

RGPD

Violation de données personnelles : quelle démarche ?

CONTEXTE

La violation de données à caractère personnel est caractérisée par la perte de disponibilité, d'intégrité ou de confidentialité d'un traitement contenant des données personnelles, et ceci de manière accidentelle ou illicite.

Dans cette situation, le RGPD (Règlement Général sur la Protection des Données) impose aux responsables de traitement :

- de documenter, en interne, les violations de données personnelles.
- de notifier, sans attendre, à la CNIL, les violations présentant un risque d'impact sur la vie privée des personnes ainsi qu'à la ou aux personne(s) concernée(s) lorsque le risque est élevé.

COMMENT PROCEDER ?

I - Constater la violation des données personnelles

Immédiatement :

II - Informer le Délégué à la protection des données

III - Rechercher l'origine de la violation : sa nature, les catégories et le nombre approximatif de personnes concernées, les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés, les conséquences probables de la violation de données.

IV - décrire les mesures prises ou envisagées pour corriger, atténuer ou éviter que cet incident se reproduise.

V - Evaluer l'échelle des risques et/ou impact de la violation.

L'ensemble de ces éléments constitue l'obligation de tenir une documentation interne.

Dans un délai de 72h maximum :

VI - Notifier à l'autorité de contrôle CNIL via le formulaire en ligne sur le site www.cnil.fr

VII - Si les risques sont élevés, notifier aux personnes concernées.

En cas de dépassement de ce délai, vous devrez expliquer, les motifs de ce retard auprès de la CNIL.

Ceci constitue l'obligation de notification auprès de l'organisme de contrôle CNIL.

CONSEQUENCE

Dès réception, la CNIL va instruire la notification.

La CNIL clôturera la procédure relative à la violation notifiée si elle 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.

A défaut, la CNIL pourra vous imposer de :

- Informer les personnes concernées si vous ne les avez pas correctement informées.
- Mettre en place des mesures techniques de protection si elles n'ont pas été prévues préalablement à la violation ou que celles mises en œuvre ne sont pas appropriées.

REFERENCES

Règlement n° 2016/679 du 27 avril 2016 – art. 33 & 34

Loi 78-17 du 6 janvier 1978, modifiée – art. 58, 83 – et son décret d'application 2019-536 du 29 mai 2019.

CONTACT/INFORMATION

Délégué à la protection des données
2, rue François Arago – 61250 Valframbert
0233804811
rgpd@cdg61.fr
www.cdg61.fr

Copyright et Exclusion de responsabilité :

Les logos figurant dans ce document sont de la propriété du Centre de gestion de la Fonction publique territoriale de l'Orne.

Nous apportons le plus grand soin à la sélection et la rédaction des informations contenues dans nos publications. Ces informations sont cependant fournies "en l'état", sans garantie d'aucune sorte, expresse ou implicite. L'utilisateur assume l'ensemble des risques découlant de l'utilisation de ces informations toutes confondues.