LES VIOLATIONS DE DONNEES – BILAN ET RECOMMANDATIONS

Définies 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 », les violations de données sont encadrées par le RGPD.

A ce titre, dès lors qu'elles sont susceptibles d'entrainer un risque pour les personnes concernées, elles doivent être notifiées à la CNIL, si possible, dans un délai de 72 heures à compter de leur connaissance par l'organisme. Une communication aux personnes concernées est également obligatoire si la violation entraine un risque élevé pour les personnes concernées.

- Sur ce point, le Comité européen de la protection des données (CEPD) renvoie à ses lignes directrices sur l'analyse d'impact pour qualifier le risque important. Pour rappel, l'évaluation du risque important est à l'égard des personnes concernées et non pour le responsable de traitement.

La CNIL dresse un bilan des notifications de violations de données intervenues depuis l'entrée en application du RGPD, il y a cinq ans. Elle y constate un nombre croissant de notifications, mais ne sait pas distinguer ce qui est dû à la prise en compte grandissante de la règlementation et de l'obligation de notifier de tels incidents de sécurité, de ce qui proviendrait de menaces grandissantes sur les données personnelles.

La CNIL fait le constat que plus de la moitié des violations de données proviennent d'actes malveillants, de piratage informatique, principalement par rançongiciels ou hameçonnage.

- Aussi, il semble recommandé que les responsables de traitement s'assurent que leurs collaborateurs soient formés à la sécurité, et aux principes élémentaires de protection des données personnelles, leur permettant d'adopter les bons réflexes en cas d'incident.
- Ce bilan fait écho à l'actualisation par la CNIL de son guide de sécurité sur les données personnelles, publié le 26 mars 2024. Cette actualisation a été enrichie notamment d'une nouvelle fiche sur le pilotage de la sécurité des données. La CNIL a également décidé de scinder son ancienne fiche 4 sur « Tracer les opérations et gérer les incidents » en deux fiches distinctes relatives à la traçabilité des opérations, et une autre concernant la gestion des incidents et les violations.

La CNIL revient également sur les délais liés aux violations de données. Si le délai indiqué dans le RGPD est de 72 heures après la connaissance par l'organisme de cette dernière, en pratique la CNIL constate que pour 75% des violations, les notifications interviennent dans les 11 jours de la qualification de l'incident.

- La bonne pratique à adopter, comme le rappelle la CNIL dans ce bilan, est d'établir une première notification même partielle dans le délai imparti, qui sera complétée par la suite.

- Article 32 et 33 du Règlement Général sur la Protection des Données
- Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, CEPD
- Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, CEPD
- Violations de données personnelles : bilan de 5 années de RGPD, CNIL
- Guide de sécurité des données personnelles – Version 2024

Version du 27 mars 2024