Violation de données personnelles & Notification

écrit par Marine de la Clergerie | 02/09/2024

Faut-il notifier tous les incidents de sécurité à l'autorité de contrôle?

Non.

L'obligation de notification concerne uniquement les violations de données à caractère personnel qui engendrent un risque pour les droits et libertés des personnes physiques.

- Les violations de données à caractère personnel: un incident de sécurité n'est pas forcément une violation de données à caractère personnel au sens du RGPD (article 4 point 12 du RGPD)

> *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*

- Un risque pour les droits et libertés des personnes physiques. Il est donc nécessaire de procéder à cette évaluation du risque.

Faut-il communiquer toutes les violations de données à caractère personnel aux personnes concernées?

Non.

L'obligation de communication aux personnes concernées est obligatoire uniquement lorsque la violation est susceptible d'engendrer un risque élevé pour

les droits et libertés d'une personne physique (article 34 du RGPD).

Il est donc nécessaire de procéder à cette évaluation de ce risque au moment de la prise de connaissance de la violation.

Auprès de quelle autorité faut-il notifier la violation de données?

En principe, il faut notifier aux autorités de chaque pays où les personnes sont affectées :

- Pour l'UE : liste : https://www.edpb.europa.eu/about-edpb/about-edpb/members_en).
- Hors UE, par exemple à l'ICO pour UK

Au sein de l'UE, il peut exister une « autorité chef de file » qui serait le point d'entrée, un guichet unique. En général il s'agit de l'autorité du lieu de l'établissement principal (cf. les lignes directrices concernant cette désignation). Il est recommandé de procéder à une analyse préalable pour déterminer l'autorité chef de file.

Donc en cas de doute, notifier l'autorité des pays où les clients sont touchés.

Chaque autorité de protection des données dispose d'une procédure de notification: https://www.edpb.europa.eu/notify-data-breach_fr