Quelle est la procédure à suivre en cas de violation de données personnelles par l'employeur au Luxembourg ?

Réponse courte

En cas de **violation de données personnelles**, l'employeur doit immédiatement **détecter**, **qualifier** et **consigner** l'incident dans un **registre interne** détaillant la nature de la violation, les catégories de données et de personnes concernées, les conséquences probables et les mesures prises. Il doit ensuite **évaluer le risque** pour les droits et libertés des personnes.

Si le risque pour les personnes est avéré, l'employeur doit **notifier la CNPD dans un délai maximal de 72 heures** à compter de la découverte de la violation, conformément à l'**article 33 du RGPD**. Si le risque est **élevé**, il doit également **informer** les personnes concernées dans les meilleurs délais (art. 34 RGPD). Toute violation, même non notifiée, doit être **documentée** dans un registre dédié, consultable par la CNPD.

Définition

Une **violation de données** est définie par l'article 4.12 du RGPD comme « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la **destruction**, la **perte**, l'**altération**, la **divulgation** non autorisée de données à caractère personnel transmises, conservées ou traitées, ou l'**accès** non autorisé à de telles données ». Les violations incluent les cyberattaques, les pertes de support, les envois erronés et les accès frauduleux.

Questions fréquentes

Dans quel délai notifier une violation à la CNPD ?

L'article 33 du RGPD impose une notification à la CNPD dans un délai maximal de 72 heures à compter de la découverte de la violation, lorsque celle-ci présente un risque pour les droits et libertés des personnes concernées.

Faut-il documenter même les violations sans risque ?

Oui, toute violation, même non notifiée, doit être documentée dans un registre interne dédié, consultable par la CNPD. Le registre précise la justification de l'absence de notification, conformément au principe d'accountability.

Faut-il toujours informer les salariés d'une violation ?

Non, l'information directe des personnes (article 34 RGPD) n'est obligatoire qu'en cas de risque élevé. Pour un risque simple, seule la notification à la CNPD est requise. En l'absence de risque, seule l'inscription au registre interne suffit.

Qu'est-ce qu'une violation de données selon le RGPD ?

L'article 4.12 du RGPD définit une violation comme une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé à des données personnelles, qu'elle soit accidentelle ou illicite.

Quelle procédure suivre en cas de violation de données ?

L'employeur doit immédiatement détecter, qualifier et consigner l'incident dans un registre interne, évaluer le risque pour les personnes, puis notifier la CNPD dans les 72 heures si le risque est avéré, conformément à l'article 33 du RGPD.

Quelle sanction en cas de défaut de notification ?

L'absence de notification dans les 72 heures, lorsqu'elle est requise, constitue une violation sanctionnée par la CNPD jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial. Une notification par excès de prudence est recommandée en cas de doute.

Qui doit notifier en cas de violation impliquant un sous-traitant ?

Le sous-traitant doit notifier immédiatement le responsable de traitement (employeur), qui reste seul compétent pour notifier la CNPD dans les 72 heures. Le contrat article 28 doit prévoir un délai contractuel court (24 à 48 heures).

Conditions d’exercice

L'article 33 du RGPD impose la notification à la CNPD sous 72 heures en cas de risque pour les droits, l'article 34 exige l'information des personnes en cas de risque élevé, tandis que les violations sans risque ne nécessitent qu'une inscription au registre interne.

Niveau de risque	Obligations
Absence de risque	Documentation dans le registre interne uniquement
Risque pour les droits	Notification à la CNPD sous 72 heures
Risque élevé	Notification CNPD + information des personnes concernées
Violation continue	Mesures immédiates de mitigation et de contention
Sous-traitant impliqué	Notification immédiate du responsable de traitement
Données sensibles	Vigilance renforcée et expertise du DPO

Modalités pratiques

Dès la détection d'une violation, l'employeur dispose de 72 heures pour notifier la CNPD via le formulaire en ligne (art. 33 RGPD), après avoir qualifié l'incident, contenu ses effets et évalué le risque pour les personnes.

Étape	Détail
Détection	Identification de l'incident par tout moyen (monitoring, alerte)
Qualification	Vérification qu'il s'agit bien d'une violation au sens du RGPD
Contention	Mesures immédiates pour limiter l'impact
Analyse de risque	Évaluation de l'impact pour les droits des personnes
Notification CNPD	Formulaire en ligne dans les 72 heures
Information personnes	Communication claire en cas de risque élevé
Registre des violations	Consignation complète, même en l'absence de notification
Retour d'expérience	Analyse post-incident et mesures correctives

Pratiques et recommandations

Établir un plan de réponse aux incidents (Incident Response Plan) intégrant la détection, la qualification, la contention et la notification, avec des rôles clairement définis.

Former les équipes à détecter et à signaler rapidement toute suspicion de violation, en instaurant une culture de la transparence en interne.

Tester régulièrement la procédure par des exercices de simulation pour vérifier la capacité de l'entreprise à respecter le délai de 72 heures.

Notifier la CNPD même en cas de doute sur l'existence d'une violation, car l'absence de notification d'une violation significative est lourdement sanctionnée.

Conserver dans le registre interne l'ensemble des violations, y compris celles non notifiées, en précisant la justification de l'absence de notification.

Cadre juridique

Le cadre juridique des violations de données repose sur le RGPD et la loi luxembourgeoise.

Référence	Objet
Art. 4.12 RGPD	Définition de la violation de données
Art. 33 RGPD	Notification à l'autorité de contrôle
Art. 34 RGPD	Communication à la personne concernée
Art. 32 RGPD	Sécurité du traitement
Loi du 1er août 2018	Régime général au Luxembourg
Lignes directrices CEPD 9/2022	Notification des violations
Art. L.261-1 Code du travail	Surveillance des salariés

L'absence de notification dans les 72 heures, lorsqu'elle est requise, constitue une violation sanctionnée par la CNPD jusqu'à **10 millions d'euros ou 2 % du chiffre d'affaires mondial**. Les notifications sont effectuées via le formulaire en ligne disponible sur le site de la CNPD.