Les violations de données personnelles

20 juin 2018

Tous les organismes qui traitent des données personnelles doivent mettre en place des mesures pour prévenir les violations de données et réagir de manière appropriée en cas d'incident. Les obligations prévues par le RGPD visent à éviter qu'une violation cause des dommages ou des préjudices aux organismes comme aux personnes concernées.

Les nouvelles obligations concernant les violations de données sont prévues par les articles 33 et 34 du RGPD. Elles précisent l'obligation générale de sécurité que doivent respecter les organismes qui traitent des données à caractère personnel.

Au titre de ce principe essentiel, ces organismes doivent mettre en place des mesures visant à :

- prévenir toute violation de données
- réagir de manière appropriée en cas de violation, c'est-à-dire mettre fin à la violation et minimiser ses effets.

Ces dispositions visent à préserver à la fois :

- les responsables du traitement : afin de protéger leur patrimoine informationnel, en leur permettant notamment de sécuriser leurs données ;
- les personnes affectées par la violation : afin d'éviter qu'elle ne leur cause des dommages ou préjudices, en leur permettant notamment de prendre les précautions qui s'imposent en cas d'incident.

Il est dès lors recommandé que les organismes qui traitent des données personnelles (responsable du traitement ou sous-traitant) prévoient et mettent en place des procédures globales en matière de violation de données personnelles. Ces procédures doivent concerner l'ensemble du processus : la mise en place de mesures visant à détecter immédiatement une violation, à l'endiguer rapidement, à analyser les risques engendrés par l'incident et à déterminer s'il convient de notifier l'autorité de contrôle, voire les personnes concernées. Ces procédures participent ainsi à la documentation de la conformité au RGPD.

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

L'article 4.12) du RGPD définit une violation de données à caractère personnel comme

une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles.

Exemples :

- suppression accidentelle de données médicales conservées par un établissement de santé et 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 scolaires et modification des résultats obtenus par les élèves.

Les obligations des responsables du traitement concernant les violations de données personnelles, et notamment leur notification à la CNIL et aux personnes concernées,

sont définies aux articles 33 et 34 du RGPD.

Qui est concerné ?

Tous les organismes, publics comme privés et quelle que soit leur taille, sont soumis à ces obligations dès lors qu'ils traitent des données personnelles et qu'ils ont connaissance d'une violation de données personnelles. Elles ne sont plus réservées, comme avant le RGPD, aux seuls fournisseurs de services de communication électronique.

Les sous-traitants, qui traitent des données personnelles pour le compte d'un organisme responsable du traitement, ont également des obligations en matière de violation : ils doivent en particulier alerter l'organisme de tout incident de sécurité dans les meilleurs délais afin qu'ils puissent remplir ses obligations.

Quelles sont les principales obligations en matière de violation de données ?

Ces obligations sont variables en fonction du risque soulevé par les violations : toutes les violations ne doivent pas nécessairement être notifiées à l'autorité de contrôle ou aux personnes concernées. Lorsqu'elle est nécessaire, cette information des personnes concernées doit en revanche être la priorité du responsable du traitement, car cela leur permet de prendre des mesures destinées à les protéger de ces risques.

Ainsi, l'obligation de notifier dépend du risque que la violation de données personnelles fait peser sur les droits et libertés des individus dont les données ont été impactées :

Si la violation n'entraîne pas de risque pour les droits et libertés des personnes concernées, le responsable du traitement :

- doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;
- ne doit pas notifier cette violation ni à la CNIL, qui peut en revanche contrôler cette documentation interne, ni aux personnes concernées.

Si la violation entraîne un risque pour les droits et libertés des personnes concernées, le responsable du traitement :

- doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;
- doit notifier cette violation à la CNIL, au plus tôt et dans un délai maximal de 72h.

Si la violation entraîne un risque élevé pour les droits et libertés des personnes concernées, le responsable du traitement :

- doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;
- doit notifier cette violation à la CNIL, au plus tôt et dans un délai maximal de 72h ;
- doit communiquer la violation aux personnes concernées, au plus tôt.

Pour les personnes concernées, la violation engendre :	**aucun risque**	**un risque**	**un risque élevé**
Documentation interne, dans le « registre des violations »	X	X	X
Notification à la CNIL, dans un délai maximal de 72h	-	X	X
Information des personnes concernées dans les meilleurs délais, hors cas particuliers	-	-	X

Existe-il des dérogations à l'obligation d'informer les personnes concernées ?

Oui : en cas de violation entraînant un risque élevé, des exceptions à l'obligation d'information des personnes sont prévues. Il s'agit des cas suivants :

- **les données à caractère personnel** affectées par la violation en cause sont protégées par des mesures de protection techniques et organisationnelles appropriées et sont ainsi **incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès**

Exemple : les données ont fait l'objet d'une mesure de chiffrement à l'état de l'art, dont la clé n'a pas été compromise et a été générée de façon à ne pas pouvoir être trouvée, par aucun moyen technologique existant, par quelqu'un qui n'est pas autorisé à l'utiliser

- le responsable du traitement a pris des mesures ultérieures qui garantissent **que le risque élevé** pour les droits et libertés des personnes n'est **plus susceptible de se matérialiser**

Exemple : 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 communication** de la violation aux personnes concernées **exigerait des efforts disproportionnés**

Exemple : le responsable du traitement ne dispose d'aucun élément permettant de contacter les personnes concernées

Attention : dans ce cas, une communication publique, ou une mesure similaire permettant aux personnes concernées d'être informées de manière aussi efficace, doit être réalisée.

Que doit contenir le « registre des violations de données » ?

La documentation doit consigner les faits concernant la violation de données à caractère personnel, ses effets et les mesures prises pour y remédier. Elle peut être contrôlée par la CNIL dans l'objectif de vérifier le respect des obligations en matière de violations.

En pratique, il est conseillé aux responsables du traitement de recenser l'ensemble des éléments relatifs aux violations et de s'appuyer sur le formulaire de notification mis en ligne par la CNIL. Ce formulaire peut en effet servir de canevas pour la documentation interne, qui peut ainsi constituer un outil unique de gestion de la conformité au RGPD en matière de violations.

Le registre des violations devrait notamment contenir les éléments suivants :

- la nature de la violation ;
- les catégories et le nombre approximatif des personnes concernées ;
- les catégories et le nombre approximatif de fichiers concernés ;
- les conséquences probables de la violation ;
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation ;
- le cas échéant, la justification de l'absence de notification auprès de la CNIL ou d'information aux personnes concernées.

Que faut-il notifier à l'autorité de contrôle ?

La notification s'effectue par le biais d'un téléservice sécurisé dédié, qui guide le déclarant dans sa démarche.

Elle doit contenir *a minima* les éléments suivants :

- la nature de la violation ;
- les catégories et le nombre approximatif des personnes concernées ;
- les catégories et le nombre approximatif de fichiers concernés ;
- les conséquences probables de la violation ;
- les coordonnées de la personne à contacter (DPO ou autre) ;
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation.

Que faut-il communiquer aux personnes concernées ?

La notification aux personnes concernées doit ***a minima*** **contenir** et exposer, en des termes clairs et précis, les éléments suivants :

- la nature de la violation ;
- les conséquences probables de la violation ;
- les coordonnées de la personne à contacter (DPO ou autre) ;
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation.

Elle doit être complétée, dès lors que cela est nécessaire, de recommandations à destination des personnes pour atténuer les effets négatifs potentiels de la violation et leur permettre de prendre les précautions qui s'imposent

Exemples de recommandations : changement de mot de passe des utilisateurs d'un service, vérification de l'intégrité des données de leur compte en ligne, sauvegarde de ces données sur un support personnel

Quand faut-il notifier à la CNIL ?

La notification doit intervenir dans les meilleurs délais et au plus tard 72h après que le responsable du traitement en a pris connaissance.

En pratique, le point de départ de ce délai est lorsque le responsable du traitement a 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 et qu'il mène au plus tôt des investigations permettant d'atteindre une telle certitude raisonnable. Durant cette phase d'investigation, le responsable du traitement n'est pas considéré comme ayant connaissance de la violation.

Exemples de situations où le responsable de traitement doit être considéré comme informé de la violation :

- en cas de perte d'une clé USB contenant des données personnelles, dès lors qu'il réalise la perte de la clé ;
- un tiers informe le responsable du traitement qu'il a reçu un courriel avec les informations concernant une autre personne et en fournit la preuve ;
- dès lors qu'un cybercriminel contacte le responsable du traitement et lui indique qu'il a pu subtiliser des données sur les serveurs de la société, après vérification de cette information

---

Est-il nécessaire de disposer de toutes les informations pour notifier la violation à la CNIL ?

Il importe bien entendu de s'assurer, au besoin par des premières investigations, qu'une violation a bien eu lieu et d'en déterminer le niveau de gravité. La nature et la source de l'incident doivent donc être présumés ou établis avant de notifier la violation à la CNIL.

En revanche, si le responsable du traitement ne dispose pas de l'ensemble des informations qui doivent être portées à la connaissance de l'autorité de contrôle, ces informations peuvent être communiquées de manière échelonnée.

En pratique, il doit effectuer au plus vite une notification initiale à la CNIL, par le

biais du téléservice mis à disposition à cet effet, qu'il complétera par la suite à l'aide d'une notification complémentaire. Cela lui permettra de procéder aux investigations complémentaires nécessaires au recensement de l'ensemble des informations. Cette notification complémentaire doit intervenir si possible dans un délai maximal de 72h.

Que faire si le délai de 72h pour notifier est dépassé ?

Le responsable du traitement doit néanmoins notifier la violation entraînant un risque pour les droits et libertés des personnes. Si ce délai est dépassé, les raisons justifiant du retard de notification doivent être indiquées à la CNIL.

En pratique, il sera demandé au responsable du traitement, directement dans le téléservice de notification, de justifier des motifs de ce délai.

Quel est le rôle du sous-traitant 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. Cela permet au responsable du traitement de respecter ses différentes obligations en matière de violation de données.

En pratique, il est conseillé de prévoir dans le contrat qui lie le sous-traitant au responsable du traitement une obligation en ce sens à la charge du sous-traitant.

L'obligation de notifier à l'autorité de contrôle peut-elle être confiée au sous-traitant ?

Oui. Le responsable du traitement peut demander au sous-traitant d'agir en son nom afin que ce dernier notifie la violation à l'autorité de contrôle, si le responsable du traitement estime que la violation en cause est susceptible de présenter un risque pour les personnes concernées.

Cela n'écarte donc ni l'obligation faite au sous-traitant d'informer le responsable du

traitement de toute violation de données, ni les obligations propres au responsable du traitement : ce dernier doit mettre à jour son registre des violations et rester maitre de la décision de notifier ou non à l'autorité de contrôle (en fonction du niveau de risque estimé).

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

Cette appréciation doit être faite au cas par cas par le responsable du traitement et doit tenir compte des éléments suivant :

- 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 n'y a pas de risque justifiant une notification à la CNIL ou aux personnes concernées : la divulgation de données divulguées déjà rendues publiques ; la suppression de données sauvegardées et immédiatement restaurées ; 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.

Quels sont les pouvoirs de la CNIL en matière de violation de données ?

La CNIL exerce deux missions principales en matière de violation de données :

- **un rôle d'accompagnement des responsables du traitement** : la notification à l'autorité de contrôle a notamment pour but de permettre aux RT de recueillir les éventuels conseils et observations de la CNIL s'agissant des mesures de sécurité à mettre en œuvre pour mettre fin à la violation ou pour minimiser ses effets ; elle permet également de vérifier si une information des personnes est nécessaire et, dans ce cas, d'obtenir des recommandations sur les modalités de cette information

- **un rôle de contrôle du respect des obligations des responsables du traitement :** la CNIL peut contrôler le respect de l'ensemble de ces obligations (inscription au registre, vérification du niveau de risque, respect des délais et du contenu des notifications, etc.) et, le cas échéant, sanctionner les organismes concernés. Elle peut également ordonner au responsable du traitement de communiquer une violation de données aux personnes concernées, si cela lui apparaît nécessaire.

Dans les deux cas, l'examen de la CNIL est susceptible de porter, au-delà de la seule violation en cause, sur le niveau de sécurité générale du traitement que la violation peut révéler.

Cas particulier : les violations touchant un traitement

transfrontalier

Pour un traitement transfrontalier, l'autorité « chef de file » constitue l'unique interlocuteur du responsable du traitement. C'est donc auprès de cette autorité que la notification d'une violation doit être réalisée. **Cette autorité n'est pas nécessairement la CNIL,** y compris si la violation affecte des personnes résidant en France et y compris si elle s'est produite sur le territoire français.

En pratique, le téléservice de la CNIL prévoit que le responsable du traitement déclarant doit indiquer si la violation touche un traitement transfrontalier et, en cas de réponse positive, d'indiquer quels sont les autres États membres de l'Union concernés par le traitement. La CNIL se charge ensuite d'informer les autres autorités.

Téléservice de notification

>Notifier une violation de données personnelles