Faut-il notifier la CNPD en cas de fuite de données issues du dispositif de surveillance ?

Réponse courte

Toute violation de données issues d'un dispositif de surveillance (vol d'images, fuite de logs, accès non autorisé aux enregistrements) doit être notifiée à la **CNPD dans les 72 heures** dès lors qu'elle présente un **risque pour les droits et libertés** des salariés concernés (article 33 du RGPD), conformément aux exigences de sécurité des données collectées. Les salariés doivent également être informés individuellement si la violation entraîne un **risque élevé** (article 34 du RGPD).

L'employeur tient un **registre interne des violations** documentant la nature de l'incident, ses conséquences et les mesures prises. L'absence de notification ou un retard injustifié constitue un manquement séparément sanctionné, indépendamment de la cause de la violation. Le délégué à la protection des données ou un référent doit être désigné pour piloter la procédure de notification.

Définition

Une **violation de données** désigne toute destruction, perte, altération ou divulgation non autorisée de données à caractère personnel, qu'elle soit accidentelle ou intentionnelle (article 4(12) du RGPD).

Pour les **données issues de la surveillance** (images de vidéosurveillance, logs de connexion, géolocalisation, enregistrements audio), la sensibilité est particulièrement élevée car ces données permettent de reconstruire le comportement et la présence des salariés.

Questions fréquentes

Faut-il informer les salariés en cas de fuite de données de surveillance ?

Oui, en cas de risque élevé, les salariés doivent être informés individuellement (article 34 RGPD). L'information doit être écrite, en termes clairs et concrets, particulièrement en cas de divulgation d'images ou de logs nominatifs.

Faut-il tenir un registre des violations de données ?

Oui, l'employeur tient un registre interne exhaustif documentant la nature de l'incident, ses conséquences et les mesures prises. Il est tenu indépendamment de la notification CNPD, même pour les incidents non notifiés, avec justification.

Qu'est-ce qu'une violation de données au sens du RGPD ?

Toute destruction, perte, altération ou divulgation non autorisée de données à caractère personnel, qu'elle soit accidentelle ou intentionnelle (article 4(12) du RGPD). Vol d'images, fuite de logs ou accès non autorisé aux enregistrements sont concernés.

Quel est le délai pour notifier une fuite de données à la CNPD au Luxembourg ?

L'employeur doit notifier la CNPD dans les 72 heures suivant la prise de connaissance de la violation (article 33 RGPD), dès lors qu'elle présente un risque pour les droits et libertés des salariés concernés.

Quel rôle joue le DPO en cas de fuite de données ?

Le DPO ou référent désigné pilote la procédure de notification, coordonne la réponse avec les équipes IT et juridique, qualifie l'incident et évalue le risque pour les droits des salariés. Il doit être accessible 24/7 pendant les périodes critiques.

Quelles sanctions en cas de retard de notification d'une violation à la CNPD ?

L'absence ou le retard de notification constitue un manquement autonome au RGPD, sanctionné jusqu'à 10 millions € ou 2 % du chiffre d'affaires mondial. Une notification tardive démontre une carence dans la gouvernance et alourdit la sanction.

Conditions d’exercice

Le délai de 72 heures court à compter de la prise de connaissance, pas de la survenance ; une notification au-delà oblige à motiver le retard, ce qui aggrave systématiquement la sanction CNPD.

Condition	Exigence
Détection	L'employeur a connaissance de la violation (interne ou signalement externe)
Risque pour les droits	Présomption de risque dès qu'il y a divulgation de données identifiantes
Délai 72 heures	Notification CNPD dans les 72 heures après la prise de connaissance
Risque élevé	Information individuelle des salariés concernés en cas de risque élevé
Documentation interne	Registre des violations tenu indépendamment de la notification
Notification immédiate du DPO	Dès la détection, le DPO ou référent pilote la réponse

Modalités pratiques

L'information individuelle des salariés est imposée dès qu'il y a risque élevé (divulgation d'images, fuite de logs nominatifs) ; le seul registre interne ne suffit pas dans ce cas.

Étape	Précision
Détection et qualification	Identification de l'incident et évaluation du risque pour les droits des salariés
Mobilisation du DPO	Pilotage de la réponse et coordination avec les équipes IT et juridique
Mesures conservatoires	Limitation immédiate de la diffusion, blocage des accès compromis, sécurisation
Notification CNPD	Formulaire en ligne sur le portail CNPD, dans les 72 heures, avec description de l'incident
Information des salariés	Communication écrite individuelle si risque élevé, en termes clairs et concrets
Registre interne	Inscription de l'incident, des causes, des conséquences et des mesures correctrices
Plan d'action correctif	Identification des failles et mise en œuvre des correctifs

Pratiques et recommandations

Préparer un plan de réponse aux violations de données avant tout incident, avec procédures écrites, contacts d'urgence et modèles de notification.

Désigner un DPO ou référent dédié comme point d'entrée unique pour toute alerte de violation, accessible 24/7 pendant les périodes critiques.

Former les administrateurs systèmes et les responsables hiérarchiques à reconnaître et signaler immédiatement une suspicion de fuite.

Tenir un registre des violations exhaustif même pour les incidents non notifiés à la CNPD, en justifiant l'absence de notification le cas échéant.

Documenter précisément la chronologie : moment de la détection, qualification, décision de notifier, envoi à la CNPD — pour démontrer la diligence en cas de contrôle.

Réexaminer annuellement les procédures de réponse à la lumière des incidents passés et des recommandations CNPD.

Cadre juridique

Référence	Objet
Art. 33 du RGPD	Notification à l'autorité de contrôle dans les 72 heures
Art. 34 du RGPD	Information individuelle des personnes concernées en cas de risque élevé
Art. 32 du RGPD	Sécurité du traitement
Art. 4(12) du RGPD	Définition de la violation de données
Loi modifiée du 1er août 2018	Procédure devant la CNPD
Lignes directrices CEPD 9/2022	Notification des violations sous le RGPD

L'absence ou le retard de notification CNPD constitue un manquement autonome au RGPD, sanctionné jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial. Une notification tardive démontre une carence dans la gouvernance des données et alourdit la sanction.