

数据保护与 IT 检查清单

适用于正在评估在 Merlin Project 中使用 AI 助手的个人信息保护负责人和 IT 部门。本清单概述 MCP 服务器的工作方式、哪些数据会离开您的组织，以及在共享项目之前需要明确的事项。

1 MCP 服务器概览

服务器在哪里运行？	作为 Merlin Project 的一部分，在用户的 Mac 上本地运行。云端没有 Merlin 服务器。
能否从网络访问？	不能。服务器没有网址，也不开放任何网络访问。只有在同一台 Mac 上运行的 AI 助手才能连接。
AI 能否修改或删除数据？	不能。服务器为只读模式，无法通过它修改、创建或删除数据。
哪些项目可见？	仅限用户通过“AI 工具”明确共享的项目。未共享时，AI 看不到任何项目。
能否撤销共享？	可以，随时可按项目逐一撤销。取消勾选后，项目会立即停止共享。
能否看出正在访问？	可以。共享启用时，“AI 工具”图标显示为实心；AI 助手连接期间，图标还会以蓝色突出显示。
哪些数据会离开 Mac？	AI 助手所执行查询的结果。原则上，已共享项目中的任何信息都可能包含在内。
数据会发送到哪里？	发送给所使用 AI 助手的提供商，例如使用 Claude 时发送给 Anthropic。适用该提供商的条款。

2 数据如何流动

用户就已共享的项目向 AI 助手提问。助手自行判断需要哪些数据，并向 MCP 服务器查询，通常分多次进行。Merlin Project 在本地处理每次查询，助手再把结果交给提供商的语言模型生成回答。在此过程中，也可能传输与最终回答无关的数据。因此，控制的关键在于项目共享，而不是单个字段。

3 AI 提供商与合同

以下各项与 Merlin Project 无关，而是针对您的组织所使用的 AI 助手。

☐ 提供商及套餐已获组织批准
个人套餐与企业套餐的条款往往差别很大。

☐ 已签订数据处理或委托处理协议
如涉及个人信息，需按适用的数据保护法律处理，例如《个人信息保护法》。

☐ 已核实数据存储地点及跨境传输
如数据传输至境外，请记录合法依据并完成所需程序。

☐ 已排除将数据用于模型训练
通过套餐或账户设置实现，并获得书面确认。

☐ 已了解对话记录的保存期限和删除方式

☐ 账户实行集中管理
例如通过管理控制台，以便随时撤销访问权限。

4 项目与使用规则

- ☐ 已明确哪些项目可以共享
- ☐ 已检查包含人员姓名的项目
资源或备注中的姓名属于个人信息。
- ☐ 已排除特别敏感的信息
如薪资、绩效评估或健康信息。可共享清理后的副本，或使用本地模型。
- ☐ 已检查客户机密信息
保密协议可能禁止向 AI 提供商传输数据。
- ☐ 员工了解相关规则
只共享需要的项目，使用后取消共享。
- ☐ 内部处理记录已更新
在内部台账等文件中记录个人信息处理情况。
- ☐ 已评估是否需要开展影响评估
视数据类型、规模及适用法律而定，例如个人信息保护影响评估。

5 IT 与运维

- ☐ 已安装包含 MCP 服务器的 Merlin Project 版本
- ☐ AI 助手在同一台 Mac 上本地运行
只有这样才能连接 MCP 服务器。
- ☐ 已考虑 AI 助手的出站连接
若不使用本地模型，防火墙和代理需允许连接提供商。
- ☐ 已为敏感项目评估本地语言模型
例如使用 LM Studio，项目数据不会离开 Mac。但本地模型的性能通常较弱。

6 检查结果

备注与待办事项：

检查人

日期

签名

更多信息：MCP 文档 (projectwizards.net/documentation/mcp)。本清单仅为技术参考，不构成法律意见。