Comment documenter un incident de sécurité informatique en télétravail ?

Réponse courte

En cas d'incident de sécurité informatique en télétravail, l'employeur doit **documenter** l'événement de manière exhaustive et, si des données personnelles sont concernées, **notifier** la CNPD dans un délai de **72 heures** conformément au RGPD. La procédure de documentation doit être formalisée dans la politique de sécurité de l'entreprise et intégrée à l'avenant de télétravail, comme précisé dans la fiche sur responsabilité en cas de piratage de données au domicile.

Définition

Un **incident de sécurité informatique** en télétravail désigne tout événement compromettant la confidentialité, l'intégrité ou la disponibilité des données professionnelles traitées depuis le domicile du salarié : intrusion, vol de matériel, perte de données, ransomware, hameçonnage ou accès non autorisé aux systèmes de l'entreprise, comme précisé dans la fiche sur règles de protection des données en télétravail frontalier.

Conditions d'exercice

La documentation d'un incident doit couvrir les éléments suivants.

Élément à documenter	Description
Date et heure	Moment précis de la découverte de l'incident
Nature de l'incident	Type de menace ou de violation identifié
Données concernées	Catégories et volume de données potentiellement affectées
Mesures prises	Actions immédiates de containment et de remédiation
Impact estimé	Évaluation des conséquences pour les personnes concernées

Modalités pratiques

L'employeur doit suivre la procédure suivante.

Élément	Détail
Isoler le système	Demander au salarié de déconnecter l'équipement affecté
Notifier le service IT	Signaler l'incident au responsable de la sécurité informatique
Rédiger un rapport	Documenter l'incident selon le modèle préétabli
Évaluer la notification	Déterminer si une notification CNPD est requise (violation de données)
Notifier la CNPD	Si applicable, notifier dans les 72 heures (art. 33 RGPD)
Informer les personnes	Si risque élevé, informer les personnes concernées (art. 34 RGPD)

Pratiques et recommandations

Il est recommandé de **préparer** un modèle de rapport d'incident adapté au contexte du télétravail et de le communiquer à tous les salariés. L'employeur doit **former** les télétravailleurs frontaliers aux gestes de premier secours numériques et **tester** régulièrement la procédure de réponse aux incidents. La tenue d'un **registre des incidents** permet d'analyser les tendances et d'améliorer la prévention.

Cadre juridique

Référence	Objet
Règlement (UE) 2016/679 (RGPD), art. 33-34	Notification des violations de données
Art. L.261-1 du Code du travail	Protection des données des salariés
Loi du 1er août 2018	Organisation de la CNPD
Convention du 20 octobre 2020	Sécurité informatique en télétravail
Art. L.312-1 du Code du travail	Obligation de sécurité de l'employeur

Le défaut de notification d'une violation de données à la CNPD dans les 72 heures expose l'employeur à des sanctions pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial. La documentation précise de l'incident est essentielle pour démontrer la conformité au RGPD.