

# 政务领域人工智能技术合作 合规指南

第十二届北京市律师协会  
数字经济与人工智能领域法律专业委员会  
2025年10月26日

# 政务领域人工智能技术合作 合规指南

第十二届北京市律师协会  
数字经济与人工智能领域法律专业委员会  
2025年10月26日



# 目录

# CONTENTS

---

关于起草《政务领域人工智能技术合作合规指南》的说明 .....	1
一、编制《指南》的必要性 .....	2
二、编制《指南》的主要思路 .....	2
三、《指南》主要内容 .....	3
<b>政务领域人工智能技术合作合规指南 .....</b>	<b>5</b>
第一章 总则 .....	5
第二章 模型合规 .....	7
第三章 数据安全 .....	9
第四章 服务规范 .....	13
第五章 合作合同重点内容 .....	17
第六章 附则 .....	20



## 关于起草 《政务领域人工智能技术合作合规指南》的说明

为深入贯彻习近平法治思想，落实国家“人工智能+”战略要求，支持人工智能技术应用的合规发展，北京市律师协会数字经济与人工智能领域法律专业委员会深入领会中央网信办、国家发展改革委于2025年10月联合印发的《政务领域人工智能大模型部署应用指引》的指导意见，根据《中华人民共和国民法典》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等相关法律，依据《人工智能生成合成内容标识办法》、GB/T45654-2025《网络安全技术 生成式人工智能服务安全基本要求》、GB/T45652-2025《网络安全技术 生成式人工智能预训练和优化训练数据安全规范》和GB/T45674-2025《网络安全技术 生成式人工智能数据标注安全规范》等规章和标准文件，结合北京市司法局研发、建设全国首个行政复议垂直大模型项目过程中积累的合规经验，经过充分调研、多方论证、专家评审等程序，形成了在政务领域可应用、可复制、可推广的合规指南，即《政务领域人工智能技术合作合规指南》（以下简称“《指南》”），为有关单位在政务领域开展人工智能技术相关的合作项目提供推荐性合规实务操作建议。

现将编制情况说明如下：

## 一、编制《指南》的必要性

为贯彻国家“人工智能+”战略，助力大模型技术在政务领域的创新与应用，各级党政机关和事业单位（简称“政务机构”）积极投身人工智能技术应用研究、成果转化工作。

为保障此类合作项目合规落地，需要针对政务领域人工智能技术合作开发的特点，结合人工智能技术应用的最新发展，以及人工智能安全治理和数据要素合规高效流通使用的需求，明确相关参与方在开展工作中的合规要求，为相关单位提供参考性合规建议，确保符合《政务领域人工智能大模型部署应用指引》的要求，符合国家关于生成式人工智能服务安全的相关要求。

## 二、编制《指南》的主要思路

《指南》坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻党的二十大和二十届二中、三中全会精神，主要遵循以下编制思路：一是坚持党的领导，确保正确的政治方向。二是依据现行法律法规及政策，参考国家标准和行业标准，结合北京市司法局全国首个行政复议垂直大模型项目建设过程中的行业实践经验、法律服务经验，确保《指南》的合法性和实用性。三是明确政务领域开展人工智能技术应用在法律合规方面的具体要求。四是突出风险防范，为相关参与方开展工作提供风险说明和防范建议。

### 三、《指南》主要内容

《指南》共六章，明确了在政务领域开展人工智能技术合作的合规原则和具体要求。主要包括：

第一章总则，明确了指南目的、适用范围，并对主要概念进行了定义。

第二章模型合规，明确了在政务领域使用人工智能技术应遵循的合规原则，以及在模型算法、技术方案设计、算力部署、服务网络方面应满足的合规要求。

第三章数据安全，明确了在政务领域的模型训练、验证、测试、应用过程中的数据处理活动的安全要求，并针对公共数据和个人信息两类数据的合规作出了具体说明。

第四章服务规范，明确了政务领域模型提供服务过程中，服务对象的相关权利义务和服务提供方应采取的合规管理措施。

第五章合作合同重点内容，提供了在此类技术合作中，建设方和承建方应签订的合作合同、数据处理协议、知识产权条款的建议内容。

第六章附则，说明了《指南》的效力和发布日期。

《指南》还包括两个附录，具体内容为：

附录一参考材料，是编制本指南时可适用的法律法规、部门规章、标准文件等依据的清单。

附录二合作合同参考样例，是结合本指南内容拟定的，可用于政务领

域人工智能技术合作的合同模板，以供相关参与方在拟定合作文件时参考。

《指南》的编制旨在为政务领域的人工智能应用研究、成果转化工作提供指南，以提高合作的效率和合规性。我们将根据法律法规的更新和行业实践的发展，适时对指南进行修订完善。

# 政务领域人工智能技术合作合规指南

## 第一章 总则

### 第一条 指南目的

为明确在政务领域开展人工智能技术相关的应用研究、成果转化合作应遵循的法律合规要点，确保符合《政务领域人工智能大模型部署应用指引》的指导意见，符合国家关于生成式人工智能服务安全的相关要求，特编制本指南，供开展人工智能技术合作相关工作的有关单位参考。

### 第二条 适用范围

本指南针对各级党政机关和事业单位（简称“政务机构”）开展的政务领域的人工智能技术合作，在模型合规、数据安全、服务规范、合作合同重点内容四个方面提供参考建议。

### 第三条 部署应用原则

政务机构应围绕政务工作中的共性、高频需求，因地制宜、结合实际，选择典型场景进行人工智能大模型探索应用。

政务机构应结合工作实际和场景特点，充分论证人工智能大模型的应用需求、实施路径、功能设计等，做到合理选择实施路径、统筹集约开展部署、探索实现统管复用、持续夯实数据基础的部署原则。

在政务领域提供和使用人工智能模型，应遵循法律、行政法规，尊重

社会公德和伦理，诚实守信，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益，不得危害他人身心健康。

#### 第四条 重要定义

本指南中使用的名词含义如下：

（一）“人工智能模型”简称“模型”，指能够基于自然对话方式理解与执行任务，提供语言理解、知识问答、逻辑推理、内容生成的人工智能产品及服务，或能够根据设定程序自主执行任务的智能体。

（二）“开源模型”指允许公众遵循开源许可证获取、使用、修改和分发的模型。开源模型作者称为“开源开发者”。

（三）“应用场景”指在政务领域中，需使用人工智能模型解决的特定问题或特定需求。

（四）“数据”指在模型训练、验证、测试过程中向模型输入的结构化或非结构化的信息、语料等任何以电子或者其他方式形成的记录，以及符合一定条件或用于特定用途的信息、语料的集合。所有直接作为模型训练输入的数据统称为“训练数据”，包括预训练数据和优化训练数据。

（五）“数据处理”指在模型训练、验证、测试、应用中的数据收集、存储、使用、加工、传输、提供、公开等活动。

（六）“个人信息”指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

(七)“生成内容”指利用生成式人工智能技术生成的文本、图片、音频、视频等。

(八)“知识产权”指双方在合作中投入、产生的全部智力劳动成果以及依法产生的相关权利,包括但不限于专利权(含专利申请权)、著作权(含邻接权)、商业秘密、技术秘密,以及商标、工业设计等其他相关权利。

(九)“建设方”指发起人工智能项目,并提供应用场景和专家意见、公共数据等项目资源的政务机构。

(十)“承建方”指根据政务机构要求提供人工智能技术服务的组织、个人。

(十一)“服务对象”指使用政务领域人工智能模型服务的组织、个人,包括政务机构及其工作人员,以及政务机构服务的社会公众。

## **第二章 模型合规**

### **第五条 算法设计**

承建方应根据应用场景的具体情况,确定模型的设计、研发、训练、测试、部署方案,确保模型功能适用、性能稳定、操作便捷、用户体验良好。

承建方应采取有效措施,提升模型算法透明度,采取技术措施确保生成内容准确、可靠,符合法律、行政法规规定,符合可参照的国家标准的安全要求,并采取有效措施防止歧视。

承建方应定期对模型进行后门存在性检测，及时对发现的后门进行处置，并保存检测和处置记录。

## **第六条 专家资源**

建设方应提供专家资源，以支持算法参数调整、计算过程优化等工作，提高算法的效率和效果。

## **第七条 模型来源**

建设方和承建方应使用已按照国家有关规定开展安全评估，并完成生成式人工智能服务备案的模型。

承建方使用开源模型的，应评估使用方式和应用场景是否符合开源许可范围、限制条件要求，避免违反开源许可协议或相关授权文件；开源范围不符合应用场景需求的，可通过与开源开发者协商等方式获取特别授权。

对于复杂应用场景，可以采用多种来源的模型共同提供服务，但应结合所使用的模型的具体情况，分别开展评估。

## **第八条 算力和部署**

承建方应在中华人民共和国境内部署模型。使用自有算力设施的，应采用本地训练、部署方式，确保算力设施来源合法合规、供应稳定。

使用云服务提供算力资源的，应采取云端训练、部署方式，宜采用符合政务机构网络安全要求的云服务类型。

对于算力需求较高的模型，可采用自有算力设施和云服务结合的方式，

以保障算力资源的可拓展性。

服务提供者应将模型训练环境与推理环境隔离，避免数据泄露、不当访问等安全事件，隔离方式可采用物理隔离或逻辑隔离。

## **第九条 网络安全**

建设方和承建方应采用符合政务机构网络安全要求的网络服务，并采取技术措施防范服务网络遭受攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，保障网络数据的完整性、保密性、可用性。

## **第三章 数据安全**

### **第十条 数据安全责任**

建设方应按照国家有关规定经过严格的批准程序，明确承建方在提供模型服务过程中的数据处理权限、保护责任等，监督承建方履行数据安全保护义务。

承建方应当依照法律、行政法规的规定和合同约定履行数据安全保护义务，承建方应建立全流程数据安全管理制度，包括数据分类分级、安全评估、应急响应等，并对关键岗位人员定期培训。

未经建设方同意，承建方不得访问、获取、留存、使用、泄露或者向他人提供数据，不得对数据进行关联分析。

承建方不得从事窃取或者以其他非法方式获取数据、非法出售或者非法向他人提供数据等非法数据处理活动。

### **第十一条 训练数据**

建设方和承建方使用自行生产或采集的自采训练数据，应确保数据来源合法合规，保留生产或采集记录，并对数据来源和已采集数据开展随机抽样安全评估。建设方和承建方不得采集法律、行政法规明确禁止采集或他人已明确拒绝采集的数据。

建设方和承建方使用以交易、合作、授权等方式获得的商业训练数据的，应与提供方签订合同，并审核其提供的数据的来源、质量、安全保护情况，并留存相关证明材料。

建设方和承建方使用开源训练数据的，应审核数据使用方式和应用场景是否符合开源许可范围、限制条件要求，避免违反开源许可协议或相关授权文件。

### **第十二条 公共数据**

建设方和承建方使用政务机构在履行职责过程中依法采集、生成、存储、管理的各类公共数据的，应确保社会公共利益和公众安全，应依据“原始数据不出域、数据可用不可见、数据可控可计量”的要求，合规使用公共数据。

建设方和承建方需使用未经加工的原始公共数据，或通过公共数据授权运营途径获取的公共数据的，应结合数据内容、使用方式、使用目的，事

前开展合规评估。

数据涉及国家秘密、工作秘密的，应当确保符合国家相关保密规定。

### **第十三条 个人信息**

承建方应当遵循合法、正当、必要和诚信的原则，采取合理措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失。

建设方和承建方收集、处理个人信息的，应获得个人同意或者符合法律、行政法规规定的其他情形。

收集、处理敏感个人信息的，应取得对应个人单独同意或者符合法律、行政法规规定的其他情形。

建设方或承建方收集、处理个人信息的活动属于依法应开展个人信息保护影响评估、个人信息保护合规审计的情形的，应自行或聘请专业机构开展评估或审计。

承建方宜对个人信息采取去标识化措施，并将去标识化信息与可恢复标识的信息隔离存储。

### **第十四条 数据处理**

建设方和承建方应在中华人民共和国境内开展数据处理活动。

未经建设方事先书面同意并依法完成数据出境安全评估等程序，承建方不得将数据传输至境外。

## 第十五条 数据标注

承建方应当对拟使用的数据开展数据预处理、标注等措施，提高数据质量，增强数据的真实性、准确性、客观性、多样性。

承建方应制定清晰、具体、可操作的数据标注规则，应对功能性数据标注以及安全性数据标注分别制定标注规则，开展数据标注质量评估，抽样核验标注内容的准确性，确保数据符合模型训练、验证、测试的目的和要求。

承建方宜对安全性标注数据进行隔离存储。

## 第十六条 数据质量和安全

建设方和承建方应对训练数据进行随机抽样安全核验，通过关键词、分类模型、人工抽检等，去除数据中的违法不良信息。

建设方和承建方应提高训练数据来源的多样性，确保所涉及的每一种语言以及每一种模态的训练数据均有多个训练数据来源。

建设方和承建方应当建立全流程数据安全管理制度，建立数据安全风险监测机制及数据泄露或安全事件的应急响应计划，对数据进行分类分级，采取差异化保护措施。

## 第十七条 数据归还和删除

承建方在项目交付后，应根据建设方要求归还因项目所获取的数据，删除全部数据备份并确保数据不可恢复，或采取建设方认可的匿名化措施。

## **第四章 服务规范**

### **第十八条 服务范围**

建设方应根据建设目标和应用场景确定人工智能模型的服务对象，充分论证在本领域应用生成式人工智能的必要性、适用性以及安全性。

建设方应以合理方式向服务对象提供模型的功能、限制和安全性的说明文件，以保障服务对象的知情权和选择权。

### **第十九条 服务协议**

建设方应当与服务对象签订服务协议，明确使用模型服务的各项权利和义务。服务协议中应向使用者告知使用生成内容的知识产权相关风险，并与使用者约定相关责任与义务。

### **第二十条 真实身份信息认证**

服务对象为政务机构工作人员的，建设方应采取合理措施验证服务对象身份。

服务对象为社会公众的，建设方应依法对服务对象进行真实身份信息认证。建设方应鼓励社会公众使用国家网络身份认证公共服务进行真实身份信息认证。

### **第二十一条 内容安全**

模型的数据和生成内容应遵守网络信息内容管理相关规定。模型的数据和生成内容不得侵犯他人知识产权，不得侵害他人肖像权、名誉权、荣誉

权、隐私权和个人信息权益。

## **第二十二条 合理使用**

建设方应当根据服务的适用人群、场合、用途，指导服务对象科学理性认识和依法使用模型服务。

建设方应通过账号管理、权限管理等方式，依法依规对服务对象的使用行为进行管理，防范滥用风险。

## **第二十三条 持续服务**

承建方应确保模型安全、稳定、持续，保障服务对象正常使用。承建方应监测、记录服务运行状态、安全事件，并依法留存相关的网络日志，保留时间应符合法律、行政法规等的规定及建设方的要求。

承建方应建立数据、模型、框架、工具等的备份机制以及恢复策略，重点确保业务连续性。

建设方和承建方应当建立用户评价反馈机制，及时收集、处理用户需求，以用户反馈驱动模型能力迭代优化。

## **第二十四条 输入内容**

承建方将服务对象的输入信息用于数据处理的，应获得服务对象的授权同意，应为使用者提供关闭其输入信息用于训练的方式，且关闭方式应便捷，应将收集使用者输入信息用于训练的状态及关闭方式显著告知使用者。

承建方不得非法留存或非法向他人提供能够识别服务对象身份的输入

信息和使用记录。

### **第二十五条 防范违法内容**

建设方和承建方在服务过程中发现违法内容的，应当及时采取停止生成、停止传输、消除等处置措施，采取模型优化训练等措施进行整改，并及时向有关主管部门报告。

### **第二十六条 防范违法活动**

建设方和承建方在服务过程中发现服务对象利用模型服务从事违法活动的，应当依法依规采取警示、限制功能、暂停或者终止向其提供服务等处置措施，保存有关记录，并及时向有关主管部门报告。

### **第二十七条 应对安全风险**

建设方和承建方在服务过程中发现模型服务存在安全缺陷、漏洞、网络安全等风险时，应当立即采取补救措施、按照规定及时告知服务对象并向有关主管部门报告；涉及危害国家安全、公共利益的，应当在 24 小时内向有关主管部门报告。

服务用于关键信息基础设施，以及如社会治理、公共安全、自动控制、医疗信息服务、心理咨询、金融信息服务等重要场合的，应具备与风险程度以及场景相适应的安全保护措施。

### **第二十八条 响应个人信息请求**

建设方和承建方应当依法及时受理和处理服务对象关于查阅、复制、

更正、补充、删除其个人信息等的请求。

### **第二十九条 投诉举报处理**

建设方和承建方应建立针对模型服务安全的投诉、举报制度，向服务对象公布投诉、举报方式等信息，及时受理并处理有关投诉和举报。

建设方和承建方应建立针对知识产权问题的投诉举报渠道，具备应对知识产权侵权风险的技术方案，并及时根据国家政策以及第三方投诉情况更新知识产权相关策略。

### **第三十条 监督管理**

建设方和承建方应对政务领域使用人工智能的影响进行审慎监督，建立对风险问题的长期监测和响应机制，通过定期开展培训、评估等方式，加强风险防范意识与风险应对处置能力。

建设方和承建方应定期对人工智能的开发框架、代码等进行安全审计，关注开源框架安全及漏洞相关问题，识别和修复潜在的安全漏洞。

建设方和承建方应建立常态化监测测评手段以及模型应急管理措施。在模型重要更新、升级后，应再次自行组织安全评估。

### **第三十一条 服务透明度**

建设方和承建方以交互界面提供服务的，应在首页等显著位置公开服务适用的人群、场合、用途等信息，宜同时公开基础模型使用情况。

建设方和承建方应在网站首页、服务协议等便于查看的位置向使用者

公开以下信息：服务的局限性；服务所使用的模型、算法等方面的概要信息；所采集的个人信息以及其在服务中的用途。

以可编程接口形式提供服务的，应在说明文档中公开上述信息。

### **第三十二条 监看要求**

承建方应设置监看人员，并及时根据监看情况提高生成内容质量及安全，监看人员数量应与服务规模相匹配。

### **第三十三条 内容标识**

建设方向公众提供人工智能生成合成内容的，承建方应在生成内容上对生成合成内容添加显式标识和隐式标识。服务协议中应明确说明生成合成内容标识的方法、样式等规范内容，并提示用户仔细阅读并理解相关的标识管理要求。

用户申请服务提供者提供没有添加显式标识的生成合成内容的，服务提供者可以在通过用户协议明确用户的标识义务和使用责任后，提供不含显式标识的生成合成内容，并依法留存提供对象信息等相关日志不少于六个月。

## **第五章 合作合同重点内容**

### **第三十四条 合作合同**

建设方和承建方应就合作事项签署书面合同，明确双方在大模型合作开发过程中的权利义务。

合同宜包括以下内容：

（一）开发目标：明确模型开发的具体目标，包括模型应用场景、模型预期功能等。

（二）交付内容：详细列举承建方需向建设方交付的具体成果，例如完整的模型文件、源代码、性能报告及相关技术文档等。

（三）验收标准：约定模型应达到的技术标准和指标。

（四）费用承担及收益分配：约定项目费用的承担方式。双方拟通过项目成果转化获取收益的，宜补充约定收益目标和分配方案。

（五）知识产权：明确开发成果的知识产权归属，约定双方对知识产权的使用权，设定知识产权保护措施。

（六）保密义务：约定双方的保密范围、保密要求。宜要求承建方工作人员单独签署保密承诺书。

（七）违约责任：对于开发成果不符合需求的情况，约定对应的违约责任。

### **第三十五条 数据处理协议**

建设方和承建方应就训练数据的收集、存储、使用、加工、传输、提供、删除等事宜签署书面数据处理协议，明确双方在数据处理过程中的权利义务。

数据处理协议宜包括以下内容：

- (一) 数据情况：明确被处理数据的内容、来源、权属情况等。
- (二) 使用目的：明确数据处理目的，例如训练、验证、测试等。
- (三) 处理方法：明确数据处理方式和范围，包括数据采集、数据清洗、数据预处理、数据特征提取与选择等。
- (四) 存储期限：结合数据处理目的、数据类型，明确数据存储期限，以及项目交付后数据归还、删除或采取匿名化措施的要求。
- (五) 安全措施：明确数据安全措施和管理要求，以及风险事件的协作应对方式及各自安全保护义务和责任。
- (六) 数据删除：明确数据使用完毕后的归还、删除的具体要求。

### **第三十六条 知识产权条款**

建设方和承建方应以书面形式就知识产权归属做出约定。

知识产权条款宜包括以下内容：

- (一) 背景知识产权：建设方和承建方在合作开始之前，或在合作范围之外获得、开发或产生的知识产权由各自享有。但为开展合作需要使用权利方的知识产权的，权利方应给予对方必要授权。
- (二) 项目知识产权：经建设方和承建方协商一致，在合作中产生的新的知识产权可约定由单方享有或双方共同共有。双方亦可以根据知识产权类型、贡献程度、管理责任等因素，按照公平原则约定各自享有的份额。
- (三) 知识产权保护：建设方和承建方应积极保护知识产权，包括但不

限于申请专利、办理软件著作权登记，落实商业秘密、技术秘密保护措施等。

## **第六章 附则**

### **第三十七条 指南效力**

本指南旨在为有关单位在政务领域开展人工智能技术相关的合作项目提供推荐性合规实务操作建议，可以参考使用，而非强制性规定或服务标准。

### **第三十八条 发布日期**

本指南于 2025 年 10 月 26 日发布。

## 附录一 指南依据

- 《中华人民共和国民法典》
- 《中华人民共和国科学技术进步法》
- 《中华人民共和国网络安全法》
- 《中华人民共和国数据安全法》
- 《中华人民共和国个人信息保护法》
- 《网络数据安全条例》
- 《国务院关于在线政务服务的若干规定》
- 《政务领域人工智能大模型部署应用指引》
- 《生成式人工智能服务管理暂行办法》
- 《互联网信息服务深度合成管理规定》
- 《互联网信息服务算法推荐管理规定》
- 《人工智能生成合成内容标识办法》
- 《科技伦理审查办法》（试行）
- 《互联网政务应用安全管理规定》
- GB/T 45654-2025《网络安全技术 生成式人工智能服务安全基本要求》
- GB/T 45652-2025《网络安全技术 生成式人工智能预训练和优化训练数据安全规范》

GB/T 45674-2025《网络安全技术 生成式人工智能数据标注安全规范》

GB/T 41867-2022《信息技术 人工智能 术语》

## 附录二 合作合同参考样例

### 项目合作合同

甲方（建设方）：

联系人：

地址：

电话：

邮箱：

乙方（承建方）：

联系人：

地址：

电话：

邮箱：

根据《中华人民共和国民法典》及其他相关法律法规，遵循平等、自愿、公平和诚实信用的原则，就甲乙双方开展 项目合作的相关事宜订立本合同，以兹双方共同遵守。

#### 1 定义

1.1 项目： \_\_\_\_\_

-----。

1.2 模型：指能够基于自然对话方式理解与执行任务，提供语言理解、知识问答、逻辑推理、内容生成的人工智能产品及服务，本合同中特指双方合作开发的“----- 模型”。

1.3 数据：指在模型训练、验证、测试过程中向模型输入的结构化或非结构化的信息、语料集合。

1.4 项目成果：指双方合作开发的“----- 模型”，包括与之相关的系统、代码、界面、文档、方案、图纸等全部阶段性产物和最终产物。

1.5 应用场景：指建设方需使用模型解决的特定问题或特定需求。

1.6 背景知识产权：指各方在合同生效之前，或在合同范围之外获得、开发或产生的知识产权。

1.7 项目知识产权：指项目成果所包含的知识产权，包括项目成果的全部智力劳动成果以及依法产生的相关权利，包括但不限于专利权（含专利申请权）、著作权（含邻接权）、商业秘密、技术秘密，以及商标、工业设计等其他相关权利。

## 2 合作内容及期限

2.1 甲乙双方合作开发 ----- 模型，用于 ----- 场景，以达到 ----- 目的。

2.2 项目期限：自 ----- 年 ----- 月 ----- 日至 ----- 年 ----- 月

\_\_\_\_日。

2.3 工作任务：双方在以下范围内开展项目工作。双方可根据项目进展、应用场景情况，在以下范围内，通过合同附件形式补充项目的具体工作内容和交付成果要求。

应用场景	功能描述	交付成果

### 3 项目资源

3.1 甲方提供的项目资源包括：

(1) 应用场景资料，包括：\_\_\_\_\_。  
\_\_\_\_\_。

(2) 算力及网络资源，包括：\_\_\_\_\_。

(3) 专家支持，包括：\_\_\_\_\_。

(4) 其他资源，包括：\_\_\_\_\_。

3.2 乙方提供的项目资源包括：

(1) 基础模型：名称：\_\_\_\_\_, 备案号：

-----。

(2) 算力及系统资源, 包括: -----。

(3) 数据清洗、标注服务, 包括:

-----。

(4) 其他资源, 包括: -----。

#### 4 双方权利义务

4.1 乙方应当委派具备专业知识及技术能力的工作人员参与项目工作, 依照甲方指示推进项目的研发进展, 根据甲方要求定期或不定期提交项目报告。乙方应确保项目工作符合数据安全、网络安全、个人信息保护、算法、深度合成、生成式人工智能相关的已发布或今后可能发布的相关法律法规, 以及有关部门规章、政策、管理制度、标准要求。

4.2 甲方应当提供项目工作所需的设备、环境、场地等工作条件, 并由指定人员与乙方对接, 传达甲方需求, 配合乙方工作。甲方有权定期或不定期组织项目例会, 以便双方就项目进度交换信息、讨论对策并解决问题。

4.3 乙方应按照本合同约定的内容、时间及要求完成各项义务, 并按约定的工作计划向甲方交付项目成果。如甲方对工作任务有变更意见的, 应当书面告知乙方, 乙方应当接受甲方的合理意见。但是因此导致项目工作内容变更或项目周期延长的, 乙方应向甲方说明具体情况, 双方另行协商并签订书面变更协议。

4.4 未经甲方事先书面许可，乙方不得将本项目工作分包、转包给第三方。甲方指定特定第三方参与项目的，其选任责任由甲方承担，该第三方的工作内容和成果均由甲方直接管理和验收，乙方应按照甲方要求与第三方签署书面协议，并积极配合第三方工作。

## 5 交付及验收

5.1 乙方应在各阶段工作完成后，向甲方提交相应项目成果。甲方在收到乙方的验收通知后及时组织验收并出具书面验收结论。双方的交付及验收安排如下：

(1) 专家评审：\_\_\_\_\_年\_\_\_\_月\_\_\_\_日前，乙方交付需求规格说明书、详细设计说明书等技术文档，甲方组织专家评审会开展论证和评估。

(2) 初步验收：\_\_\_\_\_年\_\_\_\_月\_\_\_\_日前，乙方应完成项目全部工作任务并上线，甲方组织专家评审初步验收。

(3) 试运行：自\_\_\_\_\_年\_\_\_\_月\_\_\_\_日至\_\_\_\_\_年\_\_\_\_月\_\_\_\_日，乙方针对应用场景开展试运行。试运行期间，乙方应根据甲方反馈完善项目成果。

(4) 最终验收：\_\_\_\_\_年\_\_\_\_月\_\_\_\_日前，乙方应交付经过修改完善后的最终项目成果，甲方根据约定的验收标准及试运行、成果完善情况开展最终验收。

5.2 乙方应在评审会、验收会前\_\_\_\_个工作日内向甲方提交评审、验

收(含各阶段验收,下同)申请书,甲方应在 \_\_\_\_ 个工作日内组织进行评审、验收工作。如因甲方原因造成评审、验收延误的,应顺延时间。对于阶段交付成果,乙方在收到甲方评审、验收通过的意见后,方可启动下一阶段工作。甲方评审、验收不通过,应向乙方提出书面改进意见,乙方根据该意见免费改进成果并重新提交评审、验收申请书。甲方未组织评审、验收,或在评审、验收后在合理期限内未提出异议的,视为评审、验收通过。

5.3 最终项目成果验收完毕之日起 \_\_\_\_ 年内,乙方应提供免费的技术支持,服务内容包括但不限于 \_\_\_\_\_。

## 6 项目经费

双方同意按照以下方式申请、拨付项目经费:

6.1 经费来源: \_\_\_\_\_。

6.2 拨付方式: \_\_\_\_\_。

## 7 知识产权

7.1 本协议的履行不影响双方原本拥有的背景知识产权的归属,仍归双方各自所有。双方同意向对方提供一项全球范围的、不另收取费用、不可转让、不可拆分的知识产权普通授权,以用于项目研发合作及保障项目成果的实施、应用。

7.2 项目知识产权的归属方式为(以下三种形式选一):

\_\_\_\_ 单方享有;

双方共同共有；

双方按比例共有，比例为 \_\_\_\_\_。

在共有的情况下，未经双方书面同意，任何一方不得单独实施、许可、转让项目知识产权，不得以任何形式公开项目成果的商业秘密、技术秘密。

7.3 乙方承诺背景知识产权、项目知识产权不侵犯任何第三方的知识产权或其他专有权利。如因乙方原因导致项目成果侵犯第三方知识产权的，乙方应自行承担费用以获得权利人授权，或在不影响模型运行效果的前提下，免费修改项目成果，以移除侵权内容。

7.4 双方应共同维护项目成果的知识产权，双方有权共同采取包括起诉、上诉以及申诉在内的一切措施保护双方对项目成果所享有的合法权益。如有第三方主张项目成果侵犯其知识产权或其他专有权利，收到通知的一方应立即告知对方，并共同确定处理方案。未经双方共同书面确认，任何一方不得单独就项目成果相关的争议进行起诉、应诉、反诉、和解、调解等。

7.5 如乙方因自身原因（包括公司分立、合并、破产清算、决策、转型等）无法继续履行本合同、无法为模型运行提供技术支持服务、无法参与相关后续建设，甲方有权解除本合同并自行选聘其他供应商作为承接方继续提供服务或开展后续建设，乙方应向甲方转让项目成果及其知识产权，并向承接方交接相关服务。

## 8 数据安全

8.1 乙方应当按照《中华人民共和国数据安全法》《中华人民共和国网络安全法》等法律法规及标准文件的要求，采取网络安全与数据保护措施，对甲方提供的数据严格保密。

8.2 乙方应按照本合同约定和甲方书面指示的处理目的和具体要求，以符合法律法规、标准文件规定的方式处理数据。

8.3 乙方的数据处理及存储活动所使用的技术环境、设备设施须符合甲方要求，且仅限在中华人民共和国境内。

8.4 乙方应具备符合甲方要求的数据安全能力，落实必要的管理和技术措施，并制定针对数据安全风险的应急预案。

8.5 乙方应当通过系统日志等形式记录处理活动的具体情况，并且按照甲方的要求及时提供相关材料。

8.6 本合同终止、解除或履行完毕，乙方应按照甲方的指示，立即删除或返还甲方提供的原始数据及全部备份。

## 9 开源和第三方软件

9.1 乙方为开展项目需使用开源或第三方软件、代码、数据的，应提前向甲方提供拟使用的软件、代码、数据的来源、具体内容及许可信息，并仅在获得甲方同意的情况下使用。

9.2 乙方应确保所使用的开源或第三方软件不会导致项目成果需承担任何额外的许可条件。

9.3 如经双方同意,对全部或部分项目成果通过开源或其他方式公开的,双方可在开源许可证或其他公开许可的范围内使用已公开内容,不受本合同关于授权范围的限制。

## **10 违约责任**

除本合同另有约定外,任何一方违反本合同约定的义务,违约方在收到守约方要求纠正其违约行为的书面通知之日,应当立即纠正其违约行为。如违约方继续违约或不履行其义务,守约方有权提前解除本合同,并追究其违约责任。

## **11 不可抗力**

11.1 不可抗力:指双方缔结本合同时所不能预见、并且它的发生及其后果是不能克服和不能避免的客观情况,包括但不限于:(1)自然灾害如洪水、冰雹、海啸、台风、旱灾、火灾;(2)政府或政党行为如政府当局或执政党颁布的政策、法律、法规和采取新的行为措施导致本合同不能履行;(3)社会异常现象如骚乱、战争、重大公共卫生安全事件、罢工但不包括双方内部劳资纠纷,所造成的不能履行本合同或延迟履行;(4)黑客攻击、计算机病毒、电信部门技术调整导致之影响、因政府管制而造成的暂时性关闭等在内的任何影响网络正常经营情形。

11.2 如出现以上不可抗力情形,双方在本合同中的义务在不可抗力影响范围及其持续期间内将中止履行,任何一方均不会因此而承担不履行上述

义务的责任，但受影响一方应立即书面通知另一方并提供相关的证明文件。如发生不可抗力，双方应立即协商解决问题的方案，合同期限可根据中止的期限而作相应延长。在不可抗力情况消除后，双方应依照协商的延长履行期限及解决问题方案继续履行合同或履行方案。

11.3 如不可抗力持续 \_\_\_\_\_ 日以上，且继续履行本合同将产生重大不利影响或者无法继续履行合同，则任何一方均可终止本合同且不承担违约责任。

## 12 保密条款

12.1 保密信息指披露方以书面、口头、电子或实物载体的方式向接收方提供的任何信息，包括但不限于：（1）与模型有关的商业秘密、技术诀窍、研究成果、文档模板、编程规范、开发流程，以及与项目相关的知识、创意、设想、方案，以及上述信息的衍生信息；（3）双方订立的合同条款，就项目开展的磋商、谈判情况，以及具体的合作安排及相关资料；（4）披露方不时指定为具有秘密性质而需受本合同保护的其他信息。

12.2 保密信息并不以提供方事先声明或明示保密为前提，亦无论采用何种载体。接收方不得向任何第三方公开上述保密信息，并应保证采取合理措施保护该保密信息免受公开。非经提供方事先书面同意，接收方不得将保密信息用于本合同以外的目的。

12.3 接收方在本合同项下的保密义务与责任应持续有效，不受本合同

效力影响。

### 13 通知和送达

13.1 一方向对方在本合同文首所列地址发送书面通知，应被视为在下列时间送达：以快递或专人发送，签收或拒绝签收视为送达；以挂号邮件发出，在发出之后第7个工作日；以电子邮件发出，在电子邮件成功发出之后即为送达。

13.2 双方通过本合同文首所列的双方联系人邮箱就合同约定事项的具体执行事宜进行的沟通和确认，其内容表述可以作为甲乙双方执行合同的依据，与本合同具有相同法律效力。

### 14 争议管辖

14.1 本合同的订立、效力、解释、履行、修改和终止以及争议的解决均适用于中华人民共和国法律。

14.2 双方就本合同的履行产生争议时，双方应当友好协商解决，如协商不成，则任何一方可以采取下列第 种方式加以解决：

(1) 仲裁。提交 \_\_\_\_\_ 仲裁委员会，按照申请仲裁时该委员会现行有效的仲裁规则进行仲裁，在 \_\_\_\_\_（仲裁地点）进行仲裁。仲裁裁决是终局的，对各方均有约束力。

(2) 诉讼。依法向 \_\_\_\_\_（管辖地点）有管辖权的人民法院起诉。

14.3 除争议事项外，双方应继续行使其各自在本合同项下的其他权利并继续履行其各自在本合同项下的其他义务。

## 15 其他

15.1 本合同经双方加盖公章或合同章后，于本合同 2.2 条约定的项目起始时间生效。

15.2 如有未尽事宜，双方可签订补充协议或签署合同附件。补充协议及附件均是本合同的有效组成部分，与本合同有同等法律效力。

15.3 本合同壹式 \_\_\_\_\_ 份，双方各执 \_\_\_\_\_ 份，具有同等法律效力。

(以下为双方签章处，无正文)

甲 方（盖章）：

乙 方（盖章）：

年 月 日

年 月 日

