



Leina

安全手册

把企业数据接入 AI 让访问范围清楚可控

账号由管理员连接，操作按授权执行。

让员工用上公司资料，也让企业管好数据的使用。

按需授权

明确谁能用
能读什么、能改什么

加密保护

云端敏感数据
采用信封加密

关键组件开源

连接与权限机制
可供开发者检查

TAC Security · CASA/ESOF

已通过安全评估

遵循 GDPR 个人数据保护要求。

评估与政策说明见第 5 页，可点击查看官方来源。

01 / 谁能用，能做什么

给员工完成工作所需的权限

接入一个应用后，团队仍然需要决定：哪些成员可以使用，允许哪些操作。

一次应用调用，要同时符合这些范围

01 原业务账号的权限

这个账号本来能访问哪些资料。

02 连接器开放的操作

接入方式实际支持哪些读取或修改动作。

03 团队设置的使用范围

哪些成员、权限组可以执行这些操作。

最终可执行的范围，是三者共同允许的部分。

配置示例：让运营查资料，先不开通修改

允许读取

查询页面 · 读取内容

不开放写入

创建 · 修改 · 删除

以支持 API 范围设置的连接为例：在连接权限中建立权限组，选择允许的读取操作，再加入对应成员。

还要核对具体账号能看到哪些资料。只读控制“能不能修改”；具体能读哪些文件、订单或记录，取决于原账号和接入方式。

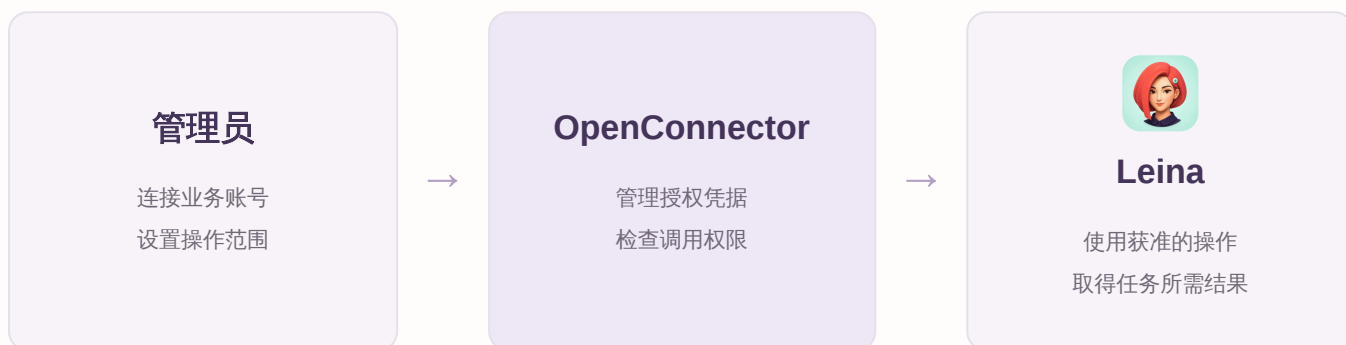
操作依据：[权限与数据访问文档](#)。不同应用支持的权限粒度可能不同。

02 / 账号与数据怎样保护

业务账号集中授权 员工不用互传密码

管理员连接账号；员工通过获准的操作使用资料，无需拿到账号密码或原始 Token。

连接与调用方式示意



账号凭据由连接运行时管理，AI 使用获准的操作与返回结果。

云端敏感数据：两层加密保护

第一层

把数据加密成密文

使用数据加密密钥保护敏感数据。

第二层

再保护这把密钥

使用另一层密钥加密数据密钥。

这就是“信封加密”：数据与数据密钥分别受到保护。

私有用户内容 不用于训练 AI 模型

这是当前隐私政策的承诺。执行任务时，所选模型或外部应用仍可能处理相关业务数据，具体按使用的服务和授权范围执行。

来源：[安全与合规](#) · [开源架构说明](#) · [隐私政策](#)

03 / 开源对企业有什么用

连接与权限如何工作 可以请技术人员直接检查

OpenConnector 是我们维护并向社区开放的应用连接基础设施。

开源连接网关

OpenConnector

负责连接业务应用，并检查工具调用权限。

Apache 2.0

开源许可证

可以检查

权限声明

要调用哪个应用
需要什么授权

可以检查

执行逻辑

请求怎样发出
凭据怎样处理

可以追踪

代码修复

改了哪些地方
如何验证改动

采购软件时，多一份可以核对的依据

技术负责人可以检查关键连接机制，也能据此评估现有业务系统如何接入、权限如何收紧，以及后续如何扩展。

其他已开放源码的组件

OpenFlow Apache 2.0

OO-CLI MIT

Connector SDK MIT

开源让关键机制更透明。具体服务的安全措施、部署方式和适用评估，仍需结合实际交付范围确认。

查看：[官方开源说明与源码入口](#) · [连接网关的工作方式](#)

04 / 评估与数据政策

核对安全依据 也看清资料如何处理

以下信息依据官方公开页面，核对日期为 2026 年 10 月 12 日。

安全评估

TAC Security

CASA / ESOF

官网披露：已通过安全评估。

[查看官方说明 →](#)

个人数据保护

GDPR

遵循相关要求

隐私政策说明处理方式与用户权利。

[查看隐私政策 →](#)

企业采购如需证书、报告或评估范围，可通过官网联系团队核对。这里的 GDPR 表述是合规承诺。

服务由谁提供？

公开隐私政策列明的数据控制者为 Oomol Studio Limited。

数据在哪里处理？

当前隐私政策披露服务器主要位于美国；使用模型或第三方应用时，也会涉及相应服务商的数据处理。

可以要求导出、更正或删除吗？

隐私政策列明相关权利和请求渠道。具体处理范围与保留期限，按适用政策和法律要求执行。

来源：[安全与合规](#)、[隐私政策](#)。评估和政策适用范围以链接中披露的产品及服务主体为准。



让权限跟着工作需要走

先接一个系统 从只读任务试起

01 选定资料与使用人员

例如运营需要查询订单与库存。管理员连接对应业务账号，核对原账号可访问的范围。

02 先开放必要的读取操作

为试用成员配置权限。需要修改或对外发送时，再按实际工作补充授权。

03 让结果说明数据来源

输入：“结合已授权的订单和库存，列出缺货风险。标明来源和时间，这次只做分析。”

leina.ai

访问官网，开始使用 →

有专门的数据存储或审计要求，可通过官网联系团队核对。