Notifier une violation de données personnelles

24 mai 2018

Le règlement général sur la protection des données (RGPD) impose aux responsables de traitement de documenter, en interne, les violations de données personnelles et de notifier les violations présentant un risque pour les droits et libertés des personnes à la CNIL et, dans certains cas, lorsque le risque est élevé, aux personnes concernées.

Qu'est-ce qu'une violation de données à caractère personnel ?

Pour qu'il y ait violation, 2 conditions doivent être réunies :

1. Vous avez mis en œuvre un traitement de données personnelles.
2. Ces données ont fait l'objet d'une violation (perte de **disponibilité**, **d'intégrité** ou de **confidentialité** de données personnelles, de manière **accidentelle** ou **illicite**).

Que faire en cas de violation ?

Dans **tous les cas**, vous devez documenter en interne l'incident en déterminant :

- la nature de la violation
- si possible, les catégories et le nombre approximatif de personnes concernées par la violation
- les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
- décrire les conséquences probables de la violation de données ;
- décrire les mesures prises ou que vous envisagez de prendre pour éviter que cet incident se reproduise ou atténuer les éventuelles conséquences négatives.

Le document récapitulatif de votre notification à la CNIL permet de répondre à l'obligation de documentation interne.
Si l'incident constitue un **risque** au regard de la vie privée des personnes concernées, vous devrez notifier l'incident à la CNIL.
En cas de **risque élevé**, vous devez également notifier les personnes concernées.

En cas de doute, notifiez à la CNIL qui vous indiquera s'il est nécessaire d'informer les personnes.

Dans quel délai notifier ?

La notification doit être transmise à la CNIL dans les meilleurs délais à la suite de la constatation d'une violation présentant un risque pour les droits et libertés des personnes.
Si vous ne pouvez pas fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, vous pouvez procéder à une notification en deux temps :

1. **Une notification initiale dans les meilleurs délais** à la suite de la constatation de la violation ;
2. Puis, **une notification complémentaire dans le délai de 72 heures si possible** après la notification initiale.
3. Si le **délai de 72 heures est dépassé, il conviendra d'expliquer**, lors de votre notification, **les motifs du retard.**

Comment notifier ?

Utilisez le télé service de notification de violations : *Démarrer une notification*

Que va faire la CNIL ?

Dès réception, la CNIL va instruire la notification. La procédure relative à la violation notifiée pourra être clôturée si la CNIL constate que :

- La violation ne porte pas atteinte aux données personnelles ou ne présente pas de risque pour les droits et libertés des personnes.
- Vous avez correctement informé les personnes concernées.
- Vous avez mis en place, préalablement à la violation, des mesures techniques de protection appropriées.

La CNIL pourra vous imposer d'informer les personnes concernées si elle constate que :

- Vous ne les avez pas correctement informées.
- Les mesures techniques de protection que vous avez mises en place préalablement à la violation ne sont pas appropriées.

Quel est le cadre légal ?

L'obligation de notifier à la CNIL les violations de données à caractère personnel est prévue à l'article 33 du règlement général sur la protection des données (RGPD). Elle concerne tous les responsables de traitement de données à caractère personnel. Dans le cas où la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, l'article 34 du RGPD impose de notifier ces dernières.