ARTICLE

RETOUR SUR L'ACTUALITÉ RÉCENTE DE LA CNIL EN MATIÈRE DE SÉCURITÉ DES DONNÉES : QUE FAUT-IL RETENIR ?

IT et données personnelles | 28/03/24 | Florence Chafiol Alexandra Antalis

> La CNIL dresse un bilan chiffré des violations de données qui lui ont été notifiées ces dernières années

Liens vers les bilans :
https://www.cnil.fr/fr/violations-de-donnees-personnelles-bilan-de-5-annees-de-rgpd
https://www.cnil.fr/sites/cnil/files/2024-03/cnil_plaquette_cybersecurite_vd_version_web_0.pdf

La sécurité des données est un enjeu majeur en matière de protection des données. La CNIL vérifie quasiment systématiquement lors de ses contrôles les mesures de sécurité mises en œuvre par les organismes et notamment (i) leur politique de mots de passe (à noter que cette dernière doit être conforme avec la délibération n° 2022-100 du 21 j uillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés), (ii) la sécurisation des bases de données et du réseau et (iii) l'existence d'un registre de violations des données (conformément à l'obligation prévue à l'article 33, paragraphe 5 du RGPD). **En 2023, un tiers des sanctions prononcées par la CNIL visait des manquements à l'obligation de sécurité des données personnelles**.

Les chiffres à retenir :

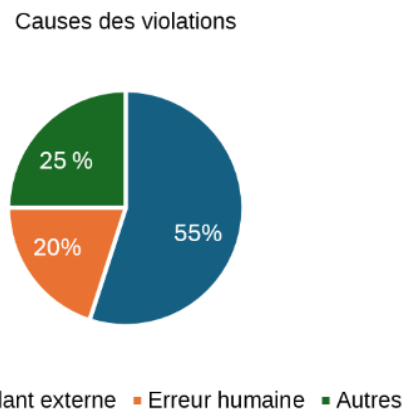
- **17 483 notifications de violations de données reçues** depuis l'entrée en vigueur du RGPD jusqu'en mai 2023, ce chiffre étant en constante augmentation (4 668 notifications en 2023 et 4 088 en 2022).

A noter cependant que ce chiffre ne reflète qu'une partie des incidents de sécurité qui se produisent en France puisqu'il ne concerne que les incidents de sécurité pour lesquels (i) les entreprises ont fait le choix de procéder à une notification à la CNIL, (ii) impliquant des données personnelles et (iii) étant susceptibles d'engendrer un risque pour les personnes concernées (conditions de l'obligation de notification à la CNIL).

- **Les deux tiers de ces notifications proviennent du secteur privé** avec en tête les activités qui traitent une quantité importante de données personnelles, à savoir (i) les activités spécialisées (terme utilisé par la CNIL sans autre explication), scientifiques et techniques, (ii) les activités financières et d'assurance et (iii) les activités en lien avec la santé humaine.

- **La moitié de ces notifications est liée à un piratage** (en 2023, cela représentait 60% du total des notifications adressées) avec en tête les **rançongiciels** (en 2023, cela représentait 22% du total des notifications adressées), puis les **attaques par hameçonnage**.

Les autres sources de violation des données les plus fréquentes sont les équipements perdus ou volés, les envois indus et les publications non volontaires.
La sensibilisation des employés aux enjeux de sécurisation des données personnelles est donc primordiale.



- **La moitié des violations est constatée en moins de 10 heures à compter de la survenance**.

- **La moitié des notifications est réalisée par les organismes 72 heures au plus tard après en avoir pris connaissance** (ce délai est celui prévu à l'article 33, paragraphe 1 du Règlement général sur la protection des données).

- **La conséquence la plus fréquente des violations notifiées est la perte de la confidentialité des données** (intrusion par un tiers qui prend connaissance des données et peut éventuellement les copier).

La CNIL considère qu'il est préférable de notifier la violation dans le délai de 72 heures même si l'organisme ne dispose pas de tous les éléments et de compléter la notification voire même de la supprimer (dans le cas où la violation n'est finalement pas avérée) par la suite. Pour ce faire, le formulaire de notification en ligne de la CNIL propose deux options :

- *La notification initiale* qui permet de répondre à l'ensemble des questions du formulaire tout en ayant la possibilité de compléter ou modifier les réponses en réalisant par la suite une notification complémentaire / modifiée, et
- *La notification complète* qui permet de répondre de manière définitive à l'ensemble des questions du formulaire. Elle doit être choisie lorsque le responsable du traitement dispose de l'ensemble des informations qui doivent être portées à la connaissance de la CNIL ce qui est rarement le cas lorsque la violation vient d'être découverte.

A la suite d'une notification d'une violation, il peut arriver que la CNIL prenne contact avec l'organisme pour vérifier que des mesures ont été prises préalablement et / ou postérieurement à la violation et pour recommander le cas échéant à l'organisme d'informer les personnes de la survenance de la violation. En effet, dans le traitement des notifications, la CNIL indique qu'elle privilégie un accompagnement des acteurs.

> La CNIL met à jour son guide de la sécurité des données personnelles

Lien vers le guide :
https://www.cnil.fr/sites/cnil/files/2024-03/cnil_guide_securite_personnelle_2024.pdf

Troisième version du guide depuis l'entrée en vigueur du Règlement général sur la protection des données, la version de 2024 contient 5 nouvelles fiches : (i) le cloud, (ii) les applications mobiles, (iii) l'intelligence artificielle (conception et apprentissage), (iv) les interfaces de programmation applicative et (v) le pilotage des données.

Pour rappel, il est important de prendre connaissance de ce guide et de respecter les précautions élémentaires qui y sont indiquées puisque la CNIL l'utilise comme référence pour apprécier, lors de ses contrôles, la conformité des mesures techniques et organisationnelles implémentées par les sociétés pour sécuriser leurs traitements de données personnelles.