6. NOTIFICATION DES VIOLATIONS DE DONNEES PERSONNELLES

En cas d'incident de sécurité impactant des données personnelles, **l'entreprise doit notifier cette violation à la CNIL et alerter les personnes concernées dans certains cas**. Cette obligation imposée par le RGPD s'applique aux responsables de traitements. **Les sous-traitants**, quant à eux, **doivent notifier au responsable du traitement toute violation de données personnelles** afin d'aider le responsable à remplir son obligation de notification.

Qu'est-ce qu'une violation de données personnelles ?
C'est un incident de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises ou encore l'accès non autorisé à de telles données.

1. Quand notifier une violation de données personnelles à la CNIL ? (Article 33)

Le responsable de traitement doit notifier une violation de données personnelles à la CNIL **lorsqu'elle est susceptible de porter atteinte aux personnes concernées**.
Cette notification doit intervenir **dans les 72 heures de la découverte de l'incident**. Le délai commence à courir à partir du moment où le responsable est certain qu'un incident de sécurité s'est produit et que des données personnelles ont été impactées.

Il ne faut toutefois pas que ce délai révèle une négligence de la part du responsable de traitement.

2. Quelles informations faut-il donner à la CNIL ?

Le responsable du traitement doit communiquer au moins :	➢ La description de la nature de la violation y compris, si possible, les catégories et le nombre approximatif de personnes concernées ; ➢ Le nom et les coordonnées du référent ou point de contact auprès duquel des informations supplémentaires peuvent être obtenues ; ➢ La description des conséquences probables de la violation ; ➢ La description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

La CNIL mettra à disposition un formulaire de notification des violations de données personnelles.

S'il n'est pas possible de fournir l'ensemble des informations nécessaires dans les 72h, **ces informations peuvent être communiquées de manière échelonnée**.

3. Quand informer la personne concernée de la violation de ses données ? (Article 34)

Lorsqu'une violation de données personnelles peut avoir des **conséquences graves pour les personnes physiques** (par exemple une usurpation d'identité, une perte financière ou une atteinte à la réputation), le responsable du traitement doit informer la personne d'une telle violation dans les meilleurs délais.

Le responsable du traitement doit au moins communiquer, **en des termes clairs et simples** :	➢ La nature de la violation ; ➢ Le nom et les coordonnées du délégué à la protection des données ou d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues ; ➢ La description des conséquences probables de la violation ;

- La description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Sauf si la CNIL l'exige, le responsable de traitement n'est pas obligé d'informer les personnes concernées de la violation de leurs données lorsque :

- ✓ il a mis en œuvre les mesures de protection appropriées pour les données concernées (comme le chiffrement) ; ou
- ✓ il a pris des mesures ultérieures pour empêcher le risque de se produire ; ou
- ✓ l'information exigerait des efforts disproportionnés (dans ce cas, il peut être procédé à une communication publique ou à une mesure similaire afin d'informer les personnes concernées)

4. Quelles sont les autres autorités à qui je dois notifier ces incidents de sécurité ?

En cas d'incident de sécurité informatique, le responsable de traitement peut être amené à notifier l'incident simultanément à plusieurs autorités :

AUPRES DE LA CNIL :

- En cas de violation de données personnelles (RGPD) ;
- Pour les opérateurs de communication électronique (directive ePrivacy)

AUPRES DE L'ANSSI :

- Pour les opérateurs de communication électronique (directive « Paquet Télécom ») ;
- Pour les opérateurs d'importance vitale (OIV – Loi de programmation militaire) ;
- Pour les opérateurs de service essentiel (OSE – directive NIS) ;
- Pour les prestataires de services de confiance (règlement eIDAS)

AUPRES DE l'ARS : (Agence Régionale de Santé)

- En cas d'atteinte aux systèmes d'information du secteur de la santé (loi de modernisation du système de santé)