ARTICLE

M-4 : NOTIFICATION DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

IT et données personnelles ANNULE - Concurrence, régulation européenne et FDI Contrats commerciaux et internationaux | 14/02/18 | Florence Chafiol

Le nouveau Règlement (UE) 2016/679 relatif à la protection des données (« RGPD » ou le « Règlement ») introduit de nouvelles obligations concernant les notifications de violation de données à caractère personnel (« violation de données ») [1] :

> Dès lors qu'une **violation de données personnelles** est susceptible d'engendrer un **risque** pour les droits et libertés des personnes concernées, le responsable du traitement doit notifier la **violation de données à l'autorité de contrôle compétente** (ex: la CNIL) dans les meilleurs délais et **au plus tard dans les 72 heures** après en avoir pris connaissance ; si le délai de 72 heures ne peut être respecté, le responsable du traitement doit être mesure d'en justifier ; **si le risque est élevé**, les personnes concernées doivent également être notifiées dans les meilleurs délais.

Le responsable du traitement doit par conséquent être en mesure d'identifier une **violation de données** (1) et de déterminer le **niveau de risque** qu'elle peut engendrer (2) afin, le cas échéant, de pouvoir **notifier les autorités et les personnes concernées** dans les délais impartis (3). Le responsable du traitement doit également **documenter toutes les violations de données** (4) et **organiser la relation contractuelle avec le(s) sous-traitant(s)** qui pourraient être concernés (5).

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

Une violation de données est définie 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* »[2].

Lors de leur identification et afin d'évaluer les risques, **les violations de données peuvent être classées en trois catégories**, une même violation pouvant concerner plusieurs catégories :

> violation de confidentialité : divulgation ou accès non autorisé ou accidentel à des données à caractère personnel ;

> violation de disponibilité : perte d'accès ou destruction accidentelle ou non autorisée des données à caractère personnel ;

> violation d'intégrité : modification non autorisée ou accidentelle des données à caractère personne.

2 - Comment déterminer le risque pour les droits et libertés des personnes concernées ?

Le responsable du traitement doit rapidement déterminer si **la violation de données est susceptible d'engendrer un risque** (élevé) afin, le cas échéant, de pouvoir **notifier l'autorité de contrôle et les personnes concernées** dans les délais impartis.

Il n'existe pas de définition précise de « risque » ou de « risque élevé » dans le Règlement. Les autorités rappellent toutefois que dans la mesure où la violation de données s'est produite, il s'agit **d'évaluer la gravité et la probabilité de survenance des conséquences de cette violation.**

Il convient, à cet effet, de prendre en compte les **circonstances spécifiques** de la violation dont notamment le **type de violation** (confidentialité, disponibilité, intégrité) **; la nature, le volume et la sensibilité des données** (ex : données de carte de paiement, données de santé) **; le nombre et type de personnes concernées** (ex : personne vulnérable, mineur, patient) **; les possibilités d'identification des personnes ; les caractéristiques du responsable du traitement ; et la gravité des conséquences** (risques susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral tel qu'une discrimination, une usurpation d'identité, une perte financière, une atteinte à la réputation ou une perte de confidentialité de données protégées par le secret professionnel).

Exemple

Les autorités considèrent, par exemple, que l'attaque d'une plateforme de vente en ligne et la publication des données (login, mot de passe, historique d'achat) est susceptible d'engendrer un risque élevé. En revanche, le vol d'un CD de sauvegarde de données chiffrées n'est pas susceptible d'engendrer de risque si les données sont chiffrées en conformité avec l'état de l'art en matière d'algorithme de chiffrement, une sauvegarde des données existe et si la clé de cryptologie n'a pas été compromise.

3 - Dans quelles conditions faut-il notifier les violations de données ?

3.1 - Obligation de notifier l'autorité de contrôle dans les 72 heures en cas de risque

Le responsable du traitement **doit notifier l'autorité de contrôle compétente** lorsque la violation de données est susceptible d'engendrer **un risque** pour les droits et libertés des personnes concernées (dans le cas d'un traitement de données transfrontalier, l'autorité compétente est l'autorité de contrôle chef de file).

Cette notification doit avoir lieu dans les meilleurs délais et si possible, dans les 72 heures après avoir pris connaissance de la violation. Encore faut-il que le responsable du traitement ait pu, dans ce délai, identifier si la violation présentait un risque pour les droits et libertés des personnes concernées, tout dépassement du délai de 72 heures devant toutefois être justifié lors de la notification.

3.1.1 - A quel moment le responsable du traitement "prend connaissance" de la violation ?

Le responsable du traitement devrait être en mesure de **prouver à quel moment il a pris connaissance de la violation** dans la mesure où il s'agit du point de départ du délai de notification.

Selon les autorités[3], le responsable du traitement a « pris connaissance » de la violation de données **dès lors qu'il a un degré raisonnable de certitude** qu'un incident de sécurité ayant conduit à la compromission de données à caractère personnel s'est produit.

En pratique, une première investigation rapide peut être nécessaire afin de recueillir des éléments permettant de confirmer avec un degré raisonnable de certitude la réalité de la violation de données.

Exemple

Les autorités considèrent que si une personne informe le responsable du traitement qu'elle a reçu un faux email de sa part contenant des données à caractère personnel la concernant, cette information ne fera que suggérer qu'une violation de données a eu lieu. Si après une première investigation, des indices révélant un accès non autorisé aux données sont recueillis, le responsable du traitement sera alors considéré comme ayant pris connaissance de l'incident.

3.1.2 - Contenu de la notification à l'autorité de contrôle

La notification devrait contenir les éléments suivants[4] :

> une description de la nature de la violation de données, y compris, si possible, les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif de données à caractère personnel concernées ;

> le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel il est possible d'obtenir plus d'informations ;

> une description des mesures prises ou envisagées, y compris des mesures visant à atténuer les éventuelles conséquences négatives ;

> une description des conséquences probables de la violation de données.

3.1.3 - Gestion des retards et notifications complexes

Si le responsable du traitement ne dispose pas de toutes les informations requises, il peut les fournir au fur et à mesure qu'il en prend connaissance.[5] Il est toutefois recommandé de l'indiquer à l'autorité de contrôle dès la première notification et de donner les raisons du retard si l'échelonnement implique le dépassement du délai de 72 heures.

Il est également possible de faire une notification commune pour des violations similaires qui se sont produites sur une courte période. Le temps de l'investigation de toutes les violations peut éventuellement justifier un retard.

3.2 - Obligation de notifier les personnes concernées dans les meilleurs délais en cas de risque élevé

Lorsque la violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement doit informer la personne concernée de la violation de données dans les meilleurs délais[6] afin qu'elle puisse prendre les précautions nécessaires.

3.2.1 - Notion de "meilleurs délais" et coopération avec les autorités

En pratique, le délai de notification peut varier en fonction de la nécessité d'atténuer un risque immédiat de dommage (notification immédiate) ou de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation de données ou la survenance de violations similaires (délai plus long). La notification devrait également être effectuée en coopération étroite avec l'autorité de contrôle, dans le respect des directives de cette dernière et/ou d'autres autorités compétentes, telles que les autorités répressives.[7]

Ainsi, à moins qu'une notification immédiate des personnes concernées ne soit nécessaire, le responsable du traitement devrait, dans le cadre de la notification de violation de données, demander conseil à l'autorité de contrôle pour évaluer la nécessité de communiquer aux personnes concernées, cette dernière pouvant également obliger le responsable du traitement à notifier les personnes concernées.

3.2.2 -Contenu et mode de notification des personnes concernées

Le contenu de la notification des personnes concernées est similaire à celle qui doit être faite aux autorités à l'exception de la description de la nature de la violation qui doit être expliqué en des termes clairs et simples. Elle devrait également inclure toute recommandation visant à atténuer les effets négatifs de la violation de données.[8]

La notification devrait, en principe, être effectuée directement auprès de la personne concernée à moins que cela implique un effort disproportionné. Dans ce cas une communication publique ou une mesure similaire doit être mise en œuvre pour que les personnes concernées soient informées.[9]

3.2.3 -Exception à l'obligation de notification

La notification n'est plus obligatoire [10] :

> dès lors que des mesures de protection technique et organisationnelle appropriées ont été appliquées aux données à caractère personnel concernées et ont, en particulier, rendu les données incompréhensibles à toute personne non autorisée (ex : chiffrement) ; ou

> si des mesures ultérieures garantissant que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser, ont été mises en œuvre.

4 - Obligation de documenter toutes les violations de données

Le responsable du traitement doit documenter toutes les violations de données et plus particulièrement celles qui n'ont pas fait l'objet d'une notification, en indiquant notamment les faits concernant la violation de données, ses conséquences et les mesures prises pour y remédier.[11]

Les autorités recommandent également que le responsable du traitement motive les décisions de ne pas notifier une violation. Cela permet de contrôler la conformité au Règlement et d'assurer un suivi notamment dans le cas d'un changement de circonstances qui pourrait obliger le responsable du traitement à notifier une violation de données passée (ex : une clé de chiffrement d'un fichier volé, dont une copie a été conservée, qui a été ultérieurement compromise).

5 - Rôle du sous-traitant

Les sous-traitants ont l'obligation de notifier au responsable du traitement toute violation de données dans les meilleurs délais après en avoir pris connaissance[12].

Les autorités considèrent que dès lors que le sous-traitant a pris connaissance de la violation, le responsable du traitement est supposé en avoir aussi pris connaissance ; aussi, elles recommandent que le sous-traitant notifie immédiatement le responsable du traitement de toute violation ayant eu lieu, des

informations supplémentaires sur la violation pouvant être fournies ultérieurement en fonction de l'avancement de l'investigation. Il est donc important de prévoir ces conditions dans les contrats et de s'assurer que les mesures techniques et organisationnelles ont été mises en place.

Il est également possible d'envisager que le sous-traitant notifie l'Autorité au nom du responsable du traitement. Ce point doit être prévu au contrat qui les lie sans pour autant que cela ne donne lieu à un transfert de responsabilité du responsable du traitement vers le sous-traitant.

SANCTION

L'autorité de contrôle compétente (en France la CNIL) est susceptible de prononcer une amende administrative d'un montant maximum de 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial total de l'exercice précédent (le montant le plus élevé étant retenu) pour toute violation des obligations incombant aux responsables du traitement et aux sous-traitants en application des articles 33 et 34 du RGPD dont notamment :

- **Le défaut de notification de l'autorité** et le cas échéant, des personnes concernées, par le responsable du traitement, dans les délais impartis et sans pouvoir justifier d'un éventuel retard ;
- **Le défaut de notification du responsable du traitement par le sous-traitant** de toute violation de données dans les meilleurs délais ;
- **La notification** effectuée par le responsable du traitement **est incomplète.**

ACTIONS DE MISE EN CONFORMITE :

1. Mettre en place les formations, procédures et dispositifs afin d'identifier les incidents de sécurité, les remonter aux personnes compétentes pour évaluer les risques, y remédier et le cas échéant, notifier les autorités et les personnes concernées dans les délais impartis ;
2. Identifier les personnes à inclure dans la procédure de notification (ex : DPO, RSSI, Juristes) et les préparer (des tests pourraient être envisagés) ;
3. Mettre en place et tenir un registre des incidents de sécurité ;
4. Mettre à jour les contrats avec les sous-traitants afin d'intégrer les conditions/modalités de notification des violations de sécurité.

---

[1] Articles 33 et 34 du RGPD

[2] Articles 4 (12) du RGPD

[3] WP250 "Guidelines on Personal data breach notification under regulation 2016/679" adoptée le 3 octobre 2017

[4] Article 33 (3) du RGPD

[5] Article 33 (4) du RGPD

[6] Article 34 (1) du RGPD

[7] Considérant 86 du RGPD

[8] Article 34 du RGPD et considérant 86

[9] Article 34 (3) (c) du RGPD

[10]Article 34 (3) (a) et (b) du RGPD

[11] Article 33 (5) du RGPD

[12] Article 33 (2) du RGPD