广州市算法备案、大模型备案及登记指引

**一、什么是算法备案、大模型备案及登记？**

（一）算法备案

算法备案是由国家网信部门主导,与公安部、工信部、国家市监总局一起联合发布出台《互联网信息服务算法推荐管理规定》后的具有强制性的备案制度。

根据《互联网信息服务算法推荐管理规定》,凡在中国境内,应用算法推荐技术向用户提供互联网信息服务的企业或机构,必须依法进行算法备案。

（二）大模型备案及登记

1.大模型备案

大模型备案一般指的是生成式人工智能服务（大语言模型）上线备案，由省级网信部门向上提交到国家网信部门，通过备案后编号在官网上对外公示并定期更新。公示链接如下： https://www.cac.gov.cn/2024-04/02/c\_1713729983803145.htm

根据《生成式人工智能服务管理暂行办法》，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，并按照《互联网信息服务算法推荐管理规定》履行算法备案和变更、注销备案手续。

2.大模型登记

网信部门会同相关部门按照《生成式人工智能服务管理暂行办法》及相关要求，对通过API接口或其他方式直接调用已备案大模型能力，且面向境内公众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开展登记工作。

**二、算法备案流程**

（一）算法备案主要材料

1.《算法备案承诺书》

2.《落实算法安全主体责任基本情况》

3.《算法安全自评估报告》

4.《拟公示内容》

（二）算法备案填报入口

登录互联网信息服务算法备案系统（以下简称备案系统）进行填报，网址为https://beian.cac.gov.cn，系统首页如图

（三）算法备案详细填报流程

算法备案流程主要有两个部分，主体备案和算法备案。主体信息审核通过后才能进行算法备案，算法备案包括算法基础信息填报、关联产品及功能信息或技术服务方式填报。具体流程如下：

（四）算法备案公示

1. 备案号公示

根据《互联网信息服务深度合成管理规定》完成备案的服务提供者和技术支持者应当在其对外提供服务的网站、应用程序等的显著位置标明其备案编号并提供公示信息链接。

2.运行机制公示

根据备案系统，企业需要公示算法的机制机理，包括算法基本原理、算法运行机制、算法应用场景以及算法目的意图等内容。

**三、大模型备案或登记流程**

（一）大模型备案或登记资料

1.信息采集：基本情况、功能服务、算法机理、训练数据、内容审核、下载通道及测试账号、企业及产品描述等；

2.重点材料：上线备案表、安全评估报告（大模型登记不需提交）、模型服务协议、隐私保护政策、语料标注规则、拦截关键词及评估测试题等；

3.对外接口：API接口信息、附加审核策略的虚拟测试账号及不附加审核策略的虚拟测试账号等。

（二）大模型备案或登记详细流程

由省级网信部门审批后提交到国家网信部门。具体流程如下：

1、向省级网信部门报备，获取备案表；

2、企业根据表格及评估要点准备材料；

3、企业内部展开评估，编写相关材料，准备测试账号；

4、提交材料和测试账号给省级网信部门审核；

5、省级网信部门材料审核及技术测试（安全测试）审核通过后，上报国家网信部门；如未通过，修改材料或调整模型能力后再次提审，具体调整内容根据省级网信部门反馈进行；

6、国家网信部门进行材料复审及技术评审，通过，企业下发备案号；未通过，需重新进行上线备案。

（三）大模型备案和登记公示

经审核合格后，网信部门将向备案大模型授予备案号，及向登记大模型授予上线编号，在官网上对外公示并定期更新，企业可在其对外提供服务的网站、应用程序等的显著位置标明备案编号或上线编号。公示链接如下：https://www.cac.gov.cn/2024-04/02/c\_1713729983803145.htm

（四）联系方式

广东省大模型备案或登记咨询电话：020-87100795（来电咨询请明确告知备案主体基本信息）。