LOGO DE LA STRUCTURE

NOM DE LA STRUCTURE

POLITIQUE DE GESTION DES INCIDENTS DE VIOLATION DES DONNEES

Le présent document est proposé aux Responsables de Traitement par l'Autorité de Protection des Données à caractère Personnel (APDP) comme modèle d'élaboration d'une politique de gestion des incidents de violation des données personnelles.

Historique des versions		
Date	**Version**	**Evolution du version**
JJ/MM/AAAA	X.X	Adoption de la première version de la politique de gestion des incidents de violation des données à caractère personnel

Table des matières

I. INTRODUCTION

A. OBJECTIF

Le présent document évalue les risques d'incidents de sécurité susceptibles d'affecter les données personnelles qui sont traitées et indique les précautions à prendre en cas de survenance d'un incident de cet ordre. Il s'agit des mesures de remédiation à l'incident et d'atténuation de l'effet de la violation de données à caractère personnel en particulier sur les personnes concernées. Par conséquent, cette politique définit une procédure à suivre si les procédures de sécurité en vigueur ne permettent pas d'éviter une violation.

L'objectif de cette politique est :

- de mettre en place des mesures techniques et organisationnelles à même de prévenir les violations ;
- de normaliser la réponse à tout incident de sécurité ;
- de veiller à ce qu'il soit enregistré et géré de manière appropriée, conformément aux meilleures pratiques;
- afin de respecter les prescriptions de l'article 427 de la loi n°2017-20 du 20 avril 2021 portant code du numérique en République du Bénin, telle que modifiée par la loi n°2020-35 du 06 janvier 2021.

B. CHAMP D'APPLICATION

Le présent document prend en compte les incidents de violation de données à caractère personnel et les précautions prises non seulement pour réagir efficacement et conformément à leurs obligations légales découlant notamment de l'article 427 du code du numérique, mais aussi celles mises en place pour prévenir ces incidents de manière proactive.

Aux fins de la présente politique, le terme "violation de données" comprend la perte de contrôle, la compromission, la divulgation non autorisée ou l'accès non autorisé ou potentiel à des informations personnellement identifiables, que ce soit sous forme physique (papier) ou électronique. Ces violations concernent l'atteinte à la disponibilité, l'atteinte à la confidentialité, l'atteinte à l'intégrité et l'atteinte à la traçabilité. Elles peuvent se produire pour un certain nombre de raisons, notamment :

- la perte, l'altération ou le vol de données ou d'équipements sur lesquels des données sont stockées (y compris l'effraction de l'un de nos locaux) ;
- accès inapproprié/non autorisé à des données confidentielles ou hautement confidentielles ;
- défaillance de l'équipement ;
- l'erreur humaine, y compris les divulgations involontaires, le manque de diligence et/ou la mauvaise utilisation des ressources technologiques ;
- des circonstances imprévues telles qu'une inondation ou un incendie ;

- un piratage informatique ;
- accès où les informations sont obtenues en trompant l'organisation qui les détient.

Aux fins de la présente politique, ces raisons seront appelées "**incidents de sécurité**". Mais tous les incidents de sécurité ne conduisent pas à une violation des données.

C. ACTEURS CLES

Rôles	**Obligations**
Le Responsable de Traitement	• Met en œuvre une politique de gestion des incidents de violation des données personnelles • Notifie à l'APDP la violation dans les meilleurs délais. La notification à la personne concernée intervient notamment si la violation est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées ; • Documente toutes les violations de données
Le Sous-Traitant	Notifie au responsable de traitement toute violation de données dans les meilleurs délais après en avoir pris connaissance
L'Autorité de Protection des Données Personnelles (APDP)	• Reçoit la notification ; • Vérifie la documentation de la violation par le responsable de traitement ; • Vérifie si les conditions de communication sont remplies ou non ; • Peut ordonner au responsable de traitement de communiquer à la personne concernée la violation de données.
La personne concernée dont les données ont été violées	Reçoit communication de la violation en cas de risque élevée pour les droits et libertés.

II. ÉVALUATION PREVENTIVE DES RISQUES ET DE LA RÉPONSE

Tous les risques en matière de sécurité d'une part et d'autre part tout incident de sécurité et toute violation réelle des données doivent être documentés et étudiés, afin que la réponse à la violation soit diligente et qu'elle soit évaluée en termes d'efficacité.

Toutes les violations de la sécurité des données seront enregistrées afin de garantir une surveillance appropriée des types et de la fréquence des incidents confirmés à des fins de gestion et d'établissement de rapports.

A. EVALUATION DU FACTEUR HUMAIN

Le facteur humain est la contribution humaine impliquée dans un événement. Il comprend des comportements, des capacités, des caractéristiques individuelles (ex : savoir-être, communication, fatigue …).

Elément	**Conséquences probables**
Le personnel a-t-il été informé des obligations liées à la protection des données personnelles ? ➢ Oui ☐ ➢ Non ☐ (Voir conséquences)	Spoofing (usurpation d'adresse mail), Mauvaise configuration des systèmes et composants informatiques et utilisation de failles liées à l'obsolescence d'une configuration de machine et de logiciel Décisions imprudentes entraînant une défaillance de la sécurité Violation du régime de protection des données Personnelles, traitement non autorisé de données personnelles Violation de la confidentialité Violation de la sécurité
Le personnel a-t-il une bonne pratique des prescriptions des documentations et des procédures connexes ? ➢ Oui ☐ ➢ Non ☐ (Voir conséquences)	Violation de la confidentialité Violation de la disponibilité Violation de l'intégrité Violation de la traçabilité
Absence de règles éthiques ☐ Absence de modalités de dissuasion du vol de données ☐ Absence de modalités de dissuasion du traitement non autorisé ☐	Violation de la confidentialité Mises en cause judiciaires Sanctions administratives

Y-a-t-il méconnaissance des types de violation, des causes et des atteintes ? ➢ Oui ☐ (Voir les conséquences) ➢ Non ☐	Partage de mot de passe, Phishing ou hameçonnage, shoulder surfing, ingenierie sociale Acceptation de cadeaux et promo connectés ou de clés USB porteurs de malwares (logiciels malveillants, virus) potentiels… Violation de la confidentialité Violation de la disponibilité Violation de l'intégrité Violation de la traçabilité
Disposer-vous d'un registre de violation de données personnelles ? ➢ Oui ☐ ➢ Non ☐ (Voir conséquences)	Violations des obligations du responsable de traitement et des obligations de sécurité
Aviez-vous désigné un délégué à la protection des données personnelles ? ➢ Oui ☐ ➢ Non ☐ (Voir conséquences)	Violations d'une des règles du régime de protection des données Personnelles.

B. EVALUATION DE LA SECURITE DES SUPPORTS DE DONNEES

Points	Questions	Enjeux (Choisissez et inscrivez dans la colonne vide la note en fonction de l'enjeu dans votre structure)	Notes	
I. Evaluation des conséquences potentielles	A. **Adhérence au système d'information (SI) :** comment jugez-vous l'importance de votre SI dans l'accomplissement de vos missions ?	Le système d'information est accessoire à l'accomplissement des missions.	0	
		Le système d'information est utile à l'accomplissement des missions.	1	
		Le système d'information est nécessaire à l'accomplissement des missions.	2	
		Le système d'information est vital à l'accomplissement des missions.	3	
		Elles ne peuvent qu'être négligeables.	0	

Points	Questions	Enjeux (Choisissez et inscrivez dans la colonne vide la note en fonction de l'enjeu dans votre structure)	Notes	
	B. **Niveau des impacts internes :** quelles sont les conséquences internes (impacts financiers, juridiques, sur l'activité...) d'un sinistre SSI ?	Elles peuvent être significatives.	1	
		Elles peuvent être graves.	2	
		Elles peuvent être fatales.	3	
	C. **Niveau des impacts externes** : quelles sont les conséquences externes (image, contrats, sécurité des personnes...) d'un sinistre SSI ?	Elles ne peuvent qu'être négligeables.	0	
		Elles peuvent être significatives.	1	
		Elles peuvent être graves.	2	
		Elles peuvent être catastrophiques.	3	
	Le niveau des conséquences potentielles est égal à la valeur maximale des trois réponses			
II. La sensibilité du patrimoine	A. **Besoins de disponibilité** : dans quelle mesure la disponibilité du(des) SI est-elle importante ?	L'inaccessibilité des SI ne gêne quasiment pas l'activité	0	
		Elle perturbe l'activité de manière significative	1	
		Elle est jugée comme grave pour l'activité	2	
		Elle peut être fatale pour l'activité	3	
	B. **Besoins d'intégrité** : dans quelle mesure l'intégrité des données manipulées ou manipulables dans le cadre de l'activité est-elle	L'altération des données ne gêne quasiment pas l'activité	0	
		Elle perturbe l'activité de manière significative	1	
		Elle est jugée comme grave pour l'activité	2	
		Elle peut être fatale pour l'activité.	3	

Points	Questions	Enjeux (Choisissez et inscrivez dans la colonne vide la note en fonction de l'enjeu dans votre structure)	Notes	
	Importante ?			
	C. **Besoins de confidentialité** : dans quelle mesure la confidentialité des informations exploitées ou exploitables dans le cadre de l'activité est-elle importante?	La compromission d'informations ne gêne quasiment pas l'activité.	0	
		Elle perturbe l'activité de manière significative.	1	
		Elle est jugée comme grave pour l'activité.	2	
		Elle peut être fatale pour l'activité.	3	
	La sensibilité du patrimoine informationnel est égale à la valeur maximale des trois réponses.			
III. Le degré d'exposition aux menaces	A**. Fréquence des sinistres SSI** : quelle est la fréquence estimée des sinistres SSI ?	Les sinistres SSI (vécus ou imaginables) sont rarissimes (moins d'une fois par an).	0	
		Plusieurs sinistres SSI dans l'année.	1	
		Plusieurs sinistres SSI par trimestre.	2	
		Plusieurs sinistres SSI par mois.	3	
	B. **Degré de motivation des attaquants** : quel est le degré de motivation des attaquants potentiels ?	Une attaque SSI ciblée sur le périmètre est relativement inimaginable.	0	
		Elle est jugée faible.	1	
		Elle peut être forte.	2	
		Elle peut être très importante.	3	
	C. **Moyens des attaquants** : quels sont les compétences et les ressources des attaquants potentiels?	Les attaquants potentiels ne disposent que de faibles moyens.	0	
		Ils peuvent disposer de moyens significatifs	1	
		Ils peuvent disposer de moyens importants.	2	
		Leurs moyens sont potentiellement illimités.	3	
	Le degré d'exposition aux menaces est égal à la valeur maximale des trois réponses			
		Le SI est jugé comme homogène.	0	

Points	Questions	Enjeux (Choisissez et inscrivez dans la colonne vide la note en fonction de l'enjeu dans votre structure)	Notes	
IV. L'importance des vulnérabilités	A. **Hétérogénéité du SI** : quel est le niveau de variété du SI ?	Il est jugé comme faiblement hétérogène.	1	
		Il est jugé comme fortement hétérogène.	2	
		Il est jugé comme extrêmement hétérogène.	3	
	B. **Ouverture du SI** : Quel est le degré d'ouverture du système d'information ?	Le SI n'est pas ouvert.	0	
		Il n'est ouvert qu'à des systèmes internes.	1	
		Il est ouvert à des systèmes externes mais sous contrôle.	2	
		Il est ouvert à des systèmes externes hors de contrôle.	3	
	C. **Variabilité du SI** : Quel est le niveau de variabilité des composants du système ?	Le SI et son contexte sont jugés stables.	0	
		Ils changent peu.	1	
		Ils changent relativement souvent.	2	
		Ils changent très souvent.	3	
	L'importance des vulnérabilités est égale à la valeur maximale des trois réponses.			

- **Méthode de calcul du niveau adéquat de maturité SSI**

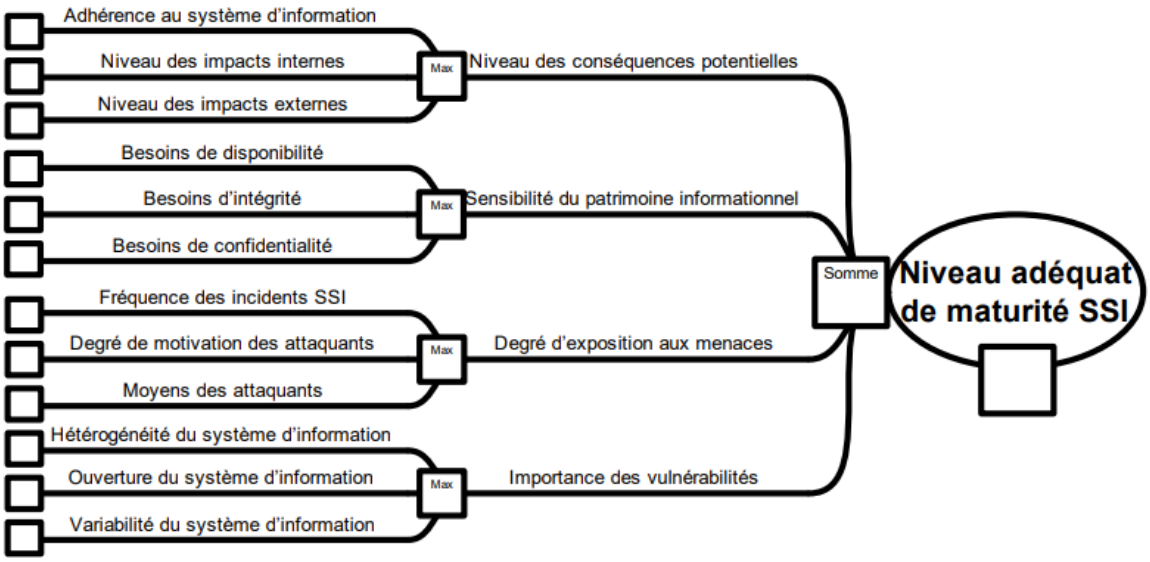
Après avoir répondu aux douze questions de l'autodiagnostic et gardé les valeurs maximales des quatre thèmes, on dispose de quatre valeurs :

- le niveau des conséquences potentielles (en cas de sinistre SSI);
- la sensibilité du patrimoine informationnel;
- le degré d'exposition aux menaces;
- l'importance des vulnérabilités.

Il s'agit alors d'additionner les quatre valeurs et de comparer le résultat au tableau suivant pour obtenir le niveau adéquat de maturité SSI.

0 à 2	Pratique informelle	😱
3 à 5	Pratique répétable et suivie	😤
6 à 8	Processus définis	😐
9 à10	Processus contrôlés	🤔
11 à 12	Processus continuellement optimisés	🫡

- **Arbre de détermination du niveau de maturité**



C. INCIDENTS DE SECURITES ET CAUSES POSSIBLES DE LA VIOLATION DES DONNEES PERSONNELLES

Un incident de sécurité est défini comme tout événement ayant un effet négatif réel sur la sécurité du réseau, des systèmes informatiques et/ou d'autres ressources d'information. Lorsque l'incident de sécurité entraîne, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées régulièrement ou non, ou l'accès non autorisé à de telles données, on parle de violation de données à caractère personnel.

Une violation de données à caractère personnel risque d'entraîner une série d'effets négatifs importants pour les personnes concernées, lesquels peuvent engendrer des dommages physiques, matériels ou un préjudice moral.

Les violations de données peuvent être causées par des employés, des parties externes à l'organisation (tiers) ou des erreurs du système informatique (bugs). Le support de la donnée peut impacter l'atteinte et la cause possible de violation.

La cause est soit :

- une négligence : il peut s'agir d'erreurs involontaires ou d'actions volontaires, le plus souvent internes à l'organisation concernée ;
- un accident ;
- un acte intentionnel : il s'agit d'actes ou d'attaques volontaires et malveillante visant à compromettre et altérer les données personnelles ;
- une défaillance technique : les failles de sécurité ou vulnérabilités.

1. **Négligences et Erreur humaine**

Les causes de violation découlant de l'erreur humaine peuvent être :

N°	Description	Atteintes probables
1	Perte d'appareils informatiques (portables ou autres), de dispositifs de stockage de données ou de registres papier contenant des données personnelles	Utilisation de clefs USB ou disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles, le disque dur contenant les informations est utilisé pour une fin non prévue (par exemple pour transporter d'autres données chez un prestataire, pour transférer d'autres données d'une base de données à une autre, etc.) Choisissez un élément.

2	Divulgation de données à un mauvais destinataire	Divulgation involontaire en conversant, écoute d'une salle de réunion avec un matériel d'amplification sensorielle
3	Mise en œuvre non autorisée ou encadrée juridiquement d'un traitement de données personnelles	Lecture, photocopie, photographie Lecture de parapheurs en circulation, reproduction de documents en transit
4	Traitement des données de manière non autorisée (par exemple : téléchargement d'une copie locale de données personnelles)	À décrire
5	Accès non autorisé ou divulgation de données personnelles par les employés (par exemple : partage d'un identifiant)	Observation d'un écran à l'insu de son utilisateur dans un train, photographie d'un écran, géolocalisation d'un matériel, captation de signaux électromagnétiques à distance
6	Élimination incorrecte des données personnelles (par exemple : disque dur, support de stockage ou documents papier contenant des données personnelles vendues ou jetées avant que les données ne soient correctement supprimées)	Modifications inopportunes dans une base de données, effacement de fichiers utiles au bon fonctionnement, erreur de manipulation menant à la modification de données Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre
7	Employés mécontents	Débauchage d'un employé, changement d'affectation, rachat de tout ou partie de l'organisation

2. **Activités malveillantes**

Les causes de violation découlant des activités malveillantes peuvent être

N°	Description	Atteintes probables
1	Incidents de piratage / Accès illégal aux bases de données contenant des données personnelles	Piégeage par un keylogger, retrait d'un composant matériel, branchement d'un appareil (ex. : clé USB) pour lancer un système d'exploitation ou récupérer des données Piégeage par un keylogger logiciel, contagion par un code malveillant, installation d'un outil de prise de contrôle à distance, substitution d'un composant par un autre lors d'une mise à jour, d'une opération de maintenance ou d'une installation (des bouts de codes ou applications sont installés ou remplacés) Interception de flux sur le réseau Ethernet, acquisition de données sur un réseau wifi
2	Piratage pour accéder à des données non autorisées via une application ou une API	Balayage d'adresses et ports réseau, collecte de données de configuration, étude d'un code source pour déterminer les défauts exploitables, test des réponses d'une base de données à des requêtes malveillantes
3	Vol d'appareils informatiques (portables ou autres), de dispositifs de stockage de données ou de dossiers papier contenant des données personnelles	Vol d'un ordinateur portable dans une chambre d'hôtel, vol d'un téléphone portable professionnel par un pickpocket, récupération d'un matériel ou d'un support mis au rebut, perte d'un support de stockage électronique

		Vol de dossiers dans les bureaux, vol de courriers dans la boîte aux lettres, récupération de documents mis au rebut
4	Les escroqueries qui poussent le personnel ou la structure à divulguer des données personnelles d individus	Influence (hameçonnage, filoutage, ingénierie sociale, corruption), pression (chantage, harcèlement moral) Utilisations de certaines informations confidentielles à des fins personnelles
5		Fouille de contenu, croisement illégitime de données, élévation de privilèges, effacement de traces, envoi de *spams* depuis la messagerie, détournement de fonctions réseaux Modification de chiffres dans un dossier, remplacement d'un document par un faux Modification, altération d'une note à l'insu du rédacteur
6	Botnet, les ordinateurs zombies.	Attaque par dénis de service

3. **Erreurs et accidents techniques**

Les causes de violation découlant d'erreurs ou d'accidents techniques peuvent être :

N°	Description	Atteintes Probables
1	Erreurs ou bugs dans l'application ou l'Application Programming Interface (API) de la structure	Choisissez un élément.

2	Défaillance des services cloud, du cloud computing ou des systèmes de sécurité / authentification / autorisation du stockage cloud	Choisissez un élément.
3	Attaque de malwares (Cheval de troie, virus)	Effacement de données, substitution d'un composant par un autre virus, bombe logique, contagion par un code malveillant, utilisation de logiciels contrefaits ou copiés.
4	Erreurs techniques	Erreur de manipulation menant à la suppression de données, manipulation inopportune lors de la mise à jour, configuration ou maintenance
5	Autres erreurs ou accidents techniques	Unité de stockage pleine, panne de courant, surexploitation des capacités de traitement, échauffement, température excessive, attaque par dénis de service
		Ajout d'un matériel incompatible menant à un dysfonctionnement, retrait d'un matériel indispensable au fonctionnement correct d'une application
		Modifications inopportunes dans une base de données, effacement de fichiers utiles au bon fonctionnement, erreur de manipulation menant à la modification de données

		Inondation, incendie, vandalisme, dégradation du fait de l'usure naturelle, dysfonctionnement d'un dispositif de stockage Sectionnement du câblage, mauvaise réception du réseau wifi, oxydation des câbles

D. TYPES DE VIOLATIONS SUSCEPTIBLES DE SURVENIR

N°	Causes	**Nature ou type de violation**
1	une négligence	Violation de la confidentialité Violation de la disponibilité Violation de l'intégrité Violation de la traçabilité
2	un acte intentionnel	
3	défaillances techniques	
4	un accident	

E. EVALUATION DE CRITICITE

Le Responsable de traitement évalue le niveau d'incident de violation des données sur la base combinée des critères de criticité suivants :

- Criticité faible : un incident de sécurité qui peut être géré dans le cadre de procédures d'exploitation normales et avec un faible impact.

- Criticité moyenne : un incident de sécurité grave et préjudiciable, nécessitant l'assistance des Responsables techniques ou d'équipes de soutien spécialisées

- Criticité élevée : un incident de sécurité majeur nécessitant des ressources importantes au-delà des procédures d'exploitation normales, nécessitant une escalade vers l'Equipe de Gestion de Crise et l'activation potentielle du Plan de continuité des opérations.

- Criticité critique : un incident de sécurité ayant un impact sérieux sur les services critiques et nécessitant des ressources importantes au-delà des procédures d'exploitation normales, nécessitant une escalade vers l'Equipe de Gestion de Crise,

l'activation potentielle du Plan de continuité des opérations, une enquête approfondie et une communication.

Probabilité de préjudice		**Négligeable**	**Faible**	**Moyenne**	**Très grande**	**extrême**
A	Volume de données	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non
B	Type et nature des données ou des traitements probables touchés	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non
C	Nombre d'éléments de données différentes touchées	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non
D	Nature du traitement	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non
E	Catégories des personnes	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non
F	Possibilité d'identification des personnes concernées	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non
G	Conséquences probables pour les personnes compte tenu de la nature, nombre et croisement	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non

Probabilité de préjudice		Négligeable	Faible	Moyenne	Très grande	extrême
H	Nombre d'éléments de données probables différentes touchées	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non
I	Autres facteurs	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non
J	Incidence globale de la violation	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non	☐ oui ☐ non

F. MESURES DE RECOUVREMENT INDICATIVES

Facteur humain	• Former et sensibiliser les collaborateurs, les prestataires et les partenaires de l'entreprise : savoir reconnaitre un phishing, s'organiser face aux tentatives de fraude au président ou à la diffusion d'un RIB frauduleux auprès des clients, le refus de cadeaux connectés ou de clés USB porteurs de malwares (logiciels malveillants, virus) potentiels… • Simuler des attaques et évaluer les réponses de l'entreprise. • Chiffrer les données personnelles et sensibles afin qu'elles ne fassent pas l'objet d'un chantage sur le Dark Web[vi]. • Réaliser des sauvegardes régulières, les conserver à l'extérieur du réseau de l'entreprise et tester régulièrement la capacité de restauration de ces sauvegardes. • Construire et – surtout – tester son plan de reprise d'activité (PRA ou « Disaster Recovery Plan ») afin de reconstituer son patrimoine informationnel au plus vite et au plus juste. • Enfin, disposer d'un système d'authentification « multi-factor » (MFA), où un utilisateur s'identifie par au moins 2 appareils

	différents référencés dans l'entreprise (PC, tablette, téléphone…). • Inventaire exhaustif et à jour des matériels et logiciels réalisé à l'aide d'une CMDB (base de données de gestion des configurations), • Réduction de la dette technique (sortie des solutions techniques obsolètes qui ne sont plus supportées par les éditeurs), • Anticipation des menaces à l'aide d'une veille régulière sur les techniques employées.
Sécurité organisationnelle	• Établir une veille active et se préparer en tenant compte des recommandations gouvernementales (site de ASIN). • Organisation annuelle d'exercices de cyber-crise, • Gouvernance par comité de sécurité réunissant les parties prenantes se tenant régulièrement sous la direction du responsable de la sécurité informatique • Souscrire une assurance cyber sécurité, qui oblige par ailleurs à mettre en place des dispositifs éprouvés de sécurité informatique.
Sécurité logique	• Réinstallation complète du ou des systèmes touchés, accompagnée, s'il y a lieu, d'une restauration des données à partir des sauvegardes. Les membres de l'équipe pourront être tenus, avant de procéder à cette réinstallation, de conserver les éléments probants concernant l'incident. • Vérification de la mise à jour du système sur le plan des correctifs. • Isoler immédiatement le système affecté pour empêcher toute nouvelle intrusion • Divulgation de données, les dommages, etc. • Utiliser le téléphone pour communiquer. L'attaquant peut être capable de surveiller • Le trafic de courrier électronique

	• Conserver tous les journaux pertinents, par exemple ceux du pare-feu, du routeur et du système de détection des intrusions • Faire des copies de sauvegarde des fichiers endommagés ou modifiés et conserver • Ces sauvegardes dans un endroit sûr • Identifier où se trouve le système affecté dans la topologie du réseau • Identifier tous les systèmes et organismes qui se connectent au système concerné • Identifier les programmes et les processus qui fonctionnent sur le(s) système(s) concerné(s), l'impact de la perturbation et la durée maximale d'indisponibilité admissible dans le cas où le système affecté est collecté comme preuve, prendre des dispositions pour assurer la continuité des services, c'est-à-dire préparer un système redondant et obtenir des sauvegardes de données • Vérification de l'activation de la protection en temps réel contre les virus et de la détection des intrusions • Vérification de la journalisation des bons événements au niveau de détails approprié • Vérification du renforcement du système grâce à la désactivation ou à la désinstallation des services non utilisés • Réinitialisation des mots de passe des utilisateurs ayant été compromis. **Il n'est pas recommandé de :** • **Supprimer, déplacer ou modifier des fichiers sur les systèmes concernés** • **Contacter l'auteur présumé des faits**

Mise en conformité	• La mise en place d'une solution de sauvegarde efficace et sécurisée ; • Le recours à des procédés de cryptage ; • La limitation de l'accessibilité aux données personnelles ; • La traçabilité des comptes disposant d'un « accès global » à une base de données ; • Le stockage sécurisé des mots de passe ; • Le contrôle permanent des vulnérabilités potentielles des technologies utilisées et la mise à jour des logiciels ; • L'information des salariés des conséquences des potentielles violations de données ; • L'application du Privacy by Design et du Privacy by Default ; • Les dispositions prises dans le cadre des analyses d'impact sur la vie privée.
Autres mesures	• Arrêtez le système compromis qui a conduit à la violation de données. • Déterminez si des mesures peuvent être prises pour récupérer les données perdues et limiter les dommages causés par la violation. (par exemple : désactiver / effacer à distance un ordinateur portable perdu contenant des données personnelles d'individus.) • Empêchez tout accès non autorisé au système. • Réinitialisez les mots de passe si les comptes et / ou les mots de passe ont été compromis. • Isolez les causes de la violation de données dans le système et, le cas échéant, modifiez les droits d'accès au système compromis et supprimez les connexions externes au système.

III. PLAN DE GESTION DES VIOLATIONS DE DONNÉES

La procédure décrite ci-après sera menée dans une fenêtre de notification obligatoire de 72 heures, ce qui signifie qu'une fois qu'une violation a été détectée, nous avons 72 heures pour mener une enquête et faire savoir au régulateur ce qui s'est passé, si des données personnelles ont été affectées et quel est le plan de confinement.

A. INFORMATION

Tout incident confirmé ou suspecté en matière de sécurité informatique ou de données personnelles doit toujours être signalé rapidement :

1°) au responsable de traitement

2°) à la sécurité informatique, à l'adresse électronique suivante : (à renseigner)

Le personnel est chargé de s'assurer qu'une protection et des contrôles appropriés et adéquats sont en place et appliqués dans chaque installation et ressource sous son contrôle et d'identifier ceux qui ne le sont pas. Les responsables sont chargés de veiller à ce que le personnel de leur secteur suive cette politique et adhère à toutes les procédures connexes.

Si un membre du personnel se rend compte/soupçonne que des données à caractère personnel ont été compromises pour une raison autre qu'un incident de sécurité informatique (par exemple, la perte d'un appareil portable, un mauvais adressage, des informations sensibles laissées à un endroit où elles pourraient être consultées sans autorisation) il doit immédiatement en informer son responsable. Et remplir le "Formulaire de rapport d'incident de sécurité" ci-joint (**annexe 3**)

Lorsqu'il existe un conflit d'intérêts potentiel ou pour toute autre raison, dans l'intérêt de la confidentialité, un tel rapport peut être fait directement au Délégué à la Protection des Données Personnelles (DPDP/DPO).

Le membre du personnel qui signale l'incident de sécurité peut être invité à remplir le rapport d'incident de violation de la sécurité des données (voir **l'annexe 3**).

Service/Direction	**Rôle dans la gestion de l'incident**	**Moyen par lequel le service est informé**

B. ORGANISATION

Le Responsable de Traitement est le principal intéressé aux incidents de violation des données personnelles. Ces incidents constituent des mises en cause des obligations qu'il assume envers le traitement de données et engagent sa responsabilité. En ce sens il est tenu d'en assurer la gestion.

Le Responsable de traitement regroupe une équipe de gestion des incidents de violation (*Data Breach Team - DBT*) pour améliorer la réponse à l'incident. Il détermine dans la politique de gestion des incidents, les procédures à mettre en œuvre, les rôles et les tâches de chacune des personnes composant cette équipe en vue d'une réaction rapide et efficace.

Le délégué à la protection des données personnelles (DPDP) est chargé de superviser la gestion de toute violation.

C. ÉVALUATION DE L'INCIDENT

Connaître l'impact des violations de données aide le Responsable de traitement à déterminer, s'il pourrait y avoir des conséquences graves pour les personnes concernées, quelles sont les mesures de remédiation adaptées et à apprécier l'obligation de notification.

Il y a un risque lorsque la violation peut entraîner des dommages physiques, matériels ou immatériels pour les personnes dont les données ont été violées.

Une violation de données à caractère personnel risque d'entraîner une série d'effets négatifs importants pour les personnes concernées, lesquels peuvent engendrer des dommages physiques, matériels ou un préjudice moral.

Lors de l'évaluation du risque, il convient de tenir compte à la fois de la gravité de l'impact potentiel sur les droits et libertés de la personne concernée et de la probabilité que cela se produise.

Le responsable de traitement peut avoir recours, afin de déterminer la cause de l'incident, à des techniques criminalistiques, notamment l'examen des journaux système, la recherche de lacunes dans la journalisation, l'examen des registres de détection d'intrusion et les interrogatoires de témoins.

Probabilité de préjudice		Négligeable	Faible	Moyenne	Très grande	Extrême
A	Ampleur de la violation					
B	Type et nature des données ou des traitements probables touchés					
C	Nombre d'éléments de données probables différentes touchées					
D	Autres facteurs					
E	Incidence globale de la violation					

N°	Criticité du risque	Probabilité de survenance sur une échelle de 10	Mesures d'atténuation	Notification à l'APDP	Notification aux personnes concernées
1	Faible	Choisissez un élément.		Choisissez un élément.	Choisissez un élément.
2	Moyenne	Choisissez un élément.		Choisissez un élément.	Choisissez un élément.
3	Elevée	Choisissez un élément.		Choisissez un élément.	. Choisissez un élément.

4	Critique	Choisissez un élément.		Choisissez un élément.	Choisissez un élément.

Une fois que des mesures ont été prises pour résoudre la violation de données, le Responsable de traitement doit examiner la cause de la violation et évaluer si les mesures et processus de protection et de prévention existants sont suffisants pour empêcher des violations similaires de se produire et, le cas échéant, mettre un terme aux pratiques qui ont conduit au violation de données.

1- Problèmes opérationnels et politiques :

• Des audits ont-ils été régulièrement menés sur les mesures de sécurité physiques et informatiques ?

……
……
……

• Existe-t-il des processus qui peuvent être rationalisés ou mis en place pour limiter les dommages en cas de futures violations ou pour empêcher une rechute ?

……
……
……

• Y avait-il des faiblesses dans les mesures de sécurité existantes telles que l'utilisation de logiciels et de mesures de protection obsolètes, ou des faiblesses dans l'utilisation de périphériques de stockage portables, de mise en réseau ou de connectivité à Internet ?

……
……
……

• Les méthodes d'accès et de transmission des données personnelles étaient-elles suffisamment sécurisées, par exemple : l'accès limité au personnel autorisé uniquement ?

……
……
……

- Les services de support des parties externes, tels que les fournisseurs et les partenaires, devraient-ils être améliorés pour mieux protéger les données personnelles ?

……
……
……

- Les responsabilités des fournisseurs et partenaires sont-elles été clairement définies en ce qui concerne le traitement des données personnelles ?

……
……
……

- Est-il nécessaire de développer de nouveaux scénarios de violation de données ?

……
……
……

2- Problèmes liés aux ressources :

- Des ressources suffisantes ont-elles été allouées pour gérer la violation de données ?

……
……
……

- Faut-il engager des ressources externes pour mieux gérer ces incidents ?

……
……
……

- Le personnel clé a-t-il reçu des ressources suffisantes pour gérer l'incident ?

……
……
……

3- Problèmes liés aux employés:

- Les employés étaient-ils conscients des problèmes de sécurité ?

……
……
……

- Une formation a-t-elle été dispensée sur les questions de protection des données personnelles et sur les compétences en gestion des incidents ?

……
……
……

- Les employés ont-ils été informés de la violation de données et des points d'apprentissage de l'incident ?

……
……
……

4- Problèmes liés à la gestion:

- Comment la direction a-t-elle été impliquée dans la gestion de la violation de données ?

……
……
……

- Y avait-il une ligne claire de responsabilité et de communication lors de la gestion de la violation de données ?

……
……
……

5- Exigences en matière de responsabilité et de documentation

Elément	Description
Décrire le mécanisme de survenance, documentation de l'incident (procédé, le service ou la personne en charge, les mesures pour y remédier) ?	
Disposez-vous de mécanisme de conservation des preuves de la violation de données personnelles ?	
Disposez-vous d'un registre de violation de données personnelles ?	

D. REMEDIATIONS

1. Actions

- **Installation de la DBT :** Le Responsable de traitement et l'équipe de gestion des violation (Data Breach Team - DBT) doivent agir dès qu ils ont connaissance d une violation de données. Dans la mesure du possible, il doit d abord confirmer que la violation de données est effective ou potentielle. Le Responsable de la sécurité informatique et l'équipe de gestion des violation (Data Breach Team - DBT) se réuniront pour s'assurer que toutes les mesures appropriées sont prises pour en atténuer l'impact et identifier les autres mesures nécessaires pour réduire le risque d'une autre violation de ce type.

  Chaque membre de l'équipe doit disposer d'un substitut pour couvrir les vacances, les congés de maladie, etc.

- **Confinement et mesure de sauvegarde :** Le Responsable de traitement doit essayer, lorsque l'incident est avéré, de contenir la violation. Il devrait envisager les mesures indicatives prévues dans la politique de gestion des incidents.

Les violations de la sécurité des données doivent être contenues et faire l'objet d'une réponse immédiate dès que l'on en a connaissance.

Le Responsable de traitement et/ou le service de sécurité informatique s’efforcera de contenir l'affaire et d'atténuer toute exposition supplémentaire des données personnelles détenues.

En fonction de la nature de la menace pour les données personnelles, cela peut impliquer une mise en quarantaine de certains ou de tous les PC, réseaux, etc. L’interdiction ou les restrictions d’accès aux PC, réseaux, etc. De même, il peut s'agir de mettre en quarantaine les zones de stockage des dossiers manuels et d'autres zones, le cas échéant.

En guise d'étape préliminaire, un audit des documents conservés ou du ou des serveurs de sauvegarde doit être entrepris afin de déterminer la nature des données personnelles qui ont pu être exposées.

- **Evaluation d’impact et criticité :** Parallèlement au confinement immédiat, il convient d'évaluer les risques qui peuvent être associés à la violation, les conséquences négatives potentielles pour les personnes concernées et le Responsable de traitement lui-même.

  L'Equipe de Gestion des Violations de Données doit utiliser le "Formulaire de notification de violation de données à caractère personnel" (**Annexe 2**) pour recueillir les informations pertinentes concernant la violation.

  Lorsque les données concernées sont protégées par des mesures technologiques de nature à les rendre inintelligibles à toute personne non autorisée, et si les mesures technologiques (telles que le chiffrement) étaient d'un niveau élevé.

- **Information du DPO : Tout incident de sécurité qui inclut des données personnelles nominatives, sensibles ou des données personnelles de nature financière doit toujours être transmis au DPDP**.

  Le DPDP, est informé sans délai par l'équipe de sécurité informatique (le responsable de l'information et de la sécurité (DSI, RSSI), le cas échéant) afin d’évaluer l'exposition/la perte potentielle. Le DPDP doit fournir des conseils et en contrôlant le respect des règles, ainsi que pendant la violation et lors de toute enquête ultérieure de l'APDP. Le DPO doit coopérer avec l'APDP et agir en tant que point de contact pour celle-ci. Les actions doivent être entreprises conformément aux directives/conseils.

2. Outils de gestion des incidents de violation des données personnelles

N°	Nom de l'outil	Version	Description de l'outil (spécifications fonctionnelles)	Description de l'outil (spécifications techniques)
1				
2				
3				
4				
5				

N°	Violations	Mesures prises	Notification à l'APDP	Information aux personnes concernées
1	Rançongiciel		Choisissez un élément.	Choisissez un élément.
2	Attaques d'exfiltration de données		Choisissez un élément.	Choisissez un élément.
3	Vol d'identité		Choisissez un élément.	Choisissez un élément.
4	Erreur d'envoi de données personnelles		Choisissez un élément.	Choisissez un élément.
5	Appareils ou documents perdus ou volés		Choisissez un élément.	Choisissez un élément.
6	Exfiltration de données par un employé de l'entreprise		Choisissez un élément.	Choisissez un élément.

7	**Indisponibilité des données du système d'information**		Choisissez un élément.	Choisissez un élément.
8	**Compromission des données du système d'information**		Choisissez un élément.	Choisissez un élément.
9	**Exposition/Fuite de données personnelles**		Choisissez un élément.	Choisissez un élément.
10	**Altération accidentelle des données**		Choisissez un élément.	Choisissez un élément.

Probabilité de préjudice		**Rare**	**Peu probable**	**Modérée**	**Probable**	**Presque certaine**	**Atteinte constatée**
1	Destinataire connu : public en général, personne déterminée, groupe déterminé de personnes (en vertu d'une entente de confidentialité) ou groupe déterminé de personnes (en vertu des lois et des règlements)						
2	Cause de la violation : accidentelle (erreur humaine), systémique ou intentionnelle (intention malveillante, risque de vol d'identité)						

Probabilité de préjudice		Rare	Peu probable	Modérée	Probable	Presque certaine	Atteinte constatée
3	Préjudice découlant de la violation (probabilité que l'information ait été indument utilisée, ou le soit un jour, à des fins frauduleuses ou préjudiciables : préjudice physique, préjudice financier, atteinte à la sécurité, atteinte à la réputation ou tout autre préjudice causé à la personne)						
4	Autres facteurs ou points à prendre en compte						
5	Probabilité de niveau global préjudice Faible/moyenne/élevée						

3- Rapport d'incident

Le Responsable de Traitement conserve un compte rendu sommaire de l'incident de sécurité. Tous les incidents de sécurité des données doivent être enregistrés de manière centralisée afin de garantir une surveillance appropriée des types et de la fréquence des incidents à des fins de gestion et d'établissement de rapports.

E. NOTIFICATIONS DE L'INCIDENT

1. Notification à l'Autorité de Protection des Données Personnelles

Le responsable de traitement doit immédiatement informer l'APDP de toute violation en utilisant le formulaire de signalement en annexe

La notification à l'APDP doit inclure les informations suivantes, lorsqu'elles sont disponibles :

- Ampleur de la violation de données ;
- Type et volume de données personnelles concernées ;
- Cause présumée de la violation ;
- Si la violation a été corrigée ;
- Mesures et processus que l'organisation avait mis en place au moment de la violation ;
- Informations indiquant si les personnes concernées de la violation de données ont été informées et, dans la négative, quand l'organisation a l'intention de le faire ;
- Coordonnées du personnel avec qui l'APDP peut se mettre en rapport pour obtenir de plus amples informations ou clarifications.

Lorsque des informations spécifiques sur la violation de données ne sont pas encore disponibles, le Responsable du traitement doit envoyer une notification intermédiaire comprenant une brève description de l'incident.

Si un incident de sécurité implique d'autres actes criminels présumés tels que le téléchargement présumé de matériel illégal, le Responsable de la sécurité informatique peut demander à la police de mener une enquête.

2. Notification aux personnes concernées

Le responsable de traitement informe les personnes concernées lorsque leurs données personnelles ont été violées. Il s'agit de prévenir les individus en vue de prendre s'il a lieu des mesures préventives susceptible de réduire pour elles l'impact de la violation de données ou de se préparer aux conséquences.

A cette fin l'équipe :

- Contacte les personnes concernées (par téléphone, courrier électronique, etc.) pour les informer qu'une divulgation, une perte, une destruction ou une modification non autorisée de leurs données personnelles a eu lieu. Il est recommandé d'utiliser les moyens les plus efficaces pour atteindre les personnes touchées, en tenant compte de l'urgence de la situation et du nombre de personnes touchées (par exemple, communiqués de presse,

médias sociaux, messagerie mobile, SMS, e-mails, appels téléphoniques).

Les notifications doivent être simples à comprendre, spécifiques et fournir des instructions claires sur ce que les individus peuvent faire pour se protéger.

Informe les personnes concernées (c'est-à-dire les individus sur lesquels portent les données) de :

- la nature des données qui ont été potentiellement exposées/compromises ;
- le niveau de sensibilité de ces données, et
- un aperçu des mesures que le Responsable de traitement a pris en matière de confinement ou d'assainissement.

Des conseils spécifiques et clairs devraient enfin être donnés aux particuliers sur les mesures qu'ils peuvent prendre pour se protéger et sur ce que le responsable de traitement peut faire pour les aider.

IV. DISPOSITIONS FINALES

Cette politique peut être révisée à la lumière des modifications de la législation, des avis juridiques, des rapports d'analyses d'incidents et des nouvelles technologies pertinentes.

Le personnel est informé de tout changement apporté à cette politique et des mesures de sécurité améliorées. Le personnel doit recevoir une formation de remise à niveau si nécessaire.

V. ANNEXES

ANNEXE 1

LOGO DE LA STRUCTURE	**NOM DE LA STRUCTURE**

NOTE D'ALERTE D'INCIDENT

Signaler un incident de sécurité réel ou présumé

À remplir par la personne qui signale l'incident de sécurité ou le membre du personnel qui reçoit un rapport verbal par téléphone.

Notice confidentielle

Les informations sur les incidents de sécurité réels et présumés sont confidentielles et doivent être partagées uniquement avec les membres du personnel ayant des responsabilités désignées pour la gestion de ces incidents de sécurité.

Formulaire de rapport d'incident de sécurité

Date de l'incident de sécurité : Lieu de l'incident de sécurité :

Nom de la personne rapportant l'incident de sécurité : Coordonnées : courriel, téléphone/adresse

L'incident de sécurité a-t-il un impact sur des données à caractère personnel?

Oui ☐ Non ☐

Pour le DPO uniquement

Commentaire du DPO ……

Nom de la personne physique impactée (si nécessaire/si possible) Coordonnées : courriel, téléphone/adresse

Brève description ou détails de l'incident de sécurité (impact, niveau de criticité estimé, emplacement, système ou application touché...)

Quelles sont les conséquences probables de l'incident de sécurité ?

Brève description de toute mesure prise au moment de la découverte (qui, quoi, quand...)

Pour le Responsable de la sécurité uniquement

Numéro de référence de l'incident de sécurité

Reçu par……

Sur

Transmis pour action à……

Sur

ANNEXE 2: FORMULAIRE DE SIGNALEMENT

LOGO DE LA STRUCTURE	**NOM DE LA STRUCTURE**

NOTIFICATION D'INCIDENT DE VIOLATION DE DONNEES PERSONNELLES

1.Identification	
Je soussigné	
☐ Madame ☐ Monsieur	
Nom de famille (ou de naissance) :	
Prénoms :	
Adresse :	
Quartier/lieu dit :	Arrondissement :
Commune :	Pays :
Votre numéro de téléphone portable : +I___I___I___II___I___I___I___I___I___I___I___I___I___I	Boite Postale :
Adresse électronique :	
2.Types de violation	

☐ Mise en œuvre d'un traitement de données personnelles non autorisé

☐ Changement de finalité sans consentement

☐ Détournement de finalité

☐ Non-respect des conditions légales de prospection directe

☐ Transfert des données vers un état tiers ou une organisation internationale sans autorisation préalable (sauf cas de dispense) de l'APDP ou du Conseil des Ministres

☐ Absence de garantie d'un/des droits des personnes concernées (droit à l'information préalable - droit d'accès – droit d'opposition – droit de rectification ou de suppression – droit à l'oubli – droit à la portabilité des données etc.) par un responsable de traitement

☐ Conservation des données à caractère personnel au-delà de la durée prévue par la déclaration adressée à l'Autorité sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques

☐ Les données traitées régulièrement ont fait l'objet d'une violation (perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite).

☐ Refus de déférer aux réclamations relatives à vos droits

☐ Autres (Préciser)
:…….

3.Information sur la violation	
a. Auteur présumé	
Nom et Prénoms / Dénomination :	
Ville :	Pays :
Contact :	
a. Date, heure et lieu de la violation	
Date et heure de la violation elle-même (si connues, ou approximation) : _____ : _____	
Date et heure de constatation de la violation : _____ : _____	
Lieu de la violation : _____	
a. Résumé de l'incident à l'origine de la violation	
Description générale :	

1.*Ex : nom, sexe, date de naissance, âge...)*
1.**Conséquences potentielles (impacts sur les données)**
Les données ont été, ou pourraient vraisemblablement être : ☐... détenues, stockées ou utilisées sans consentement ou de manière illicite ; ☐... diffusées plus que nécessaire et avoir échappé à la maîtrise des personnes concernées (ex. : diffusion plus ou moins large, diffusion non désirée d'une photo sur Internet, perte de contrôle d'informations publiées sur un réseau social...); ☐... corrélées avec d'autres informations relatives aux personnes concernées (ex. : corrélation d'adresses de résidence et de données de géolocalisation en temps réel...); ☐... exploitées à d'autres fins que celles prévues et/ou de manière injuste (ex. : fins commerciales, usurpation d'identité, utilisation à l'encontre des personnes concernées...). ☐... modifiées en des données invalides, qui ne seront pas utilisées de manière correcte, le traitement pouvant engendrer des erreurs, des dysfonctionnements, ou ne plus fournir le service attendu (ex.: altération du bon déroulement de démarches importantes...); ☐... modifiées en d'autres données valides, de telle sorte que les traitements soient détournés (ex.: exploitation pour usurper des identités en changeant la relation entre l'identité des personnes et les données biométriques d'autres personnes...). ☐... manquantes à des traitements qui ne peuvent plus du tout fournir le service attendu (ex.: ralentissement ou blocage de processus administratifs ou commerciaux, impossibilité de fournir des soins du fait de la disparition de dossiers médicaux, impossibilité pour des personnes concernées d'exercer leurs droits...); ☐... manquantes à des traitements et générer des erreurs, des dysfonctionnements, ou fournir un service différent de celui attendu (ex.: certaines allergies ne sont plus signalées dans un dossier médical, certaines informations figurant dans des déclarations de revenus ont disparu, ce qui empêche le calcul du montant des impôts...).
1.**Observations techniques**
1.**Pièces**

1……

2. ……

3. ……

4. ……

Le présent signalement a pour objet d'informer l'Autorité de Protection des Données à caractère Personnel d'une violation relative à des données personnelles. Veuillez le remplir de manière exhaustive et l'adresser comme suit :

Adresse électronique : contact@apdp.bj

Adresse physique : Rue 6.076 Immeuble El Marzouk Joël

Adresse postale : 01 BP 04837 Cotonou

ANNEXE 3 RAPPORT D'INCIDENT

LOGO DE LA STRUCTURE

NOM DE LA STRUCTURE

RAPPORT D'INCIDENT DE VIOLATION DE DONNEES PERSONNELLES

Nom du Responsable de traitement : ……	Nom de la structure: ……
Référence d'autorisation ou de déclaration du traitement	
Qui signale la violation : Nom/Dept/	
DESCRIPTION DE L'INCIDENT	
Description de l'incident de sécurité/de la violation des données	*Veuillez fournir autant d'informations/ détails que possible ou référence au signalement*
Date et heure de l'identification de l'incident/de l'atteinte à la sécurité et par qui.	

Y avait-il d'autres témoins ? Si oui, indiquez leurs noms.	
CATEGORISATION DE L'INCIDENT	
Violation confirmée ou suspectée ?	
Type de violation des données	• Confidentialité • Intégrité • Disponibilité
Cause de la violation ? • Accident ou négligence, • Erreur technique, • Vol ou méfait intentionnel, • Navigation non autorisée, • Autre (décrire), • Inconnu	Sources humaines Sources non humaines
EVALUATION DE CRITICITE	

Nature des données affectées	• Données publiques • Données internes • Données personnelles • Simples • Sensibles • Judiciaires • Sécurité et Défense
Volume des données concernées	
Volume de personnes	• Très peu (moins de 20) • Groupe identifié et limité (>20 et <100) • Grand nombre d'individus touchés (>100) • Les chiffres ne sont pas connus
Catégories des personnes	

Possibilité d'identification des personnes concernées **Connaissez-vous les personnes concernées (joindre une liste) ?**	• Maximale • Important • Limité • Négligeable
Les données concernent-elles des groupes vulnérables ?	
À qui les données ont-elles été divulguées ou consultées, si vous le savez ?	
Types de préjudice pouvant résulter de la violation	• Vol d'identité • Préjudice physique • Blessure, humiliation, atteinte à la réputation • Perte d'opportunités commerciales ou d'emploi • Violations des obligations contractuelles
La violation est-elle circonscrite ou en cours ?	
Si c'est le cas, quelles sont les mesures de remédiation?	
Des systèmes informatiques ont-ils été utilisés ? Si oui, veuillez les	

énumérer.	
Des protections par cryptage étaient-elles en place au moment de la violation ?	
Une violation de cette nature s'est-elle déjà produite auparavant ?	
D'autres personnes pourraient-elles donner des conseils sur les risques et les mesures à prendre ?	
Toute autre information pertinente	
Date/heure :	
Breach ID :	
Signature du Responsable de Traitement	