Les données des salariés peuvent-elles être hébergées hors de l'UE par un fournisseur d'IA ?

Réponse courte

Les données des salariés peuvent être hébergées hors de l'UE par un fournisseur d'IA, mais uniquement si des **garanties adéquates** sont en place conformément au RGPD (articles 44-49). Le transfert est autorisé vers les pays bénéficiant d'une **décision d'adéquation** de la Commission européenne. Pour les autres pays, l'employeur doit recourir à des **clauses contractuelles types** (CCT) ou des règles d'entreprise contraignantes (BCR).

Pour les fournisseurs américains d'IA (OpenAI, Google, Microsoft), le transfert est possible si le fournisseur est certifié sous le **EU-US Data Privacy Framework**. L'employeur reste **responsable** de la conformité du transfert et doit réaliser un Transfer Impact Assessment (TIA). En cas de non-conformité, les sanctions AI Act et RGPD peuvent atteindre **20 millions d'euros** ou 4 % du chiffre d'affaires mondial.

Définition

L'**hébergement hors UE** des données des salariés désigne toute situation dans laquelle les données personnelles des salariés sont stockées, traitées ou accessibles depuis des serveurs situés en dehors de l'Union européenne et de l'Espace économique européen. Cette situation est fréquente avec les fournisseurs d'IA cloud dont les infrastructures sont réparties mondialement.

Le RGPD considère tout accès distant aux données depuis un pays tiers comme un **transfert international**, même si les données sont physiquement stockées dans l'UE. L'employeur, en tant que responsable du traitement au regard des obligations RGPD, doit garantir un **niveau de protection essentiellement équivalent** à celui de l'UE.

Questions fréquentes

Comment vérifier la certification EU-US Data Privacy Framework d'un fournisseur ?

En consultant le registre officiel du Department of Commerce des États-Unis. La certification doit être vérifiée avant tout transfert et documentée. Une réévaluation périodique est nécessaire car la certification peut être retirée. Le DPA doit refléter cette certification.

Faut-il des mesures techniques complémentaires pour les transferts hors UE ?

Oui, fortement recommandé. Le chiffrement de bout en bout, la pseudonymisation avant transfert et le contrôle des accès depuis des pays tiers renforcent la protection. Ces mesures sont particulièrement importantes face aux risques d'accès gouvernemental dans le pays de destination.

L'accès distant aux données depuis un pays tiers constitue-t-il un transfert ?

Oui. Le RGPD considère tout accès distant aux données depuis un pays tiers comme un transfert international, même si les données sont physiquement stockées dans l'UE. Cette interprétation large impose une vigilance sur les sous-traitants ultérieurs et les administrateurs distants.

Le DPA suffit-il à transférer la responsabilité au fournisseur d'IA ?

Non. L'employeur reste responsable du traitement même en cas de sous-traitance. Le DPA encadre la relation mais ne transfère pas la responsabilité. L'obligation de diligence et de contrôle persiste, avec un risque de sanctions CNPD jusqu'à 20 millions d'euros ou 4 % du CA mondial.

Les données des salariés peuvent-elles être hébergées hors de l'UE par un fournisseur d'IA ?

Oui, mais sous conditions strictes. Les transferts sont autorisés vers les pays bénéficiant d'une décision d'adéquation. Pour les autres pays, l'employeur doit recourir à des clauses contractuelles types ou des règles d'entreprise contraignantes. Pour les USA, vérifier la certification EU-US Data Privacy Framework.

Quelles alternatives en cas d'invalidation du EU-US Data Privacy Framework ?

Anticiper en identifiant des alternatives européennes pour chaque outil d'IA critique (Mistral, Aleph Alpha, options européennes des grands cloud). Mettre en place les CCT comme mécanisme de secours. Prévoir un plan de migration en cas d'invalidation pour assurer la continuité.

Conditions d’exercice

Le transfert de données des salariés vers un fournisseur d'IA hors UE est soumis à des mécanismes de protection hiérarchisés.

Critère	Détail
Décision d'adéquation	Transfert libre vers les pays reconnus par la Commission : Japon, Corée du Sud, Royaume-Uni, Canada (secteur commercial), Suisse, Nouvelle-Zélande, Israël, entre autres
EU-US Data Privacy Framework	Transfert vers les USA autorisé si le fournisseur est certifié ; vérification obligatoire sur le site du Department of Commerce ; réévaluation périodique
Clauses contractuelles types	Mécanisme subsidiaire pour les pays sans décision d'adéquation ; CCT adoptées par la Commission (2021) ; complétées par des mesures supplémentaires si nécessaire
Transfer Impact Assessment	Évaluation obligatoire du niveau de protection dans le pays de destination ; analyse de la législation locale (accès gouvernemental aux données) ; mesures techniques complémentaires
Responsabilité	L'employeur reste responsable même en cas de sous-traitance ; le DPA avec le fournisseur ne transfère pas la responsabilité ; obligation de diligence et de contrôle
Données sensibles	Vigilance renforcée pour les données de santé, biométriques ou syndicales ; AIPD recommandée pour tout transfert de données sensibles hors UE

Modalités pratiques

La mise en conformité des transferts vers un fournisseur d'IA hors UE suit un processus en plusieurs étapes.

Étape	Détail
Identification des transferts	Cartographier tous les flux de données vers les fournisseurs d'IA ; identifier la localisation effective des serveurs (stockage ET traitement) ; vérifier les sous-traitants ultérieurs
Choix du mécanisme	Vérifier l'existence d'une décision d'adéquation ; pour les USA : vérifier la certification DPF du fournisseur ; à défaut : mettre en place les CCT
Transfer Impact Assessment	Évaluer le cadre juridique du pays de destination ; identifier les risques d'accès gouvernemental ; documenter les mesures techniques complémentaires (chiffrement, pseudonymisation)
Contractualisation	Conclure un DPA conforme à l'article 28 RGPD ; intégrer les CCT si applicables ; prévoir des clauses d'audit, de localisation et de notification en cas de demande gouvernementale
Suivi et réévaluation	Surveiller le maintien de la certification DPF ; suivre les évolutions jurisprudentielles (CJUE) ; réévaluer le TIA en cas de changement législatif dans le pays de destination

Pratiques et recommandations

Vérifier la certification EU-US Data Privacy Framework de chaque fournisseur d'IA américain avant tout transfert, en consultant le registre officiel du Department of Commerce et en documentant la vérification.

Exiger contractuellement que le fournisseur n'utilise pas les données des salariés pour entraîner ses modèles d'IA, en incluant une clause d'interdiction explicite dans le DPA.

Privilégier les options d'hébergement européen proposées par certains fournisseurs d'IA cloud (Azure EU Data Boundary, AWS Europe, Google Cloud EU), en vérifiant que le traitement effectif reste dans l'UE.

Mettre en place des mesures techniques complémentaires (chiffrement de bout en bout, pseudonymisation avant transfert) pour renforcer la protection en cas de transfert vers un pays tiers.

Anticiper les risques d'invalidation des mécanismes de transfert en identifiant des alternatives européennes pour les outils d'IA critiques et en prévoyant un plan de migration.

Cadre juridique

Référence	Objet
RGPD - Articles 44-49	Encadrement des transferts de données vers des pays tiers
RGPD - Article 45	Transferts fondés sur une décision d'adéquation
RGPD - Article 46	Garanties appropriées (CCT, BCR)
RGPD - Article 28	Obligations du sous-traitant et contenu du DPA
Décision d'exécution (UE) 2023/1795	EU-US Data Privacy Framework
CJUE, Schrems II (C-311/18)	Obligation de vérification au cas par cas ; TIA requis
Art. L.261-1	Encadrement du traitement des données personnelles des salariés

L'hébergement hors UE des données des salariés par un fournisseur d'IA n'est pas interdit mais strictement encadré. L'employeur doit exercer une diligence raisonnable dans le choix et le contrôle de ses fournisseurs. La jurisprudence Schrems II a renforcé les obligations de vérification et tout mécanisme de transfert peut être remis en cause par la CJUE, ce qui impose une veille juridique constante.