Quelles sont les recommandations de la CNPD pour l'utilisation des logiciels de surveillance en entreprise au Luxembourg ?

Réponse courte

La CNPD impose que tout logiciel de surveillance soit limité à un **intérêt légitime démontré**, dans le respect strict du principe de **proportionnalité** et de **minimisation des données**. La surveillance généralisée, permanente ou réalisée à l'insu des salariés est prohibée et expose l'employeur à des sanctions administratives importantes.

Avant la mise en place, l'employeur doit informer **individuellement** chaque salarié, consulter la délégation du personnel (article L.414-9 dès **150 salariés**), réaliser une analyse d'impact si le risque est élevé (article 35 du RGPD) et tenir un registre des traitements. Les durées de conservation doivent être strictement limitées à la finalité, et l'accès aux données réservé aux personnes habilitées avec traçabilité documentée.

Définition

Les **logiciels de surveillance** regroupent les dispositifs informatiques permettant à l'employeur de collecter, enregistrer ou analyser les activités des salariés sur les outils numériques professionnels (contrôle d'accès, vidéosurveillance, journalisation des connexions, surveillance de la messagerie ou de la navigation).

Au Luxembourg, leur usage relève du **principe d'accountability** posé par le RGPD et la loi modifiée du 1er août 2018 : l'employeur est responsable de démontrer la conformité du traitement, sans déclaration préalable à la CNPD.

Questions fréquentes

À partir de combien de salariés faut-il consulter la délégation pour un logiciel de surveillance ?

À partir de 150 salariés selon l'article L.414-9 du Code du travail, la délégation du personnel co-décide. La consultation est préalable et formalisée par procès-verbal avant le déploiement du dispositif.

Faut-il déclarer un logiciel de surveillance à la CNPD ?

Non, il n'y a plus de déclaration préalable depuis le RGPD. L'employeur applique le principe d'accountability : il est responsable de démontrer la conformité du traitement à tout moment via son registre et son AIPD.

La surveillance à l'insu des salariés est-elle autorisée au Luxembourg ?

Non, elle est prohibée. L'information individuelle et collective préalable est obligatoire. Une surveillance clandestine rend les preuves irrecevables et expose l'employeur à des sanctions administratives jusqu'à 4 % du CA mondial.

Quand l'AIPD est-elle obligatoire pour un logiciel de surveillance ?

L'AIPD est obligatoire dès que la surveillance présente un risque élevé pour les salariés (article 35 RGPD). À défaut d'AIPD, l'employeur doit documenter l'analyse de risque dans son registre des traitements.

Quelles sanctions pénales en cas de surveillance illicite des salariés ?

L'article L.261-2 du Code du travail prévoit 251 € à 125 000 € d'amende, applicables en sus des sanctions administratives RGPD. La nullité du dispositif entraîne celle des sanctions disciplinaires fondées.

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

Quelles sont les recommandations de la CNPD pour les logiciels de surveillance en entreprise au Luxembourg ?

Tout logiciel de surveillance doit reposer sur un intérêt légitime démontré, respecter la proportionnalité et la minimisation des données. La surveillance généralisée, permanente ou à l'insu des salariés est prohibée.

Conditions d’exercice

La CNPD considère présumée disproportionnée toute surveillance généralisée ou permanente : chaque dispositif doit être justifié individuellement par sa finalité et l'absence d'alternative moins intrusive.

Condition	Exigence
Intérêt légitime	Sécurité des biens et des personnes, prévention des infractions, protection des intérêts économiques
Nécessité	Aucun moyen moins intrusif ne permet d'atteindre la finalité
Proportionnalité	Périmètre, durée et données strictement limités au but poursuivi
Minimisation	Collecte des seules données indispensables (article 5(1)(c) RGPD)
Transparence	Information individuelle et collective préalable, jamais de surveillance à l'insu des salariés
Consultation	Délégation du personnel selon les seuils de l'article L.414-9

Modalités pratiques

L'AIPD est obligatoire dès que la surveillance présente un risque élevé pour les salariés ; à défaut, l'employeur doit documenter l'analyse de risque dans son registre.

Démarche	Précision
Analyse d'impact (AIPD)	Article 35 du RGPD, obligatoire si risque élevé
Registre des traitements	Article 30 du RGPD, finalités, durées, destinataires
Information individuelle	Notice écrite remise à chaque salarié : finalité, base légale, durée, droits
Consultation de la délégation	Préalable et formalisée par procès-verbal (article L.414-9)
Habilitation des accès	Liste nominative et traçabilité des consultations
Sécurité du traitement	Chiffrement, authentification, journalisation (article 32 RGPD)

Pratiques et recommandations

Limiter strictement le périmètre et la durée de la surveillance à ce qui est nécessaire à la finalité poursuivie.

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

Désactiver les dispositifs en dehors des heures d'activité lorsque la finalité ne justifie pas un fonctionnement continu.

Réévaluer périodiquement la pertinence et la proportionnalité du dispositif avec la délégation du personnel.

Documenter chaque consultation des données et chaque extraction utilisée à des fins probatoires.

Encadrer par contrat tout sous-traitant chargé du déploiement ou du visionnage (article 28 du RGPD).

Cadre juridique

Référence	Objet
Art. L.261-1 du Code du travail	Traitement de données pour surveillance des salariés (loi du 1er août 2018)
Art. L.414-9 du Code du travail	Co-décision de la délégation du personnel ? 150 salariés
Loi modifiée du 1er août 2018	Protection des données à caractère personnel
Règlement (UE) 2016/679 (RGPD)	Articles 5, 6, 12-13, 28, 30, 32, 35
Lignes directrices CNPD	Recommandations sur la cybersurveillance et la vidéosurveillance

La surveillance à l'insu des salariés ou sans information préalable rend les preuves irrecevables et expose l'employeur à des sanctions jusqu'à 4 % du chiffre d'affaires mondial. Les sanctions pénales de l'article L.261-2 (251 € à 125 000 €) restent applicables. La nullité du dispositif entraîne celle des sanctions disciplinaires fondées sur ses résultats.

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.