Quels sont les critères de souveraineté des données pour le choix d'un outil d'IA en entreprise ?

Réponse courte

Le choix d'un outil d'IA en entreprise au Luxembourg doit intégrer des critères stricts de **souveraineté des données** pour garantir la conformité aux obligations RGPD et protéger les informations sensibles. Les données personnelles des salariés doivent être traitées et stockées dans l'**Espace économique européen** (EEE), sauf garanties adéquates pour les transferts hors EEE (articles 44-49 RGPD).

L'employeur doit vérifier la **localisation des serveurs**, l'identité juridique du fournisseur, les conditions de sous-traitance et les garanties contractuelles de protection des données. L'annulation du Privacy Shield et les incertitudes sur le Data Privacy Framework UE-USA renforcent l'importance de privilégier des solutions **hébergées en Europe**. La CNPD recommande une vigilance particulière sur les transferts internationaux de données et la capacité de l'employeur à exercer un contrôle effectif sur ses données.

Définition

La **souveraineté des données** désigne la capacité d'une organisation à maîtriser le cycle de vie complet de ses données : localisation du stockage, conditions de traitement, droits d'accès, portabilité et suppression. En matière d'IA, cette notion est critique car les outils d'IA traitent souvent des volumes importants de données personnelles des salariés.

Au Luxembourg, la souveraineté des données s'inscrit dans le cadre de la réglementation IA et du RGPD (règles strictes sur les **transferts internationaux**) et de la stratégie nationale de cybersécurité. Le pays dispose d'infrastructures de data centers de premier plan en Europe, ce qui facilite le choix de solutions hébergées localement.

Questions fréquentes

Faut-il chiffrer les données traitées par un outil d'IA ?

Oui, le chiffrement des données en transit et au repos est une mesure de sécurité essentielle (article 32 RGPD). La gestion des clés de chiffrement par l'entreprise ou un tiers de confiance européen renforce la souveraineté des données.

Faut-il prévoir un droit d'audit du fournisseur IA ?

Oui, il est recommandé de négocier contractuellement un droit d'audit permettant de vérifier régulièrement les pratiques du fournisseur en matière de protection des données. C'est une exigence contractuelle issue de l'article 28 RGPD sur la sous-traitance.

Le Luxembourg dispose-t-il de data centers conformes RGPD ?

Oui, le Luxembourg dispose d'infrastructures de data centers de premier plan en Europe, ce qui facilite le choix de solutions hébergées localement et conformes au RGPD. La loi du 1er août 2018 encadre nationalement la protection des données.

Peut-on utiliser un outil d'IA hébergé hors de l'UE ?

Les transferts hors EEE sont interdits sauf décision d'adéquation, clauses contractuelles types ou binding corporate rules (articles 44-49 RGPD). Au vu des incertitudes sur le Data Privacy Framework UE-USA, l'hébergement européen est fortement recommandé.

Qu'est-ce qu'une solution d'IA on-premise ?

Une solution on-premise est hébergée sur les serveurs de l'entreprise plutôt que dans le cloud. Elle est recommandée pour les traitements les plus sensibles (données de santé, données financières) car elle maximise le contrôle sur les données.

Quels critères de souveraineté des données pour le choix d'un outil d'IA ?

Les critères incluent la localisation du stockage et du traitement (privilégier l'EEE), l'identité juridique du fournisseur, les garanties contractuelles, le chiffrement, la portabilité et le droit d'audit. Les transferts hors EEE sont strictement encadrés (articles 44-49 RGPD).

Conditions d’exercice

Le choix d'un outil d'IA conforme aux exigences de souveraineté des données repose sur des critères cumulatifs.

Critère	Détail
Localisation du stockage	Données stockées dans l'EEE ; privilégier le Luxembourg ou l'UE ; éviter les pays tiers sans décision d'adéquation
Localisation du traitement	Vérifier que le traitement algorithmique s'effectue également dans l'EEE, pas uniquement le stockage
Identité du fournisseur	Société de droit européen ou disposant d'un établissement dans l'EEE soumis au RGPD
Sous-traitance	Identification de tous les sous-traitants, localisation, garanties contractuelles (article 28 RGPD)
Transferts internationaux	Si transfert hors EEE : clauses contractuelles types (CCT), décision d'adéquation ou binding corporate rules (articles 44-49 RGPD)
Chiffrement	Chiffrement des données en transit et au repos ; gestion des clés de chiffrement par l'entreprise ou un tiers de confiance européen
Portabilité et réversibilité	Capacité d'extraire les données dans un format standard et de migrer vers un autre fournisseur
Droit d'audit	Droit contractuel de l'employeur d'auditer les pratiques du fournisseur en matière de protection des données

Modalités pratiques

L'évaluation de la souveraineté des données d'un outil d'IA suit un processus de due diligence structuré.

Étape	Détail
Grille d'évaluation	Préparer une grille de critères pondérés couvrant localisation, juridiction, sous-traitance, chiffrement, portabilité
Questionnaire fournisseur	Soumettre un questionnaire détaillé sur l'architecture technique, la localisation des données et les mesures de sécurité
Analyse juridique	Vérifier la compatibilité avec le RGPD, identifier les risques de transfert hors EEE, évaluer les garanties proposées
AIPD	Réaliser une analyse d'impact si le traitement présente un risque élevé pour les droits des personnes (article 35 RGPD)
Clauses contractuelles	Négocier des clauses spécifiques : localisation garantie, notification en cas de changement, droit d'audit, pénalités en cas de non-conformité
Revue périodique	Réévaluation annuelle de la conformité du fournisseur, notamment en cas de changement de localisation ou de sous-traitant

Pratiques et recommandations

Privilégier les solutions d'IA hébergées au Luxembourg ou dans l'UE pour minimiser les risques juridiques liés aux transferts internationaux de données.

Exiger contractuellement que le fournisseur notifie tout changement de localisation des données ou de sous-traitant avec un préavis suffisant pour permettre une évaluation.

Vérifier que les données utilisées pour l'entraînement des modèles d'IA ne sont pas transférées vers des juridictions non conformes, même de manière temporaire.

Envisager des solutions d'IA on-premise (hébergées sur les serveurs de l'entreprise) pour les traitements les plus sensibles, notamment ceux impliquant des données de santé ou des données financières.

Consulter la CNPD en cas de doute sur la conformité d'un transfert international de données et documenter les analyses de risque réalisées.

Cadre juridique

Référence	Objet
RGPD - Articles 44-49	Conditions de transfert de données personnelles vers des pays tiers
RGPD - Article 28	Obligations du sous-traitant, clauses contractuelles
RGPD - Article 35	Analyse d'impact relative à la protection des données
RGPD - Article 32	Mesures de sécurité techniques et organisationnelles
AI Act (UE 2024/1689)	Exigences de documentation et de traçabilité des systèmes d'IA
CNPD	Autorité de contrôle, recommandations sur les transferts internationaux
Loi du 1er août 2018	Loi nationale d'application du RGPD au Luxembourg

La souveraineté des données est un critère décisif pour le choix d'un outil d'IA, particulièrement au Luxembourg où les secteurs bancaire et financier imposent des exigences renforcées de localisation des données. Les entreprises doivent maintenir une vigilance continue face aux évolutions jurisprudentielles sur les transferts internationaux de données.