

Claude dans Microsoft 365 Copilot : défense et secret industriel, ce que vous exposez

Où passent les données quand le modèle Claude répond dans Copilot, ce que cela déclenche pour une entreprise sensible, et comment garder la main. Lecture courte et factuelle, sans dramatisation.

Date de vérification : 23 juillet 2026 Registre : DSI, RSSI, direction générale

Portée : générique, défense et secret industriel

SOMMAIRE

- | | |
|--|--|
| 01 L'essentiel | 05 Défense et secret industriel : la ligne rouge |
| 02 La réponse directe | 06 Matrice d'exposition |
| 03 Les trois portes d'entrée de Claude | 07 Garder la main et recommandations |
| 04 Ce que deviennent vos données | 08 Sources |

■ 01

L'essentiel

Microsoft 365 Copilot repose sur plusieurs modèles. Tant que Copilot s'appuie sur un modèle opéré par Microsoft, le traitement reste dans la frontière européenne des données. Dès que le modèle Claude d'Anthropic entre en jeu, il sort de cette frontière et s'effectue le plus souvent aux États-Unis.

Pour une entreprise du secteur défense ou détentrice de secrets industriels, la conséquence est nette. Le socle Copilot, sans Claude, reste maîtrisé et conforme. Mais certaines données, information classifiée, Diffusion Restreinte, donnée technique sous contrôle export, savoir-faire critique, ne doivent pas être soumises à un assistant qui les traite en clair hors du périmètre souverain. Ce n'est pas un risque résiduel, c'est une incompatibilité à traiter en amont. La bonne nouvelle, c'est que la maîtrise tient à quelques réglages, tous entre les mains de l'administrateur.

■ 02

La réponse directe : oui, sous conditions

Des données passent-elles par les États-Unis ? Oui, mais seulement quand le modèle qui répond est un Claude.

Le socle Microsoft 365 Copilot est couvert par l'EU Data Boundary pour un client de l'Union. Vos courriels, fichiers et l'historique de vos échanges avec Copilot restent stockés en Europe, chiffrés, non utilisés pour l'entraînement. Quand l'utilisateur ou un agent choisit Claude, la requête, le contexte tiré de vos documents et la réponse sont traités par Anthropic, hors de cette frontière. Anthropic héberge Claude sur sa propre infrastructure, sur Amazon Web Services et Google Cloud, et son centre de confidentialité indique stocker ses données aux États-Unis. Le transit et le stockage outre-Atlantique sont donc la conséquence normale du choix de Claude, pas une hypothèse.

LE POINT QUI TRANCHE

Le clivage n'est pas Copilot contre pas Copilot. Il est modèle Microsoft contre modèle Anthropic. Le premier reste en Europe, le second sort aux États-Unis. Toute la gouvernance consiste à décider qui a le droit d'ouvrir la seconde porte, et pour quels contenus.

■ 03

Les trois portes d'entrée de Claude

Claude s'active par trois voies, qui répondent à des besoins différents et partagent la même conséquence sur la localisation des données.

PORTE 1

Le mode Chat

Dans Copilot Chat, l'utilisateur choisit Claude via le sélecteur de modèle. Le choix de modèle exige une licence Microsoft 365 Copilot.

PORTE 2

Sous licence spécifique

Le sélecteur de modèle et l'agent Researcher supposent la licence payante. Les agents sont facturés à l'usage en Copilot Credits.

PORTE 3

Copilot Studio

Le concepteur choisit Claude comme modèle primaire à la création, après une double autorisation de l'administrateur.

Claude motorise aussi l'agent Researcher, Copilot dans Word, Excel et PowerPoint, et les agents. Peu importe la porte : dès que le modèle retenu est un Claude, la donnée sort d'Europe. Point rassurant pour un locataire français, ces modèles sont désactivés par défaut ; leur emploi suppose une activation délibérée d'un administrateur.

■ 04

Ce que deviennent vos données

Deux régimes cohabitent, et tout se joue sur l'étiquette du modèle.

En régime standard, depuis janvier 2026, Anthropic est intégré comme sous-traitant de Microsoft : les conditions contractuelles de Microsoft s'appliquent, sans entraînement sur vos données, mais l'inférence reste hors de la frontière européenne. En régime à rétention, qui concerne des modèles de prévisualisation avancés, Anthropic sort du cadre Microsoft et opère sous ses propres conditions : il conserve alors la plupart des entrées et sorties jusqu'à 30 jours, jusqu'à 2 ans pour un contenu signalé par ses classificateurs de sécurité, et les scores de classification jusqu'à 7 ans. Ces modèles sont désactivés par défaut partout.

DEUX RÉFLEXES DE GOUVERNANCE

D'abord, laisser fermés les modèles à rétention, ce qui est leur état par défaut. Ensuite, garder à l'esprit que même sur le chemin standard, sans rétention de ce type ni entraînement, le traitement s'effectue toujours hors d'Europe.

Défense et secret industriel : la ligne rouge

Pour la plupart des données, l'exposition se gère avec des clauses et une analyse de transfert. Pour la défense et les secrets industriels, elle devient une ligne à ne pas franchir, parce que le simple fait de faire lire ces contenus par un modèle hors périmètre pose problème.

Le volet défense

L'information classifiée relève de l'instruction générale interministérielle n° 1300, avec ses deux niveaux Secret et Très Secret, et n'a jamais sa place dans un service commercial comme Copilot. La Diffusion Restreinte, mention de protection des informations sensibles non classifiées, est encadrée par l'instruction interministérielle n° 901, qui impose un chiffrement par des moyens agréés par l'ANSSI et un hébergement maîtrisé ; l'ANSSI ne préconise pas le cloud commercial pour ces données, la menace visée étant d'origine étatique. La qualification SecNumCloud a précisément pour objet de résister à une injonction extraterritoriale d'un État hors Union, la garantie même qui fait défaut sur le chemin Claude. Enfin, le contrôle export américain, ITAR et EAR, interdit de communiquer une donnée technique contrôlée à une personne non américaine ou de la faire sortir du territoire sans autorisation ; l'exemption de chiffrement ne s'applique pas, car un assistant lit forcément la donnée en clair pour produire sa réponse.

Le volet secret industriel

La protection d'un secret d'affaires, au sens de la directive européenne de 2016, n'est acquise que si son détenteur a pris des dispositions raisonnables de protection. La sécurisation effective, contrôle d'accès, chiffrement, traçabilité, n'est donc pas qu'une bonne pratique, c'est une condition juridique de la protection. Envoyer un savoir-faire critique, un plan ou un procédé vers un modèle hébergé hors d'Europe et hors de votre maîtrise fragilise cette protection au moment même où l'exposition à l'espionnage industriel est réelle.

La règle dirigeante tient en une ligne : classer la donnée d'abord, et ne jamais soumettre à Copilot commercial une information classifiée, à Diffusion Restreinte, sous contrôle export ou constituant un secret industriel critique, quel que soit le modèle.

Matrice d'exposition

Une lecture rapide, par type de donnée. À gauche, le socle Microsoft, qui reste en Europe. À droite, le chemin Claude, hors d'Europe. Le régime à rétention aggrave encore la colonne de droite.

TYPE DE DONNÉE	MODÈLE MICROSOFT (EN EUROPE)	MODÈLE CLAUDE (HORS EUROPE, ÉTATS-UNIS)
Courante, non sensible	☐ Faible	☐ Faible
Entreprise sensible : RH, commercial, données personnelles	☐ Faible	☒ Modéré
Secret industriel, savoir-faire critique	☒ Modéré	☒ Élevé
Défense : classifiée, Diffusion Restreinte, ou sous contrôle export	☒ À proscrire	☒ À proscrire

☐ Faible ☒ Modéré ☒ Élevé ☒ À proscrire

COMMENT LIRE LA MENTION À PROSCRIRE

Elle traduit une incompatibilité réglementaire ou une non-conformité d'environnement, pas un pronostic d'incident. Pour la défense et les données contrôlées, la règle de base est de ne pas soumettre ces contenus à Copilot commercial, quel que soit le modèle. Sur les modèles Microsoft, la donnée reste en Europe mais l'environnement n'est pas homologué pour ces contenus ; sur le chemin Claude, s'ajoute la sortie hors d'Europe.

■ 07

Garder la main et recommandations

La maîtrise tient à quelques leviers, tous entre les mains de l'administrateur, et à une règle de discipline qui prime sur tout l'outillage.

Anthropic se désactive depuis le Microsoft 365 admin center, avec une portée réglable par groupes, et le verrou se répercute sur Copilot Studio et le Power Platform. Désactiver Anthropic ne prive pas de Copilot : les fonctions concernées basculent sur un modèle opéré par Microsoft, qui reste en Europe. En amont, les étiquettes de sensibilité et les politiques de protection empêchent le traitement des contenus sensibles, étant entendu qu'elles agissent sur le contenu et non sur le choix du modèle. Le levier le plus efficace n'est pas technique, il est de discipline : classer la donnée, et prévenir le recours non maîtrisé aux IA grand public.

01 Laisser Anthropic désactivé par défaut.

Son état natif en France. L'activer seulement par périmètre restreint et sur besoin métier mesuré, et ne jamais activer les modèles à rétention.

02 Poser une interdiction ferme sur les données sensibles.

Aucune donnée classifiée, à Diffusion Restreinte, sous contrôle export ou constituant un secret industriel critique dans Copilot commercial, quel que soit le modèle.

03 Router les usages par sensibilité.

Diriger les usages sensibles vers les modèles Microsoft, qui restent en Europe, et réserver Claude aux contenus non sensibles.

04 Outiller la règle.

Étiquettes de sensibilité et prévention des pertes de données, prévention du recours non maîtrisé aux IA grand public au poste de travail.

05 Documenter et garder l'humain aux commandes.

Une analyse d'impact du transfert avant tout usage d'Anthropic sur des données personnelles. Cette note éclaire l'exposition, elle ne vaut pas conseil juridique.

■ 08

Sources

Sources primaires et datées. Vérification au 23 juillet 2026.

MICROSOFT ET ANTHROPIC

- 1 Anthropic models in Microsoft Online Services. learn.microsoft.com/microsoft-365/copilot/connect-to-ai-subprocessor
- 2 Data, Privacy, and Security for Microsoft 365 Copilot. learn.microsoft.com, confidentialité Copilot
- 3 Enterprise data protection in Microsoft 365 Copilot. learn.microsoft.com, enterprise data protection
- 4 Learn about DLP to protect interactions with Microsoft 365 Copilot. learn.microsoft.com, DLP Copilot

5 Anthropic, localisation des serveurs et stockage aux États-Unis. privacy.claude.com, serveurs

6 Anthropic, rétention des modèles Mythos-class. support.claude.com, rétention

RGPD ET DROIT AMÉRICAIN

1 EU-US data transfers, décision d'adéquation (Commission européenne). commission.europa.eu

2 Adéquation des États-Unis, questions-réponses (CNIL). cnil.fr

3 Recommandations 01/2020 sur les mesures supplémentaires (CEPD). edpb.europa.eu

4 Unpacking the CLOUD Act (eucrim). eucrim.eu

DÉFENSE ET SECRET INDUSTRIEL

1 Instruction générale interministérielle n° 1300 (ANSSI). cyber.gouv.fr, IGI 1300

2 Instruction interministérielle n° 901, Diffusion Restreinte (ANSSI). cyber.gouv.fr, II 901

3 Qualification SecNumCloud (ANSSI). cyber.gouv.fr, SecNumCloud

4 Directive (UE) 2016/943 sur la protection des secrets d'affaires (EUR-Lex). eur-lex.europa.eu, directive 2016/943

5 ITAR, activités qui ne sont pas des exports, chiffrement de bout en bout, 22 CFR 120.54 (eCFR). ecfr.gov, 22 CFR 120.54



Veille Cyber AI. Étude à usage interne, registre dirigeant. Elle éclaire une exposition et ne vaut pas conseil juridique. L'activation, la publication ou tout partage restent une décision humaine.

Vérifié le 23 juillet 2026
Version générique
Défense et secret industriel