Violation de données de santé : la CNIL rappelle les obligations des organismes à la suite d'une fuite de données massive annoncée dans les médias

24 février 2021

A la suite de la publication dans la presse de plusieurs articles concernant une fuite de données de santé massive, la CNIL rappelle aux responsables de traitement leurs obligations en cas de violation.

La CNIL a été informée par les médias de la publication d'un fichier contenant des données médicales de près de 500 000 personnes. Elle procède actuellement à des contrôles pour constater officiellement la mise à disposition du fichier.

Les constatations préliminaires semblent indiquer qu'il s'agit effectivement d'une violation de données d'une ampleur et d'une gravité particulièrement importante, et laissent à penser que les données proviendraient de laboratoires d'analyse médicale. Si ces éléments devaient être confirmés, il incombe aux organismes concernés qui ne l'auraient pas déjà fait, de procéder à une notification auprès de la CNIL, dans les 72 heures suivant le moment où ils en ont pris connaissance. En outre, lorsque la fuite de données est susceptible d'engendrer un risque élevé pour les droits et les libertés, les organismes responsables ont l'obligation d'informer individuellement les personnes concernées du fait que leurs données ont été compromises et publiées en ligne. Cela peut être le cas si, comme la presse s'en est fait l'écho, des données de santé particulièrement sensibles ont été divulguées et en nombre important.

Par ailleurs la CNIL rappelle que les responsables de traitement ont l'obligation d'assurer la sécurité des données qu'ils traitent par des moyens proportionnés aux risques, et tout particulièrement pour des données sensibles telles que les données de santé.

En cas de manquement à ces obligations la CNIL pourrait engager des actions répressives, sans préjudice des actions que les autres autorités compétentes seraient susceptibles de mener.

Le rôle de la CNIL en matière de cybersécurité

La CNIL accompagne les administrations et les entreprises dans la prise en compte de la sécurité informatique. L'obligation de sécurité, inscrite dans la loi depuis plus de 40 ans, a été renforcée par le RGPD et complétée de nouveaux outils comme la notification des violations, l'analyse d'impact sur la protection des données ou les codes de conduite.

Quelques chiffres :

- **+ 24 %** de notifications de violation de données en 2020 (2825 en 2020)
- **Une multiplication par 3** des violations liées à des attaques par cryptolockers sur des établissements de santé (centre hospitalier, clinique, EPHAD, maison de santé, établissements de soin, laboratoires etc) :
    - 12 violations en 2019
    - 36 violations en 2020

- **2/3 des sanctions** prononcées par la CNIL visent des manquements à l'obligation de sécurité des données
- **20 agents spécialisés** en sécurité informatique au sein de Direction des Technologies et de l'Innovation et de la Direction de la protection des droits et des sanctions de la CNIL

En savoir plus

- Notifier une violation de données personnelles
- Les violations de données personnelles
- Sécurité des données
- L'analyse d'impact relative à la protection des données (AIPD)
- Le code de conduite