

Liste de contrôle : protection des données et informatique

Pour les délégués à la protection des données et les services informatiques qui évaluent l'utilisation d'assistants IA avec Merlin Project. Cette liste résume le fonctionnement du serveur MCP, les données qui quittent votre organisation et les points à clarifier avant de partager des projets.

1 Le serveur MCP en bref

Où le serveur fonctionne-t-il ?	En local sur le Mac de l'utilisateur, au sein de Merlin Project. Il n'existe aucun serveur Merlin dans le cloud.
Est-il accessible depuis le réseau ?	Non. Le serveur n'a pas d'adresse web et n'ouvre aucun accès réseau. Seul un assistant IA exécuté sur le même Mac peut s'y connecter.
L'IA peut-elle modifier ou supprimer des données ?	Non. Le serveur fonctionne en lecture seule. Il ne permet ni de modifier, ni de créer, ni de supprimer des données.
Quels projets sont visibles ?	Uniquement les projets que l'utilisateur a explicitement partagés via « Outils IA ». Sans partage, l'IA ne voit aucun projet.
Le partage peut-il être révoqué ?	Oui, à tout moment et pour chaque projet individuellement. Dès que la case est décochée, le projet est de nouveau fermé.
Un accès actif est-il visible ?	Oui. Lorsque le partage est actif, l'icône « Outils IA » apparaît pleine. Lorsqu'un assistant IA est connecté, elle est en outre surlignée en bleu.
Qu'est-ce qui quitte le Mac ?	Les résultats des requêtes effectuées par l'assistant IA. En principe, toute information d'un projet partagé peut en faire partie.
Où vont les données ?	Chez le fournisseur de l'assistant IA utilisé, par exemple Anthropic si vous utilisez Claude. Les conditions de ce fournisseur s'appliquent.

2 Comment circulent les données

L'utilisateur pose une question à l'assistant IA sur un projet partagé. L'assistant décide lui-même des données dont il a besoin et interroge le serveur MCP, souvent en plusieurs étapes. Merlin Project traite chaque requête en local. L'assistant transmet ensuite les résultats au modèle de langage du fournisseur, qui génère la réponse. Des données sans rapport avec la réponse finale peuvent aussi être transmises. Le contrôle repose donc sur le partage des projets, et non sur des champs individuels.

3 Fournisseur d'IA et contrat

Ces points ne concernent pas Merlin Project, mais l'assistant IA utilisé par votre organisation.

- ☐ Le fournisseur et l'offre sont autorisés dans l'organisation
Les offres pour particuliers et pour entreprises diffèrent souvent nettement.
- ☐ Un contrat de sous-traitance est en place
Exigé par de nombreuses lois sur la protection des données en cas de transfert de données personnelles, par exemple l'art. 28 du RGPD dans l'UE.
- ☐ Le lieu de stockage et les transferts internationaux ont été vérifiés
En cas de transfert vers un autre pays, la base juridique est documentée.

☐ L'utilisation des données pour l'entraînement des modèles est exclue
Via l'offre ou les paramètres du compte, confirmée par écrit.

☐ La durée de conservation et la suppression des conversations sont connues

☐ Les comptes sont gérés de manière centralisée
Par exemple via une console d'administration, afin de pouvoir retirer les accès.

4 Projets et utilisation

☐ Les projets pouvant être partagés sont définis

☐ Les projets contenant des noms de personnes ont été vérifiés
Les noms figurant dans les ressources ou les notes sont des données personnelles.

☐ Les informations particulièrement sensibles sont exclues
Salaires, évaluations ou données de santé : partager une copie nettoyée ou utiliser un modèle local.

☐ Les données confidentielles des clients ont été vérifiées
Les accords de confidentialité peuvent interdire la transmission à un fournisseur d'IA.

☐ Les collaborateurs connaissent les règles
Ne partager que les projets nécessaires et retirer le partage après utilisation.

☐ La documentation interne des traitements est à jour
Par exemple le registre des activités de traitement selon l'art. 30 du RGPD dans l'UE.

☐ La nécessité d'une analyse d'impact a été examinée
Selon la nature et le volume des données et la législation applicable.

5 Informatique et exploitation

☐ Merlin Project est installé dans une version incluant le serveur MCP

☐ L'assistant IA fonctionne en local sur le même Mac
C'est la condition pour qu'il puisse se connecter au serveur MCP.

☐ Les connexions sortantes de l'assistant IA sont prises en compte
Le pare-feu et le proxy doivent autoriser la connexion au fournisseur, sauf si un modèle local est utilisé.

☐ Un modèle de langage local a été évalué pour les projets sensibles
Par exemple avec LM Studio. Aucune donnée de projet ne quitte alors le Mac. Les modèles locaux sont généralement moins performants.

6 Résultat de la vérification

Notes et points en suspens :

Vérifié par

Date

Signature

Plus d'informations : [documentation MCP sur projectwizards.net/documentation/mcp](https://projectwizards.net/documentation/mcp). Cette liste de contrôle est un guide technique et ne constitue pas un conseil juridique.