Mon entreprise doit-elle réaliser une analyse d'impact (AIPD) et dans quels cas ?

Réponse courte

L'**analyse d'impact relative à la protection des données (AIPD)**, aussi appelée **DPIA** (Data Protection Impact Assessment), est une procédure formalisée prévue par l'**article 35 du RGPD**. Elle consiste à évaluer, **avant la mise en œuvre** d'un traitement susceptible d'engendrer un **risque élevé** pour les droits et libertés des personnes, les impacts potentiels sur la vie privée et à définir les mesures permettant de les réduire.

L'AIPD est **obligatoire** dans les cas de surveillance systématique à grande échelle, de traitement de données sensibles à grande échelle, d'évaluation systématique fondée sur un traitement automatisé et pour tous les traitements figurant dans la **liste publiée par la CNPD**. Elle doit être **documentée**, validée par le **DPO** et peut faire l'objet d'une **consultation préalable** de la CNPD lorsque le risque résiduel reste élevé.

Définition

L'**AIPD** est un outil de **gestion des risques** permettant au responsable de traitement de démontrer sa conformité au RGPD (principe d'accountability). Elle s'inscrit dans une approche **Privacy by Design** et doit être menée avant tout lancement de traitement à risque élevé, notamment en matière de RH (vidéosurveillance, géolocalisation, biométrie, scoring).

Questions fréquentes

Faut-il consulter la délégation lors d'une AIPD RH ?

Oui, lorsque le traitement concerne les salariés, la délégation du personnel doit être consultée conformément à l'article L.261-1 du Code du travail. Cette consultation s'ajoute à l'avis du DPO requis par l'article 35.2 du RGPD.

Qu'est-ce qu'une AIPD au sens du RGPD ?

L'AIPD (analyse d'impact relative à la protection des données) ou DPIA est une procédure formalisée prévue par l'article 35 du RGPD. Elle évalue les impacts potentiels d'un traitement sur la vie privée avant sa mise en œuvre.

Quand faut-il réviser une AIPD ?

L'AIPD doit être révisée à chaque évolution substantielle du traitement : changement de finalité, nouveau sous-traitant, modification technique. Cette révision permet de maintenir la pertinence de l'analyse et la conformité au principe d'accountability.

Quand une AIPD est-elle obligatoire au Luxembourg ?

L'AIPD est obligatoire en cas de surveillance systématique à grande échelle, de traitement de données sensibles à grande échelle, d'évaluation systématique fondée sur un traitement automatisé, ou pour tous les traitements figurant dans la liste publiée par la CNPD.

Quelle sanction en cas d'absence d'AIPD obligatoire ?

L'absence d'AIPD lorsqu'elle est obligatoire constitue une violation du RGPD sanctionnée par la CNPD jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial. C'est un instrument essentiel de démonstration de la conformité.

Quelles sont les étapes d'une AIPD ?

Une AIPD se conduit en cinq étapes : description du traitement (finalités, données, flux), analyse de nécessité et proportionnalité, analyse des risques, définition des mesures de mitigation, consultation du DPO et éventuellement de la CNPD.

Qui doit valider une AIPD dans l'entreprise ?

L'AIPD doit être validée par le DPO (délégué à la protection des données). Lorsque le risque résiduel reste élevé après mitigation, une consultation préalable de la CNPD est obligatoire conformément à l'article 36 du RGPD.

Conditions d’exercice

L'article 35 du RGPD impose une AIPD en cas de surveillance systématique à grande échelle, profilage avec effets juridiques, traitement de données sensibles à grande échelle, nouvelles technologies, interconnexion de fichiers ou traitements figurant sur la liste publiée par la CNPD.

Cas d'obligation	Détail
Surveillance systématique	Suivi à grande échelle de zones accessibles au public
Évaluation automatisée	Profilage produisant des effets juridiques
Données sensibles à grande échelle	Santé, origine, opinions, biométrie
Liste CNPD	Traitements figurant sur la liste publiée
Nouvelle technologie	Déploiement de solutions innovantes
Combinaison de fichiers	Interconnexion de bases hétérogènes
Risque élevé	Probabilité et gravité élevées pour les droits

Modalités pratiques

Une AIPD se conduit en décrivant le traitement, en analysant sa nécessité et ses risques, en définissant des mesures de mitigation, puis en recueillant l'avis du DPO avant éventuelle consultation préalable de la CNPD.

Étape	Détail
Description du traitement	Finalités, données, flux, durée, destinataires
Analyse de nécessité	Proportionnalité et minimisation
Analyse des risques	Identification des menaces et de leurs impacts
Mesures de mitigation	Actions techniques et organisationnelles
Consultation DPO	Avis formel du délégué à la protection des données
Consultation CNPD	Si risque résiduel élevé (art. 36 RGPD)
Révision	Mise à jour lors de tout changement substantiel

Pratiques et recommandations

Utiliser la méthodologie et les outils recommandés par la CNPD ou l'outil PIA de la CNIL française, adaptés au contexte luxembourgeois.

Associer le DPO, les équipes métiers, la DSI et le service juridique à la rédaction de l'AIPD pour garantir une analyse complète des risques.

Consulter la délégation du personnel lorsque le traitement concerne les salariés, conformément à l'article L.261-1 du Code du travail.

Documenter rigoureusement les choix de mitigation et les arbitrages, pour démontrer la conformité en cas de contrôle de la CNPD.

Réviser l'AIPD à chaque évolution substantielle du traitement (changement de finalité, nouveau sous-traitant, modification technique).

Cadre juridique

Le cadre juridique de l'AIPD repose sur le RGPD et les recommandations européennes.

Référence	Objet
Art. 35 RGPD	Analyse d'impact relative à la protection des données
Art. 36 RGPD	Consultation préalable de l'autorité de contrôle
Art. 25 RGPD	Protection des données dès la conception (Privacy by Design)
Art. 32 RGPD	Sécurité du traitement
Loi du 1er août 2018	Régime général au Luxembourg
Liste CNPD	Traitements soumis à AIPD obligatoire
Lignes directrices WP248	AIPD (adoptées par le CEPD)

L'absence d'AIPD lorsqu'elle est obligatoire constitue une violation du RGPD sanctionnée par la CNPD jusqu'à **10 millions d'euros ou 2 % du chiffre d'affaires mondial**. L'AIPD est un instrument essentiel de démonstration de la conformité.