

大模型备案

一、什么是大模型备案

大模型备案的全称是《生成式人工智能服务管理暂行办法》备案。它是指根据国家法律法规，对于生成式人工智能服务进行的一种管理和监督措施。这项措施要求利用生成式人工智能产品向公众提供服务的机构，在服务前必须向网信部门申报安全评估，并履行算法备案及相关手续。备案的目的是确保算法产品的安全合规性，以便进行监督和投诉。

二、申请大模型备案具备的条件

- 1、有相应的申请主体；
- 2、完成互联网信息服务算法备案；
- 3、内容符合国家相应的法律法规。

三、申请大模型备案需要提供的材料

- 1、大模型基本情况：模型名称、主要功能、适用人群、服务范围以及服务器信息等；
- 2、大模型语料来源及证明文件；
- 3、拦截关键词列表（总规模不少于 1w 个）；
- 4、评估测试题；
- 5、大模型服务协议。
- 6、提供的所有人员联系方式：法人、算法技术人员、公司联系人员手机号及邮箱、公司固话、传真等；

四、服务指南：

- 1、确认备案算法类型
- 2、收集主体备案材料，进行主体备案
- 3、收集算法基础信息
- 4、若产品需 UI 调整，反馈 UI 修改建议
- 5、撰写算法备案材料
- 6、提交到备案平台