

Lista de comprobación: protección de datos y TI

Para delegados de protección de datos y departamentos de TI que evalúan el uso de asistentes de IA con Merlin Project. Esta lista resume cómo funciona el servidor MCP, qué datos salen de su organización y qué debe aclararse antes de compartir proyectos.

1 El servidor MCP de un vistazo

¿Dónde se ejecuta el servidor?	En local, en el Mac del usuario, como parte de Merlin Project. No existe ningún servidor de Merlin en la nube.
¿Es accesible desde la red?	No. El servidor no tiene dirección web ni abre ningún acceso desde la red. Solo un asistente de IA que se ejecute en el mismo Mac puede conectarse a él.
¿Puede la IA modificar o eliminar datos?	No. El servidor es de solo lectura. A través de él no se pueden modificar, crear ni eliminar datos.
¿Qué proyectos son visibles?	Solo los proyectos que el usuario ha compartido expresamente mediante «Herramientas de IA». Sin esa autorización, la IA no ve ningún proyecto.
¿Se puede revocar la autorización?	Sí, en cualquier momento y para cada proyecto por separado. Al desmarcar la casilla, el proyecto queda cerrado de inmediato.
¿Se ve si hay un acceso activo?	Sí. Con la autorización activa, el icono «Herramientas de IA» aparece relleno. Mientras un asistente de IA está conectado, además se resalta en azul.
¿Qué sale del Mac?	Los resultados de las consultas que realiza el asistente de IA. En principio, puede incluir cualquier información de un proyecto compartido.
¿Adónde van los datos?	Al proveedor del asistente de IA utilizado, por ejemplo a Anthropic si utiliza Claude. Se aplican las condiciones de ese proveedor.

2 Cómo fluyen los datos

El usuario hace una pregunta al asistente de IA sobre un proyecto compartido. El asistente decide qué datos necesita y los consulta al servidor MCP, a menudo en varios pasos. Merlin Project responde cada consulta en local. El asistente envía los resultados al modelo de lenguaje del proveedor, que genera la respuesta. También pueden transmitirse datos que no influyen en la respuesta final. Por eso, el control está en la autorización de los proyectos, no en campos individuales.

3 Proveedor de IA y contrato

Estos puntos no afectan a Merlin Project, sino al asistente de IA que utiliza su organización.

- ☐ El proveedor y el plan están autorizados en la organización
Los planes personales y empresariales suelen diferir de forma notable.
- ☐ Existe un contrato de encargo del tratamiento
Lo exigen muchas leyes de protección de datos cuando se transfieren datos personales, por ejemplo el art. 28 del RGPD en la UE.
- ☐ Se han revisado la ubicación de los datos y las transferencias internacionales
Si los datos se transfieren a otro país, la base jurídica está documentada.

-
- ☐ Se excluye el uso de los datos para entrenar modelos
Mediante el plan o la configuración de la cuenta, confirmado por escrito.
 - ☐ Se conocen el plazo de conservación y la eliminación de los chats
 - ☐ Las cuentas se gestionan de forma centralizada
Por ejemplo, mediante una consola de administración, para poder retirar accesos.
-

4 Proyectos y uso

-
- ☐ Está definido qué proyectos pueden compartirse
 - ☐ Se han revisado los proyectos con nombres de personas
Los nombres en recursos o notas son datos personales.
 - ☐ Se excluye la información especialmente sensible
Salarios, evaluaciones o datos de salud: compartir una copia depurada o usar un modelo local.
 - ☐ Se han revisado los datos confidenciales de clientes
Los acuerdos de confidencialidad pueden prohibir la transmisión a un proveedor de IA.
 - ☐ Los empleados conocen las reglas
Compartir solo los proyectos necesarios y retirar la autorización después de usarlos.
 - ☐ La documentación interna de los tratamientos está actualizada
Por ejemplo, el registro de actividades de tratamiento según el art. 30 del RGPD en la UE.
 - ☐ Se ha valorado la necesidad de una evaluación de impacto
Según el tipo y el volumen de los datos y la legislación aplicable.
-

5 TI y operación

-
- ☐ Merlin Project está instalado en una versión con servidor MCP
 - ☐ El asistente de IA se ejecuta en local en el mismo Mac
Solo así puede conectarse al servidor MCP.
 - ☐ Se han tenido en cuenta las conexiones salientes del asistente de IA
El cortafuegos y el proxy deben permitir la conexión con el proveedor, salvo que se use un modelo local.
 - ☐ Se ha evaluado un modelo de lenguaje local para proyectos sensibles
Por ejemplo, con LM Studio. En ese caso, ningún dato del proyecto sale del Mac. Los modelos locales suelen ser menos potentes.
-

6 Resultado de la revisión

Notas y puntos pendientes:

Revisado por

Fecha

Firma

Más información: documentación MCP en projectwizards.net/documentation/mcp. Esta lista es una guía técnica y no constituye asesoramiento jurídico.