

Checklist for Data Protection and IT

For data protection officers and IT departments evaluating the use of AI assistants with Merlin Project. This checklist summarizes how the MCP server works, which data leaves your organization and what to clarify before projects are shared.

1 The MCP server at a glance

Where does the server run?	Locally on the user's Mac, as part of Merlin Project. There is no Merlin server in the cloud.
Can it be reached from the network?	No. The server has no web address and opens no network access. Only an AI assistant running on the same Mac can connect to it.
Can the AI change or delete data?	No. The server is read-only. Data cannot be changed, created or deleted through it.
Which projects are visible?	Only projects the user has explicitly shared via "AI Tools". Without sharing, the AI sees no project at all.
Can sharing be revoked?	Yes, at any time and for each project individually. Once unchecked, the project is closed again immediately.
Is active access visible?	Yes. When sharing is active, the "AI Tools" icon appears filled. While an AI assistant is connected, it is also highlighted in blue.
What leaves the Mac?	The results of the queries the AI assistant makes. In principle, any information from a shared project can be included.
Where does the data go?	To the provider of the AI assistant in use, for example to Anthropic if you use Claude. The provider's terms apply.

2 How the data flows

The user asks the AI assistant a question about a shared project. The assistant decides which data it needs and queries the MCP server, often in several steps. Merlin Project answers each query locally. The assistant passes the results to the provider's language model, which generates the answer. Data that turns out to be irrelevant to the final answer may also be transferred. Control therefore lies in the sharing of projects, not in individual fields.

3 AI provider and contract

These points do not concern Merlin Project but the AI assistant your organization uses.

- ☐ The provider and plan are approved within the organization
Personal and business plans often differ significantly.
- ☐ A data processing agreement is in place
Required by many data protection laws when personal data is transferred, for example Art. 28 GDPR in the EU.
- ☐ Data location and international transfers have been reviewed
If data is transferred to another country, the legal basis is documented.
- ☐ Use of the data for model training is excluded
Through the plan or an account setting, confirmed in writing.
- ☐ Retention and deletion of chats are known

-
- ☐ Accounts are managed centrally
For example via an admin console, so that access can be revoked.

4 Projects and usage

- ☐ It is defined which projects may be shared
-
- ☐ Projects containing names of people have been reviewed
Names in resources or notes are personal data.
-
- ☐ Particularly sensitive information is excluded
Salaries, performance reviews or health information: share a cleaned-up copy or use a local model.
-
- ☐ Confidential client data has been reviewed
Non-disclosure agreements may prohibit sharing with an AI provider.
-
- ☐ Employees know the rules
Share only the projects needed and remove sharing after use.
-
- ☐ Internal documentation of processing activities is up to date
For example the record of processing activities under Art. 30 GDPR in the EU.
-
- ☐ The need for a privacy impact assessment has been reviewed
Depending on the type and scope of the data and on applicable law.

5 IT and operations

- ☐ Merlin Project is installed in a version that includes the MCP server
-
- ☐ The AI assistant runs locally on the same Mac
Only then can it connect to the MCP server.
-
- ☐ Outbound connections of the AI assistant are accounted for
Firewall and proxy must allow the connection to the provider unless a local model is used.
-
- ☐ A local language model has been evaluated for sensitive projects
For example with LM Studio. No project data then leaves the Mac. Local models are usually less capable.

6 Review result

Notes and open items:

Reviewed by

Date

Signature

More information: MCP documentation at projectwizards.net/documentation/mcp. This checklist is a technical guide and does not constitute legal advice.