AUTORITÉ DE PROTECTION DES DONNÉES PERSONNELLES
(APDP)

FORMATION DES DELEGUES À LA PROTECTION DES DONNEES PERSONNELLES

Thème: Gestion des violations de données Personnelles

Intervenant : **Emmanuel ZOSSOU**

Décembre 2021

SOMMAIRE

INTRODUCTION

De la gestion à la production en passant par le marketing, quel que soit le secteur d'activité, l'informatique et plus généralement les réseaux sont omniprésents et rendent vulnérable toute organisation face aux failles de sécurité.

- Qu'est-ce qu'une violation de données?

- Comment notifier à l'Autorité de contrôle et informer les clients et partenaires lorsque la faille de sécurité a conduit à une violation de données à caractère personnel ?

- Quelles sont les organisations soumises à cette obligation de notification et d'information ?

INTRODUCTION

- Quelles sont les mesures de protection appropriées et les actions qui doivent être mises en œuvre ?

- Quels sont les recours et sanctions en cas d'exploitation d'une faille de sécurité par des pirates informatiques ?

- Comment ce cyber risque est-il couvert par les assureurs?

Les réponses à ces questions intéressent toutes les organisations en général et les Délégués à la Protection des Données (DPD ou DPO en anglais) en particulier, quel que soit leur secteur d'activité.

INTRODUCTION

- L’article 1 de la LOI N°2017 -20 du 20 Avril 2018, Portant Code du Numérique en République du BENIN, définit une **violation de données à caractère personnel**, également appelé dans le langage courant “faille de sécurité”, comme :

« une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».

- Cette expression recouvre tous les éléments qui portent atteinte à un système de traitement automatisé de données :
  - ✓ les erreurs,
  - ✓ les bogues, mais aussi
  - ✓ les fraudes internes et externes.

INTRODUCTION

Il existe trois (03) types, en termes de niveaux de risques et également de types de violation. trois typologies ressortent :

1. **la violation de la confidentialité**, *qui est la plus courante. Elle consiste en la divulgation ou l'accès non autorisé ou accidentel à des données à caractère personnel.*

2. **la violation de l'intégrité** : *l'altération non autorisée ou accidentelle de données à caractère personnel.*

3. **la disponibilité** : *la destruction ou la perte accidentelle ou non autorisée de données personnelles.*

I. ACTEURS ET OBLIGATIONS

A. Acteurs impliqués et responsabilités dans la gestion des violations

Tous les organismes, publics comme privés et quelle que soit leur taille, sont soumis à ces obligations dès lors qu'ils traitent des données personnelles et qu'ils ont connaissance d'une violation de données personnelles.

Les sous-traitants, qui traitent des données personnelles pour le compte d'un organisme responsable du traitement, ont également des obligations en matière de violation :

ils doivent en particulier alerter l'organisme de tout incident de sécurité dans les meilleurs délais afin qu'ils puissent remplir ses obligations.

L'APDP peut recevoir les notifications des cas de violations et peut contrôler les registres du responsable de traitement .

I. ACTEURS ET OBLIGATIONS

B. Les principales obligations en matière de violation de données

Les principales obligations en matière de violation de données sont :
- **La documentation de la violation par le responsable de traitement**
- **La notification ou non de la violation l'APDP ou à la personne concernée.**

Ces obligations sont variables en fonction du risque soulevé par les violations :

toutes les violations ne doivent pas nécessairement être notifiées à l'autorité de contrôle ou aux personnes concernées.

Lorsqu'elle est nécessaire, cette information des personnes concernées doit en revanche être la priorité du responsable du traitement, car cela leur permet de prendre des mesures destinées à les protéger de ces risques.

Ainsi, l'obligation de notifier dépend du risque que la violation de données personnelles fait peser sur les droits et libertés des individus dont les données ont été impactées :

I. ACTEURS ET OBLIGATIONS

B. Les principales obligations en matière de violation de données

Si la violation n'entraîne pas de risque pour les droits et libertés des personnes concernées, **le responsable du traitement** :

- doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;
- ne doit pas notifier cette violation ni aux personnes concernées, ni à l'Autorité de Contrôle, qui peut en revanche contrôler cette documentation interne,

Si la violation entraîne un risque pour les droits et libertés des personnes concernées, le responsable du traitement :

- doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;
- doit notifier cette violation à l'Autorité de Contrôle, au plus tôt et dans un délai maximal de 72h.

I. ACTEURS ET OBLIGATIONS

B. Les principales obligations en matière de violation de données

Si la violation entraîne un risque élevé pour les droits et libertés des personnes concernées, **le responsable du traitement** :

- doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;

- doit notifier cette violation à l'Autorité de Contrôle, au plus tôt et dans un délai maximal de 72h ;

-doit communiquer la violation aux personnes concernées, au plus tôt.
-

I. ACTEURS ET OBLIGATIONS

C. Le registre des violations

- La documentation doit consigner les faits concernant la violation de données à caractère personnel, **ses effets** et **les mesures** prises pour y remédier.

- Elle peut être contrôlée par l'APDP dans l'objectif de vérifier le respect des obligations en matière de violations.

- En pratique, il est conseillé aux responsables du traitement de recenser l'ensemble des éléments relatifs aux violations et de s'appuyer sur le formulaire de notification mis en ligne par l'Autorité de Contrôle le cas échéant.

- Ce formulaire peut en effet servir de canevas pour la documentation interne, qui peut ainsi constituer un outil unique de gestion de la conformité avec le Code Numérique en matière de violations.

I. ACTEURS ET OBLIGATIONS

C. Le registre des violations

....

- **Le registre des violations devrait notamment contenir les éléments suivants :**

✓la nature de la violation ;
✓les catégories et le nombre approximatif des personnes concernées ;
✓les catégories et le nombre approximatif de fichiers concernés ;
✓les conséquences probables de la violation ;
✓les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation ;
✓le cas échéant, la justification de l'absence de notification auprès de l'APDP ou d'information aux personnes concernées.

II. La mise en œuvre pratique des obligations

A. Le contenu de la notification et de la correction

Que faut-il notifier à l'autorité de contrôle ?

La notification doit **contenir *à minima*** les éléments suivants :

- ✓ la nature de la violation ;
- ✓ les catégories et le nombre approximatif des personnes concernées ;
- ✓ les catégories et le nombre approximatif de fichiers concernés ;
- ✓ les conséquences probables de la violation ;
- ✓ les coordonnées de la personne à contacter (**DPO** ou autre) ;
- ✓ les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation.

II. La mise en œuvre pratique des obligations

A. Le contenu de la notification et de la correction

Que faut-il communiquer aux personnes concernées ?

La notification aux personnes concernées doit *à minima* **contenir** et exposer, en des termes clairs et précis, les éléments suivants :

- ✓ La nature de la violation ;
- ✓ les conséquences probables de la violation ;
- ✓ les coordonnées de la personne à contacter (DPO ou autre) ;
- ✓ les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation.

Elle doit être complétée, dès lors que cela est nécessaire, de recommandations à destination des personnes pour atténuer les effets négatifs potentiels de la violation et leur permettre de prendre les précautions qui s'imposent

Exemples de recommandations : changement de mot de passe des utilisateurs d'un service, vérification de l'intégrité des données de leur compte en ligne, sauvegarde de ces données sur un support personnel

II. La mise en œuvre pratique des obligations

B. La mise en œuvre de l’obligation de notification

Quel est le rôle du sous-traitant en cas de violation de données ?

Le sous-traitant doit notifier au responsable du traitement toute violation de données dans les meilleurs délais après en avoir pris connaissance.

Cela permet au responsable du traitement de respecter ses différentes obligations en matière de violation de données.

En pratique, il est conseillé de prévoir dans le contrat qui lie le sous-traitant au responsable du traitement une obligation en ce sens à la charge du sous-traitant.

Les contrats entre responsables et sous-traitants peuvent prévoir des obligations plus strictes en termes de notification (e.g. délais spécifiques, devoir de collaboration spécifique…).

Il existe donc un risque de manquement contractuel en l’absence de notification rapide.
Les contrats entre responsables et sous-traitants peuvent également prévoir que la notification est déléguée au sous-traitant.

II. La mise en œuvre pratique des obligations

B. La mise en œuvre de l'obligation de notification

L'obligation de notifier à l'autorité de contrôle peut-elle être confiée au sous-traitant ?

Oui. Le responsable du traitement peut demander au sous-traitant d'agir en son nom afin que ce dernier notifie la violation à l'autorité de contrôle, si le responsable du traitement estime que la violation en cause est susceptible de présenter un risque pour les personnes concernées.

Cela n'écarte donc ni l'obligation faite au sous-traitant d'informer le responsable du traitement de toute violation de données, ni les obligations propres au responsable du traitement : ce dernier doit mettre à jour son registre des violations et rester maitre de la décision de notifier ou non à l'autorité de contrôle (en fonction du niveau de risque estimé).

II. La mise en œuvre pratique des obligations

B. La mise en œuvre de l'obligation de notification

Quels sont les pouvoirs de l'APDP en matière de violation de données ?

L'APDP exerce deux missions principales en matière de violation de données : un rôle d'accompagnement des responsables de traitement et un rôle de contrôle du respect des obligations par les responsables du traitement.

1. **Du rôle d'accompagnement des responsables du traitement** :
   la notification à l'autorité de contrôle a notamment pour but de permettre :

   - ✓ aux responsables du traitement de recueillir les éventuels conseils et observations de l'APDP s'agissant des mesures de sécurité à mettre en œuvre pour mettre fin à la violation ou pour minimiser ses effets ;

   - ✓ de vérifier si une information des personnes est nécessaire et, dans ce cas, d'obtenir des recommandations sur les modalités de cette information

II. La mise en œuvre pratique des obligations

B. La mise en œuvre de l'obligation de notification

Quels sont les pouvoirs de l'APDP en matière de violation de données ?

2. Un rôle de contrôle du respect des obligations des responsables du traitement **:**

L'APDP peut contrôler le respect de l'ensemble de ces obligations

- inscription au registre,
- vérification du niveau de risque,
- respect des délais et du
- contenu des notifications, etc. et,

Le cas échéant, elle peut sanctionner les organismes concernés.

Elle peut également ordonner au responsable du traitement de communiquer une violation de données aux personnes concernées, si cela lui apparaît nécessaire.

Dans les deux cas, l'examen de l'APDP est susceptible de porter, au-delà de la seule violation en cause, sur le niveau de sécurité générale du traitement que la violation peut révéler.

II. La mise en œuvre pratique des obligations

B. La mise en œuvre de l'obligation de notification

Quelles mesures peuvent être mises en place par les entreprises pour prévenir ces violations ?

- Il faut d'abord porter une grande attention à la sécurité.

- Il est important de faire une analyse des risques et de mettre en place les mesures élémentaires de sécurité.

Les failles de sécurité peuvent résulter d'un manquement ou d'un agissement des **sous-traitants**.

*C'est pourquoi dans les relations entre les responsables et les sous-traitants, la sécurité doit être **très bien encadrée** .*

L'encadrement des sous-traitants doit être beaucoup plus contrôlé aujourd'hui : il faut que le sous-traitant soit en mesure d'expliquer les mesures de sécurité mises en place afin que le responsable puisse les valider, les vérifier et être informé de toute modification.

II. La mise en œuvre pratique des obligations

B. La mise en œuvre de l'obligation de notification

Quelles mesures peuvent être mises en place par les entreprises pour prévenir ces violations ?

.....

- Il convient également :
  - ✓ D'adopter des mesures organisationnelles en sensibilisant le personnel des entreprises sur le sujet de la protection des données et de la sécurité ;
  - ✓ De formaliser des procédures afin d'être préparé lorsqu'une violation survient en créant une cellule de crise,
  - ✓ De faire des tests, opérer des audits de sécurité et des tests de ***pénétration ou d'intrusion*** afin de repérer les failles…

- L'anticipation est primordiale.

- Par ailleurs, les entreprises peuvent **faire appel à certains logiciels ou services spécialisés** qui permettent de détecter les incidents de sécurité, ou d'identifier les fuites d'informations sur Internet et sur le « **dark web** », qui se développent sur le marché.

II. La mise en œuvre pratique des obligations

B. La mise en œuvre de l’obligation de notification

Cas particulier : les violations touchant un traitement transfrontalier

Pour un traitement transfrontalier, l’autorité « chef de file » constitue l’unique interlocuteur du responsable du traitement.

C’est donc auprès de cette autorité que la notification d’une violation doit être réalisée.

Cette autorité n’est pas nécessairement l’APDP.

CONCLUSION

Au regard de ce qui précède il est évident qu'Il existe un réel enjeu pour les entreprises dans la gestion des violation des DP.

Tous les organismes qui traitent des données personnelles doivent donc impérativement mettre en place des mesures pour :

- ✓ prévenir les violations de données et
- ✓ réagir de manière appropriée en cas d'incident.

Ces mesures viseront ou concerneront à la fois :

- ✓ **les responsables du traitement** : afin de protéger leur patrimoine informationnel, en leur permettant notamment de sécuriser leurs données ; et
- ✓ **les personnes affectées par la violation** : afin d'éviter qu'elle ne leur cause des dommages ou préjudices, en leur permettant notamment de prendre les précautions qui s'imposent en cas d'incident.

CONCLUSION

- Il est dès lors recommandé que les organismes qui traitent des données personnelles (responsable du traitement ou sous-traitant) prévoient et **mettent en place des procédures globales en matière de violation de données personnelles.**

- Ces procédures doivent concerner l'ensemble du processus : la mise en place de mesures visant à détecter immédiatement une violation, à l'endiguer rapidement, à analyser les risques engendrés par l'incident et à déterminer s'il convient de notifier l'autorité de contrôle, voire les personnes concernées.

- Afin de mettre en œuvre rapidement et efficacement les procédures, il faut donc de la sécurité, de l'organisation et de l'anticipation.

Merci pour votre aimable attention

Veuillez retrouver le présent slide : https://apdp.bj/formation-des-dpo-2021/

Pour plus de renseignements rendez-vous sur le site de l’APDP aux liens suivants :

- https://www.apdp.bj
- https://apdp.bj/les-outils-de-la-conformite/
- https://apdp.bj/procedures/