Quelles sont les obligations RGPD liées à l'utilisation de l'IA en entreprise ?

Réponse courte

L'utilisation de l'IA en entreprise implique un traitement de données personnelles soumis aux obligations du **RGPD**. L'employeur doit disposer d'une **base légale** valide (consentement, intérêt légitime, contrat), respecter les principes de **minimisation** et de limitation de la finalité, informer les personnes et garantir leurs droits. L'article 22 interdit les décisions automatisées fondées exclusivement sur un traitement automatisé.

Pour les usages RH, le RGPD impose une **AIPD** (article 35) en cas de profilage ou d'évaluation systématique. Le **DPO** doit être consulté sur tout projet IA impliquant des données personnelles. Les salariés disposent d'un droit d'accès, d'un droit d'**explication** de la logique algorithmique et d'un droit de rectification. La **CNPD** contrôle la conformité et peut prononcer des amendes jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial.

Définition

Le **RGPD** (Règlement général sur la protection des données, Règlement UE 2016/679) est le cadre juridique européen de protection des données personnelles, applicable depuis le 25 mai 2018. Il s'applique à tout traitement de données personnelles effectué dans le cadre des activités d'un établissement dans l'UE, y compris les traitements automatisés par des systèmes d'IA.

En contexte IA, le RGPD régit à la fois les **données d'entraînement** des modèles (si elles contiennent des données personnelles) et les **données traitées** en production. Chaque interaction d'un salarié avec un système d'IA constitue potentiellement un traitement de données personnelles soumis au RGPD, de la saisie d'une requête dans un chatbot à l'analyse d'un CV par un algorithme de recrutement.

Questions fréquentes

Faut-il contractualiser avec un fournisseur d'IA selon l'article 28 du RGPD ?

Oui. L'article 28 du RGPD impose un contrat de sous-traitance avec le fournisseur d'IA définissant la nature et la finalité du traitement, les types de données, les obligations du sous-traitant et les mesures de sécurité applicables.

Quand le DPO doit-il être consulté sur un projet IA ?

Selon l'article 39 du RGPD, le DPO doit être consulté dès la phase de conception de tout projet IA impliquant des données personnelles. Cette consultation s'inscrit dans une démarche de privacy by design et privacy by default.

Que faire en cas de transfert de données IA hors de l'UE ?

Il faut vérifier les garanties appropriées selon les articles 44-49 du RGPD : décision d'adéquation, clauses contractuelles types, règles d'entreprise contraignantes. Tout transfert non encadré est illicite et expose à de lourdes sanctions CNPD.

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

Quelles bases légales possibles pour un traitement IA en RH ?

L'article 6 du RGPD prévoit le consentement, l'exécution du contrat, l'obligation légale, la sauvegarde des intérêts vitaux, la mission d'intérêt public ou l'intérêt légitime. Le consentement est rarement valable en contexte salarié (déséquilibre de pouvoir).

Quelles sanctions CNPD pour non-conformité RGPD d'un système IA ?

Les sanctions CNPD peuvent atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial annuel. L'absence d'AIPD est sanctionnable de manière autonome jusqu'à 10 millions d'euros ou 2 % du CA mondial selon l'article 83 du RGPD.

Quelles sont les obligations RGPD liées à l'utilisation de l'IA en entreprise ?

L'employeur doit disposer d'une base légale (article 6 RGPD), respecter la minimisation et la limitation de finalité, informer les personnes (articles 13-14), garantir leurs droits, réaliser une AIPD (article 35) et consulter le DPO sur les projets IA.

Conditions d'exercice

Les obligations RGPD applicables à l'IA en entreprise couvrent l'ensemble du cycle de vie du traitement.

Obligation	Article RGPD	Application à l'IA
Base légale	Art. 6	Identifier la base légale pour chaque traitement IA (intérêt légitime, contrat, consentement)
Minimisation	Art. 5, §1, c)	Ne collecter que les données strictement nécessaires au fonctionnement du système
Limitation de la finalité	Art. 5, §1, b)	Ne pas utiliser les données pour une finalité incompatible avec celle initialement prévue
Exactitude	Art. 5, §1, d)	Garantir la qualité et la mise à jour des données traitées par l'IA
Information	Art. 13-14	Informer les salariés de l'utilisation de l'IA et de la logique sous-jacente
Droits des personnes	Art. 15-22	Garantir l'accès, la rectification, l'effacement, la portabilité et la contestation
AIPD	Art. 35	Obligatoire pour le profilage, l'évaluation systématique et les décisions automatisées
DPO	Art. 37-39	Consultation obligatoire sur les projets IA impliquant des données personnelles

Modalités pratiques

La mise en conformité RGPD pour les projets IA nécessite une approche structurée.

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

Action	Détail
Registre des traitements	Inscrire chaque traitement IA dans le registre avec sa finalité et sa base légale
AIPD	Réaliser l'analyse d'impact avant le déploiement si profilage ou évaluation systématique
Information	Rédiger les notices d'information pour les salariés et les candidats
Contrat sous-traitant	Contractualiser avec le fournisseur d'IA les obligations de l'article 28 du RGPD
Transferts hors UE	Vérifier les garanties si les données sont transférées hors de l'Espace économique européen
Exercice des droits	Mettre en place les procédures de traitement des demandes d'accès et d'explication

Pratiques et recommandations

Impliquer le DPO dès la phase de conception de tout projet IA dans une démarche d'IA responsable pour intégrer la protection des données dès la conception (privacy by design) et par défaut (privacy by default).

Vérifier les flux de données avec les fournisseurs d'IA, en portant une attention particulière aux transferts vers des serveurs situés hors de l'UE, qui nécessitent des garanties appropriées.

Limiter la conservation des données traitées par l'IA au strict nécessaire, en définissant des durées de conservation proportionnées et en mettant en place des mécanismes d'effacement automatique.

Former les utilisateurs aux bonnes pratiques de saisie de données dans les outils d'IA, en interdisant la saisie de données personnelles sensibles dans des systèmes non sécurisés.

Cadre juridique

Référence	Objet
RGPD - Article 5	Principes fondamentaux du traitement (licéité, minimisation, exactitude)
RGPD - Article 6	Bases légales du traitement
RGPD - Article 22	Décisions individuelles automatisées
RGPD - Article 28	Obligations du sous-traitant (fournisseur d'IA)
RGPD - Article 35	Analyse d'impact relative à la protection des données
Art. L.261-1	Traitement de données de surveillance au Luxembourg

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

Le RGPD est le pilier de la protection des données dans les projets IA. Les entreprises doivent veiller à la conformité de bout en bout, des données d'entraînement aux résultats produits en production. Les amendes CNPD peuvent atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial annuel.

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.