Une analyse d'impact sur la protection des données est-elle obligatoire avant de déployer un outil d'IA ?

Réponse courte

L'**AIPD** (analyse d'impact relative à la protection des données) est obligatoire avant le déploiement d'un outil d'IA dès que le traitement est susceptible d'engendrer un **risque élevé** pour les droits et libertés des personnes. L'article 35 du RGPD identifie trois cas nécessitant systématiquement une AIPD : l'**évaluation systématique** de personnes physiques, le traitement à grande échelle de données **sensibles**, et la **surveillance systématique** à grande échelle d'une zone accessible au public.

En pratique, la plupart des usages RH de l'IA nécessitent une AIPD, car ils impliquent du **profilage** ou des décisions automatisées affectant les salariés. L'AIPD doit être réalisée **avant le déploiement**, en consultation avec le DPO, et mise à jour en cas de modification du traitement. L'absence d'AIPD est sanctionnable par la CNPD avec des sanctions AI Act jusqu'à **10 millions d'euros** ou 2 % du chiffre d'affaires mondial.

Définition

L'**analyse d'impact relative à la protection des données** est une démarche documentée d'évaluation des risques que présente un traitement de données personnelles pour les droits et libertés des personnes concernées. Elle comprend une description systématique du traitement, une évaluation de sa nécessité et de sa proportionnalité, une analyse des risques et les mesures envisagées pour les atténuer.

L'AIPD n'est pas une simple formalité administrative : c'est un outil d'aide à la **décision** qui permet au responsable du traitement de vérifier la conformité de son projet et d'identifier les mesures techniques et organisationnelles nécessaires. Pour les projets IA, elle constitue la première étape concrète de la mise en conformité RGPD.

Questions fréquentes

Faut-il réévaluer l'AIPD régulièrement ?

Oui. L'AIPD doit être réévaluée au moins annuellement et systématiquement après toute modification significative du traitement, du système d'IA ou de son périmètre d'utilisation. La documentation doit être conservée pendant la durée du traitement.

Quand doit-on consulter la CNPD avant un déploiement IA ?

L'article 36 du RGPD impose une consultation préalable de la CNPD si le risque résiduel reste élevé après les mesures d'atténuation. Cette consultation est obligatoire et la CNPD dispose d'un délai pour rendre son avis.

Quelles étapes suivre pour réaliser une AIPD ?

La méthodologie comprend : description du traitement, évaluation de la nécessité et proportionnalité, analyse des risques, définition des mesures d'atténuation, consultation du DPO et, si nécessaire, consultation préalable de la CNPD.

Quelles sanctions en cas d'absence d'AIPD ?

L'article 83, paragraphe 4 du RGPD prévoit des sanctions jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial. L'absence d'AIPD est une infraction autonome sanctionnable indépendamment de la conformité du traitement lui-même.

Quels usages RH de l'IA nécessitent systématiquement une AIPD ?

Le scoring de performance, l'évaluation de candidatures, l'analyse comportementale, la prédiction de turnover, le matching compétences et le tri automatique de CV nécessitent systématiquement une AIPD selon l'article 35 du RGPD.

Une AIPD est-elle obligatoire avant de déployer un outil d'IA en entreprise ?

Oui, dès que le traitement engendre un risque élevé pour les droits des personnes. L'article 35 du RGPD identifie trois cas : évaluation systématique, traitement à grande échelle de données sensibles et surveillance systématique d'une zone publique.

Conditions d’exercice

Les critères déterminant l'obligation de réaliser une AIPD sont définis par le RGPD et précisés par la CNPD.

Critère	Source	Exemples en contexte IA
Évaluation systématique	RGPD Art. 35, §3, a)	Scoring de performance, évaluation de candidatures, analyse comportementale
Traitement de données sensibles	RGPD Art. 35, §3, b)	Données de santé (absences maladie), données biométriques
Surveillance systématique	RGPD Art. 35, §3, c)	Surveillance de la productivité, contrôle des accès, analyse des communications
Profilage	RGPD Art. 35 + lignes directrices	Prédiction de turnover, matching compétences, analyse de risques
Décision automatisée	RGPD Art. 22	Tri automatique de CV, pré-sélection algorithmique
Liste CNPD	Délibération CNPD	Traitements identifiés par la CNPD comme nécessitant une AIPD

Modalités pratiques

La réalisation de l'AIPD suit une méthodologie en quatre étapes conformément aux lignes directrices du Comité européen de la protection des données.

Étape	Détail
Description du traitement	Finalité, nature, portée, contexte, données traitées, personnes concernées, destinataires
Évaluation de la nécessité	Proportionnalité, minimisation, base légale, droits des personnes, mesures de conformité
Analyse des risques	Identifier les sources de risque, les scénarios de menace et évaluer la gravité et la vraisemblance
Mesures d'atténuation	Mesures techniques (chiffrement, anonymisation) et organisationnelles (supervision, formation)
Consultation du DPO	Avis obligatoire du DPO avant validation de l'AIPD
Consultation CNPD	Consultation préalable obligatoire si le risque résiduel reste élevé (Art. 36)

Pratiques et recommandations

Systématiser l'AIPD pour tout projet IA impliquant des données personnelles de salariés, même en cas de doute sur l'obligation, car la démarche constitue une preuve de diligence en cas de contrôle.

Impliquer les parties prenantes (DPO, service informatique, RH, représentants du personnel) pour bénéficier d'une vision complète des risques et des mesures d'atténuation possibles.

Documenter l'ensemble de la démarche de manière détaillée et la conserver pendant toute la durée du traitement, car elle devra être présentée à la CNPD en cas de contrôle ou de réclamation.

Réévaluer l'AIPD au moins annuellement et systématiquement après toute modification significative du traitement, du système d'IA ou de son périmètre d'utilisation.

Cadre juridique

Référence	Objet
RGPD - Article 35	Obligation d'AIPD pour les traitements à risque élevé
RGPD - Article 36	Consultation préalable de la CNPD si risque résiduel élevé
RGPD - Article 39, §1, c)	Rôle consultatif du DPO dans l'AIPD
RGPD - Article 83, §4	Sanctions : jusqu'à 10 M EUR ou 2 % du CA pour non-réalisation de l'AIPD
Art. L.261-1	Information préalable de la délégation du personnel
AI Act - Article 27	Analyse d'impact sur les droits fondamentaux (complémentaire à l'AIPD)

L'AIPD est un prérequis incontournable pour tout projet IA en entreprise impliquant des données de salariés. Son absence constitue une infraction autonome sanctionnable par la CNPD, indépendamment de la conformité du traitement lui-même. La démarche est complémentaire de l'analyse d'impact sur les droits fondamentaux prévue par l'AI Act.