Quelles clauses inclure dans un contrat avec un fournisseur de solution d'IA ?

Réponse courte

Un contrat avec un fournisseur de solution d'IA doit intégrer des clauses couvrant la **conformité réglementaire** (obligations RGPD et AI Act), la **transparence algorithmique**, la **responsabilité en cas de dysfonctionnement** et la **protection des données personnelles**. Le RGPD impose un contrat de sous-traitance détaillant les finalités de traitement, tandis que l'AI Act exige des garanties sur la documentation technique et la gestion des risques.

Les clauses de **propriété intellectuelle**, d'**auditabilité**, de **réversibilité des données** et de **localisation du traitement** dans l'UE/EEE sont indispensables. L'employeur doit également prévoir des clauses de **niveau de service** (SLA), de notification des incidents et de mise à jour réglementaire pour couvrir l'évolution du cadre juridique européen.

Définition

Les **clauses contractuelles IA** désignent l'ensemble des stipulations juridiques spécifiques à l'acquisition ou à l'utilisation d'une solution d'intelligence artificielle. Elles complètent les clauses classiques d'un contrat de prestation de services en intégrant les exigences propres à la réglementation européenne sur l'IA et la protection des données.

Au Luxembourg, ces clauses doivent satisfaire simultanément les exigences du **RGPD** (contrat de sous-traitance article 28), de l'**AI Act** (obligations fournisseur-déployeur) et du **droit luxembourgeois** applicable aux nouvelles technologies en milieu professionnel.

Conditions d’exercice

Le contrat avec un fournisseur d'IA doit contenir des clauses obligatoires et des clauses recommandées couvrant l'ensemble du cycle de vie de la solution.

Type de clause	Détail
Sous-traitance RGPD (art. 28)	Nature et finalité du traitement, durée, types de données, catégories de personnes concernées, obligations de confidentialité et de sécurité
Conformité AI Act	Engagement du fournisseur à respecter les obligations applicables selon la classification du système (haut risque ou non), documentation technique, système de gestion des risques
Transparence algorithmique	Obligation de fournir une description compréhensible du fonctionnement de l'algorithme, des critères utilisés et de la logique de décision
Responsabilité et indemnisation	Répartition des responsabilités en cas de dysfonctionnement, plafonds d'indemnisation, assurance responsabilité civile professionnelle
Propriété intellectuelle	Propriété des données d'entrée, des résultats produits et des modèles entraînés sur les données de l'entreprise
Auditabilité	Droit d'audit par l'entreprise ou un tiers, accès aux logs, fréquence et modalités des audits
Réversibilité	Restitution des données en fin de contrat, format d'export, calendrier de suppression chez le fournisseur
Localisation et transferts	Localisation du traitement et stockage dans l'UE/EEE, encadrement des transferts hors UE
SLA et performance	Niveaux de service, disponibilité, temps de réponse, pénalités en cas de non-respect
Notification d'incidents	Délai de notification en cas d'incident de sécurité, de biais détecté ou de dysfonctionnement critique

Modalités pratiques

La négociation et la rédaction du contrat impliquent une collaboration entre les services juridiques, informatiques et métiers.

Étape	Détail
Cahier des charges	Définir précisément les fonctionnalités attendues, les données traitées et les résultats escomptés
Due diligence fournisseur	Vérifier les certifications, la conformité RGPD et AI Act, les références clients et la solidité financière
Négociation des clauses clés	Priorité aux clauses de responsabilité, d'auditabilité, de réversibilité et de conformité réglementaire
Validation juridique	Revue par un avocat spécialisé en droit du numérique et protection des données
AIPD	Réaliser l'analyse d'impact avant signature si le traitement présente un risque élevé
Clause de revue périodique	Prévoir une révision contractuelle annuelle pour intégrer les évolutions réglementaires

Pratiques et recommandations

Privilégier des contrats-cadres modulables permettant d'adapter les obligations aux évolutions de l'AI Act, en prévoyant des avenants pour chaque nouveau cas d'usage déployé au sein de l'entreprise.

Exiger systématiquement une clause de conformité réglementaire engageant le fournisseur à adapter son système aux nouvelles exigences sans surcoût pour le déployeur, dans la limite des évolutions raisonnablement prévisibles.

Intégrer des indicateurs de performance mesurables dans les SLA, incluant la précision algorithmique, le taux de faux positifs et le temps de traitement, pour objectiver l'évaluation de la solution.

Documenter l'ensemble du processus de sélection et de contractualisation pour démontrer la diligence de l'employeur en cas de contrôle par la CNPD ou de litige.

Cadre juridique

Référence	Objet
RGPD - Article 28	Contenu obligatoire du contrat de sous-traitance
RGPD - Article 32	Obligations de sécurité du traitement
RGPD - Article 35	Analyse d'impact relative à la protection des données
RGPD - Articles 44-49	Encadrement des transferts de données hors UE/EEE
AI Act - Articles 9-15	Exigences pour les systèmes à haut risque
AI Act - Article 25	Obligations des fournisseurs de systèmes d'IA
AI Act - Article 26	Obligations des déployeurs de systèmes d'IA
Art. L.414-4	Consultation de la délégation du personnel sur les nouvelles technologies

La rédaction du contrat avec un fournisseur d'IA nécessite une expertise juridique combinant droit du numérique, protection des données et droit du travail. Les clauses types proposées par les fournisseurs sont rarement suffisantes pour couvrir l'ensemble des obligations réglementaires luxembourgeoises et européennes.

L'entrée en vigueur progressive de l'AI Act impose une **veille contractuelle active** pour adapter les contrats existants aux nouvelles exigences, notamment celles applicables aux systèmes à haut risque à partir du 2 août 2026.