La CNPD doit-elle être notifiée lors de la mise en place d'un contrôle de l'activité informatique des salariés ?

Réponse courte

Depuis le **25 mai 2018**, **aucune notification ni autorisation préalable** n'est due à la CNPD pour la mise en place d'un contrôle de l'activité informatique des salariés. Le régime déclaratif a été remplacé par le **principe d'accountability** : l'employeur reste pleinement responsable de la conformité du dispositif et doit pouvoir la documenter à tout moment.

L'employeur doit néanmoins réaliser une AIPD (article 35 du RGPD) si le traitement présente un risque élevé pour les droits et libertés des salariés. Si l'AIPD révèle un **risque résiduel élevé** non maîtrisable par les mesures envisagées, une **consultation préalable de la CNPD** s'impose au titre de l'article 36 du RGPD. Le registre des traitements, l'**information individuelle** des salariés et la **consultation de la délégation** (L.414-9) restent obligatoires en toutes hypothèses.

Définition

Le **principe d'accountability** (article 5(2) du RGPD) inverse la logique du régime déclaratif : c'est désormais à l'employeur de documenter la conformité de chaque traitement, sans intervention systématique de la CNPD avant la mise en œuvre.

La **consultation préalable** de l'article 36 du RGPD constitue une exception à ce principe : elle s'impose uniquement lorsque l'AIPD ne permet pas de réduire le risque résiduel à un niveau acceptable.

Questions fréquentes

Faut-il une AIPD pour tout contrôle de l'activité informatique ?

L'AIPD est obligatoire si le traitement présente un risque élevé pour les droits et libertés des salariés (article 35 RGPD). Son absence quand elle est requise constitue un manquement autonome, indépendamment de toute consultation préalable de la CNPD.

La CNPD doit-elle être notifiée pour un contrôle de l'activité informatique des salariés ?

Non, depuis le 25 mai 2018, aucune notification ni autorisation préalable n'est due à la CNPD. Le régime déclaratif a été remplacé par le principe d'accountability : l'employeur reste pleinement responsable de la conformité du dispositif et doit pouvoir la documenter.

Quand une consultation préalable de la CNPD devient-elle obligatoire ?

Si l'AIPD révèle un risque résiduel élevé non maîtrisable par les mesures envisagées, conformément à l'article 36 du RGPD. Hors ce cas, l'employeur documente sa conformité sans intervention systématique de la CNPD avant la mise en œuvre du dispositif.

Que faire en cas de modification d'un dispositif de cybersurveillance ?

Toute modification substantielle (extension, nouvelle finalité, nouveau prestataire) impose une révision documentée de l'AIPD et, le cas échéant, une nouvelle consultation préalable. Le registre des traitements doit également être mis à jour.

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

Quelles obligations subsistent malgré la suppression de la déclaration CNPD ?

Registre des traitements (article 30 RGPD), information individuelle des salariés (notice écrite ou charte), consultation de la délégation (L.414-9), AIPD si risque élevé. Toutes les pièces doivent être tenues à disposition de la CNPD à tout moment.

Quelles sanctions en cas d'absence d'AIPD pour la cybersurveillance ?

Violation autonome exposant l'employeur à des sanctions administratives jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial. La CNPD effectue des contrôles a posteriori et peut sanctionner toute non-conformité documentée.

Conditions d’exercice

L'AIPD est l'élément central du régime actuel : son absence quand elle est requise constitue un manquement autonome, indépendamment de toute consultation préalable de la CNPD.

Condition	Exigence concrète
Pas de notification systématique	Régime déclaratif supprimé depuis le 25 mai 2018
AIPD obligatoire	Article 35 du RGPD si risque élevé pour les droits et libertés
Consultation préalable	Article 36 du RGPD si risque résiduel élevé non maîtrisable
Accountability	Documentation complète et opposable à la CNPD à tout moment
Registre des traitements	Article 30 du RGPD : finalités, durées, destinataires

Modalités pratiques

L'AIPD doit être tenue à jour ; toute modification substantielle du dispositif (extension, nouvelle finalité, nouveau prestataire) impose une révision documentée et, le cas échéant, une nouvelle consultation préalable.

Démarche	Précision
AIPD documentée	Article 35 du RGPD : analyse des risques et mesures d'atténuation
Évaluation du risque résiduel	Si élevé, consultation CNPD obligatoire (article 36)
Dossier de consultation	Description, AIPD, mesures envisagées, transmis à la CNPD
Registre des traitements	Article 30 RGPD : mis à jour à chaque modification
Information individuelle	Notice écrite ou charte informatique remise aux salariés
Consultation délégation	Procès-verbal préalable conformément à L.414-9
Conservation des preuves	Toutes les pièces tenues à disposition de la CNPD

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

Pratiques et recommandations

Réaliser systématiquement une AIPD pour tout dispositif de contrôle informatique étendu.

Documenter précisément les mesures techniques et organisationnelles d'atténuation des risques.

Mettre à jour l'AIPD à chaque modification substantielle du dispositif.

Tenir le registre des traitements à jour avec finalités et durées.

Solliciter un avis informel de la CNPD en cas de doute, sans attendre une situation litigieuse.

Désigner un DPO ou un référent en cas de dispositif d'envergure.

Cadre juridique

Référence	Objet
Art. 5(2) du RGPD	Principe d'accountability
Art. 30 du RGPD	Registre des activités de traitement
Art. 35 du RGPD	Analyse d'impact relative à la protection des données
Art. 36 du RGPD	Consultation préalable de l'autorité de contrôle
Art. L.261-1 du Code du travail	Traitement de données pour surveillance des salariés
Art. L.414-9 du Code du travail	Co-décision de la délégation du personnel
Loi modifiée du 1er août 2018	Régime général de protection des données

L'absence d'AIPD quand elle est requise ou de consultation préalable lorsque l'article 36 l'impose constitue une violation autonome exposant l'employeur à des sanctions administratives jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial. La CNPD effectue des contrôles a posteriori et peut sanctionner toute non-conformité documentée.

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.