contrast

VOS ACTIVITÉS • MARS 2020

Violations de données : trucs & astuces.

Ce que vous devez savoir.

Lorsqu'une entreprise apparait dans les journaux en raison d'une violation du GDPR, cela est souvent dû à une violation de données. Outre les conséquences commerciales et le risque de devoir payer des amendes importantes, une telle violation de données porte également, de manière significative, préjudice à la réputation d'une entreprise.

Le GDPR comprend plusieurs obligations relatives aux violations de données. Une première obligation est l'adoption de mesures de sécurité visant à garantir l'intégrité, la confidentialité et la disponibilité des données à caractère personnel.

Il est question d'une violation de données lorsqu'il y a, de manière accidentelle ou illicite, une infraction à:

- la confidentialité des données à caractère personnel : à savoir, lorsqu'il y a eu un accès non autorisé aux données, via un hacker par exemple;
- la disponibilité des données à caractère personnel : à savoir, lorsqu'une entreprise n'a plus le contrôle sur ou l'accès aux données, par exemple, en raison du fait que le système informatique où sont stockées les données est défaillant (temporairement ou non);
- l'intégrité des données à caractère personnel : à savoir, lorsque les données ont été altérées, par une modification erronée par exemple.

Lorsque l'une de ces infractions se produit, les responsables du traitement des données ont l'obligation de documenter la violation des données dans un registre interne. Ils doivent signaler la violation des données à l'autorité de contrôle dans les 72 heures, à moins que la violation des données ne soit pas de nature à présenter un risque dans le chef des personnes concernées. Si la violation des données présente un risque élevé pour les personnes concernées, elle doit leur être également immédiatement signalée. A titre d'exemple, si un ordinateur portable professionnel contenant des données de RH et sécurisé contre les accès non autorisés, est volé, il semble peu probable qu'une notification soit nécessaire. En revanche, si l'ordinateur portable est volé alors qu'il n'est pas sécurisé et permet donc d'accéder, par exemple, aux informations financières des employés, une notification à l'autorité de

contrôle et aux personnes concernées peut s’avérer nécessaire.

Les sous-traitants ont également des obligations en cas de violation de données. Les sous-traitants doivent signaler les violations de données aux responsables du traitement dès qu'ils en ont connaissance. Ils doivent également aider les responsables du traitement à remplir leurs obligations en cas de violation de données.

Ce que vous devez faire.

En tant qu'entreprise, vous devez veiller à élaborer une politique en matière de sécurité et de violation de données :

- Identifiez, par opération de traitement et par système de données, les violations de données qui peuvent survenir. Ne perdez pas de vue les situations moins évidentes, telles que les documents sortis pour la collecte des déchets ou les documents envoyés par la poste mais perdus ou retournés ouverts.
- Au-delà de l’élaboration d’une politique de sécurité visant à prévenir les violations de données, prenez également des mesures pour détecter et remédier à ces incidents lorsqu'ils se produisent. Cela implique, entre autres, la formation des employés afin qu’ils puissent identifier les violations de données. Vos employés sont-ils au courant que l'envoi d'un email contenant des données au mauvais destinataire et la perte d'un ordinateur portable professionnel constituent des violations de données ? Revoyez la politique en matière de sécurité de temps à autre (en particulier lorsqu'une violation de données s'est produite) et adaptez-la si nécessaire.
- Développez des procédures internes afin d’être en mesure d’agir rapidement et correctement en cas de violation de données. Ces procédures doivent indiquer clairement où les violations de données doivent être signalées en interne, qui analysera la violation de données et, si nécessaire, la signalera à l'autorité de contrôle et aux personnes concernées, ou au responsable du traitement, ...
- Veillez à ce que des accords clairs soient conclus entre les responsables du traitement et les sous-traitants, d'une part, et/ou les responsables conjoints du traitement, d'autre part. Par exemple, le sous-traitant pourrait être mieux placé que le responsable du traitement pour signaler une violation de données aux personnes concernées. Etant donné que les entreprises doivent agir rapidement lors de la survenance d’une violation de données, la qualification des parties en tant que sous-traitant ou responsable (conjoint) du traitement doit être claire avant la survenance d’une violation de données.