RGPD AVOIR TOUJOURS LES BONS RÉFLEXES

Fiche n°7

Que faire si je constate une fuite de données au sein de mon organisation ?

CONTEXTE

Qu'est ce qu'une fuite de données ?
Une fuite de données est la transmission non autorisée de données d'une organisation vers un destinataire externe de manière intentionnelle ou fortuite.

Les fuites de données se produisent généralement via l'intrusion sur des sites web et l'envoi de courrier électronique, mais peuvent également se produire par la perte ou le vol de périphériques tels que les clés USB ou les ordinateurs portables.

L'ESSENTIEL À RETENIR

- Prévoir en amont dans le contrat entre le Responsable de Traitement (RT) et le Sous-Traitant (ST) une procédure de gestion des violations et le délai de notification par le ST au RT.

- Prévoir un document permettant de documenter la traçabilité des violations de données personnelles.

ACTIONS À RÉALISER

Analyse du risque :
Demander au DSI d'indiquer si la fuite de données a pour conséquence une violation de données personnelles.
Pour mémoire, il y a violation de données personnelles, lorsqu'il y a une :
- Perte de disponibilité : perte de données
- Perte d'intégrité : altération de données
- Perte de confidentialité : accès non autorisé

Notification selon risque :
- Pas de risques pour les individus : pas de notification.
- Risque pour les droits et libertés des personnes : notification à l'autorité de contrôle.
- Risque élevé pour les droits et libertés des personnes : notification à l'autorité de contrôle + communication aux personnes.

Délai de notification :
La notification doit être faite dans les meilleurs délais et si possible, 72 heures au plus tard après en avoir pris connaissance.
En cas d'impossibilité de notifier en raison de la nécessité d'investiguer :
- Notification initiale dans un délai de 72 heures à la suite de la constatation avec la nécessité d'expliquer les motifs du dépassement du délai,
- Notification complémentaire dès que les informations complémentaires sont disponibles.

Documentation :
Pour toute violation de données personnelles, il y a obligation de documenter la traçabilité des violations de données personnelles (RGPD – Article 33). Cette obligation est applicable à tout responsable de traitement et sous-traitant.

Investigation :
Conduire une investigation afin d'identifier la source de la fuite (compromission du système d'information, malveillance interne, ...).

Notification de la direction générale :
L'objectif de cette notification est d'évaluer les différents impacts sur les personnes et les conséquences juridiques et financières (prévoir le déclenchement d'une cellule de crise selon la gravité de l'incident).

Sensibilisation :
Prévoir des séances de sensibilisation pour éviter d'autres fuites.

POINTS DE VIGILANCE

Une vigilance particulière devra être apportée dans plusieurs cas.

Traitement de données à risque, dites sensibles, c'est-à-dire :

- Révélant l'origine prétendument raciale ou ethnique ;
- Portant sur les opinions politiques, philosophiques ou religieuses ;
- Relatives à l'appartenance syndicale ;
- Concernant la santé ou l'orientation sexuelle ;
- Génétiques ou biométriques.

Traitement ayant pour objet ou pour effet :

- L'évaluation d'aspects personnels ou notation d'une personne (exemple : scoring financier) ;
- Une prise de décision automatisée ;
- La surveillance systématique de personnes (exemple : télésurveillance) ;
- Le traitement de données sensibles (exemple : santé, biométrie, etc.) ;
- Le traitement de données concernant des personnes vulnérables (exemple : mineurs) ;
- Le traitement à grande échelle de données personnelles ;
- Le croisement d'ensembles de données ;
- Des usages innovants ou l'application de nouvelles technologies (exemple : objet connecté) ;
- L'exclusion du bénéfice d'un droit, d'un service ou contrat (exemple : liste noire).

Si les traitements de données répondent à au moins 2 de ces 9 critères, il faut a priori conduire une analyse d'impact relative à la protection des données (DPIA), avant de commencer les opérations de traitement.
En complément de l'établissement du registre et de la description du traitement, cette analyse de l'impact sur la vie privée permettra d'identifier les risques associés à ces données personnelles. Il ne s'agit donc pas du même travail. Il conviendra d'être également très vigilant en cas de transfert de données en dehors de l'Union Européenne.

RISQUES

Atteinte à l'image et à la réputation de l'organisation, sanction pénale pouvant être de cinq ans d'emprisonnement et de 300 000 euros d'amende, Amende administrative en cas de sanction de la CNIL ou d'une autorité administrative (au minimum 20 millions d'euros pouvant atteindre jusqu'à 4% du CA du groupe) frais de notification, responsabilité civile... Connaître les peines encourues.

Au regard des droits et libertés, un risque est élevé si l'implication peut être :
Discrimination, vol ou usurpation d'identité, Perte financière, atteinte à la réputation, perte de confidentialité de données protégées par le secret professionnel.

POUR ALLER PLUS LOIN

- Formulaire de notification : Notification (cnil.fr)
  Notifications d'incidents de sécurité aux autorités de régulation : comment s'organiser et à qui s'adresser ?
- S'abonner à un service permettant d'être notifié en cas de fuite de données. Certains sites tels que haveibeenpwned?, regroupent les bases de données fuitées.
- Utiliser des mots de passe robustes et uniques.
- Utiliser des gestionnaires de mots de passe.
- Changer de mots de passe régulièrement.
- Activer l'authentification à double facteur.