Qu'est-ce qu'un accord de traitement des données (DPA) avec un fournisseur d'IA ?

Réponse courte

Un accord de traitement des données (Data Processing Agreement ou DPA) est un **contrat obligatoire** entre l'employeur (responsable du traitement) et le fournisseur d'IA (sous-traitant) qui encadre le traitement des données personnelles des salariés. L'article 28 du RGPD impose ce contrat dès qu'un sous-traitant traite des données personnelles pour le compte du responsable. Son absence expose l'employeur à des sanctions AI Act et CNPD pouvant atteindre **20 millions d'euros**.

Le DPA doit préciser l'**objet et la durée** du traitement, la **nature et la finalité**, les types de données traitées, les **obligations de sécurité**, les conditions de sous-traitance ultérieure et les modalités d'**audit** par l'employeur. Pour les fournisseurs d'IA, des clauses spécifiques sur la **non-utilisation des données pour l'entraînement** des modèles et la **localisation des serveurs** sont essentielles.

Définition

Le **Data Processing Agreement** (DPA) ou accord de traitement des données est le contrat prévu par l'article 28 du RGPD qui régit la relation entre un responsable du traitement et un sous-traitant. Dans le contexte de l'IA en entreprise, l'employeur est le responsable du traitement et le fournisseur de l'outil d'IA est le sous-traitant qui traite les données des salariés pour le compte de l'employeur.

Ce contrat est **juridiquement obligatoire** au titre des obligations RGPD et distinct du contrat commercial de fourniture de services. Il constitue la base de la conformité RGPD dans la relation avec les prestataires d'IA et doit être conclu **avant** tout traitement de données personnelles.

Questions fréquentes

Le DPA doit-il être négocié ou peut-on accepter celui du fournisseur ?

Il doit être activement négocié. Les DPA standardisés des grandes plateformes IA ne couvrent pas suffisamment les spécificités de l'IA (entraînement, localisation). L'employeur doit ajouter des clauses spécifiques pour obtenir des garanties effectives, sous peine de voir sa conformité remise en cause.

Qu'est-ce qu'un accord de traitement des données (DPA) avec un fournisseur d'IA ?

Un contrat obligatoire prévu par l'article 28 du RGPD entre l'employeur (responsable de traitement) et le fournisseur d'IA (sous-traitant) qui encadre le traitement des données personnelles des salariés. Son absence expose à des sanctions CNPD jusqu'à 20 millions d'euros ou 4 % du CA mondial.

Quand signer le DPA avec un fournisseur d'IA ?

Avant tout traitement de données personnelles. La conclusion du DPA est un préalable obligatoire. Il doit être archivé avec le contrat commercial, intégré au registre des traitements et faire l'objet d'un suivi périodique pour vérifier le respect des clauses et l'absence de modifications non autorisées.

Quel droit d'audit prévoir face à un fournisseur d'IA ?

Un droit d'audit effectif et non simplement un rapport de conformité produit par le fournisseur. Prévoir la possibilité d'un audit sur site ou par un tiers indépendant. La coopération avec les autorités (CNPD) doit être contractuellement prévue, ainsi que l'accès aux informations de conformité.

Quelles clauses spécifiques inclure dans un DPA avec un fournisseur d'IA ?

L'interdiction d'utiliser les données pour entraîner ou améliorer les modèles, la localisation effective des serveurs de traitement et stockage, la conformité AI Act pour les systèmes à haut risque, le droit d'audit indépendant et la suppression effective des données en fin de contrat.

Quelles mentions obligatoires doit contenir un DPA ?

L'objet, la durée, la nature et la finalité du traitement, les types de données et catégories de personnes concernées, les droits et obligations du responsable, les obligations de sécurité, les conditions de sous-traitance ultérieure et les modalités d'audit selon l'article 28 du RGPD.

Conditions d’exercice

Le contenu du DPA avec un fournisseur d'IA est encadré par l'article 28 du RGPD avec des exigences spécifiques liées à l'IA.

Critère	Détail
Mentions obligatoires (art. 28)	Objet, durée, nature et finalité du traitement ; types de données personnelles et catégories de personnes concernées ; droits et obligations du responsable du traitement
Obligations du sous-traitant	Traiter les données uniquement sur instruction documentée ; garantir la confidentialité ; assister le responsable pour les demandes de droits des salariés ; supprimer les données à la fin du contrat
Sécurité	Mesures techniques et organisationnelles appropriées (art. 32 RGPD) ; chiffrement, pseudonymisation, contrôle d'accès ; notification des violations dans les 72 heures
Sous-traitance ultérieure	Autorisation préalable du responsable ; mêmes obligations imposées au sous-traitant ultérieur ; notification de tout changement de sous-traitant
Clauses IA spécifiques	Interdiction d'utiliser les données pour entraîner les modèles ; localisation des serveurs de traitement et de stockage ; conformité AI Act pour les systèmes à haut risque
Audit	Droit d'audit par le responsable ou un tiers indépendant ; accès aux informations nécessaires pour démontrer la conformité ; coopération avec les autorités (CNPD)

Modalités pratiques

La négociation et la mise en place d'un DPA avec un fournisseur d'IA suivent un processus structuré.

Étape	Détail
Évaluation du fournisseur	Vérifier les certifications de sécurité (ISO 27001, SOC 2) ; évaluer la conformité RGPD déclarée ; demander les références de conformité AI Act
Négociation du DPA	Adapter le DPA standard du fournisseur aux exigences de l'entreprise ; ajouter les clauses IA spécifiques ; intégrer les CCT si transfert hors UE
Points critiques à négocier	Non-utilisation des données pour l'entraînement IA ; localisation effective des traitements ; notification en cas de changement de sous-traitant ; modalités d'audit ; suppression effective en fin de contrat
Signature et archivage	Signer le DPA avant tout traitement ; archiver avec le contrat commercial ; mettre à jour le registre des traitements
Suivi contractuel	Auditer périodiquement le respect du DPA ; vérifier les changements de sous-traitants ; renouveler l'évaluation en cas de modification du service

Pratiques et recommandations

Négocier activement le DPA plutôt que d'accepter sans modification le contrat standard du fournisseur d'IA, en ajoutant des clauses spécifiques sur la non-utilisation des données pour l'entraînement et la localisation des serveurs.

Vérifier que le DPA couvre explicitement tous les types de données des salariés traités par l'outil d'IA, y compris les données dérivées (scores, recommandations, profils) qui constituent des données personnelles au sens du RGPD.

Exiger un droit d'audit effectif et non pas simplement un rapport de conformité produit par le fournisseur, en prévoyant la possibilité d'un audit sur site ou par un tiers indépendant.

Prévoir des clauses de sortie claires garantissant la restitution et la suppression effective des données en fin de contrat, avec un certificat de destruction.

Maintenir un registre des DPA conclus avec les fournisseurs d'IA, en documentant les dates de signature, les renouvellements, les modifications et les audits réalisés.

Cadre juridique

Référence	Objet
RGPD - Article 28	Contenu obligatoire du contrat entre responsable et sous-traitant
RGPD - Article 32	Mesures de sécurité du traitement
RGPD - Article 33	Notification des violations de données dans les 72 heures
RGPD - Article 44-49	Transferts internationaux de données
AI Act (UE 2024/1689) - Article 26	Obligations des déployeurs de systèmes d'IA
Art. L.261-1	Encadrement du traitement des données personnelles des salariés
Loi du 1er août 2018	Loi nationale RGPD au Luxembourg

Le DPA constitue la pierre angulaire de la conformité RGPD dans la relation avec les fournisseurs d'IA. Beaucoup de grandes plateformes d'IA proposent des DPA standardisés qui ne couvrent pas suffisamment les spécificités de l'IA (entraînement des modèles, localisation des traitements). L'employeur doit exercer sa responsabilité de négociation pour obtenir des garanties effectives, sous peine de voir sa conformité remise en cause lors d'un contrôle CNPD.