MANDIL AVOCATS

Les violations de données personnelles

Fiche n°08 - Février 2020

Le RGPD impose aux entreprises qui traitent des données personnelles de mettre en œuvre des mesures globales de sécurité visant à :

- **prévenir toute violation de données personnelles ;**
- **mettre fin à la violation et minimiser ses effets ;**
- **Notifier les violations de données personnelles.**

A savoir

Qu'est-ce qu'une violation de données personnelles ?

Il s'agit d'une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles, ou l'accès non autorisé à ces données. Exemples :

- suppression accidentelle de données bancaires ou de santé non sauvegardées par ailleurs ;
- perte d'une clef USB non sécurisée contenant une copie de la base clients d'une société ;
- introduction malveillante dans une base de données et modification des informations qui y sont stockées.

I. Prévenir et minimiser une violation de données personnelles

Les organismes qui traitent des données personnelles doivent mettre en œuvre des **mesures physiques, logiques et organisationnelles** appropriées de manière à prévenir les violations de données personnelles et à minimiser les effets de toute éventuelle violation :

1 **Certaines mesures concernent la sécurité des supports des traitements (matériels, logiciels, canaux de communication, supports papiers…) : gestion des accès, antivirus, sécurité des locaux, gouvernance…**

2 **D'autres mesures s'appliquent directement aux données traitées. Exemples :**

Anonymisation

Le recours (facultatif) à l'anonymisation irréversible des données permet de ne plus traiter de données personnelles. Pour cela :

- aucune mesure technique ne doit permettre de ré-identifier les individus ; ET
- il doit être impossible de déduire directement ou indirectement (via les données d'un tiers) l'identité d'un individu.

Exemples : altérer la véracité des données afin d'empêcher tout lien entre ces données et un individu, agréger les données de manière suffisamment importante…

Minimisation

Le RGPD prévoit que seules les données personnelles adéquates, pertinentes et limitées à ce qui est nécessaire pour atteindre les finalités prévues (LCLF, gestion du personnel…) doivent être collectées et conservées.

Exemples :

- ne pas collecter d'informations concernant les opinions politiques ou religieuses de clients dans un CRM.
- ne pas conserver 20 ans des données collectées uniquement à des fins de LCB/FT puisque l'obligation légale de les conserver n'est que de 5 ans.

Pseudonymisation

Le recours à la pseudonymisation doit être mis en œuvre dès que possible.

Cette mesure consiste à remplacer un attribut par un autre de telle façon que les données personnelles ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires.
L'identification indirecte est en théorie toujours possible mais le risque de mise en corrélation d'un ensemble de données avec un individu est réduit.

Exemples : chiffrement, hachage, tokenisation…

II. Notifier les violations de données personnelles

En cas de violation, le RGPD prévoit une notification sur trois niveaux qui dépend de la **gravité du risque pour les droits et libertés des personnes concernées** :

Pour les personnes concernées, la violation engendre :	aucun risque	un risque	un risque élevé
Documentation dans le registre interne des violations (à la disposition de la CNIL)	OUI	OUI	OUI
Notification à la CNIL, dans un délai maximal de 72h (motivation en cas de retard)	-	OUI	OUI
Information des personnes concernées (dans la mesure du possible de manière individuelle) dans les meilleurs délais	-	-	OUI

1. Comment apprécier l'absence de risque, le risque et le risque élevé ?

Cette appréciation doit être faite au cas par cas et doit tenir compte des éléments suivants :

- le type de violation (affectant l'intégrité, la confidentialité ou la disponibilité des données) ;
- la nature, la sensibilité et le volume des données personnelles concernées ;
- la facilité d'identifier les personnes touchées par la violation ;
- les conséquences possibles de celles-ci pour les personnes;
- les caractéristiques de ces personnes (enfants, personnes vulnérables, etc.) ;
- le volume de personnes concernées ;
- les caractéristiques du responsable du traitement (nature, rôle, activités).

Exemples de situations dans lesquelles il pourrait ne pas y avoir de risque justifiant une notification à la CNIL et / ou aux personnes concernées :

La divulgation de données déjà rendues publiques	La suppression de données sauvegardées et immédiatement restaurées
Des mots de passe d'employés ayant accès à une base de données sensibles ont été subtilisés, mais n'ont pas été utilisés et ont été réinitialisés	La perte de données protégées par un algorithme de chiffrement à l'état de l'art, si la clé de chiffrement n'est pas compromise et si une copie des données reste disponible

2. Quel est le point de départ du délai de notification

Le point de départ de la notification court dès lors que le responsable du traitement acquiert un degré de certitude raisonnable qu'un incident a eu lieu et a touché des données personnelles. Cela implique :

- Qu'il ait mis en place des mesures de détection des violations des données
- Qu'il mène au plus tôt des investigations permettant d'atteindre une telle certitude raisonnable

3. Quel est le rôle des sous-traitants en cas de violation de données ?

Le sous-traitant doit notifier au responsable du traitement toute violation de données **dans les meilleurs délais** après en avoir pris connaissance afin que le responsable du traitement puisse s'acquitter de ses obligations.

Le responsable du traitement peut également demander contractuellement au sous-traitant d'agir en son nom afin que ce dernier notifie directement la violation à la CNIL et aux personnes concernées.