

汉坤法律评述

2026 年 8 月 5 日

北京 | 上海 | 深圳 | 杭州 | 武汉 | 海口 | 香港 | 新加坡 | 纽约 | 硅谷 | 伦敦

流水有源，行舟有界 — AI 中转站的合规边界

作者：段志超 | 王雨婷 | 张雪晨 | 李雅琪

引言

随着人工智能（AI）大模型快速迭代，不同模型在推理、编程、图像生成和智能体（Agent）等场景下各具优势，用户同时调用多个模型的需求日益增加。但不同模型厂商在账户注册、接口规范、计费方式、数据处理和服务地域等方面存在差异，部分境外模型的官方服务亦未向中国大陆地区开放。在此背景下，介于用户与模型厂商之间、提供多模型聚合和请求转发能力的平台 — 通常被称为“AI 中转站” — 逐渐兴起。

在典型业务链路中，用户只需注册一个账户、完成一次充值或者对接一套 API，即可调用多个模型，无需分别管理不同模型厂商的账户、密钥和 Token 计费规则。这一模式能够降低模型选型和技术接入成本，但也在用户与模型厂商之间增加了一层技术和商业链路，使模型来源、授权范围、数据流向、内容治理和计量结算等问题更为复杂。

AI 中转的合规性取决于平台如何取得上游模型能力、向何种下游用户提供何种服务，以及平台在模型调用、数据处理和内容管理中实际发挥的作用。本文将围绕该业务模式的主要形态、合规条件和典型风险展开分析。

一、AI 中转站的业务形态与法律关系

即使均被称为“中转站”，不同平台的法律属性和风险也可能存在显著差异。特别是在调用境外模型的场景下，应同时考察两个维度：一是平台以何种方式取得上游模型能力；二是平台向哪些下游用户、以何种形式和用途提供该等能力。

从技术链路看，用户请求通常先发送至中转站的服务器或 API 网关，中转站完成用户鉴权、余额校验、模型路由和格式转换后，再使用其掌握的上游账户或 API Key 向模型厂商发起请求，最后将模型输出返回下游用户。平台由此掌握连接用户和模型厂商的关键链路，但其具备技术接入能力，并不当然意味着已经取得向下游提供服务的法律授权。

根据上游模型能力的取得方式，常见模式包括：

（一）基于模型厂商正式 API 或专项商业授权提供服务

平台以企业客户或合作伙伴身份与模型厂商签约，在协议许可范围内将模型能力集成至自身产品，或者取得代理、分销等明确权限后向下游客户提供服务。

（二）通过模型厂商认可的云服务或模型市场间接接入

部分境外模型可通过国际云服务商或其他授权渠道向特定企业客户提供。该等渠道能够解决模型能力“从哪里取得”的问题，但不当然解决平台“能否再次聚合、转售或者向特定地区用户提供”的问题，仍需遵守云服务协议、模型专项条款和终端用户限制。

（三）通过普通用户订阅、会员账户或者多个账户形成“账号池”

该模式将原本限于特定账户或用户使用的订阅权益，以自动化方式开放给多个下游用户。模型厂商的用户条款通常限制账户共享、转让、出租和多人使用，因而容易引发合同违约、账户封禁及服务中断。

（四）通过非授权技术手段取得模型能力

例如逆向接口、破解协议、盗用 API Key、撞库或者规避平台规则批量获取免费额度。相关行为通常已经超出普通合同违约范围，如具有绕过身份认证、安全措施或计费系统的性质，还可能涉及网络不正当竞争、计算机信息系统安全乃至刑事责任。

从下游交付形式看，平台既可能直接向个人或企业用户提供网页端、客户端的对话服务，也可能以统一 API 接口向企业提供模型调用能力，供企业内部研发、办公或生产使用，或者嵌入企业自行开发的产品和服务后进一步面向终端用户提供。交付形式不同，将直接影响生成式人工智能服务备案或登记、电信业务准入、内容安全和数据处理责任的判断。

上游能力来源	典型安排	主要合规观察
官方 API 或 专项商业授权	通过模型厂商合同直接接入，或取得代理、分销等明确授权。	合规风险相对可控，但仍应核查应用集成、转售或再许可、地域范围、终端用户及数据处理限制。
授权云服务或 模型市场	通过国际云服务商、模型市场或其他授权渠道间接接入。	上游渠道有权提供模型，不当然意味着中转站有权再次聚合、转售或向特定地区用户提供。
订阅账户或 “账号池”	将普通用户订阅、会员账户或多个账户自动化共享给下游用户。	通常存在账户共享、转让、出租及多人使用限制，合同违约、封号和服务中断风险较高。
非授权技术接入	逆向接口、破解协议、盗用 API Key、撞库或规避计费 and 调用限制。	通常超出合同风险范围，可能涉及网络不正当竞争、计算机信息系统安全及刑事责任。

二、业务模式合规性分析

AI 中转站在境内开展业务，可能同时涉及生成式人工智能服务备案或登记、算法备案、电信业务准入、模型授权、个人信息和重要数据出境、内容安全、生成合成内容标识以及网络与系统安全等要求。具体义务取决于平台的技术路径、服务对象、交付方式和实际运营安排。

（一）生成式人工智能服务备案、登记与算法备案

根据《互联网信息服务深度合成管理规定》第十九条、《生成式人工智能服务管理暂行办法》第十七条以及网信部门发布的备案公告，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，相关主体应结合服务形态评估算法备案，以及生成式人工智能服务备案或登记要求。对于通过 API 接口或其他方式直接调用已备案模型能力的生成式人工智能应用或功能，由地方网信部门开展登记；已

上线的应用或功能还应在显著位置或产品详情页面公示所使用模型的名称、备案号或上线编号¹。

AI 中转站通常同时接入多个第三方模型，模型清单和版本变化较快，平台又未必能够取得模型机理、训练数据来源等备案所需材料，因而履行相关程序存在现实障碍。尤其是直接调用境外未备案模型的服务，通常难以仅通过“直接调用已备案模型”的应用登记路径解决合规问题。

《生成式人工智能服务管理暂行办法》不适用于行业组织、企业等机构研发、应用生成式人工智能技术且未向境内公众提供生成式人工智能服务的情形。但企业客户身份本身并不当然等于“内部使用”：平台面向不特定企业持续提供标准化 API 服务，或者允许企业客户将模型能力继续嵌入面向境内公众的产品，仍可能超出该例外的适用边界。判断时应重点考察客户范围是否封闭、用途是否限于机构内部、平台是否允许对外开放，以及合同限制和技术控制是否能够得到实际执行²。

（二）电信业务准入资质

AI 中转站是否需要取得电信业务经营资质，应分两个层面判断：一是相关活动是否构成在中华人民共和国境内经营电信业务；二是结合实际服务内容，判断其是否落入《电信业务分类目录》中的具体业务类型及相应许可或备案要求。

1. 是否在境内经营电信业务

现行电信法规未针对 AI 中转站规定判断“境内经营”的单一标准。实践中，可结合运营主体和业务控制是否位于境内、核心运营人员和客户服务是否在境内开展、主要服务设施是否部署在境内，以及用户签约、费用收取等经营活动是否主要在境内完成等因素综合判断。服务器或上游模型部署在境外，不当然排除境内电信业务准入要求的适用。

2. 业务类型及对应资质

根据《电信业务分类目录（2015 年版）》，信息服务业务（B25）是指通过信息采集、开发、处理和信息平台建设，经由公用通信网或互联网向用户提供信息服务的业务。AI 中转站如自行运营统一服务平台，持续向用户提供访问入口、账户管理、模型路由、生成内容交互和计量收费等服务，可能具有经营性互联网信息服务特征；如其实际业务落入信息服务业务分类，应依法取得相应增值电信业务经营许可。若经营者仅向特定客户提供定制化软件开发或技术服务，并不自行运营面向用户的信息服务平台，则仍需根据合同安排、收费对象、系统控制权和实际交付方式作个案判断。

未取得许可擅自经营电信业务或者超范围经营的，可能面临责令改正、没收违法所得、罚款以及责令停业整顿等后果。《电信条例》中对应的主要罚则为第六十九条。平台如进一步自行建设或控制相关设施，并独立向下游提供服务器托管、互联网资源协作、内容分发或者互联网接入等服务，还可能涉及 IDC、CDN、ISP 等其他增值电信业务许可³。

国家网信办于 2026 年 7 月 3 日再次就《互联网信息服务管理办法（修订草案征求意见稿）》公开征求意见，意见反馈已于 2026 年 8 月 2 日截止。截至本文定稿之日，该草案尚未正式公布施行，本文

¹ 参见《生成式人工智能服务管理暂行办法》及国家网信办《关于发布生成式人工智能服务已备案信息的公告（2026 年 3 月至 4 月）》（https://www.cac.gov.cn/2026-05/13/c_1780413225190669.htm）。

² 参见《生成式人工智能服务管理暂行办法》第二条第三款。

³ 参见《中华人民共和国电信条例》第七条、第六十九条及《电信业务分类目录（2015 年版）》。

仍以现行有效规定为分析基础，但其后续立法进展值得持续关注⁴。

（三）数据处理与数据出境合规

AI 中转站能够接触的数据通常不止用户输入和模型输出，还可能包括账户和联系人信息、API 调用日志、IP 地址和设备信息、鉴权信息、模型路由与异常切换记录、Token 用量、账单及支付信息。平台应先识别各类数据的性质、来源、处理目的、保存期限和接收方，再判断个人信息保护、数据安全和数据出境义务。

境内用户提交至中转站的内容如被传输至境外模型服务商或境外服务器，且其中包含个人信息或重要数据，应根据《个人信息保护法》《数据出境安全评估办法》《促进和规范数据跨境流动规定》等落实相应要求。涉及个人信息出境的，原则上应履行告知、取得单独同意和开展个人信息保护影响评估等义务，并根据主体身份、数据类型和数量等适用数据出境安全评估、个人信息出境标准合同、个人信息保护认证或者法定豁免；涉及已被相关地区、部门告知或者公开发布为重要数据的数据出境的，应依法申报数据出境安全评估。

履行相关义务的主体不宜仅按照“客户自主选模型”与“平台自主选模型”作简单二分，而应结合各方对处理目的、处理方式、境外接收方、模型路由、日志留存和后续使用的实际决定权，判断企业客户和平台分别属于个人信息处理者、受托处理者、共同处理者或者就特定处理活动构成独立个人信息处理者。合同中的角色约定是重要因素，但不能单独改变各方基于实际处理活动承担的法定义务。

1. 境内企业直接使用境外运营和部署的中转站

境内企业将个人信息或重要数据传输至境外中转站或模型服务商时，通常构成境内数据传输方，应自行评估并落实适用的数据出境义务。

2. 境内平台按照企业客户指示提供转发和聚合服务

如企业客户自主决定具体境外模型、处理目的和数据范围，平台不为自身目的进一步处理，企业客户通常对出境活动具有主要决定权；平台仍应作为受托处理者履行安全保障、协助、返还或删除等义务，并向客户充分披露境外接收方、传输路径、存储地点、分包商和数据使用安排。

3. 境内平台自行选择、路由模型并将能力整合为自有服务

如客户无法决定具体模型或境外接收方，而平台自主决定模型范围以及路由、日志留存等处理安排，平台更可能就相关处理活动构成个人信息处理者，并承担相应告知、合法性基础、影响评估和数据出境义务。

无论采用何种模式，平台均应在服务协议和数据处理协议中明确输入输出数据、日志、训练使用、留存期限、第三方共享、境外接收方和安全事件响应安排，并提供与其实际技术链路一致的透明度。

（四）模型厂商的合同约束与服务地域

AI 中转站能否合法、稳定地取得模型能力，首先取决于模型厂商通过服务条款或专项协议授予的使用权。对于以向中国大陆用户提供境外模型调用能力为主要卖点的平台，模型厂商的支持地区、账户、API Key、转售和再许可限制往往构成实质性业务障碍。

⁴ 参见国家网信办：《关于〈互联网信息服务管理办法（修订草案征求意见稿）〉再次公开征求意见的通知》。

部分境外模型厂商通过支持地区列表和服务条款限制特定地区主体注册、访问或使用服务。以截至本文定稿之日的公开信息为例，OpenAI 的 API 支持国家和地区页面以及 Anthropic 公布的 Claude 可用地区清单均未列入中国大陆；OpenAI 同时提示，从不受支持地区访问或向该等地区提供访问可能导致账户被封禁或暂停。相关列表和条款可能动态调整，平台应持续核验⁵。

需要区分的是，模型厂商未将中国大陆列入官方支持地区，首先意味着相关访问或向该地区提供访问可能违反模型厂商的合同规则，并带来封号、终止服务或索赔风险；不宜仅据此直接推导为中国企业或用户使用相关模型本身当然违反中国法律。是否违反中国法律，仍应分别根据生成式人工智能服务、内容安全、数据出境、电信业务和其他适用规定判断。

不同厂商对“应用集成”和“API 转售”的边界并不完全相同。以现行《OpenAI 服务协议》为例，客户可将 API 集成至自有应用并向终端用户提供该应用，但不得转售或出租账户访问、与第三方买卖或转让 API Key，也不得规避速率、使用量和安全限制。平台自行保管上游账户和密钥，并不当然意味着其下游服务符合授权范围；仍需判断其提供的是具有独立功能和具体应用场景的获准集成，还是实质上向第三方转售或再许可 API 能力⁶。

中国企业在特定情况下可能通过国际云服务商或其他授权渠道使用部分境外模型，但该等使用权仍受云服务商和具体模型条款约束。渠道方有权向企业客户提供模型，不当然意味着企业客户或其他中间服务商有权再次聚合、转售或向境内下游用户提供。

（五）内容安全管理

《网络安全法》以及生成式人工智能、深度合成等相关规定对网络信息内容安全提出了管理要求。AI 中转站面向境内用户提供生成式人工智能服务时，应根据其在服务链路中的实际作用，建立对用户输入和模型输出的风险识别、审核、处置、申诉和投诉机制，避免传输或展示中国法下的违法和不良信息。

境外模型服务商的内容安全标准未必与中国法要求一致，平台不宜仅依赖上游模型自身的审核机制。平台可以结合服务对象和使用场景，采取模型前后置过滤、敏感场景限制、人工复核、用户分级、异常调用监测和应急停止等措施，并在与下游企业客户的协议中明确内容安全责任、接口能力和处置协作机制。

（六）生成合成内容标识与备案信息公示

《人工智能生成合成内容标识办法》及配套强制性国家标准已于 2025 年 9 月 1 日起施行，对文本、图片、音频、视频和虚拟场景等生成合成内容的显式标识、文件元数据中的隐式标识，以及下载、复制、导出等环节的标识提出要求⁷。

AI 中转站如向境内用户直接提供生成合成服务，应结合具体内容类型和交互方式评估自身标识义务。采用 API 转发模式的，还应在与上游模型服务商和下游客户的协议及技术接口中，明确标识的添加、传递、保留和展示责任，并提供必要的技术支持。境外模型输出未必自带符合中国规则的标识，平台不能当然依赖上游完成。

⁵ 截至 2026 年 8 月 5 日，参见 OpenAI API 支持国家和地区（<https://help.openai.com/en/articles/5347006-openai-api-supported-countries-and-territories>）、OpenAI 服务协议（<https://openai.com/policies/services-agreement/>）及 Anthropic 支持国家和地区（<https://support.anthropic.com/en/articles/8461763-where-can-i-access-claude-ai>）。

⁶ 同脚注 5。

⁷ 参见国家网信办等四部门发布的《人工智能生成合成内容标识办法》及配套强制性国家标准。

此外，对于已经完成生成式人工智能服务备案或应用、功能登记的服务，平台还应按照网信部门公告要求，在显著位置或产品详情页面公示所使用模型名称、备案号或上线编号。

（七）网络与系统安全、业务连续性

中转站掌握上游账户、APIKey、用户鉴权、模型路由和计量结算等关键能力，一旦发生密钥泄露、越权访问、接口滥用或上游账户封禁，可能同时影响数据安全、客户业务和平台计费。因此，运营方应结合网络和系统实际情况评估网络安全等级保护等要求，并建立覆盖身份鉴别、最小权限、密钥分级管理和轮换、传输与存储加密、日志审计、漏洞管理、异常调用监测和安全事件响应的控制体系。

平台还应开展上游模型厂商、云服务商和其他分包商的管理，通过合同等方式明确服务可用性、数据处理、安全事件通知和退出安排。对于上游账户可能因地区限制、服务条款或异常调用被暂停的情形，平台不宜向下游用户作出无条件、长期稳定或者“永久可用”的承诺，而是建议设置合理的充值上限、退款和余额处置机制，并预先制定服务中断后的用户通知、数据导出和迁移方案。

三、典型违规行为及合规风险

前述备案、许可、模型授权、数据处理、内容安全、标识和系统安全要求，是平台开展相关业务可能需要满足的基础条件。除此之外，平台还可能因模型能力取得、请求转发、数据留存、宣传推广和计量结算等具体行为超出授权范围或违反法律规定，而产生进一步的民事、行政乃至刑事风险。

（一）模型能力“来路不明”

部分平台为降低模型调用成本，可能通过破解网页接口、盗用 API Key、撞库获取账户、绕过调用或计费限制等方式套取模型能力。相关行为不仅可能构成合同违约，还可能触及计算机信息系统安全和网络不正当竞争规则。

1. 非法获取计算机信息系统数据、非法控制计算机信息系统罪

如平台通过盗用 API Key、撞库、破解认证机制等方式，非法获取模型厂商计算机信息系统中存储、处理或传输的数据，或者对相关账户、系统实施非法控制，可能构成《刑法》第二百八十五条第二款规定的非法获取计算机信息系统数据罪或非法控制计算机信息系统罪。

2. 提供侵入、非法控制计算机信息系统程序、工具罪

如果经营者自行开发、出售专门用于撞库、破解认证、绕过安全措施或非法控制系统的程序、工具，或者明知他人从事相关违法犯罪活动仍为其提供此类工具，可能触及《刑法》第二百八十五条第三款规定的提供侵入、非法控制计算机信息系统程序、工具罪。

普通 API 网关、反向代理程序或通用爬虫不会仅因具有请求转发或自动化功能而当然构成犯罪。风险判断的关键在于相关工具是否以突破计算机信息系统安全保护措施为专门用途，以及提供者是否明知其将被用于违法犯罪。

最高人民检察院指导性案例检例第 68 号中，相关人员通过撞库软件和验证码识别批量登录他人账户并获取账号数据，分别被认定构成提供侵入计算机信息系统程序罪和非法获取计算机信息系统数据罪。该案虽非 AI 中转站案件，但反映出司法机关通常会重点考察程序是否突破系统安全措施、行为入

是否取得未经授权的数据，以及工具提供者是否明知其违法用途⁸。

3. 妨碍模型服务正常运行或不正当获取数据

平台如通过共享账号、破解接口、绕过地域或调用频率限制等不正当方式接入第三方模型服务，并实质上妨碍、破坏模型服务的正常运行，或者以欺诈、胁迫、避开或破坏技术管理措施等方式获取、使用模型服务商合法持有的数据，可能构成《反不正当竞争法》第十三条规定的网络不正当竞争行为。根据现行法第二十九条，相关经营者可能被责令停止违法行为并处以罚款；情节严重的，罚款幅度进一步提高⁹。

（二）数据“过路即留存”

AI 中转站作为客户与模型厂商之间的技术中介，通常有能力访问、记录和留存用户输入、模型输出和调用日志。部分高风险平台可能擅自保存相关内容，乃至将其出售给第三方、用于模型训练或其他未经授权的商业目的，导致个人信息、商业秘密和其他敏感数据泄露。

在此情形下，平台可能同时面临以下法律后果：

1. 合同违约

违反与客户之间关于数据使用、保密、留存或删除的约定，可能需要承担停止使用、删除数据和赔偿损失等责任。

2. 个人信息保护责任

如输入输出和日志中包含个人信息，平台未经授权擅自留存、使用或向第三方提供，可能违反个人信息处理的合法性、必要性和透明度要求，面临行政处罚和损害赔偿。

3. 侵犯公民个人信息罪

如平台向他人非法出售或提供公民个人信息并达到“情节严重”标准，可能构成侵犯公民个人信息罪。

4. 商业秘密责任

如数据中包含客户未公开的技术信息、经营信息等商业秘密，平台擅自披露、使用或允许他人使用，可能构成商业秘密侵权；情节严重的，还可能构成侵犯商业秘密罪。

（三）服务“名不副实”

AI 中转站负责展示模型名称、确定模型路由并计算 Token 费用。下游用户通常只能看到平台前端信息，难以直接核对后台实际调用的模型、上游授权关系和原始账单。平台如攀附模型厂商商誉、虚假描述底层模型、以低价模型替代所宣传的高价模型，或者虚增 Token 用量，可能引发商业混淆、合同违约、虚假宣传、消费欺诈乃至诈骗犯罪风险。

1. 商业混淆

根据现行《反不正当竞争法》第七条，经营者不得擅自使用他人有一定影响的名称、网站或新媒体

⁸ 参见最高人民法院第十八批指导性案例“叶源星、张剑秋提供侵入计算机信息系统程序、谭房妹非法获取计算机信息系统数据案”（检例第 68 号）。

⁹ 参见《中华人民共和国反不正当竞争法》（2025 年修订）第七条、第九条、第十三条、第二十九条。

账号名称、应用程序名称、图标等标识，引人误认为是他人商品或与他人存在特定联系。AI 中转站如未经授权以第三方模型产品或官方服务名义提供服务，或者擅自使用第三方模型厂商的名称、图标和近似页面设计，使用户误认为其属于官方或授权服务，可能构成商业混淆¹⁰。

市场监管总局 2026 年公布的人工智能领域不正当竞争典型案例中，上海某公司运营名为“ChatGPT 在线”的微信公众号，使用与 OpenAI 官方图像高度近似的头像，并自称“ChatGPT 中文版”，但实际仅通过 API 接入基础模型，并非 ChatGPT 产品本身。监管机关认定其构成商业混淆，责令停止违法行为并处以罚款¹¹。

2. 服务与收费不实

(1) 未按约提供服务，可能构成合同违约及民事欺诈

模型型号、版本、性能、调用数量和计费规则通常属于服务合同的重要内容。平台承诺提供特定模型，却实际调用性能或价格明显较低的其他模型，或者扣取的 Token 数量、费用与约定不符，可能构成违约；如平台故意作出虚假陈述或隐瞒真实情况并诱使用户购买服务，还可能构成民事欺诈。平台直接面向消费者提供服务的，消费者还可能依法主张惩罚性赔偿。

(2) 实际服务与宣传不符，可能构成虚假宣传

根据现行《反不正当竞争法》第九条，经营者不得对商品或服务的性能、功能、质量等作虚假或引人误解的商业宣传。平台宣称接入特定旗舰模型，却实际路由至其他低成本模型，或者虚标 Token 用量、响应性能及服务能力的，可能构成虚假宣传¹²。

(3) 以虚假服务骗取款项，可能构成诈骗罪

诈骗罪除要求存在虚构事实或隐瞒真相外，还要求行为人具有非法占有目的。运营者自始未接入所宣传的模型却长期收费，通过伪造调用记录、系统性虚增 Token 骗取费用，或者以明显不合理的低价和充值优惠吸收大量预付款后关闭平台、转移资金的，在达到相应数额标准时，可能进一步构成诈骗罪。

(四) 犯罪活动“借道中转”

根据《刑法》第二百八十七条之二，明知他人利用信息网络实施犯罪，为其提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的，可能构成帮助信息网络犯罪活动罪。

如平台明知下游客户利用其服务批量生成虚假信息实施诈骗、非法侵入计算机信息系统、制作或传播淫秽内容等犯罪，仍为其提供 API 转发、IP 地址切换等具有针对性的技术支持，达到“情节严重”标准的，可能构成帮助信息网络犯罪活动罪。是否构成犯罪，需要结合平台是否明知下游犯罪活动、所提供服务的关联程度、异常特征和危害后果综合判断。

¹⁰ 同脚注 9。

¹¹ 参见市场监管总局：《市场监管总局公布五起人工智能领域不正当竞争典型案例》（https://www.samr.gov.cn/xw/zj/art/2026/art_0bea53d4e3904015a340b4e83241a8ec.html）。

¹² 同脚注 9。

四、合规建议

AI 中转站降低了多模型接入门槛，但也增加了模型来源、数据流向和责任分工的不透明性。运营方应确保经营资质、模型授权、数据处理、内容治理和计量结算合法、透明；个人和企业用户则应重点关注平台资质、模型来源、数据安全、收费真实性和服务连续性。

（一）对中转站运营方的建议

1. 完善经营资质和模型授权

结合服务功能、技术架构、收费对象和交付方式，评估是否构成经营性互联网信息服务或其他电信业务；建立可追溯的模型能力采购和授权体系，逐项确认模型来源、应用集成、终端用户、地域、转售或再许可权限。

2. 准确识别备案、登记和服务边界

根据平台提供的是基础模型服务、直接调用已备案模型的应用或功能，还是调用境外未备案模型，分别评估生成式人工智能服务备案、应用或功能登记及算法备案要求；已完成备案或登记的，应落实相应信息公示。对未备案模型，应审慎限定服务对象、用途和范围，避免相关能力实际面向境内公众提供。

3. 明确数据处理角色和跨境安排

围绕输入输出、日志、账单、训练使用、留存和第三方共享，识别平台与客户各自的个人信息处理角色；披露境外接收方、存储地点和分包商，依法落实个人信息保护影响评估及适用的数据出境机制，并通过数据处理协议明确协助、安全事件和删除义务。

4. 建立内容安全和标识机制

根据中国法要求设置输入输出审核、违法和不良信息处置、投诉申诉和应急停止机制；对生成合成内容落实显式、隐式标识及下载、复制、导出环节要求，并在 API 链路中明确标识责任的添加、传递和保留。

5. 强化网络安全和业务连续性

落实身份鉴别、最小权限、API Key 分级管理和轮换、加密、日志审计、漏洞管理及异常调用监测；开展上游供应商管理，设置合理的充值上限、退款和余额处置机制，并制定账户封禁或服务中断后的通知、数据导出和迁移方案。

6. 建立“真实模型、真实用量、真实计费”的审计机制

在遵循数据最小化和安全保护要求的前提下，留存必要的上游模型标识、请求时间、Token 用量、路由结果和异常切换记录，使下游账单与上游调用记录能够合理对应，并对模型降级或替换向用户作出清晰披露。

7. 完善客户和滥用风险管理

根据服务风险开展必要的客户识别、用途说明和异常行为监测；对明显涉及诈骗、非法侵入、批量违法内容生成等高风险活动，及时限制、暂停或终止服务，并保留必要记录和处置证据。

（二）对 AI 中转站用户的建议

1. 核验平台资质和模型来源

核验运营主体、经营资质、备案或登记情况和上游模型清单，了解模型能力来自官方 API、授权云服务商还是其他渠道，避免使用依赖共享账户、非授权接口或规避技术接入的平台。

2. 控制输入数据范围并评估跨境风险

不应向来源和安全措施不明的平台输入重要数据、商业秘密、个人信息及其他敏感数据。企业确需处理相关数据的，应事先评估平台的数据留存、训练使用、第三方共享和境外传输安排，并采取筛选、脱敏和访问控制等措施。

3. 限定境外模型的企业使用场景

企业通过中转站调用境外未备案模型时，应对使用目的、应用场景和下游开放范围作出限制，避免未经评估即将相关能力嵌入面向境内公众的产品或服务。

4. 审慎评估收费和服务连续性

关注实际模型、Token 计算方式、模型替换、充值退款和中断处理机制；对于明显低于官方价格的套餐、大额预付费和“永久可用”等承诺，应保持审慎，并通过合同约定数据导出、迁移和余额处置安排。

五、结语

AI 中转站回应了市场对多元模型能力和灵活接入方式的现实需求，在降低使用门槛、促进模型能力普及和应用创新方面具有积极价值。对于这一快速发展的新业态，合规的意义并非简单否定或限制，而是帮助市场形成更清晰、稳定和可持续的发展边界。

AI 中转站的合规关键，不在于“中转”这一名称，而在于看清每一段业务链路：模型能力是否取得合法授权，平台是否具备相应经营资质，服务是否触及境内公众，数据和内容是否在可控边界内流转，模型、用量和计费是否真实透明。通过提高模型来源、服务边界、数据流向和责任分工的透明度，AI 中转站降低接入门槛的商业价值才能得到更稳健和可持续的释放。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123

Email: kevin.duan@hankunlaw.com