Quelles sont les obligations de souveraineté des données pour les outils d'IA en entreprise ?

Réponse courte

La souveraineté des données pour les outils d'IA en entreprise au Luxembourg repose principalement sur le RGPD qui encadre strictement les **transferts de données hors UE/EEE**. L'employeur doit s'assurer que les données traitées par les systèmes d'IA sont hébergées dans l'UE ou, en cas de transfert vers un pays tiers, que des **garanties adéquates** sont en place (décision d'adéquation, clauses contractuelles types, règles d'entreprise contraignantes).

L'AI Act ajoute des exigences de **documentation et de traçabilité** qui impliquent que l'employeur connaisse précisément la localisation des serveurs de traitement. Au Luxembourg, la CNPD contrôle le respect de ces obligations. Les données des salariés traitées par des fournisseurs d'IA cloud nécessitent une attention particulière car les traitements peuvent impliquer des **transferts internationaux non apparents**.

Définition

La **souveraineté des données** désigne le principe selon lequel les données à caractère personnel sont soumises aux lois et à la juridiction du pays où elles sont collectées ou traitées. Pour les données des salariés au Luxembourg, le cadre applicable est le RGPD (voir les obligations RGPD), complété par la loi du 1er août 2018 et contrôlé par la CNPD.

Dans le contexte de l'IA en entreprise, la souveraineté des données pose des questions spécifiques liées au **cloud computing**, à l'entraînement des modèles d'IA sur des serveurs étrangers et au traitement des données par des fournisseurs établis hors de l'UE. L'employeur, en tant que **responsable du traitement**, est garant de la conformité.

Conditions d'exercice

Les obligations de souveraineté des données pour les outils d'IA couvrent plusieurs aspects réglementaires.

Critère	Détail
RGPD - Transferts	Transferts intra-UE/EEE : libres ; transferts vers pays avec décision d'adéquation : autorisés (ex. : Japon, Corée du Sud, Royaume-Uni) ; autres pays : garanties appropriées requises
Garanties appropriées	Clauses contractuelles types (CCT) de la Commission européenne ; règles d'entreprise contraignantes (BCR) ; codes de conduite approuvés ; certifications RGPD
USA - Data Privacy Framework	Le cadre UE-US Data Privacy Framework permet les transferts vers les entreprises américaines certifiées ; vérifier la certification du fournisseur d'IA
AI Act - Localisation	Documentation technique précisant la localisation des serveurs ; traçabilité des données d'entraînement et de traitement ; accessibilité des logs pour les autorités européennes
Responsabilité	L'employeur (responsable du traitement) est responsable de la conformité des transferts ; la sous-traitance à un fournisseur d'IA ne transfère pas la responsabilité
Secteurs sensibles	Secteur financier : exigences CSSF supplémentaires ; secteur de la santé : localisation UE recommandée ; secteur public : hébergement national parfois requis

Modalités pratiques

La mise en conformité des outils d'IA avec les obligations de souveraineté des données suit un processus structuré.

Étape	Détail
Cartographie des flux	Identifier tous les flux de données vers les fournisseurs d'IA ; localiser les serveurs de traitement et de stockage ; identifier les sous-traitants ultérieurs
Évaluation des transferts	Pour chaque transfert hors UE : identifier le mécanisme de protection applicable ; vérifier la validité des garanties ; réaliser un Transfer Impact Assessment (TIA) si nécessaire
Contractualisation	Conclure un accord de traitement des données (DPA) avec chaque fournisseur ; inclure les CCT si transfert hors UE ; prévoir des clauses d'audit et de localisation
Vérification technique	S'assurer que le fournisseur n'utilise pas les données pour entraîner ses modèles ; vérifier le chiffrement en transit et au repos ; contrôler les accès depuis des pays tiers
Suivi continu	Surveiller les évolutions réglementaires (invalidation de décisions d'adéquation) ; auditer régulièrement les fournisseurs ; mettre à jour les TIA

Pratiques et recommandations

Privilégier des fournisseurs d'IA hébergeant les données dans l'UE/EEE, en vérifiant que le traitement effectif (pas seulement le stockage) s'effectue sur des serveurs européens.

Vérifier systématiquement que le fournisseur d'IA n'utilise pas les données des salariés pour entraîner ou améliorer ses modèles d'IA, en incluant une clause contractuelle explicite d'interdiction.

Réaliser un Transfer Impact Assessment (TIA) pour chaque transfert de données vers un pays tiers, en évaluant le niveau de protection du pays de destination et les risques pour les droits des salariés.

Maintenir une cartographie à jour des flux de données vers les fournisseurs d'IA, en documentant la localisation exacte des serveurs, les sous-traitants impliqués et les mécanismes de protection applicables.

Prévoir un plan de contingence en cas d'invalidation d'un mécanisme de transfert (comme l'a montré l'arrêt Schrems II), en identifiant des alternatives européennes pour chaque outil d'IA critique.

Cadre juridique

Référence	Objet
RGPD - Articles 44-49	Encadrement des transferts de données vers des pays tiers
RGPD - Article 46	Garanties appropriées : clauses contractuelles types, BCR
RGPD - Article 28	Obligations du responsable du traitement envers le sous-traitant
AI Act (UE 2024/1689) - Article 11	Documentation technique incluant la localisation des données
Art. L.261-1	Encadrement du traitement des données personnelles des salariés
Loi du 1er août 2018	Loi nationale RGPD au Luxembourg
CJUE, arrêt Schrems II (C-311/18)	Invalidation du Privacy Shield ; obligation de vérification au cas par cas

La souveraineté des données est un enjeu stratégique pour les entreprises luxembourgeoises utilisant l'IA, en particulier celles du secteur financier soumises à des exigences CSSF supplémentaires. L'utilisation de services cloud américains (OpenAI, Google, Microsoft) nécessite une vigilance particulière quant aux mécanismes de transfert et aux garanties contractuelles. La responsabilité du transfert incombe toujours à l'employeur, même en cas de recours à un sous-traitant.