Comment sécuriser les données collectées lors de la surveillance des salariés ?

Réponse courte

L'employeur doit garantir la **confidentialité**, l'**intégrité** et la disponibilité des données issues de la surveillance par des mesures techniques et organisationnelles appropriées au risque (article 32 du RGPD applicable en entreprise). Cela impose le **chiffrement** des supports de stockage, l'**authentification forte** des accès, la journalisation des consultations et une habilitation nominative limitée aux fonctions strictement nécessaires.

La durée de conservation des images de vidéosurveillance est limitée à **8 jours** en principe et **30 jours maximum** avec justification documentée. Une **AIPD** est obligatoire pour les traitements à risque élevé (article 35 RGPD), un **registre des traitements** doit être tenu, et toute violation de données suivie d'un risque pour les salariés impose une notification à la **CNPD dans les 72 heures**.

Définition

La sécurisation des données de surveillance désigne l'ensemble des **mesures techniques et organisationnelles** que l'employeur met en œuvre pour protéger les informations issues de dispositifs de contrôle (vidéosurveillance, géolocalisation, logs informatiques, contrôle d'accès) contre tout accès non autorisé, perte, altération ou divulgation.

Ces mesures relèvent du principe d'**accountability** posé par le RGPD et la loi modifiée du 1er août 2018, qui impose au responsable de traitement de pouvoir démontrer la conformité du dispositif à tout moment.

Questions fréquentes

Combien de temps peut-on conserver les images de vidéosurveillance au Luxembourg ?

La conservation est limitée à 8 jours en principe et 30 jours maximum avec justification documentée. Au-delà, la durée doit être justifiée par une procédure judiciaire ou un incident de sécurité tracé.

Comment sécuriser les données collectées lors de la surveillance des salariés ?

L'employeur doit garantir confidentialité, intégrité et disponibilité par chiffrement, authentification forte, journalisation des consultations et habilitation nominative limitée aux fonctions strictement nécessaires (article 32 RGPD), avec mesures proportionnées au risque.

Que faire en cas de violation de données issues de la surveillance des salariés ?

Notifier la CNPD sous 72 heures (article 33 RGPD) et, en cas de risque élevé, informer les salariés concernés (article 34 RGPD). Chaque incident, mesure correctrice et notification doit être documenté.

Quelles sanctions pour défaut de sécurité des données de surveillance ?

L'absence de mesures appropriées est sanctionnée par la CNPD jusqu'à 10 millions € ou 2 % du chiffre d'affaires mondial (article 83 RGPD). Une violation non notifiée dans les délais aggrave la sanction.

Qui doit être désigné pour superviser la sécurité des données de surveillance ?

Un Délégué à la Protection des Données (DPO) doit être désigné pour le suivi et le dialogue avec la CNPD. Les personnes habilitées doivent être formées aux obligations de confidentialité et au signalement des incidents.

Une AIPD est-elle obligatoire pour un dispositif de surveillance des salariés ?

Oui, l'AIPD (article 35 RGPD) est obligatoire pour tout traitement à risque élevé. Elle doit être documentée, révisée à chaque modification et présentable à la CNPD lors d'un contrôle.

Conditions d’exercice

Les mesures de sécurité doivent être proportionnées au risque : un dispositif générant des données sensibles ou à fort volume exige un niveau de protection plus élevé qu'un simple contrôle d'accès.

Condition	Exigence
Confidentialité	Chiffrement au repos et en transit, authentification forte, cloisonnement réseau
Intégrité	Empreintes numériques, journalisation infalsifiable des accès et modifications
Disponibilité	Sauvegardes régulières, plan de continuité, restauration testée
Minimisation	Collecte limitée aux seules données nécessaires à la finalité (article 5 RGPD)
Habilitation	Liste nominative restreinte aux personnes dont la fonction le justifie

Modalités pratiques

Toute violation de données présentant un risque pour les droits des salariés doit être notifiée à la CNPD dans les 72 heures (article 33 RGPD) et, si le risque est élevé, communiquée aux salariés concernés (article 34 RGPD).

Démarche	Précision
Analyse d'impact (AIPD)	Obligatoire si risque élevé (article 35 RGPD), documentée et révisée
Registre des traitements	Article 30 RGPD : finalités, durées, destinataires, mesures de sécurité
Conservation des images	8 jours en principe, 30 jours maximum avec justification écrite
Habilitation des accès	Liste nominative et journalisation systématique des consultations
Sous-traitance	Contrat conforme à l'article 28 RGPD avec engagements de sécurité
Notification de violation	CNPD sous 72 heures, salariés si risque élevé (articles 33 et 34 RGPD)
Effacement à terme	Suppression irréversible à l'expiration de la durée de conservation

Pratiques et recommandations

Chiffrer systématiquement les supports de stockage et les flux de données, y compris les sauvegardes et les exports.

Restreindre les accès par authentification forte avec journalisation horodatée des consultations.

Former les personnes habilitées aux obligations de confidentialité et au signalement immédiat des incidents.

Auditer périodiquement la pertinence des habilitations et la conformité des mesures techniques mises en place.

Documenter chaque incident de sécurité, chaque consultation à des fins probatoires et chaque mise à jour de l'AIPD.

Désigner un délégué à la protection des données (DPO) chargé du suivi et du dialogue avec la CNPD.

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.261-2 du Code du travail	Sanctions pénales en cas de violation
Art. L.414-9 du Code du travail	Co-décision de la délégation du personnel pour les installations de contrôle
Loi modifiée du 1er août 2018	Protection des personnes à l'égard du traitement des données à caractère personnel
Art. 5, 28, 30, 32, 33, 34, 35 du RGPD	Principes, sous-traitance, registre, sécurité, notifications, AIPD
Lignes directrices CNPD	Recommandations techniques sur la sécurité des dispositifs de surveillance

L'absence de mesures de sécurité appropriées est sanctionnée par la CNPD jusqu'à 10 millions € ou 2 % du chiffre d'affaires mondial (article 83 RGPD). Une violation non notifiée dans les délais aggrave la sanction. Les preuves issues d'un dispositif insuffisamment sécurisé peuvent être déclarées irrecevables par le tribunal du travail.