数据处理协议（DPA）

DATA PROCESSING AGREEMENT

版本 v1.0 · 生效日期 2026-10-23 · 最近更新 2026-10-23

运营主体（受托处理者）	**青硕秦皇岛文化传播有限公司**
平台名称 / 域名	**StarHub Ai 星枢云 · www.starhubc.com**
数据保护事务邮箱	**59780138@qq.com**
商务与签署邮箱	**kf@qsccl.com**

本协议是您与青硕秦皇岛文化传播有限公司之间就 StarHub Ai 星枢云在受托处理您的个人信息时应遵守的数据保护义务所订立的专项协议，是《服务协议》《隐私政策》的补充与细化。企业、机构客户可下载签署版盖章回传或电子签，与主协议具有同等效力。

一、 定义

除本协议另有约定，下列用语具有如下含义：

个人信息处理者（客户）：指决定个人信息处理目的和处理方式的组织，即通过本服务提交调用请求的一方。

受托处理者（平台）：指接受客户委托、按客户指示处理个人信息的青硕秦皇岛文化传播有限公司，即 StarHub Ai 星枢云的运营主体。

委托处理：指平台基于客户指示，为提供大模型 API 聚合分发服务而对接入数据进行的传输、转发、缓存（内存级）、计量与记录元数据等操作。

再委托（子处理者）：指平台将客户数据进一步交由上游模型渠道或基础设施服务商处理的行为，详见附件一。

境外接收方：指位于中华人民共和国境内以外、接收并处理客户数据的法人或组织，详见附件三。

接入数据：指客户通过接口提交的内容，包括提示词、图片、音频、视频、文件及其元数据。

元数据：指为计费、对账、风控与排障所必需的请求描述信息，不含接入数据正文，字段范围见附件二第 2.2 项。

安全事件：指接入数据或个人信息发生或者可能发生泄露、篡改、丢失、毁损，或未经授权被访问的事件。

二、 角色、适用范围与效力

角色划分：就本服务项下的接入数据，客户为个人信息处理者，平台为受托处理者。平台仅按客户指示处理接入数据，不为自身目的处理。

适用对象：本协议适用于注册为企业、机构或其他组织，或虽为个人但代表组织采购服务的客户。个人开发者注册时同意《服务协议》《隐私政策》即已覆盖其个人信息处理规则，无需单独签署本协议。

与主协议的关系：本协议是《服务协议》的组成部分。就数据保护事项，本协议与《服务协议》《隐私政策》不一致时，**以本协议为准**；本协议未约定的事项适用《服务协议》。

签署方式：客户可在本页下载签署版，盖章回传或通过双方认可的电子签名平台签署；签署版与本页在线文本内容一致的，具有同等效力。未签署本协议的客户，其数据保护关系适用《服务协议》第十六条与《隐私政策》。

三、 客户指示与目的限制

平台仅按客户通过接口、控制台或书面工单发出的指示处理接入数据，处理目的限于：完成模型推理调用、返回结果、计量计费、故障排查与安全防护。

禁止用途：平台不得将接入数据用于训练、微调、评测任何模型，不得用于画像、广告投放，不得出售、出租或以其他方式向无关第三方提供。

超出指示的处理：平台认为客户的某项指示违反法律法规或可能造成数据泄露的，应立即通知客户并有权暂停执行该指示，由此产生的服务延迟不视为平台违约。

客户自身义务：客户应确保其提交接入数据具有合法性基础（包括取得必要的同意或具备其他合法性事由），并对其内容合法性负责。客户知悉本服务为通用模型接入服务，**不应在未做脱敏的情况下提交与业务无关的敏感个人信息（含生物识别、医疗健康、金融账户、行踪轨迹、不满十四周岁未成年人信息等）**。

四、 处理的数据类别与数据主体类别

平台不主动收集个人信息，接入数据的类别由客户自行决定。可能涉及：

（1）**账号与交易类**：用户名、昵称、邮箱、手机号、登录 IP、充值消费流水、发票信息；

（2）**接入数据**：客户提交的提示词与多模态文件，其中可能包含客户业务场景中的个人信息；

（3）**技术与日志类**：请求 ID、模型标识、渠道标识、Token 用量、配额、耗时、状态码、客户端 IP、User-Agent。

数据主体类别：客户的员工、客户自身的终端用户，以及接入数据中可能涉及的第三方个人。

五、 处理方式与不留存承诺

平台的处理方式为：接收请求 → 内存中解析与转发至上游渠道 → 返回结果 → 记录元数据并结算计费。**接入数据正文仅在转发链路的内存中短暂存在，不落盘、不入库、不写入文件系统**。

元数据留存：请求日志只记录《附件二》第 2.2 项列明的字段，不含请求与响应正文，留存 **24 个月**，用于计费对账、渠道核验与争议处理。

例外情形：仅在下列情形下平台可能接触正文内容——① 客户主动提供并授权排障（如工单附 Request ID 与复现文本）；② 依法律法规或有权机关要求；③ 经客户书面同意的专项排查。上述情形下的数据仅在授权范围内使用，排查结束后按本条留存期限删除。

服务器端缓存：平台不使用上游厂商的上下文持久化能力，不为客户保留会话上下文；会话上下文由客户自行在请求中携带。

六、 技术与组织安全措施

平台采取与业务风险相适应的措施，**完整清单见附件二**，要点包括：

（1）**凭据保护**：API 密钥仅存 SHA-256 哈希、明文只展示一次；上游渠道密钥以 AES-256-GCM 加密存储，加密主密钥不落数据库，由部署环境独立注入；

（2）**传输安全**：对外与对上游均使用 HTTPS/TLS；

（3）**访问控制**：用户 / 代理商 / 管理员三端隔离，接口按最小权限与角色校验；敏感字段（渠道密钥、API 密钥、收款账户）后台脱敏展示；

（4）**网关加固**：请求体与上传体积上限、SSRF 防护、限流与并发闸门、上游返回保真校验、异常计量拦截、连续失败自动熔断；

（5）**审计与对账**：关键管理操作留痕；钱包、流水与缓存三方定时对账。

诚实声明：截至本协议版本生效日，平台**尚未取得**网络安全等级保护测评备案证明、ISO/IEC 27001 认证或 SOC 2 报告；平台不就上述未取得的认证作出任何承诺。上述认证的取得进度可应客户书面要求提供说明，相关承诺见附件四。

七、 人员与保密

平台按最小必要原则授予内部人员系统访问权限，权限变更留痕；有权接触接入数据的人员（如运维、客服）负有保密义务，该义务在劳动关系或合作关系终止后继续有效。

平台在人员离职或岗位调整时于 **1 个工作日内**回收其系统账号与凭据。

八、 再委托（子处理者）

概括同意：客户同意平台为完成调用而将接入数据转发至上游模型渠道及必要的基础设施服务商，当前清单见**附件一**。

变更通知：平台新增、替换或停止使用再委托方，应提前 **15 日**在 /dpa 页面与本协议附件一更新，并通过站内公告或邮件通知客户。

客户异议权：客户对新增或替换的再委托方有合理异议的，可在通知期内书面提出，双方协商；协商不成的，客户有权就受影响的服务终止使用并按《服务协议》第八条申请未消费部分退款，此为客户的唯一救济。

背靠背义务：平台应与再委托方约定不低于本协议水平的数据保护义务；再委托方违反义务的，平台就客户损失按本协议第十四条承担责任。

渠道切换说明：本服务的核心能力之一是渠道故障自动降级切换。客户知悉并同意：为保障可用性，平台可在附件一清单范围内自动切换同一模型的承载渠道，该切换属于已获概括同意的再委托行为，无需逐次取得客户同意。

九、 跨境传输

平台部分模型由境外节点承载，接入数据将被传输至境外接收方处理。**境外接收方清单、所在国家或地区、处理目的与传输机制见附件三**。

传输条件：平台依据《个人信息保护法》第三十八条，就境外传输活动与境外接收方订立个人信息出境标准合同，并按规定向河北省互联网信息办公室备案；备案完成情况可应客户书面要求提供证明文件。

告知与单独同意：客户作为个人信息处理者，应就境外接收方的名称、联系方式、处理目的与方式、个人信息种类以及向其行使权利的方式向相关个人履行告知义务并取得单独同意；平台在《隐私政策》与本协议附件三中向客户充分披露上述信息，以协助客户履行该义务。

客户选择权：客户可书面要求将其调用范围限制在境内渠道的模型内，平台在技术条件允许的范围内配合，具体可用模型清单由双方书面确认。因该限制导致的模型覆盖减少或可用性下降，不视为平台违约。

十、 数据主体权利协助

平台提供必要协助，使客户能够响应数据主体依《个人信息保护法》提出的查阅、复制、更正、删除、撤回同意、注销账号等请求。

客户可通过控制台工单或 `59780138@qq.com` 提出协助请求。平台在 **15 个工作日**内答复；需核验身份的，核验时间不计入上述期限。

数据主体直接向平台提出的请求，平台在核实其身份后转交客户处理，不擅自处分客户数据。

十一、 安全事件与通知

平台发现安全事件的，应立即启动应急预案、采取补救措施，并在 **72 小时**内通知客户，通知内容包括：事件基本情况、可能影响的接入数据范围与类别、已采取的措施、客户可采取的降低风险建议、平台联系人。

平台配合客户履行其向监管部门和个人的报告义务，并在客户合理要求下提供必要的技术说明。

因客户自身系统、客户端或被授权人员的过错导致的安全事件，由客户承担相应责任；平台在其过错范围内承担责任。

十二、 审计与合规证明

平台以**书面方式**提供合规证明，不开放现场审计。客户每年可提出不超过 **1 次**书面审计请求，平台在 **20 个工作日**内提供下列材料之一或组合：

（1）数据安全与隐私保护自评问卷的书面答复（问卷由客户提供，经双方确认后填写）；

（2）平台已取得的第三方检测或测评报告的结论页（涉及第三方保密义务的，做必要脱敏）；

（3）本协议附件二安全措施清单的执行情况说明。

客户对材料有合理疑问的，双方可通过技术会议澄清。客户不得要求进入机房、查看源代码、获取其他客户数据或渗透测试。

十三、 删除与返还

服务终止或本协议解除后，平台在 **30 个自然日**内删除或匿名化处理客户的相关数据，法律法规要求保存的除外。

元数据：请求日志元数据按 24 个月留存期自然到期；客户可要求提前删除指定范围，平台在 **15 个工作日**内执行并书面确认。

账务记录：充值、消费、发票、佣金等交易与账务记录按《中华人民共和国电子商务法》等要求自交易完成之日起保存 **3 年**，不因本协议终止而删除。

返还：接入数据不留存，故无正文可返还；客户可通过控制台账单与日志导出自助导出元数据。

备份：备份介质中的数据按备份周期自然覆盖，不单独执行定向删除；平台承诺不超过 30 个自然日的覆盖周期。

十四、 责任与赔偿

双方就本协议项下的赔偿责任适用《服务协议》第十一条与第十九条：**平台累计赔偿上限为客户前 1 个自然月实际支付的服务费用，且以补偿配额方式承担，不赔偿间接损失、预期利益损失、商誉损失及第三方索赔**。

平台因违反本协议导致客户被监管部门处罚且该处罚直接归因于平台过错的，平台在赔偿上限内承担相应部分；客户未履行其告知、同意或脱敏义务的，相应责任由客户承担。

本条不限制法律强制规定不得限制的责任。

十五、 期限、变更与终止

本协议自双方签署（或客户线上确认）之日起生效，有效期与《服务协议》一致，至客户账号注销或服务终止且数据删除义务履行完毕之日止。

平台修改本协议的，提前 **15 日**在本页公布新版本并标注版本号与生效日期；修改涉及客户义务加重或权利减损的，平台以站内公告或邮件通知客户，客户不同意的可在生效前终止使用。

任一方严重违反本协议且在收到书面通知后 **15 日**内未纠正的，另一方有权解除本协议。

十六、 适用法律、争议解决与其他

本协议适用中华人民共和国法律（为本协议之目的，不含香港特别行政区、澳门特别行政区与台湾地区法律）。

因本协议产生的争议，双方应友好协商；协商不成的，提交**秦皇岛市有管辖权的人民法院**诉讼解决。

本协议条款部分无效不影响其他条款的效力。

附件：附件一《再委托方（上游渠道）清单》、附件二《技术与组织安全措施清单》、附件三《跨境传输与境外接收方清单》、附件四《政企及金融客户增强条款》。四个附件均为本协议不可分割的组成部分。

联系：数据保护事务 `59780138@qq.com`；商务与签署 `kf@qsccl.com`。

附件一　再委托方（上游渠道）清单

清单基准日：2026-10-23。标注「境外」的条目将导致接入数据出境，详见附件三。

境内再委托方（均为厂商官方直连，数据在中华人民共和国境内处理）：

1. DeepSeek 官方 — `api.deepseek.com`；2. 阿里云百炼（通义千问官方）— `*.aliyuncs.com`（华北2·北京）；3. 百度千帆（文心一言官方）— `qianfan.baidubce.com`；4. 火山方舟（豆包官方）— `ark.cn-beijing.volces.com`；5. 智谱官方 — `open.bigmodel.cn`；6. MiniMax 官方 — `api.minimaxi.com`；7. 月之暗面 Kimi 官方 — `api.moonshot.cn`；8. **Agnes 中国站（境内主通道）** — 境内已备案主体运营，服务器位于境内（深圳），数据在中华人民共和国境内处理。

境外再委托方（接入数据出境，本协议统称「境外模型节点」，不在此公开具体服务商与地址）：

9. **境外模型节点 A** — 承担多模型聚合转发与容灾，承载模型数量占比最高；节点位于境外，由平台签约的境外服务商提供推理转发。

10. **境外模型节点 B** — 仅在境内主通道不可用或余量不足时作为降级通道；另有少数模型仅在境外节点上架，仅当客户调用该等模型时才涉及出境。

安全、可控、可审计：① 平台向境外节点出网采用**固定地址白名单**，不接受动态下发与任意跳转；② 渠道凭据在平台侧以 AES-256-GCM 加密存储、不落日志、不回显明文；③ **每次调用均记录元数据**（请求 ID、模型、渠道编号、Token 用量、耗时、状态码），可逐次审计、对账与追溯；④ 传输全程 HTTPS/TLS；⑤ 客户可书面要求仅使用境内渠道模型，平台书面确认为其开放的可用模型清单。

境外接收方的**注册名称、注册地址与数据保护联系方式**，随《境外接收方清单》（附件三）于签署时或客户书面要求时提供，不在本页公开披露。

平台将在清单变更时按第八条提前 15 日更新本附件。客户可随时在本页查看最新清单，也可要求平台出具带公章的版本。

附件二　技术与组织安全措施清单

2.1 非留存设计：API 网关（Go 服务）在内存中读取请求体、转发至上游并流式回传，**不将请求与响应正文写入数据库、日志文件或磁盘**；请求体设有体积上限以防止内存与磁盘滥用。

2.2 日志字段白名单：`request_id / user_id / token_id / channel_id / model_id / input_tokens / output_tokens / cached_tokens / quota_consumed / cost_quota / is_stream / duration_ms / first_token_ms / status / error_code / http_status / error_type / error_msg / client_ip / user_agent / created_at`。该表结构不含任何正文字段。

2.3 凭据与加密：客户 API 密钥仅存 SHA-256 哈希、明文仅签发时展示一次；上游渠道密钥以 AES-256-GCM 认证加密存储（可检测篡改），主密钥由部署环境注入、不存数据库。

2.4 传输：对外接口与上游调用均启用 HTTPS/TLS。

2.5 访问控制：用户 / 代理商 / 管理员三端鉴权隔离，接口按角色与最小权限校验；后台对渠道密钥、API 密钥、收款账户等敏感字段脱敏展示。

2.6 网关加固：请求体与上传体积上限、SSRF 防护、按 Key/模型的 RPM 与并发限流、上游返回保真校验、异常计量拦截、连续失败自动熔断与渠道降级。

2.7 审计：管理端关键操作写入操作日志；登录尝试与高危操作留痕。

2.8 对账与资金安全：钱包、流水与缓存三方定时对账，余额异常与低余额提醒。

2.9 组织措施：最小授权、保密义务、离职 1 个工作日内回收账号；安全事件应急预案与 72 小时客户通报机制。

2.10 尚未具备（如实披露）：未取得网络安全等级保护测评备案、ISO/IEC 27001、SOC 2；未设立独立的数据保护官（DPO）职位，个人信息保护负责人联系邮箱为 `59780138@qq.com`。

附件三　跨境传输与境外接收方清单

3.1 出境场景：当客户调用由境外节点承载的模型时，接入数据（提示词、图片、音频等）将被传输至境外接收方完成推理，结果回传至境内。

3.2 境外接收方（统称「境外模型节点」，具体名称与联系方式见《境外接收方清单》）：

（1）**境外模型节点 A** — 部署地：境外（美国）；处理目的：多模型聚合转发与容灾；处理方式：接收请求、调用底层模型、返回结果；

（2）**境外模型节点 B** — 部署地：境外（美国，经全球加速网络接入）；处理目的：境内主通道不可用时的降级推理，以及少数仅在境外上架的模型推理；处理方式：同上。

可控性与可审计性：平台对该等节点采取固定出网地址白名单、凭据加密存储与逐次调用元数据留痕，调用链路可审计、可追溯；平台要求境外接收方不得将客户数据再传输至其他司法辖区。

境外接收方的注册名称、注册地址与数据保护联系方式，以《境外接收方清单》书面版本为准（签署时或客户书面要求时提供；清单变更前 15 日更新）。

3.3 传输机制：平台依据《个人信息保护法》第三十八条与《个人信息出境标准合同办法》，与境外接收方订立个人信息出境标准合同，并向河北省互联网信息办公室备案；备案进度可应客户书面要求提供说明或证明文件。

3.4 客户的告知与同意义务：客户应向其终端用户告知境外接收方名称、联系方式、处理目的与方式、个人信息种类及行使权利的方式，并取得**单独同意**。平台通过《境外接收方清单》向客户提供上述信息，供客户在其隐私政策中引用；该清单不公开披露，客户不得将其用于本协议之外的目的或对外公开。

3.5 客户选择权：客户可书面要求仅使用境内渠道模型；平台在技术条件允许范围内配合并书面确认可用模型清单。因该限制导致的模型覆盖减少或可用性下降，不视为平台违约。

3.6 再传输限制：平台要求境外接收方不得将客户数据再传输至其他司法辖区，法律要求或为完成推理所必需的基础设施调度除外；后者应在《境外接收方清单》中披露。

附件四　政企及金融客户增强条款

适用说明：本附件仅在客户属于政府机关、事业单位、国有企业、金融机构或其供应商，且双方另行书面确认适用时生效。**本附件中的增强义务均为「另行协商」事项，未书面确认前对平台不产生约束力**——平台不作虚假承诺，以免签约后无法履行。

4.1 等保与认证：平台将网络安全等级保护定级备案纳入建设计划；具体定级、测评机构与完成时间以双方书面确认的整改计划为准。客户不得以本附件主张平台已取得等保备案或测评报告。

4.2 专有化部署：客户要求独立部署、专属实例、专属渠道或私有化网关的，另行签署部署与运维协议，费用与工期单独议定。

4.3 数据本地化：客户要求全部数据不出境的，按附件三第 3.5 项执行，平台提供境内渠道模型清单并书面确认。

4.4 驻场与应急：客户要求驻场支持、专属应急响应通道或缩短事件通报时限（如 24 小时）的，另行议定服务级别与费用。

4.5 审计升级：客户要求第三方审计或现场核查的，需经平台书面同意并签署保密协议，费用由客户承担；平台有权拒绝涉及其他客户数据或核心源代码的范围。

4.6 合同与发票：政企采购要求的合同模板、廉洁条款、保密协议、验收单与发票类型，按客户采购流程另行签署，与本协议冲突时以更严格者为准（仅就数据保护事项）。

双方签署

本协议一式两份，双方各执一份，具有同等法律效力。签署版内容与 www.starhubc.com/dpa 在线文本一致；在线文本更新时以更新后版本为准，平台提前 15 日公示。

甲方（客户）

公司 / 机构全称：_____

统一社会信用代码：_____

注册地址：_____

联系人：_____

联系电话 / 邮箱：_____

签署日期：_____

（盖章）_____

乙方（受托处理者）

公司全称：青硕秦皇岛文化传播有限公司

统一社会信用代码：_____

注册地址：_____

联系人：_____

联系电话 / 邮箱：kf@qsccl.com

签署日期：_____

（盖章）_____