EDPS

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

LA VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL EN QUELQUES NOTIONS

QU'EST-CE QU'UNE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL?

Une **violation de données à caractère personnel** est un incident de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération ou la divulgation non autorisée de données à caractère personnel transmises, stockées ou traitées de quelque autre manière que ce soit, ou l'accès à ces données.

Tout incident lié à la sécurité de l'information n'est pas nécessairement une violation de données à caractère personnel, mais toute violation de données à caractère personnel est un incident lié à la sécurité de l'information.

Des violations de données à caractère personnel peuvent se produire en raison:

- d'erreurs humaines, lorsque des informations sont envoyées par courrier électronique à la mauvaise personne;
- de la perte ou du vol de dispositifs contenant des données à caractère personnel non cryptées;
- de méthodes d'authentification faibles qui permettent un accès non autorisé aux bases de données.

QUE FAIRE EN CAS DE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL?

- Identifier l'incident de violation des données à caractère personnel.
- Notifier la violation à votre délégué à la protection des données (DPD) – il s'agit d'une **obligation** en vertu de la législation européenne sur la protection des données.
- Traiter **immédiatement** la violation de données afin d'atténuer tout risque immédiat pour les données à caractère personnel des personnes concernées.
- Documenter la violation des données selon le principe de **responsabilisation**.
- Évaluer l'impact de la violation des données à caractère personnel sur les droits et libertés des personnes.
- Si vous êtes un **sous-traitant**, vous devez immédiatement en informer le **responsable du traitement** des données de votre organisation ou de votre institution de l'Union européenne (UE).
- En tant qu'institution, organe ou agence de l'UE, vous êtes tenu d'informer le Contrôleur européen de la protection des données (CEPD) sans retard injustifié et, si possible, au plus tard 72 heures après la violation.
- Informer les personnes concernées de la violation des données à caractère personnel, si nécessaire.
- Réviser vos procédures et mettre à jour vos mesures.

QUELS SONT LES TYPES DE VIOLATIONS QUI PEUVENT SE PRODUIRE?

Violation de la confidentialité: une entité ou une personne accède à des données à caractère personnel sans y avoir droit.

Violation de la disponibilité: perte de l'accès aux données à caractère personnel et de leur contrôle, ou suppression inappropriée de données à caractère personnel.

Violation de l'intégrité: toute modification inadéquate de données à caractère personnel.

QUI EST CONCERNÉ EN CAS DE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL?

- La direction (appelée à rendre des comptes)
- Le propriétaire
- Le délégué à la protection des données
- Le département informatique (le cas échéant)
- Les sous-traitants (le cas échéant)
- L'équipe de communication (le cas échéant)

QUE FAIT UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES?

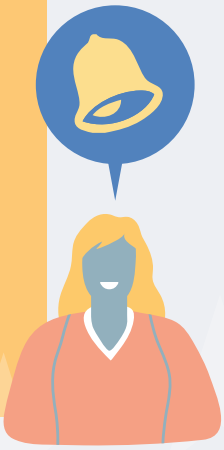
Un DPD:

- donne des conseils sur l'évaluation de l'impact pour les personnes concernées et sur la nécessité de notifier les violations de données à caractère personnel, sur demande;
- recommande des mesures pour limiter les risques liés à la violation des données;
- est la personne de contact pour les particuliers;
- est la personne de contact pour le CEPD;
- communique avec les responsables de la sécurité sur la gestion des risques liés à la sécurité de l'information et sur la politique en matière de violation des données;
- prépare et met en œuvre des programmes de sensibilisation à l'intention du personnel;

COMMENT NOTIFIER UNE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL AU CEPD

En cas de violation de données à caractère personnel, toutes les institutions de l'UE doivent informer le CEPD:

- en utilisant le formulaire web spécialement prévu où la communication est cryptée;
- en envoyant la notification dès que possible et au plus tard 72 heures (si possible) après la détection de la violation. En cas de retard, vous devez en expliquer les raisons.;
- si toutes les informations concernant l'incident ne sont pas disponibles, vous devez notifier la violation par étapes. Cela suppose d'envoyer une première notification et une évaluation initiale du risque, puis, dès que possible, de faire suivre toute information susceptible de compléter votre première notification de la violation.



QUAND FAUT-IL COMMUNIQUER UNE VIOLATION DES DONNÉES À DES PARTICULIERS?

La communication d'une violation de données à caractère personnel à des particuliers est obligatoire lorsque cette violation est susceptible d'entraîner **des risques élevés pour les droits et libertés des personnes concernées**.

Toutefois, certaines exemptions existent, par exemple:

- quand des mesures techniques ou organisationnelles ont déjà été appliquées aux données concernées par la violation, comme le cryptage;
- quand des mesures ultérieures ont été prises afin que le risque élevé pour les droits et libertés des personnes concernées ne soit plus une menace.

QUAND COMMUNIQUER UNE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL À DES PARTICULIERS?

- Utilisez un langage clair et intelligible, de préférence sous forme écrite. Évitez les termes techniques sources de confusion pour les personnes.
- Décrivez l'incident, expliquez ce qui s'est passé et pourquoi, comment les données des personnes concernées ont été compromises et quelles en sont les conséquences.
- Indiquez les coordonnées de votre DPD et les mesures que vous avez prises, en tant que responsable du traitement des données à caractère personnel, pour remédier à la violation des données à caractère personnel.
- Au besoin, proposez aux personnes concernées des mesures pour se protéger (par exemple, si des mots de passe ont été volés, recommandez-leur d'en changer si elles utilisent des mots de passe identiques pour d'autres sites web).

Si la communication de cette violation suppose un effort disproportionné, il est possible d'envisager une communication publique ou une mesure similaire, mais il faut veiller à ce que les personnes concernées soient informées d'une manière tout aussi efficace.

PRENEZ DES MESURES PROACTIVES POUR MINIMISER LES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL!

Afin de minimiser les risques de violation des données à caractère personnel, le CEPD vous recommande d'instaurer au sein de votre organisation une culture de la protection et de la sécurité des données. En d'autres termes, redéfinissez vos opérations de traitement des données afin que les considérations de sécurité soient au cœur de celles-ci par défaut. Ces considérations devraient surtout porter sur:

- une politique et une formation du personnel en vue d'une utilisation prudente des courriers électroniques;
- l'emploi de mots de passe sécurisés et d'une authentification à deux facteurs;
- des copies de sauvegarde de vos systèmes;
- des mises à jour régulières et obligatoires du système.
- des précautions visant à éviter l'exposition de vos services sur l'internet;
- l'utilisation du cryptage sur vos outils informatiques.

EN CAS DE DOUTES, CONTACTEZ-NOUS!

Pour plus d'informations:

- visionnez notre vidéo informative sur les violations de données à caractère personnel;
- consultez les pages web du CEPD sur les violations de données à caractère personnel;
- lisez les Lignes directrices du CEPD sur les notifications de violations de données à caractère personnel.

edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor

QT-02-21-587-FR-N ISBN: 978-92-9242-693-4 DOI: 10.2804/225599