Violations de données personnelles : bilan de 5 années de RGPD

27 mars 2024

Depuis le 25 mai 2018, les violations de données personnelles susceptibles d'engendrer un risque pour les droits et libertés des personnes doivent être notifiées à la CNIL. Cinq ans après l'entrée en application du RGPD, la CNIL dresse un premier bilan chiffré.

La sécurité des données personnelles est un enjeu majeur pour tous les organismes publics et privés, ainsi que pour tous les individus. Le RGPD impose que les violations de données personnelles soient notifiées à la CNIL dès qu'un risque est engendré pour les droits et libertés des personnes concernées. Les organismes sont tenus de mettre en place des moyens permettant de détecter les incidents de sécurité. Ils doivent ensuite être en mesure de les qualifier, ou non, en tant que violations de données.

Une violation de données correspond à une perte de **disponibilité**, d'**intégrité** ou de **confidentialité** de données personnelles, que son origine soit **accidentelle** ou la conséquence d'une **action malveillante**.

Le développement rapide des usages numériques et des échanges de données élargit les possibilités que les données des employés, consommateurs, citoyens, patients ou autres fassent l'objet d'une violation. Certaines violations sont susceptibles d'engendrer des risques importants, tels que financiers par exemple, quand un pirate intercepte des données de carte bancaire.

C'est pourquoi le RGPD impose aux entités subissant une violation de prendre les mesures pour en limiter les conséquences. En particulier, si les risques sont élevés, elles sont tenues d'informer les personnes concernées, si possible, individuellement et de les conseiller sur la manière de se prémunir de ces risques.

La CNIL dresse ci-dessous un premier bilan chiffré couvrant **la période de mai 2018 à mai 2023**.

Le bilan des 17 483 violations de données notifiées en 5 ans

Un nombre de violations reçues croissant

> Consulter au format PDF

Entre mai 2018 et mai 2023, la CNIL a reçu 17 483 notifications de violations de données. Ce volume ne reflète pas le nombre réel d'incidents puisqu'un même évènement, tel qu'un piratage, peut donner lieu à de multiples notifications. Cela correspond souvent aux situations où un prestataire est touché par une

attaque et la notifie à ses clients, conformément au RGPD, qui eux même effectuent leurs propres notifications.

En regroupant les notifications liées à une même origine, il apparaît que **le nombre de violations de données notifiées à la CNIL est croissant au fil des années**. Sur ce constat, il est cependant difficile de faire la part entre la meilleure prise en compte du RGPD par les acteurs et une éventuelle amplification des menaces sur les données personnelles.

Note : la tendance est la moyenne glissante du nombre de notifications reçues par la CNIL corrigée des séries issues d'un même incident.

> Consulter au format PDF

La répartition par secteur et par type d'activité

Le secteur privé est à l'origine d'environ deux tiers des déclarations de violations à la CNIL dont 39 % de PME. Le **secteur public** représente quant à lui **22 %** des notifications.

S'agissant de la répartition par activité, les administrations publiques représentent 18 % des notifications. Les activités spécialisées, scientifiques et techniques sont les plus représentées au sein du privé, suivies par les activités financières et d'assurance. **Ce sont des secteurs en fort lien avec les données personnelles**. De même, les activités en lien avec la santé humaine représentent aussi 12 % des notifications.

> Consulter au format PDF

Ces chiffres ne reflètent qu'une partie des incidents de sécurité qui se produisent en France. En effet, la présence importante de délégués à la protection des données dans certains secteurs, la prise en compte et l'appropriation du RGPD dans d'autres, ont un impact direct sur la représentation de telle ou telle activité. Ainsi, les secteurs les plus représentés ne subissent pas forcement plus d'incidents que les autres et/ou ne protègent pas moins bien les données personnelles. La montée en puissance de la détection et du traitement engendre, dans les faits, une hausse de cette partie visible de l'iceberg.

Les origines des violations de données

> Consulter au format PDF

Sur les origines des violations de données, les tendances observées depuis 2018 correspondent à celles du bilan d'étape réalisé 4 mois après l'entrée en application du RGPD et des bilans intermédiaires publiés dans les rapports annuels de la CNIL.

Plus de la moitié des violations notifiées trouvent leur **origine dans du piratage** : les **rançongiciels** sont au premier rang, suivis par les attaques par **hameçonnage**. Ces dernières sont généralement préalable à d'autres intrusions, sur le même système voire sur des systèmes d'autres responsables de traitement. Les analyses montrent que le **secteur public** est plus touché par l'**hameçonnage**, tandis que le **secteur privé** est davantage concerné par les **rançongiciels**.

Les **équipements perdus ou volés**, les **envois indus** et les **publications non volontaires** constituent les autres sources de violations de données les plus fréquentes.

Deux grandes tendances se dessinent :

- Les piratages et vols intentionnels imputables à un tiers malveillant ;
- Les erreurs involontaires d'une ou plusieurs personnes agissant pour le compte du responsable de traitement.

Dans les autres cas, il s'agit le plus souvent de causes inconnues ou non déterminées par l'organisme qui notifie ou d'actes internes malveillants.

Pour prévenir la majeure partie de ces incidents engendrant des violations de données personnelles, la CNIL rappelle qu'il est essentiel :

- de penser la sécurité dès le lancement d'un projet ;
- de prendre systématiquement des mesures minimales pour la sécurité des données ;
- d'effectuer régulièrement les mises à jour de sécurité sur les systèmes d'exploitation, les serveurs applicatifs, ou les bases de données ;
- et d'informer régulièrement le personnel sur les risques et enjeux de la cybersécurité.

Le guide de la sécurité des données personnelles de la CNIL rappelle les précautions élémentaires qui devraient être mises en œuvre de façon systématique par les professionnels.

La géographie des violations

> Consulter au format PDF

La répartition des notifications de violations de données personnelles au sein de l'hexagone n'est pas homogène. On observe une concentration de ces dernières au sein de la région Île-de-France, suivie par les Hauts-de-France et la région Auvergne-Rhône-Alpes.

Afin de comprendre cette répartition, il convient de prendre en compte que la notification est faite par le responsable de traitement, même si l'incident à l'origine de la violation s'est produit dans un établissement secondaire, géographiquement distant. **Ainsi, cette répartition géographique correspond à la densité économique du territoire, en particulier la densité des sièges sociaux.** Elle ne permet donc pas de tirer de conclusions sur des menaces ou tendances particulières.

La temporalité des notifications

En moyenne, un organisme met 113 jours à constater une violation. Ce chiffre est naturellement tiré à la hausse par les situations où il faut parfois plusieurs mois, sinon années, pour se rendre compte qu'une violation a eu lieu. **Dans les faits, la moitié des violations sont constatées en moins de 10 heures.**

> Consulter au format PDF

En cas de violation de données personnelles, le responsable de traitement notifie la violation en question à l'autorité de contrôle compétente dans les meilleurs délais, et si possible, 72 heures au plus tard après en avoir pris connaissance (article 33.1 du RGPD). Lorsque la notification à l'autorité de contrôle n'a pas lieu

dans les 72 heures, elle doit être accompagnée des motifs du retard.

Dans les faits, **la moitié des notifications sont effectuées dans ce délai**. Les violations sont notifiées pour 75 % d'entre elles dans les 11 jours de la qualification de l'incident.

> Consulter au format PDF

En cas de retard, les **raisons principales** sont :

- la **méconnaissance de l'obligation de notification de la CNIL**, les déclarants l'apprenant lors du dépôt d'une plainte ou lors de la prise de contact avec leur assurance cyber par exemple,
- la **volonté des organismes d'attendre de disposer d'éléments tangibles et de résultats d'expertises.**

Vu de la CNIL, il préférable de notifier la violation auprès dans le délai de 72 h quitte à ne fournir que des éléments partiels, qui pourront être complétés par la suite voire même supprimés, dans le cas où la violation ne serait pas avérée.

Sans motif légitime, le non-respect de l'obligation de notification dans les 72 h constitue un manquement au RGPD, qui peut être sanctionné par la CNIL. Un tel manquement est passible d'une amende de 10 millions d'euros ou 2 % du chiffre d'affaires. Si la gestion d'une violation par le responsable de traitement laisse apparaître une négligence volontaire ou une volonté manifeste de cacher des éléments, le CNIL adoptera une approche répressive à son encontre.

Le rôle de la CNIL

> Consulter au format PDF

Dans son traitement des notifications, la CNIL privilégie l'accompagnement des acteurs. Son but d'aider les professionnels concernés à prendre toutes les mesures pour limiter les conséquences d'une violation, pour les personnes concernées en premier lieu, ainsi que pour les professionnels eux-mêmes. Elle peut en outre apporter un conseil sur les mesures préventives en matière de cybersécurité.

Lorsque cela est nécessaire, la CNIL prend contact avec les organismes pour :

- **Vérifier que des mesures ont été prises** préalablement et / ou postérieurement à la violation :
  - elle indique au responsable, les améliorations à mettre en œuvre par exemple sur l'utilisation d'un algorithme de chiffrement adapté ou l'optimisation de la gestion des mots de passe ;
  - elle renvoie également les responsables vers les services de police pour porter plainte, ou vers la plateforme cybermalveillance.gouv.fr afin de trouver une information ou un prestataire.

- **Évaluer la nécessité, prévue par le RGPD, de réaliser une information des personnes.** Pour chaque notification, la CNIL estime le risque engendré pour les personnes puis peut être amenée à recommander à l'organisme de les informer de la violation.

Il est toujours possible de contacter les services de la CNIL en charge de la gestion des notifications de violations de données personnelles par courriel à l'adresse violations@cnil.fr.

Pour approfondir

- Les violations de données personnelles
- Tous les contenus de la CNIL sur la cybersécurité