GESTION DES INCIDENTS DE VIOLATION DES DONNEES A CARACTERE PERSONNEL

APDP, Cotonou 21 Décembre 2022

JURISTE

Alao Olayodé ADJASSA

Juriste spécialisé en droit du numérique,

Président de 360 Conseils SAS

+229 67 10 30 10 / 67 96 72 72

infos@360conseils.com

www.360conseils.com

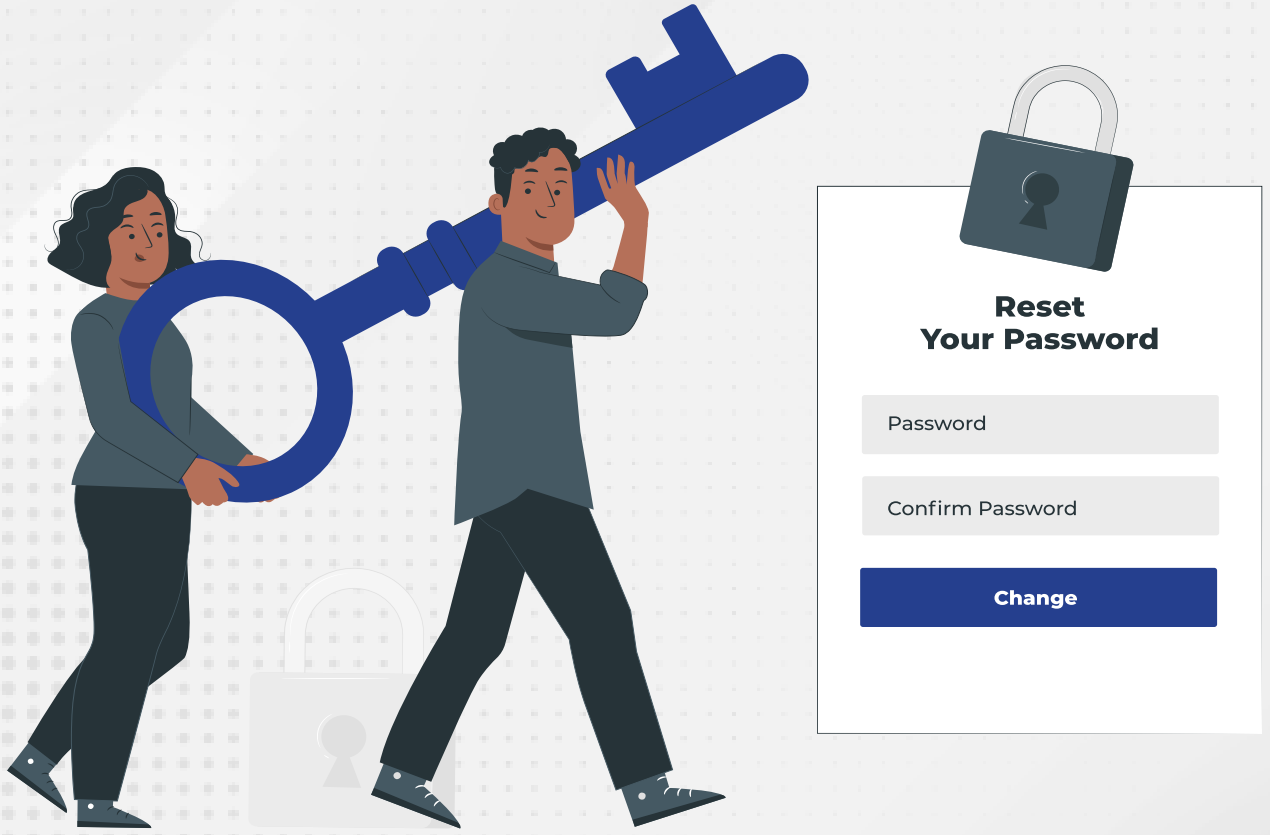
Table des matières

A. INTRODUCTION

La sécurité des données est un corollaire de l'accountability et une prescription de l'article 426 du Code du numérique. Au regard de la difficulté à protéger les données à cette ère numérique, l'obligation de sécurité parait rude.

Néanmoins la rigueur de l'obligation est nuancée par la prise en compte de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié tenant compte, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

Comme en gestion de risques, dans le cadre du pilotage de sa politique des données, il incombe donc au responsable du traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées, pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, l'interception notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.



Ainsi, la gouvernance interne devrait-elle permettre de mettre en place des procédures qui garantissent la protection des données à tout instant, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement

(ex : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire).

Un outil important de cette gouvernance interne se révèle être la politique de gestion des incidents de violation des données à caractère personnel.

B. CLARIFICATIONS SEMANTIQUES

La notion de violation de données à caractère personnel est définie à l'article 1er du Code du numérique comme :

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

Une violation de données est donc un incident de sécurité portant sur des données à caractère personnel (en revanche, tout incident de sécurité ne constitue pas nécessairement une violation de données à caractère personnel).

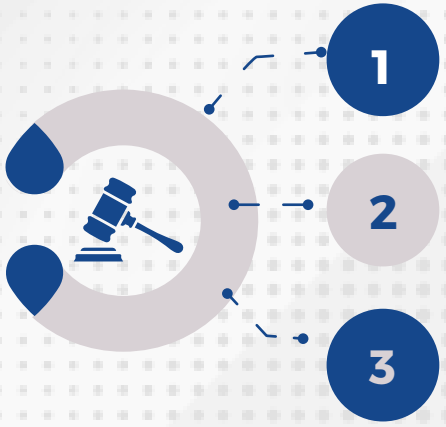
Il existe trois grandes catégories de violations de données à caractère personnel :

1. **Les violations portant sur la confidentialité :** accès potentiel ou avéré aux données à caractère personnel par des personnes autres que celles autorisées à y accéder pour une finalité particulière (accès non autorisé).

2. **Les violations portant sur la disponibilité des données :** destruction, perte ou altération accidentelle ou non autorisée de données à caractère personnel rendant les données inaccessibles (perte de contrôle de l'accès aux données),

3. **Les violations portant sur l'intégrité des données :** altération non autorisée ou accidentelle des données à caractère personnel (modifications indésirées).

Une violation de données à caractère personnel peut survenir notamment pour les raisons suivantes :



1. La perte/le vol d'un moyen de communication ;
2. Une sécurité insuffisante/ une défaillance technique.
3. Des processus opérationnels erronés/ des erreurs/négligences humaines dans le traitement des données/ des actes intentionnels malveillants par des acteurs internes ou externes ;

Exemples :

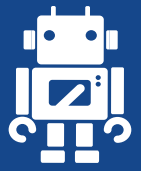
- Perte d'un ordinateur portable, d'une clé USB Vol/destruction d'équipements
- Accès au système donné par erreur à une mauvaise personne
- Envoi d'un courriel à la mauvaise personne
- Utilisation d'un canal de communication non sécurisé pour échanger des données à caractère personnel sensibles
- Accès à des données à caractère personnel par des collaborateurs en dehors du cadre de leur autorisation professionnelle
- Divulgation non autorisée de données à caractère personnel
- Utilisation non autorisée/contraire aux finalités du système d'information
- Documents papiers non rangés laissé à la portée de tiers
- Attaque informatique (hameçonnage, rançongiciel)
- Défaillance système
- Absence de mot de passe sécurisé sur les ordinateurs, les appareils ou les applications contenant des données à caractère personnel.

Les principaux types de violations de données peuvent être regroupés par catégories :

Rançongiciel

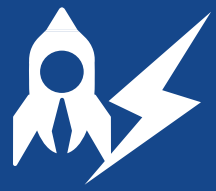
Sans exfiltration de données et avec sauvegarde ; Sans sauvegarde ; Dans un hôpital (avec sauvegarde et sans exfiltration) ; Avec exfiltration et sans sauvegarde.

Attaque exfiltration de données



Exfiltration de données de candidature à des offres d'emploi ; Exfiltration de mots de passe hachés ; Bourrage d'identifiants sur un site bancaire (credential stuffing).

Source interne risque humain

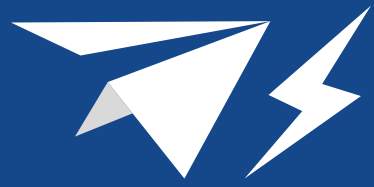


Exfiltration de données d'entreprise par un employé ; Transmission accidentelle à un tiers.

Appareils ou documents papier perdus ou volés

Matériel volé contenant des données personnelles chiffrées ; Matériel volé stockant des données personnelles non chiffrées ; Documents papier volés contenant des données sensibles.

Erreur d'envoi



Erreur d'envoi postal de factures d'achat en ligne ; Données personnelles hautement confidentielles envoyées par courriel par erreur ; Données personnelles envoyées par courriel par erreur ; Erreur d'envoi postal de documents d'assurance.

Ingénierie sociale

Vol d'identité; Exfiltration de courriels.

ANTICIPER LA VIOLATION

Aux termes du Code du numérique, le traitement des données à caractère personnel doit être réalisé par un responsable du traitement accountable, dans le respect du principe de confidentialité et de sécurité et surtout dans le respect du principe de privacy by design, by default.

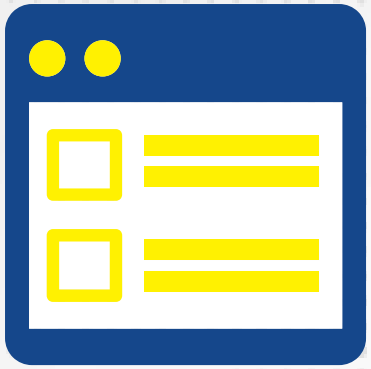
Le responsable du traitement accountable est un responsable du traitement qui se comporte en bon père de famille qui met en œuvre toute mesure appropriée pour être conforme aux exigences du Code du numérique. Il respecte à ce titre le principe de confidentialité et de sécurité des données à caractère personnel en préservant du mieux qu'il peut, leur Confidentialité, leur Intégrité, leur Disponibilité et la non-répudiation des actions passées sur elles.

Enfin, le responsable du traitement doit prendre en compte la protection de la vie privée dès la conception de son traitement et par défaut.

La démonstration de ce sens de responsabilité passe entre autres par la mise en place des politiques et procédures efficientes, connues et maîtrisées des acteurs intervenant dans la chaîne du traitement des données à caractère personnel exploitée. En effet, ce serait une peine perdue d'élaborer une politique de gestion des violations des données qui n'est ni connue ni adopter par ceux qui sont impliqués dans le traitement de ces données.

A La charte informatique

La charte informatique est un document qui précise les règles à respecter en matière de sécurité informatique, mais aussi celles relatives au bon usage de la téléphonie, de la messagerie électronique ou encore d'internet.
En pratique, la charte informatique permet d'informer le salarié sur :

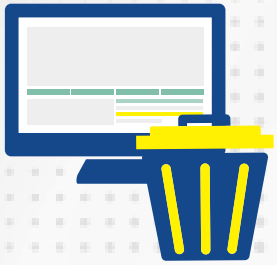


- les usages permis des moyens informatiques mis à sa disposition ;
- ses droits et obligations en matière de traitement de données à caractère personnel ;
- les règles de sécurité en vigueur ;
- les mesures de contrôle prises par l'employeur pour assurer notamment le respect de ces règles ;
- les sanctions encourues en cas de non-respect de ces règles.

La charte informatique doit préciser les obligations auxquelles sont tenus les salariés au titre de la protection des données personnelles, ainsi :

- signaler au service informatique interne toute violation ou tentative de violation suspectéedesoncompteinformatiqueetdemanièregénéraletoutdysfonctionnement
- verrouiller son ordinateur dès que l'on quitte son poste de travail ;
- respecter certaines procédures (par exemple, demander l'accord d'un supérieur hiérarchique) afin d'encadrer certaines opérations (par exemple, la copie de données sur des supports amovibles).

La charte informatique listera également les interdictions faites aux salariés. Par exemple, l'interdiction de :



- confier ses identifiant et mot de passe à un tiers ;
- copier, installer, modifier ou détruire des logiciels sans autorisation ;
- supprimer des informations si cela ne relève pas des tâches incombant au salarié.

Pour donner à cette charte informatique une force contraignante, celle-ci pourra être intégrée ou annexée au règlement intérieur.

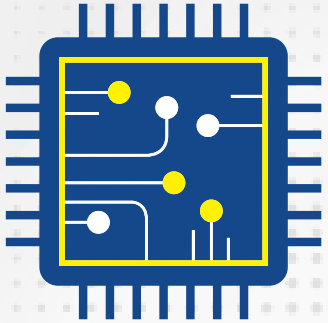
B La politique de gestion des violations

Le respect de l'obligation d'accountability impose la mise en place d'une procédure destinée à assurer la détection de telles violations, d'en évaluer la gravité et de mettre en œuvre les mesures appropriées afin de minimiser les risques, réduire les impacts pour les personnes concernées et identifier toute action utile permettant de prévenir la survenance de nouvelles violations.

La procédure devrait permettre de définir la conduite à tenir en cas de survenance d'une violation de donnée à caractère personnel et identifier les responsabilités afin de permettre la réalisation des notifications prévues par le Code du numérique et organiser la traçabilité des violations de données à caractère personnel.

> *La procédure devra s'adresser tant à l'ensemble du personnel (salariés, intérimaires, stagiaires…), qu'au personnel des prestataires du responsable de traitement ayant la qualité de sous-traitant au sens de l'article 386 du Code du numérique et appelés à ce titre à traiter des données à caractère personnel pour le compte du responsable de traitement ainsi que d'une manière générale à toute personne traitant/détenant des données à caractère personnel pour son compte.*

Dans une optique de gestion des risques, il convient de procéder à plusieurs mesures comme étape incontournable en amont de tout incident :



- mise en place d'une cellule de crise ;
- analyse des risques possibles et proposition de mesures en cas de survenance de chacun de ces risques ;
- prévision des étapes que les opérationnels vont devoir suivre pour mettre fin à l'incident de sécurité ;
- mise en place d'un système continu de détection des incidents de sécurité, afin de pouvoir réagir au plus tôt, et ainsi limiter les dommages.

La cellule de crise doit être mobilisée, conformément au dispositif de gestion de crise définie, dès l'apparition d'une crise liée à une violation de données.

Cette cellule est composée d'acteurs clés au sein de l'entreprise, mobilisés en fonction de la nature de la crise et de leur domaine d'expertise. Il peut s'agir par exemple du Responsable de la Sécurité des Systèmes d'Information (RSSI), du Délégué à la Protection des Données (DPO), du Directeur juridique et du Directeur de communication.

Cette cellule définit le plan d'action à mettre en œuvre et permettant :

- d'identifier le périmètre de la violation de donnée : quelles sont les données concernées, les personnes concernées ciblées ;
- d'identifier les impacts potentiels sur les personnes concernées ;
- d'identifier les impacts potentiels sur l'entreprise afin d'identifier les activités (critiques ou non) qui sont touchées par cette violation.

Ces précautions préalables doivent permettre de faire en sorte que, lors d'un incident de sécurité, il n'y ait plus qu'à agir en suivant les étapes prédéterminées, permettant ainsi de disposer rapidement de l'ensemble des éléments nécessaires afin de pouvoir informer l'autorité de contrôle.

De plus, prévoir de manière détaillée la conduite à tenir en cas d'incident a aussi un intérêt probatoire à l'égard de l'autorité de contrôle ou en cas de recherche de responsabilité : cela sert pour documenter sa bonne foi et l'absence de faute.

Mathias Avocats, cabinet français spécialisé en protection des DCP a proposé 5 étapes clés suivante à détailler dans une telle procédure.

Etape n°1 : prévoir un système interne de signalement

Tout rédacteur d'une procédure de notification de violation des données veillera à préciser les modalités internes de signalement d'une violation. Si aucun moyen interne de signalement de violation de données réelle ou supposée n'a été mis à disposition des collaborateurs, la rédaction de la procédure sera l'occasion de créer un mécanisme de signalement.

Etape n°2 : prévoir une investigation

La seconde étape à détailler dans la procédure porte sur l'investigation en tant que telle. Elle survient donc après le signalement de la violation de données.

Il s'agit notamment d'indiquer la composition de l'équipe interne qui sera chargée d'investiguer. Dans ce cas, seules les fonctions seront désignées et non des personnes. Par ailleurs, on traitera les situations dans lesquelles il pourra être fait appel à un conseil externe selon la politique interne de la structure. Les modalités de création de la cellule d'investigation seront ainsi précisées, notamment en cas d'urgence.

Il conviendra de préciser également que l'investigation donnera lieu à un rapport (un modèle peut éventuellement être annexé à la procédure), auquel seules les personnes habilitées pourront accéder.

Etape n°3 : prévoir la mise en œuvre de mesures correctrices

La troisième étape concernant la mise en œuvre de mesures correctrices et/ou visant à limiter l'impact de la violation de données sur les personnes concernées sera également traitée dans la procédure.

Ces actions de recherche et de mise en œuvre de mesures correctrices sont fondamentales car, si une notification à l'Autorité devait être réalisée, l'agent qui traitera le dossier pourrait demander des informations complémentaires qu'il vaut mieux avoir déjà sous la main.

Etape n°4 : prévoir une phase d'évaluation des impacts

Afin de déterminer si une notification à l'autorité de contrôle doit être réalisée, il est nécessaire d'étudier l'impact de la violation à l'égard des personnes concernées. Pour cela, le type de violation ainsi que le caractère sensible ou non des données à caractère personnel seront notamment pris en compte.

De même, évaluer la gravité de la violation de données et le nombre de personnes concernées sera important ; et ce d'autant plus que ces informations sont demandées dans le formulaire de notification en ligne sur le site de l'Autorité.

Etape n°5 : prévoir les modalités de notification

Si les précédentes étapes ont bien été suivies, l'entité qui a subi la violation de données doit non seulement être en mesure de déterminer si une notification est nécessaire ou non, mais également être en possession de tous les éléments nécessaires pour procéder à une notification le cas échéant. Un arbre de décision pourra notamment être inséré dans la procédure.

A noter que cette procédure est à rédiger en lien avec la procédure de gestion des incidents de sécurité qui existe peut-être déjà au sein de la structure.

Qu'une violation de données donne lieu ou non à une notification, il sera nécessaire de documenter cet événement en indiquant notamment les causes, les conséquences et les mesures prises pour y remédier, conformément au principe d'accountability et à l'article 427 du CDN.

427 du CDN

Dans ce contexte, il conviendra d'expliquer le raisonnement suivi par le responsable de traitement et/ou le sous-traitant aux termes duquel il a décidé de ne pas notifier la violation à l'autorité de contrôle. Cela fera donc l'objet d'un rappel particulier dans le corps de la procédure.
Les éléments essentiels des livrables attendus à l'issue de ces différentes étapes doivent être décrits dans la procédure et des modèles pourront être annexés.

En outre, il sera utile de documenter le fait que les agents ou salariés ont été informés de l'existence d'une telle procédure et formés à l'utilisation du mécanisme de signalement des violations de données.

C

La formation /sensibilisation

Le principal risque en matière de sécurité informatique est l'erreur humaine.
Les utilisateurs du système d'information du responsable du traitement doivent donc être particulièrement sensibilisés aux risques informatiques liés à l'utilisation de bases de données.

La première clé pour une adaptation réussie à la réglementation est de sensibiliser, et ce en amont de toute action, l'ensemble des personnes (décisionnaires et salariés).

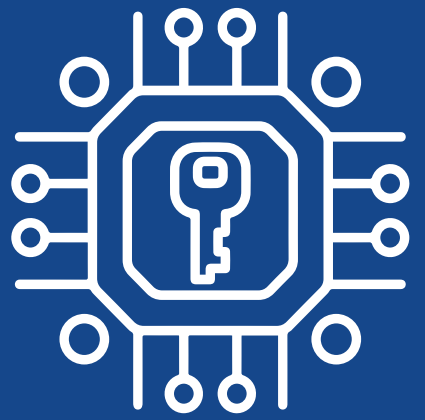
- **Formations**
- **Scéances de sensibilisation**
- **Diffusion de notes internes**
- **Envoi périodique de fiches pratique**

Les responsables du traitement devront dans ce cadre prévoir de **sensibiliser et former leurs collaborateurs** sur la gestion de ces risques (sensibiliser les salariés aux cyberattaques telles que les techniques de phishing, à l'importance du respect de la charte informatique...). Tous doivent être en mesure de connaître la procédure à suivre en cas de violation :

- **Qui doit être prévenu au sein de l'entreprise ?**
- **Quel processus activer pour identifier la violation ?**
- **Quelles sont les premières actions à mettre en place en cas d'identification d'une violation et afin d'en minimiser les conséquences ?**

Cela passe par une documentation précise devant répertorier notamment :

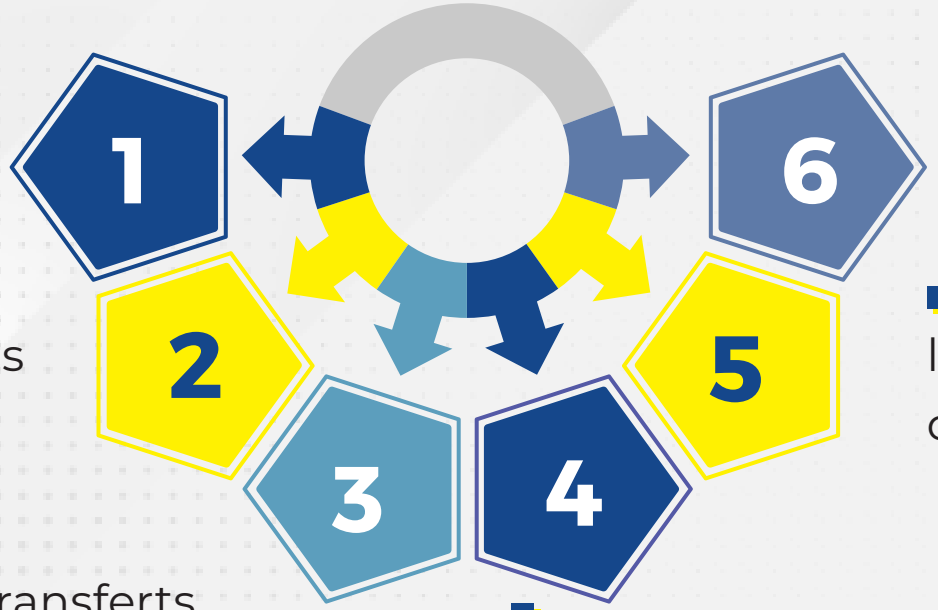
- les solutions de sauvegarde disponibles sur les différents serveurs en backup ;
- les firewall, antivirus, chiffrement à activer sur chaque ordinateur des salariés ;
- les procédures de cryptages devant être respectées ;
- les différents niveaux d'accès des salariés à certaines informations (permet de limiter par exemple les risques de fraudes telles que les fraudes au président par exemple) ;
- les cas de violations déjà subis, la manière dont ils ont été traités, qui a été touché, quelles solutions ont été mises en œuvre.



Par ailleurs, il est recommandé de formaliser une politique d'utilisation des données personnelles précisant les conditions dans lesquelles un salarié peut créer un traitement contenant des données à caractère personnel.

Cette politique devra comprendre l'ensemble des principes nécessaires pour garantir la mise en œuvre de traitements équitables et transparents, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées, en particulier :

- la mise en œuvre de traitements licites ;
- le respect des droits des personnes ;
- les éventuels transferts vers un pays tiers ;
- les destinataires des données collectées ;
- la durée de conservation des données collectées ;
- les mesures de sécurité des données.



D La continuité de l’activité

Quelle que soit la taille du responsable du traitement, la question de la continuité de son activité en temps de crise doit être prévue. En effet, les organismes doivent identifier des solutions de contournement envisageables en fonction de grands scénarios de risques, réfléchissant en termes d’impact du risque et non pas de cause.

Dans le cadre de la formalisation d’un plan de continuité d’activités, l’objectif est d’être en capacité de réagir à un grand nombre d’aléas engendrant la même conséquence.

Une réflexion est alors à mener soit par l'équipe contrôle interne, gestion des risques, soit directement par le Comité de Direction afin :

- d'identifier les activités critiques pour lesquelles une interruption de service est inacceptable;
- d'identifier les outils et tiers impactant ces activités ;
- d'identifier les personnes clés à mobiliser en cas de survenance d'un tel incident, appelés « cellule de crise » ;
- d'identifier les procédures de gestion en mode dégradé de l'activité ainsi que les procédures de reprise de celle-ci permettant de réduire au maximum le délai d'interruption de l'activité concernée.

Ce plan de continuité d'activité intègre des procédures organisationnelles de gestion de l'activité, des procédures organisationnelles et techniques de reprise des systèmes d'informations ainsi que des procédures spécifiques relatives à la gestion de crise.
La préparation d'une telle documentation permet de limiter les impacts de la crise en réduisant le temps de réaction, cependant, pour s'assurer de la pertinence du dispositif identifier, il est important de pouvoir le tester lors d'exercices de gestion de crise.

D

GÉRER LES VIOLATIONS

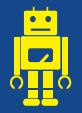
A La notification

Aux termes de l'article 427 du Code du numérique, la notification est apparue comme la première diligence obligatoire à laquelle doit satisfaire le responsable du traitement dès la survenance d'une violation.
L'article rend obligatoire la notification à l'Autorité, à la personne concernée et au responsable de traitement par le sous-traitant.
La notification doit intervenir sans délai et doit contenir certaines informations dont :

1. La description de la nature de la rupture de sécurité ayant affecté des données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la rupture et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
2. Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
3. La description des conséquences probables de la rupture de sécurité ;
4. La description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la rupture de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Pour éclairer les usages, l'Autorité a mis en ligne sur son site www.apdp.bj un formulaire de signalement qui spécifie plus clairement les informations à transmettre.
La communication à la personne concernée visée à l'alinéa 1er n'est pas nécessaire à la rencontre de certaines conditions :

Exceptions à l'obligation d'information en cas de violation entraînant un risque élevé



le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite rupture, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès,

Exemple

Les données ont fait l'objet d'une mesure de chiffrement à l'état de l'art, dont la clé n'a pas été compromise et a été générée de façon à ne pas pouvoir être trouvée, par aucun moyen technologique existant, par quelqu'un qui n'est pas autorisé à l'utiliser

Exceptions à l'obligation d'information en cas de violation entraînant un risque élevé	Exemple
Le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes n'est plus susceptible de se matérialiser	Des mots de passe d'employés ayant accès à une base de données sensibles ont été subtilisés, mais n'ont pas été utilisés et ont été réinitialisés
La communication de la violation aux personnes concernées exigerait des efforts disproportionnés	Le responsable du traitement ne dispose d'aucun élément permettant de contacter les personnes concernées

Néanmoins, il est prévu, dans les cas susmentionnés, une communication publique, ou une mesure similaire permettant aux personnes concernées d'être informées de manière aussi efficace.

Les obligations issues de ce système de notification et communication sont ***régulièrement sanctionnées,*** ce qui fait peser d'autant plus de responsabilité sur le responsable de traitement ou sous-traitant. Par exemple récemment :

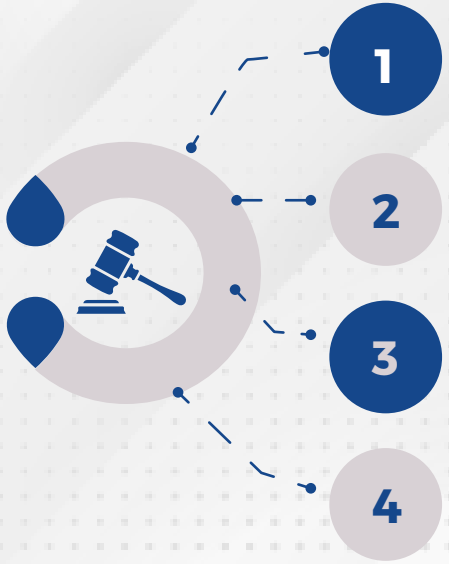
Le 28 décembre 2021, la formation restreinte de la CNIL a sanctionné la **société SLIMPAY** d'une amende de **180 000 euros** notamment pour avoir insuffisamment protégé les données personnelles des utilisateurs et **ne pas les avoir informés d'une violation de données.**

28 décembre 2021
la formation
restraine dde la
CNIL

société SLIMPAY

amande de
180 000 euros

En effet, l'autorité de contrôle a considéré que le risque associé à la violation est élevé :



1. compte tenu de la nature des données personnelles : **notamment des informations bancaires**
2. du volume de personnes concernées : **plus de 12 millions**
3. de la possibilité d'identification des personnes concernées par la violation
4. des conséquences possibles pour les personnes concernées : **risque d'usurpation d'identité ou d'hameçonnage**

Ainsi, la société SIMPLAY aurait dû informer les personnes concernées.
En résumé, toute violation fait naître une obligation dont le manquement peut être lourd de conséquences pour le responsable du traitement.

B La documentation

En raison du principe de responsabilité, les incidents de violations de sécurité doivent être documentés dans un registre des activités de traitement ou un registre des violations de données.

Il s'agit de consigner l'évènement dans le registre. Lorsqu'un incident de ce type se produit, il est nécessaire de documenter à minima les faits, les conséquences de la violation, ainsi que les mesures prises pour atténuer voire remédier à cette violation.

Il contiendra en effet l'intégralité des violations de données personnelles connues par le responsable du traitement, y compris lorsque celles-ci ne sont pas automatiquement sujettes à une notification externe.

Ce registre doit contenir au moins les informations suivantes :

Date et heure de la violation

La date et l'heure exactes auxquelles le responsable du traitement a eu connaissance de la fuite de données à caractère personnel. Ces informations sont importantes pour respecter le délai pour la notification à l'Autorité de protection des données et à toute personne concernée.

Chronologie et description de la violation

Description des événements relatifs à la fuite de données à caractère personnel : date à laquelle la fuite a été signalée, date à laquelle elle a (vraisemblablement) eu lieu, aperçu des systèmes concernés et autres descriptions.

Personne de contact

Il est important d'avoir une personne de contact centrale, qui est informée des circonstances de la violation et qui peut être contactée en cas de questions de suivi. En général, la personne qui a signalé la fuite est le délégué à la protection des données ou le responsable du service concerné.

Parties externes concernées

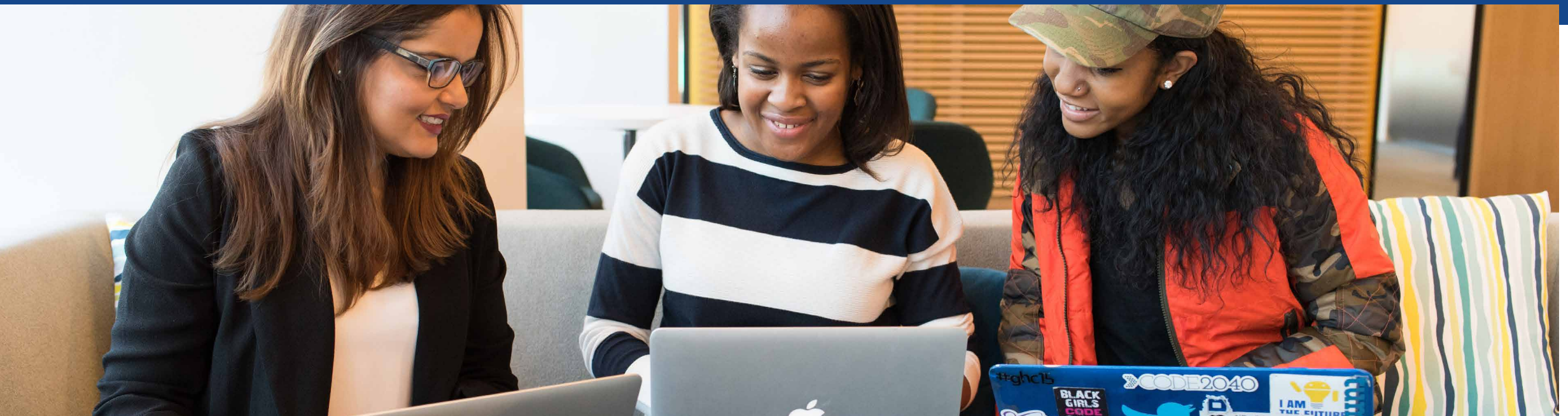
Contient des informations sur la nature et le rôle de l'organisation (responsable du traitement, sous-traitant, responsable conjoint du traitement) et les tiers qui peuvent être affectés et doivent donc être informés.

Évaluation des risques - motivation et conclusion

Analyse détaillée des risques et évaluation globale des risques, sur la base des éléments permettant de déterminer le niveau de risque.

Contrôles et mesures correctives existants

Une liste des mesures techniques et organisationnelles existantes, et de celles qui seront prises pour réduire les risques existants pour les personnes concernées.



C La leçon

Une fois l'incident résolu, il convient d'en gérer les conséquences et d'en tirer enseignement en apportant des réponses à un certain nombre de questions :

- **Qu'est-ce qui était vulnérable ?**
- **Comment pallier cette vulnérabilité ?**
- **Quels ont été les points difficiles pour les opérationnels ?**
- **Qu'est-ce qui a fonctionné et qu'est-ce qui n'a pas fonctionné par rapport aux mesures prévues initialement ?**

MERCI