

大模型备案指南

一、备案法规依据与核心要求

大模型备案工作主要依据以下法规开展：

《生成式人工智能服务管理暂行办法》（2023 年 8 月施行）：明确要求提供生成式 AI 服务的主体需完成大模型备案与算法备案（即“双备案”），尤其涉及舆论属性或社会动员能力的服务。

《互联网信息服务算法推荐管理规定》（2022 年 3 月施行）：要求算法推荐服务同步完成算法备案，与大模型备案形成互补。

《科技伦理审查办法（试行）》（2023 年 9 月施行）：涉及伦理风险的大模型需提交伦理审查报告，明确数据隐私、算法偏见等风险防控措施。

备案范围：覆盖面向公众提供文本、图像、音频、视频生成服务的大模型，包括自研模型、第三方模型二次开发及 API 调用服务（后者需登记）。

二、备案类型与核心说明

根据服务形态，备案分为两类：

● 大模型备案

适用场景：自研大模型、调用第三方模型进行微调和训练的应用

备案重点：训练数据来源合法性证明（如区块链存证）、模型架构图、黑盒测试报告（敏感问题拒答率 $\geq 95\%$ ）。

典型案例：某科技公司自主研发的智能写作大模型，需提交训练数据授权协议及伦理审查报告。

● 大模型登记

适用场景：直接调用已备案模型 API 且未进行二次开发的应用

备案重点：说明调用接口的功能路径、用户数据传输协议、内容审核机制。

典型案例：某企业通过 API 接入已备案的图像生成模型，需提交接口调用日志及安全承诺书。

服务指南

- 1、下单后，快法务服务专员将在 2 个工作日内联系您
- 2、提出您需要进行算法备案的类型；
- 3、我方给您评估确定；
- 4、我方整理材料，发现问题，会以文档的形式统一给您反馈；
- 5、提供给我方材料后，我方提交； 最终版的打印、盖章的材料，并且附有详细的说明文档；
- 5、办理完成后，取证完成交付给您。