一、什么是大模型备案？

大模型备案是指生成式人工智能服务提供者向国家网信部门履行的法定登记程序，全称为 "生成式人工智能（大语言模型）上线备案"。

核心法律依据是《生成式人工智能服务管理暂行办法》（2023 年 8 月生效），该办法明确规定："提供具有舆论属性或者社会动员能力的生成式人工智能服务的，应当按照国家有关规定开展安全评估，并履行算法备案手续"。

二、为什么要备案？

1. **法律强制**：未完成备案的服务将面临下架、罚款甚至刑事责任
2. **安全保障**：通过审查模型安全性、数据合规性，防范风险
3. **市场准入**：备案是面向公众提供服务的必要条件，已成为行业 "通行证"
4. **政策支持**：多地提供备案奖励（如深圳最高 100 万元）和算力补贴

三、哪些大模型需要备案？

必须备案的条件（同时满足）：

- 提供生成式 AI 服务（文本、图像、音频、视频等内容生成）
- 面向境内公众用户（C 端服务）
- 具备 "舆论属性或社会动员能力"（影响公众观点或能组织动员人群）
- 中国境内注册的独立法人企业，信用良好

无需备案的情况：

- 企业内部自用、不面向公众的模型
- 仅调用已备案第三方 API 且未进行微调的服务（只需 "登记"）

四、备案流程详解（约 6 个月完成）

1. **前期准备**（2-4 周）：深入研究《生成式人工智能服务管理暂行办法》等法规，进行技术自查（语料安全、模型安全测试）
2. **属地申报**（1-2 周）：向企业注册地网信办提交备案意向，获取备案表，准备全套申请材料和测试账号
3. **材料审核**（45 天 +）：属地网信办初审（材料完整性、合规性），可能需 4-6 次反馈修改
4. **专家评审**（1-2 个月）：一对多答辩会，重点评估安全性和内容过滤能力

5. **中央网信办复审**（1-2 个月）：跨部门联审（网信、公安、工信等），重点核查供应链安全、知识产权、跨境数据问题
6. **公示与获证**（1-2 周）：通过后获全国统一备案编号，在官网公示 7 天，企业需在服务显著位置展示备案号

五、核心备案材料清单

备案申请表：模型基本信息、服务范围、研制情况、安全措施

安全评估报告（核心材料，100 + 页）：语料来源合法性分析、模型风险评估（31 类安全风险）、应急预案

拦截关键词库：规模≥1 万词，覆盖 17 类安全风险（北京要求 20-50 万）

评估测试题集：≥2000 题，包括生成内容测试（≥2000 题）、拒答测试（≥500 题）、非拒答测试（≥500 题）

服务协议：用户权益保护、隐私条款、投诉渠道、责任划分

语料标注规则：标注流程、质量控制标准、团队资质

技术测试要求：

- 语料安全：人工抽检 4000 条合格率≥96%；技术筛查 10% 合格率≥98%
- 模型安全：300 条敏感问题测试，拒答率≥95%；非拒答测试拒答率≤5%
- 境外语料占比≤30%，需提供安全评估报告