名称、标识，或未经授权使用官方商标进行商业宣传，误导消费者产生授权关联认知；

2. 专利侵权风险：研发的AI agent技术方案落入他人现有专利保护范围，或使用的插件、技能包含侵犯他人专利权的技术内容；

3. 数据知识产权风险：通过AI agent爬虫功能非法爬取他人受保护数据，未经授权使用第三方数据进行模型微调与训练，

或违规将轨迹数据用于商业用途、二次训练；

4. 商业秘密风险：AI agent 权限配置不当导致企业商业秘密泄露，或通过 AI agent 非法获取、使用他人商业秘密，构成不正当竞争。

（二）AI agent 知识产权保护规范

1. 商标保护：在品牌名称确定前开展全面商标检索，避免与现有注册商标冲突，在商标核准注册前避免大规模商业推广，定期监控商标使用情况，发现侵权及时开展维权行动；

2. 专利保护：在研发前，通过国家知识产权局专利数据库进行查新检索，避免与现有授权专利冲突；若存在技术重合，及时进行规避设计，形成具有独创性的技术方案；技术方案形成后先申请专利再公开，避免因技术公开丧失新颖性。

3. 数据知识产权保护：仅使用合法取得、权属清晰的数据训练和优化 AI agent，杜绝非法爬取、未经授权使用第三方数据的行为；本地部署 AI agent，将核心轨迹数据、客户私密数据与公共平台隔离，避免核心数据回流至第三方平台；明确约定轨迹数据归属，与员工、合作方签署书面数据权属协议。

4. 商业秘密保护：实行 AI agent 权限最小化管控，仅授予 AI agent 完成具体任务必需的权限，关闭非必要公网访问入口；建立数据分级制度，将涉密文件、核心商业秘密与 AI agent 处理范围隔离；定期审计 AI agent 操作日志，对异常操作及时预警处置；研发过程中使用开源代码、开源库时，优先选用 MIT、

Apache2.0 等商业友好型协议,避免使用 GPL 等强开源协议代码,避免因协议约束触发技术秘密公开义务。

第四章 合作规范——跨主体协作知识产权权属与责任约定

AI agent 相关市场主体开展联合开发、项目协作、对外服务等跨主体合作时,需提前明确知识产权权属、使用范围、收益分配及侵权责任,防范权属纠纷与侵权风险,保障合作各方合法知识产权权益。

(一) 联合开发场景知识产权分配

联合开发 AI agent 插件、技能、行业解决方案时,建议签订书面的《知识产权权属分配协议》,明确专利、商标、数据知识产权、商业秘密的所有权、使用权、许可转让权及后续收益分配方式;严格界定轨迹数据的采集范围、归属主体与使用限制,严禁无书面约定擅自使用合作方轨迹数据;区分底层通用技术成果与项目特定技术成果权属,明确客户数据的保管主体与使用边界,不得擅自使用或泄露客户数据。

(二) 商业合作合同知识产权条款约定

合作合同中需明确四大核心知识产权条款:一是商标使用授权条款,明确商标授权使用的范围、期限、地域与方式,约定合作方不得超出授权范围使用,不得擅自修改、衍生品牌标识。二是侵权免责条款,约定合作方保证其所提供的技术、数据、服务未侵犯第三方知识产权,若因合作方原因引发知识产权侵权纠纷,

由合作方承担全部赔偿责任。三是知识产权保留条款，提供技术服务/研发服务的一方，可约定在甲方付清全部费用前，服务过程中产生的专利申请权、数据知识产权、商业秘密归乙方所有，甲方付清费用后，按协议约定办理知识产权权利移交手续，涉及数据资产的需同步完成数据知识产权登记变更。四是轨迹数据权属与使用条款，明确 AI agent 运行过程中产生的轨迹数据归用户方所有，提供商不得回流、使用、流转，明确数据的匿名化处理标准、删除机制与保密责任。

第五章 实操指引——AI agent 知识产权管理自检清单

为强化 AI agent 全流程知识产权风险防控，可在部署与配置、使用与开发、合作与交付、固证与维权等关键阶段制定知识产权管理自检清单，相关市场主体可按阶段逐项开展合规核查，实现知识产权管理的标准化、规范化，确保无漏洞、无死角。

（一）部署与配置阶段

1. 全面审核 AI agent 用户协议，明确数据归属、回流规则、使用限制等核心条款；

2. 实行 AI agent 权限最小化配置，关闭非必要权限与公网访问入口，启用多因素认证机制，防范未授权访问；

3. 建立数据分级隔离制度，划定 AI agent 禁止访问的涉密数据范围并设置访问屏，避免核心数据泄露。

（二）使用与开发阶段

1.自有品牌上线前完成商标全面检索与申请，规避商标近似与侵权风险或被他人抢注；

2.对具备专利申请条件的 AI agent 技术方案，及时启动专利查询与申请工作，避免创新成果被他人抢先申请；

3.对高价值轨迹数据、行业专业化数据集，及时申请数据知识产权专项登记，明确权属获得法定保护；

4.对核心工作流、提示词工程、参数配置采取加密存储，完成区块链电子存证。

（三）合作与交付阶段

1.合作前协议约定，明确知识产权权属、责任分担、数据使用与保密规则，避免后续权属纠纷；

2.对外交付 AI agent 开发成果时，明确知识产权转移范围、使用限制与后续权利归属；

3.交付前开展知识产权合规核查，确保成果不包含侵犯第三方知识产权的内容。

（四）固证与维权阶段

1.发现知识产权被侵权后，第一时间通过区块链存证平台对侵权证据进行截图、录屏，完成证据固定，避免证据灭失；

2.立即联系知识产权管理部门（吴江区市场监督管理局知识产权科，开平路 550 号 415 办公室，0512-63983216），递交侵权证据与权属证明等相关材料，启动维权程序。