Comment gérer une violation des données ?

Une violation de données est un incident de sécurité qui concerne les données personnelles que détient un responsable du traitement. Or, la Loi n° 1.565 du 3 décembre 2024 introduit une nouvelle obligation à la charge du responsable du traitement : la notification de **toute violation des données à caractère personnel dont il a connaissance** dès lors que celle-ci est **susceptible** d'engendrer un **risque pour les droits et libertés des personnes concernées.**

Le risque zéro n'existant pas, il est important de mettre en place des mesures en amont pour prévenir la survenance de toute violation mais également un plan d'action afin de faire face au mieux à la survenance d'un incident et d'y répondre conformément à la Loi.

Pour cela 6 étapes à suivre sont recommandées, qui peuvent se résumer comme suit :

- Prévention
- Détection
- Evaluation
- Atténuation des risques
- Communication
- Gestion post-incident

Etape 1 : Prévention

Mieux vaut prévenir que guérir…

Une violation de données peut arriver n'importe quand, à n'importe qui. Il est donc sage d'être proactif et de se préparer au pire, en mettant en place une véritable politique de sécurité informatique.

Les 15 règles de bases de la sécurité informatique

1. Protection des locaux
2. Sécurisation des postes de travail, des serveurs et de l'informatique mobile
3. Formation et sensibilisation des utilisateurs du Système d'Information
4. Authentification des utilisateurs
5. Gestion des habilitations
6. Encadrement de la sous-traitance
7. Traçabilité des opérations
8. Sécurisation des échanges avec l'extérieur
9. Sauvegardes régulières
10. Encadrement de la maintenance et de la fin de vie des matériels et logiciels
11. Procédures d'alertes
12. Politique de gestion des incidents de sécurité
13. Analyse des risques
14. Audits de sécurité
15. Politique de continuité et de reprise de l'activité

Etape 2 : Détection

Si la plupart des incidents se produisent en quelques secondes seulement, la détection, elle, prend en général beaucoup plus de temps. Il est donc important d'avoir en place des mécanismes de surveillance et d'alertes afin de remonter au plus vite tout activité anormale pouvant survenir en interne. Une détection précoce d'une violation est en effet essentielle pour en minimiser son impact.

Exemples d'activités suspectes :

- Des accès inhabituels et nombreux à des fichiers
- Des mouvements de données en masse
- Des tentatives de connexion non autorisées
- Un accès non autorisé à des données sensibles
- Un trafic réseau inhabituel
- Des courriels suspects
- Une demande de rançongiciels

Cette étape doit être menée en concertation avec tous acteurs concernés (Equipe informatiques, Service des Ressources Humaines, prestataires externes, etc.)

Etape 3 : Evaluation

Une violation de données est un incident de sécurité mais tout incident ne constitue pas une violation.

Aussi, dès la constatation d'un incident, il convient d'en évaluer la portée et l'impact afin de déterminer s'il s'agit effectivement d'une violation de données et s'il convient de notifier l'Autorité de Protection des Données et, si besoin, les personnes concernées.

Un questionnaire « *violation des données* » et une grille d'analyse des risques élaborés en amont seront utiles pour évaluer la gravité de la violation.

Exemple de questionnaire « *violation de données* » :

- Quand s'est produit la violation ?
- Quelle est la cause de la violation ?
  - interne
  - externe
- Quelle est la nature de la violation ?
  - violation accidentelle
  - violation intentionnelle (vol, piratage etc.)
- Quelles sont les données concernées par la violation ?
  - ordinaires (identité, adresses, caractéristiques financières, etc.)
  - sensibles (sensibles, appartenance politiques, etc.)
- Combien de personnes sont concernées par la violation ?
- Quel est l'impact de la violation ?
  - violation de la confidentialité (divulgation des données ou accès non autorisé ou accidentel aux données)
  - violation de l'intégrité (altération non autorisée ou accidentelle des données)
  - violation de la disponibilité (destruction ou perte accidentelle ou non autorisée de l'accès aux données)
- Quel est le degré de risque pour les droits et libertés des personnes concernées ?
  - risque faible
  - risque moyen
  - risque élevé
- L'APDP doit-elle être notifiée ?
- Les personnes concernées doivent-elles être informées ?

Etape 4 : Atténuation des risques

Répondre à une violation de données consiste avant tout à contenir et à isoler l'incident afin d'empêcher que les données ne soient davantage compromises et de limiter la propagation de cet incident. Un plan d'intervention en cas d'incident élaboré en amont pourra vous y aider. Celui-ci doit décrire les mesures préventives et les procédures détaillées à suivre.

Exemples d'actions :

- Déconnecter les appareils ou logiciels concernés
- Bloquer les adresses IP ou les domaines malveillants
- Bloquer les comptes compromis
- Modifier les mots de passe
- Mettre en place des barrières virtuelles pour contenir l'incident
- Restaurer les données à partir de sauvegardes

Il est important de documenter toutes les actions effectuées.

Etape 5 : Communication

Toute violation de données n'a pas à être notifiée à l'APDP.

L'article 32 de la Loi n° 1.565 du 3 décembre 2024 dispose en effet que le responsable du traitement doit notifier à l'APDP **toute violation dont il a connaissance et qui est susceptible** d'engendrer **un risque pour les droits et libertés des personnes concernées.**

Cette notification doit intervenir **dans les meilleurs délais**, et si possible dans un délai maximum de **72 heures après en avoir pris connaissance**.

Par ailleurs, si la violation est **susceptible** d'engendrer un **risque élevé pour les droits et libertés** d'une personne physique, le responsable du traitement doit également **communiquer** cette violation à la personne concernée **dans les meilleurs délais.**

L'appréciation du risque élevé se fait à la lumière d'un incident particulier et repose sur les conséquences qui en découlent.

La communication doit en principe s'effectuer **directement** auprès des personnes concernées, à moins que cela n'exige des efforts disproportionnés. Elle doit par ailleurs être **claire** et **transparente**.

Exemples de moyens de communication :

- messages directs (e-mail, SMS, message directe)
- notifications ou bannières bien visibles sur le site Internet
- communications postales
- annonces bien visibles dans des médias imprimés

L'informations des personnes concernées peut être accompagnée de **recommandations pour atténuer les effets négatifs potentiels de la violation** et leur permettre de prendre les précautions qui s'imposent.

Etape 6 : Gestion post-incident

« L'erreur est une formidable opportunité d'apprentissage. » - Jane Nelsen

La violation de données a été contenue et si nécessaire l'APDP a été notifiée et les personnes concernées contactées. Reste maintenant à analyser l'incident afin d'éviter qu'une violation similaire ne se reproduise.

Il faut donc comprendre ce qui s'est passé, pourquoi l'incident s'est produit, comment il a été géré et ce qui peut être amélioré.

Il convient également de surveiller les actions correctives qui ont été prises afin de les améliorer si besoin.

Enfin, il faudra tirer les enseignements de cette violation et mettre en place un processus d'amélioration continue qui pourra contenir des recommandations, telles que l'amélioration de la sensibilisation des collaborateurs à la sécurité, la formation, les tests ou l'audit.

L'importance du registre des violations de données

Le responsable du traitement **doit documenter** toute violation de données personnelles, même quand il n'est pas tenu de notifier l'APDP.

Cette documentation doit indiquer :

- **les faits** concernant la violation,
- **ses effets** et
- **les mesures** prises pour y remédier.

Il est recommandé de documenter également les **décisions prises en réaction à la violation**, notamment lorsque le responsable du traitement n'a pas notifié la violation de données, les raisons pour lesquelles il a estimé que cette violation était peu susceptible d'engendrer des risques.

[Pour plus d'information, voir **Les notifications de violations de données personnelles**]