Comment évaluer la fiabilité d'un fournisseur d'IA avant de le sélectionner ?

Réponse courte

L'évaluation de la fiabilité d'un fournisseur d'IA est une étape indispensable pour l'employeur luxembourgeois, car il reste **responsable** des traitements réalisés par l'outil déployé (article 26 AI Act, article 28 RGPD). Le processus de sélection doit couvrir la **conformité réglementaire** (RGPD, AI Act), la solidité technique, la transparence algorithmique et la viabilité financière du fournisseur.

L'employeur doit exiger une documentation complète sur les **données d'entraînement**, les mesures de sécurité, les tests de biais algorithmiques, la localisation des données et les certifications obtenues. La due diligence inclut la vérification des **références clients**, l'analyse des conditions contractuelles et la capacité du fournisseur à répondre aux exigences de l'AI Act pour les systèmes à haut risque. Le recours à un fournisseur non fiable expose l'employeur à des sanctions financières et à des **atteintes à la réputation**.

Définition

La **due diligence fournisseur IA** désigne le processus d'évaluation approfondie d'un fournisseur d'intelligence artificielle avant la signature d'un contrat. Cette démarche vise à vérifier la capacité du fournisseur à garantir la conformité réglementaire, la sécurité des données, la transparence algorithmique et la continuité de service.

Au Luxembourg, cette évaluation est d'autant plus importante que l'AI Act établit une **responsabilité partagée** entre le fournisseur (obligations de conception) et le déployeur (obligations d'utilisation). L'employeur déployeur ne peut pas s'exonérer de sa responsabilité en invoquant les assurances du fournisseur.

Conditions d’exercice

L'évaluation d'un fournisseur d'IA repose sur des critères cumulatifs couvrant plusieurs dimensions.

Critère	Détail
Conformité RGPD	Vérifier la désignation d'un DPO, la politique de protection des données, les clauses de sous-traitance (article 28 RGPD)
Conformité AI Act	Documentation technique, évaluation des risques, tests de biais, système de management de la qualité pour les systèmes à haut risque
Transparence algorithmique	Capacité du fournisseur à expliquer le fonctionnement de l'algorithme, les données utilisées, les limites connues
Sécurité des données	Mesures techniques (chiffrement, contrôle d'accès, sauvegarde), certifications (ISO 27001, SOC 2), audits de sécurité
Localisation des données	Hébergement dans l'EEE, identification des sous-traitants, absence de transferts non conformes
Viabilité financière	Solidité financière du fournisseur, pérennité de la solution, plan de continuité d'activité
Références et réputation	Clients existants dans le secteur, retours d'expérience, incidents publics, contentieux connus
Support et maintenance	Disponibilité du support technique, SLA, réactivité, capacité de mise à jour et d'évolution

Modalités pratiques

Le processus de sélection d'un fournisseur d'IA suit une démarche structurée de due diligence.

Étape	Détail
Cahier des charges	Définition des exigences fonctionnelles, techniques, juridiques et éthiques ; pondération des critères
Appel d'offres	Sollicitation de plusieurs fournisseurs, questionnaire standardisé, démonstrations
Évaluation technique	Tests en environnement contrôlé, évaluation de la performance, des biais et de la robustesse
Audit juridique	Revue des conditions générales, des clauses de protection des données, des garanties de conformité AI Act
Vérification des références	Contact avec des clients existants, analyse des retours d'expérience, recherche d'incidents publics
Négociation contractuelle	Clauses de conformité, pénalités, droit d'audit, clause de réversibilité, conditions de résiliation

Pratiques et recommandations

Exiger du fournisseur une documentation technique détaillée incluant les données d'entraînement, les métriques de performance, les tests de biais et les limites identifiées du système.

Vérifier l'existence de certifications reconnues (ISO 27001, SOC 2, certification AI Act si disponible) et ne pas se contenter des déclarations de conformité sans preuve.

Inclure dans le contrat des clauses de droit d'audit permettant de vérifier régulièrement les pratiques du fournisseur en matière de protection des données et de conformité.

Prévoir une clause de réversibilité garantissant la récupération des données dans un format standard et la continuité de service en cas de changement de fournisseur.

Consulter le DPO et, si nécessaire, des experts en droit du numérique pour analyser les conditions contractuelles avant la signature.

Cadre juridique

Référence	Objet
AI Act (UE 2024/1689) - Article 26	Obligations du déployeur, responsabilité partagée avec le fournisseur
AI Act - Articles 9-15	Obligations des fournisseurs de systèmes à haut risque
RGPD - Article 28	Obligations du sous-traitant, clauses contractuelles obligatoires
RGPD - Article 32	Mesures de sécurité techniques et organisationnelles
RGPD - Article 35	Analyse d'impact relative à la protection des données
RGPD - Articles 44-49	Conditions de transfert de données vers des pays tiers
CNPD	Autorité de contrôle, recommandations sur la sélection des sous-traitants

L'évaluation approfondie du fournisseur d'IA est un investissement qui protège l'entreprise contre les risques juridiques, financiers et réputationnels. Les exigences de l'AI Act renforcent la nécessité d'une due diligence rigoureuse, l'employeur déployeur ne pouvant pas déléguer sa responsabilité au fournisseur.