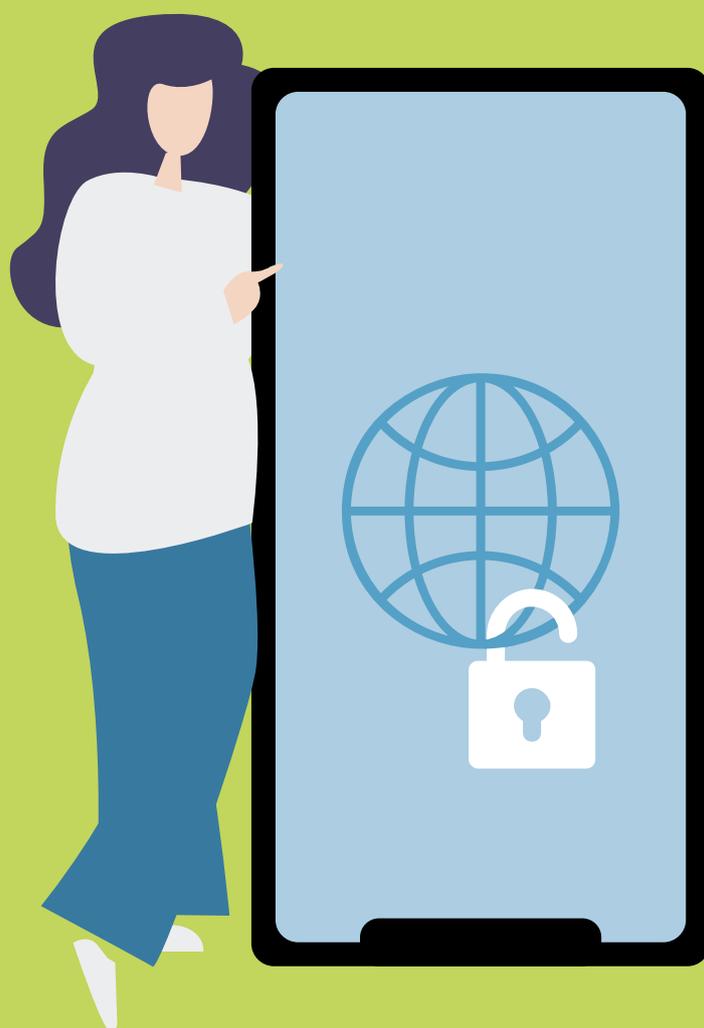


RGPD



Les Actus

Mars - Mai 2024

● 6ème anniversaire du RGPD : où en êtes-vous dans votre conformité ?

Entré en vigueur le 25 mai 2018, le RGPD fête cette année ses 6 ans.

Créé dans un contexte d'évolution technologique et sociétale (développement du commerce en ligne notamment), et dans la continuité de la Loi Informatique et Libertés de 1978, le RGPD permet d'harmoniser les règles en Europe en matière de protection des données personnelles et d'offrir un cadre juridique unique aux professionnels. Tout organisme, public ou privé, est soumis aux règles du RGPD.

La mise en conformité au RGPD est l'occasion de revoir et d'améliorer ses pratiques en matière de traitement de données personnelles (Cf. notre article du 16/03/2023 à [ce lien](#)).

Petite liste de choses à faire pour votre mise en conformité :

- Rédiger le registre des traitements
- Mettre à jour les formulaires
- Rédiger les mentions d'information RGPD
- Encadrer les relations avec les prestataires (logiciels...)
- Mettre en place des mesures de sécurité adéquates
- Réaliser les analyses d'impact le cas échéant
- Gérer les demandes de droit d'accès
- Gérer les violations de données



Et vous, combien de cases avez-vous cochées ?

● La CNIL publie le premier bilan de 5 années de violations de données

Suppression accidentelle de données, perte ou vol de matériel informatique, piratage de messagerie ou incendie détruisant le local des archives ne sont que quelques exemples de violations de données. Incident de sécurité d'origine malveillante ou non, se produisant de manière intentionnelle ou non, la violation de données compromet l'intégrité, la confidentialité ou la disponibilité des données personnelles.

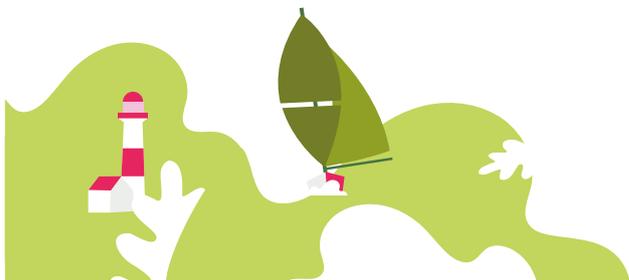
Depuis l'entrée en vigueur du RGPD, les violations de données doivent être notifiées à la CNIL **dans les 72 heures dès qu'il existe un risque pour les droits et libertés des personnes concernées**. Dans certains cas la violation devra être également notifiée aux personnes concernées.

La CNIL a publié le 27 mars 2024 le premier bilan des violations de données de ces 5 dernières années. Il en ressort que :

- 17 483 violations de données ont été notifiées à la CNIL ;
- Les administrations publiques représentent 18% de ces notifications ;
- Plus de la moitié des violations sont dues à du piratage : les rançongiciels tout d'abord qui touchent plutôt le secteur privé et ensuite l'hameçonnage qui concerne davantage le secteur public ;
- Les équipements volés ou perdus, les envois indus et les publications non volontaires sont les autres violations de données les plus fréquemment notifiées ;
- L'Île-de-France est la région la plus touchée avec environ 7500 notifications, en raison de la forte densité économique de ce territoire, suivie des Hauts-de-France et de l'Auvergne-Rhône-Alpes qui comptent entre 800 et 1200 notifications pour chaque région. La Bretagne quant à elle fait partie des régions qui comptent entre 200 et 800 notifications.

Pour répondre à ses obligations de sécurité et ainsi se prémunir des violations de données en constante évolution, le responsable de traitement est tenu de prendre toutes les mesures nécessaires pour protéger les données personnelles qu'il détient.

-> En cas de violation de données, contactez votre délégué à la protection des données.



● Guide de sécurité de la CNIL : de nouvelles fiches pour répondre aux évolutions

La CNIL a restructuré son guide de sécurité et y a intégré des nouvelles fiches : Intelligence artificielle, applications mobiles, informatique en nuage (cloud) et interfaces de programmation applicative (API). Pour faire face aux évolutions et aux -nouvelles- menaces pesant sur les données personnelles détenues par les responsables de traitement, la CNIL propose au travers de ce guide, les précautions élémentaires à mettre en œuvre et les mesures permettant de renforcer la protection des données.

Le lien vers le guide de la CNIL est disponible dans la rubrique « Pour en savoir plus ».

● Sanctions : la CNIL accélère la cadence

Avec sa procédure simplifiée, la CNIL a déjà prononcé 15 sanctions depuis le début de l'année*, représentant un montant total de 98500 euros, contre 24 sanctions pour l'année 2023.

On pourra citer parmi les principaux manquements retenus, un défaut de coopération avec la CNIL, un défaut de sécurité des données et un non-respect des droits des personnes.

Un organisme a également été sanctionné pour n'avoir pas associé son délégué à la protection des données aux questions relatives à la protection des données et à la sécurité des systèmes d'information, ni informé ses employés des coordonnées et des missions de celui-ci.

Mise en œuvre depuis 2022, la procédure simplifiée permet à la CNIL d'agir plus rapidement pour faire face aux plaintes de plus en plus nombreuses (plus de 12000 en 2022 et plus de 16000 en 2023). Pour les dossiers ne présentant pas de difficultés particulières, la CNIL peut ainsi prononcer une amende d'un montant maximum de 20000€, une injonction avec astreinte plafonnée à 100€ par jour de retard ou un rappel à l'ordre.

* Données au 12 mars 2024

● Focus : le délégué à la protection des données

Souvent qualifié de chef d'orchestre de la mise en conformité au RGPD, le délégué à la protection des données reste encore assez méconnu. Petit focus sur cet acteur majeur du RGPD.

Les missions du délégué à la protection des données

Multiplées et variées, les principales missions du délégué à la protection des données sont énumérées à l'article 39 du RGPD :

- informer et conseiller le responsable de traitement ainsi que le personnel qui procède aux traitements de données personnelles ;
- contrôler le respect du RGPD en matière de protection des données et des règles internes du responsable de traitement ;
- sensibiliser et former le personnel participant aux opérations de traitement ;
- dispenser des conseils, sur demande, en ce qui concerne la réalisation d'analyses d'impact et en vérifier l'exécution ;
- coopérer avec l'autorité de contrôle ;
- être le point de contact de l'autorité de contrôle et des personnes concernées par un traitement de données.



Les moyens du délégué à la protection des données

Le délégué à la protection des données doit être associé à toutes les questions relatives à la protection des données personnelles, notamment avant la mise en œuvre de tout nouveau traitement de données.

Désignation d'un délégué à la protection des données

La désignation est en principe facultative sauf pour les autorités ou organismes publics qui sont dans l'obligation de désigner un délégué à la protection des données.

● Pour en savoir plus

Bilan de la CNIL relatif aux violations des données

<https://www.cnil.fr/fr/violations-de-donnees-personnelles-bilan-de-5-annees-de-rgpd#:~:text=Sans%20motif%20l%C3%A9gitime%2C%20le%20non,%25%20du%20chiffre%20d'affaires>

Guide de sécurité de la CNIL

<https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles-nouvelle-edition-2024>

Sanctions de la CNIL dans le cadre de la procédure simplifiée

<https://www.cnil.fr/fr/la-cnil-prononce-quinze-nouvelles-sanctions-dans-le-cadre-de-la-procedure-simplifiee-depuis-janvier>

Délégué à la protection des données

<https://www.cnil.fr/fr/le-delegue-la-protection-des-donnees-dpo>



Service protection des Données

Direction Développement Numérique
et Assistance Métiers

02 96 58 63 66
cil@cdg22.fr