LES BRÈVES

LES BRÈVES - LEGAL INFORMATION

PROPOSED BY DS GROUP

11 mars 2021

Comment gérer des violations de données personnelles ?

Le 14 janvier 2021, le Comité européen pour la protection des données personnelles (CEPD) a publié un projet de lignes directrices sur la gestion des violations de sécurité des données personnelles riche d'exemples pratiques. Ce document opère un rappel quant aux bonnes pratiques à mettre en œuvre dans la prévention et la gestion des atteintes à la sécurité des données personnelles.

Un guide pratique pour accompagner les responsables de traitement

Aujourd'hui, le projet de lignes directrices n°01/2021 fait l'objet d'une consultation publique ; il est donc sujet à d'éventuelles modifications par le CEPD.

Selon le degré de risque généré par la faille, les obligations du responsable de traitement varient. Ainsi, le responsable de traitement doit :

- notifier la Cnil lorsqu'il existe un risque pour les droits et libertés des personnes concernées ;
- informer les personnes affectées par la faille de sécurité lorsque ce risque est élevé.

Ces obligations sont à distinguer de la notification du sous-traitant au responsable de traitement, qui s'impose quelque soit le niveau de risque.

Afin d'aider les entreprises, le CEPD inclut dans les lignes directrices des **exemples concrets de failles** de sécurité, accompagnés d'analyses détaillées du niveau de risque et des obligations de notification.

Les entreprises peuvent s'appuyer sur ces lignes directrices pour estimer le niveau de risque associé à une faille de sécurité.

Face à une faille, déployer les moyens matériels et humains appropriés

Le responsable de traitement doit mobiliser des **moyens matériels et humains** pour effectuer une analyse approfondie de chaque faille de sécurité. Si besoin, le responsable de traitement peut **externaliser** à un prestataire spécialisé qui établira avec précision les caractéristiques techniques de la faille.

Cette analyse doit comprendre des informations exhaustives sur, entre autre :

- la qualité et l'intégrité du chiffrement appliqué aux données personnelles,
- les flux de données entrants et sortants,
- le périmètre des personnes affectées.

Lorsque des incertitudes demeurent sur ces différents aspects, le responsable de traitement doit faire preuve de **prudence** et retenir les hypothèses les moins favorables. Par exemple, lorsqu'un ransomware a chiffré la base clients et que l'analyse ne permet pas de déterminer si les hackers ont, oui ou non, extrait les données des clients de la base, avant de la chiffrer, l'entreprise doit considérer que les données ont été extraites.

Le responsable de traitement doit s'assurer que la **documentation** des failles de sécurité est **complète et adaptée à son activité** et à l'ampleur des failles de sécurité constatées. Cette documentation sert en effet de fondement à l'analyse sur les risques pour les personnes concernées, et peut à ce titre faire l'objet d'une **demande de communication par la Cnil**.

<u>Apprécier le niveau de risque de façon extensive</u>

Les lignes directrices du CEPD donnent des pistes de gestion des violations les plus courantes :

- attaques par ransomware,
- exfiltration de données,
- erreurs d'employés entraînant une divulgation accidentelle,
- vol ou perte de matériel ou de fichiers papier.

La réponse à apporter variera selon l'organisation interne de l'entreprise :

- L**'existence** ou l'**absence de mesures préventives**. Par exemple, lorsque les données sont indisponibles et que l'entreprise n'a pas de sauvegarde, le risque est aggravé pour les personnes concernées. A l'inverse, si les données sont hackées avant une exfiltration de mots de passe, alors le risque pour les personnes concernées est sensiblement réduit voire nul.

- La **mise en œuvre rapide de mesures d'atténuation** réduit l'ampleur des conséquences et donc le niveau de risque pour les personnes concernées.

- Des **éléments factuels** issus des caractéristiques techniques de la faille – **volume de données personnelles, présence de données sensibles, nombre de personnes affectées** – peuvent justifier une notification à la Cnil et une information des personnes concernées, même lorsque le responsable de traitement a adopté des mesures préventives ou d'atténuation.

- Le responsable de traitement doit aussi prendre en compte de façon **concrète** les **conséquences potentielles** de la faille pour les personnes concernées.

Par exemple, un hôpital a adopté des mesures préventives poussées mais est attaqué par un ransomware. L'hôpital doit notifier la faille de sécurité en raison de la nature sensible des données (données de santé) et du nombre élevé de patients. De plus, le risque est élevé pour les personnes concernées car, de façon très concrète, l'attaque peut décaler des opérations.

Dans une entreprise, le risque élevé peut être lié à des pertes financières (report d'un paiement ou d'une livraison), ou à un risque de sollicitation marketing non autorisée.

Les responsables de traitement doivent donc mener une **analyse approfondie des risques** induits par la faille de sécurité, en identifiant de façon précise les conséquences, avérées ou potentielles, de celle-ci sur les personnes concernées.

Bien réagir en cas de faille interne ou accidentelle

Les entreprises sont régulièrement confrontées à des erreurs humaines, qui peuvent être des failles de sécurité. L'entreprise doit les analyser avec le **même niveau de vigilance**.

Parmi ces situations courantes, on retrouve :

- l'envoi de mails à des destinataires erronés,
- la perte de fichiers électroniques, de fichiers papier, de clés USB, d'ordinateurs portables, etc.,
- la mauvaise configuration des accès dans une base de données.

Ces failles sont sanctionnables. Ainsi une entreprise polonaise a écopé d'une amende de 20 000 € : elle avait envoyé par e-mail une police d'assurance contenant les données personnelles – dont le numéro de sécurité sociale – d'un de ses clients à une adresse erronée. La sanction est prononcée pour deux manquements : ne pas avoir notifié cette faille à l'autorité de contrôle et ne pas avoir informé la personne concernée des potentielles conséquences négatives de la faille de sécurité[1].

Le responsable de traitement doit toujours s'interroger sur les conséquences possibles d'une erreur, même anodine.

Mises à jour des mesures techniques et des procédures

Les entreprises doivent procéder à un **réexamen périodique** des mesures techniques déployées et des procédures en place. Le responsable de traitement doit adopter une approche proactive afin de continuer à assurer un niveau approprié de sécurité des données personnelles et de ses systèmes IT.

Pour toutes autres informations, veuillez contacter l'auteure, Inès Jousset[2] ou notre équipe Propriété Intellectuelle, Technologie, Data.

Inès Jousset
Avocate Collaboratrice
jousset@dsavocats.com
Paris

Sylvain Staub
Avocat Associé
staub@dsavocats.com
Paris

[1] UODO, 9 déc. 2020, Warta (DKN.5131.5.2020) - Résumé sur le site du CEPD
[2] Cette brève a été rédigée avec le concours de Louis Mutz, Stagiaire DS Avocats