	PROCEDURE **Lors d'une violation de données à caractère personnel**	**Réf : RGPD/PR/05** **Version : 01**

DESCRIPTION DE LA PROCEDURE		
DOMAINE D'APPLICATION	Ce document a pour objectif : • de donner un cadre de traitement de la violation de données à caractère personnel • d'indiquer les acteurs au sein de la structure lors de la violation • de gérer l'information de la violation • de résoudre la violation dans les meilleurs délais	
LIEUX D'APPLICATION	☐ Mennecy siège ☐ Mennecy médical ☐ Evry ☐ Etampes ☐ Saint Michel/Orge ☐ Les Ulis	☐ Milly-la-Forêt ☐ Dourdan ☐ Méréville ☐ Breuillet ☐ Local en entreprise ☒ Tous les centres
FONCTIONS CONCERNÉES	☒ Médecin du travail et assimilé ☒ Médecin coordinateur ☒ Infirmière en Santé Travail ☒ Coordinatrice secrétaire ☒ Secrétaire médicale ☐ Ergonome ☐ Psychologue du travail ☐ Médecin écoutant ☐ Hygiéniste du travail et de l'environnement ☐ AST/ Assistant en Santé Travail ☐ Assistante sociale ☐ Assistante du service social ☐ Assistante administrative du service social	☒ Directeur général ☐ Directrice des activités ☐ Directrice des ressources humaines ☐ Responsable comptable et financier ☐ Assistante de Direction ☐ Chargée des RH ☐ Comptable ☐ Référente Qualité ☐ Responsable de la communication ☐ Chargée des SI et de la sécurité des données numériques ☐ Chargé des services généraux ☒ Référente RGPD ☒ DPO ☐ Toutes les fonctions
DOCUMENTS LIÉS		

	Rédacteur	**Validation**	**Approbation**
Date	19/03/2024	02/04/2024	02/04/2024
Nom	Séverine LEYGUES	Comité de Pilotage	J. LE-NY
Fonction	Référente qualité	Comité de Pilotage	Directeur général

CHANGEMENT DE VERSION			
Versions	**Dates**	**Motif**	**Pages concernées**

Date de publication 10/03/2025

1. Définitions, Abréviations et Terminologie

ARS : Agence Régionale de Santé
CNIL : Commission Nationale de l'Informatique et des Libertés
DPO : Délégué à la protection des données
RGPD : Règlement Général sur la Protection des Données

2. Références

Le Règlement Général sur la Protection des Données (RGPD) impose aux responsables de traitement des obligations particulières en cas de violation des données à caractère personnel.
Notamment de **documenter en interne** les violations de données personnelles et de **notifier les violations** présentant un risque pour les droits et libertés des personnes à la CNIL et, dans certains cas, lorsque le risque est élevé, aux personnes concernées.

Dès lors que l'ASTE a le statut de responsable de traitement et qu'elle est victime d'une violation de données à caractère personnel, elle doit respecter cette procédure.

Il s'agit de garantir en toute transparence l'intégrité des données qui lui sont confiées par les personnes concernées et en cela de maintenir leur confiance.

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

Définition : Article 4.12 du RGPD :
« 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. »

Il s'agit donc de tout incident de sécurité, d'origine malveillante ou non, se produisant de manière intentionnelle ou non, ayant pour conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité des données personnelles.

Pour qu'il y ait violation, 2 conditions doivent être réunies :

- L'organisme a mis en œuvre un traitement de données personnelles.
- Ces données ont fait l'objet d'une violation.

Origine des violations :

- Piratage
- Données envoyées au mauvais destinataire
- Equipement perdu ou volé (Ex : Perte d'une clé USB non sécurisée contenant le fichier client)
- Publication involontaire d'informations
- Suppression accidentelle de données personnelles non sauvegardées
- Autres…

Les obligations des responsables de traitement concernant les violations de données personnelles, et notamment leur notification à la CNIL et aux personnes concernées sont définies aux articles 33 et 34 du RGPD.

3. Matériel, Consommable et Approvisionnements

Registre des violations

4. Description de l'activité

1) Qui est concerné

L'ASTE, comme tous les organismes publics comme privés et quelle que soit leur taille, est soumise à ces obligations dès lors qu'elle traite des données personnelles et qu'elle a connaissance d'une violation de données personnelles.

Les sous-traitants, qui traitent des données personnelles pour le compte de l'ASTE, 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'il puisse remplir ses obligations.

2) Que faire en cas de violation de données

Si une violation de données à caractère personnel est détectée ou suspectée, ou si un sous-traitant en informe l'ASTE, il convient de :

1. Signaler immédiatement la violation au référent RGPD ;
2. Investiguer la violation ;
3. Rechercher et mettre en œuvre des actions correctives ;

4. Evaluer les impacts de la violation ;
5. Notifier la violation à la CNIL (le cas échéant) ; (Art 33 du RGPD)
6. Notifier en complément l'ARS dans le cas d'une violation des données de santé ; (Art D1111-16-4 et Art D1111-16-2 du code de santé publique)
7. Notifier les personnes concernées (le cas échéant) ;
8. En tirer les enseignements ;
9. Assurer un suivi et archiver.

Dans tous les cas, il faudra documenter en interne l'incident.

3) Schéma de traitement de la violation de données

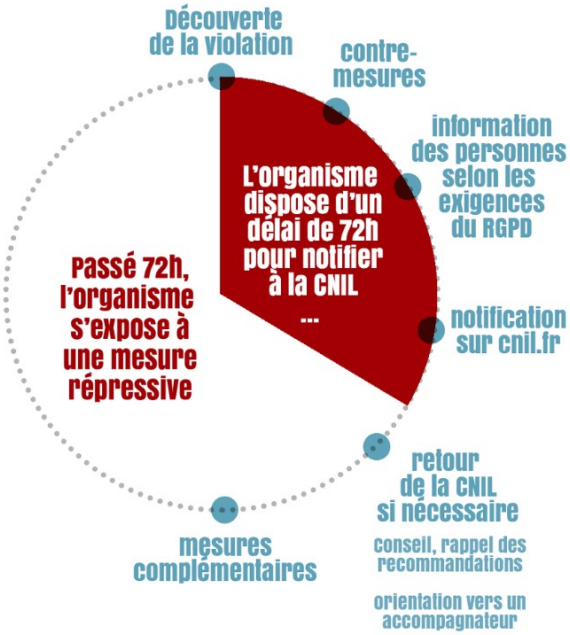

Schéma du site de la CNIL : https://www.cnil.fr/fr/violations-de-donnees-personnelles-1er-bilan-apres-lentree-en-application-du-rgpd

4) Signaler la violation

Dès lors qu'un membre de l'ASTE ou bien un sous-traitant se rend compte d'une violation, **il doit informer instantanément** les personnes habilitées à traiter la violation, **en précisant toutes les informations pertinentes**.

La référente RGPD et le délégué à la protection des données (société Pro archives systems) doivent en être informés **immédiatement** sur l'adresse mail DPO-RGPD@santetravailessonne.fr

5) Investiguer la violation

La référente RGPD désigne une équipe ou bien une personne pour investiguer les circonstances de la violation (ex : perte de confidentialité, d'intégrité, de disponibilité des données, destruction des données) et le type de données concernées.

Le cas échéant, elle pourra faire appel au(x) sous-traitant(s) acteurs du traitement de données.

La référente RGPD procède à l'inscription de la violation dans le registre des violations.

La personne ou l'équipe en charge de la violation créé un dossier qui portera le nom de l'ID que la référente aura communiqué dans le dossier Excel enregistré sur le serveur.

6) Rechercher et mettre en oeuvre des actions correctives

L'équipe ou bien la personne désignée et le cas échéant le sous-traitant doivent apprécier le risque au mieux afin d'adopter la bonne démarche.
Cela implique la mise en oeuvre de mesures de détection des violations et de lancer au plus tôt des investigations permettant d'atteindre une telle certitude raisonnable.

Comment apprécier le risque ?
Il faut analyser les risques pour les personnes concernées par la violation de données en ayant une approche similaire au PIA puis évaluer l'impact et la probabilité de la violation pour les personnes concernées.

L'appréciation du risque doit être réalisée au cas par cas en tenant compte des éléments suivants :

- Le type de violation (affectant l'intégrité, la confidentialité ou la disponibilité des données) ;
- La nature, la sensibilité et le volume des données personnelles concernées ;
- La facilité d'identifier les personnes touchées par la violation ;
- Les conséquences possibles de celles-ci pour les personnes ;
- Les caractéristiques de ces personnes (enfants, personnes vulnérables, etc.) ;
- Le volume de personnes concernées ;
- Les caractéristiques du responsable du traitement (nature, rôle, activités).
- **Définir le niveau du risque**

POUR LES PERSONNES CONCERNEES, LA VIOLATION ENGENDRE :	AUCUN RISQUE	UN RISQUE	UN RISQUE ELEVE
Documentation interne, dans le « registre des violations »	X	X	X
Notification à la CNIL, dans un délai maximal de 72h	-	X	X
Information des personnes concernées dans les meilleurs délais, hors cas particuliers	-	-	X

Le DPO procède à l'inscription des éléments ci-dessus dans le registre des violations.

Le référent en qualité de responsable de traitement prendra la décision de notifier la CNIL et les personnes concernées.
Il pourra s'appuyer sur les informations fournies par l'équipe d'investigation et de l'avis du Délégué à la Protection des Données.

Exemples de situations ne devant pas être notifiées à la CNIL ou aux personnes concernées :

- Divulgation de données déjà rendues publiques.
- Suppression de données sauvegardées immédiatement restaurées.
- Perte de données protégées par un algorithme de chiffrement à l'état de l'art (si la clé de chiffrement n'est pas compromise et si une copie des données reste disponible).

7) Notifier la violation à la CNIL

a) Quand ?

La notification doit intervenir dans les meilleurs délais **et au plus tard 72h** après que le responsable du traitement en a pris connaissance.

En pratique, le point de départ de ce délai est lorsque l'ASTE a un degré de certitude raisonnable qu'un incident a eu lieu et a touché des données personnelles.

Durant cette période d'investigation, l'ASTE n'est pas considérée comme ayant connaissance de la violation.

b) Comment ?

La notification s'effectue par le biais d'un téléservice sécurisé dédié par la CNIL.
Le document récapitulatif de la notification à la CNIL doit être intégré dans la documentation interne de la violation.

c) Contenu

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.

d) Notification incomplete

Si des investigations complémentaires sont nécessaires pour fournir toutes les informations requises dans ce délai, l'ASTE pourra procéder à une notification en deux temps :

1. Une notification initiale dans un délai de 72 heures comprenant les motifs du retard ;
2. Une notification complémentaire dès lors que les informations complémentaires sont disponibles.

e) Violations sur 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 la CNIL, y compris si la violation affecte des personnes résidant en France et y compris si elle s'est produite sur le territoire français.

f) Suites de la procédure en cas de notification à la CNIL

Dès réception, la CNIL va instruire la notification, et exercera deux missions principales :

- Un rôle d'accompagnement des responsables du traitement
- Un rôle de contrôle du respect des obligations des responsables du traitement

Dans les deux cas, l'examen de la CNIL pourra porter sur le niveau de sécurité générale du traitement que la violation peut révéler.

La procédure relative à la violation notifiée pourra être clôturée si la CNIL constate que :

- La violation ne porte pas atteinte aux données personnelles ou ne présente pas de risque pour les droits et libertés des personnes.
- Les personnes concernées ont été correctement informées, lorsque cela est obligatoire.
- Il a été mis en place, préalablement à la violation, des mesures techniques de protection appropriées.

La CNIL pourra imposer d'informer les personnes concernées si elle constate que :

- Celles-ci n'ont pas été correctement informées.
- Les mesures techniques de protection qui ont été mises en place préalablement à la violation ne sont pas appropriées.

8) Notifier les personnes concernées

a) Quand ?

La notification doit intervenir dans les meilleurs délais après que le responsable du traitement en a pris connaissance.

En pratique, le point de départ de ce délai est lorsque l'ASTE a un degré de certitude raisonnable qu'un incident a eu lieu et a touché des données personnelles.
Il est rappelé qu'elle peut être imposée par la CNIL.

b) Comment ?

La notification s'effectuera au cas par cas des violations de données en fonction des canaux de contact disponibles permettant de l'informer.

c) Contenu

La notification doit contenir à minima 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, référent ou autre…) ;
- Les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation.

Si nécessaire, les recommandations pour atténuer les effets négatifs potentiels de la violation et leur permettre de prendre les précautions qui s'imposent :

- Changement de mot de passe ;
- Vérification des données du compte en ligne
- Sauvegarde sur un support personnel
- …

d) Dérogation à l'information des personnes concernées

Malgré l'existence d'un risque élevé, il existe des dérogations à l'information des personnes concernées dans les cas suivants :

- Les données à caractère personnel affectées par la violation sont protégées par des mesures techniques et organisationnelles appropriées et sont ainsi incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès ;
- Des mesures ultérieures ont été prises qui garantissent que le risque élevé pour les droits et libertés des personnes n'est plus susceptible de se matérialiser ;
- La communication de la violation aux personnes concernées exigerait des efforts disproportionnés.

Dans ce cas, une communication publique, ou une mesure similaire permettant aux personnes concernées d'être informées de manière aussi efficace, doit être réalisée.

9) En tirer les enseignements

Dès lors que la violation sera soit résolue ou soit contenue, il faudra en tirer les enseignements nécessaires pour éviter qu'elle ne se reproduise dans le futur.

Cela en :

- Mettant les processus et les procédures à jour ;
- Surveillant le SI pour détecter les incidents ;
- Maintenant le SI à jour ;
- S'appuyant sur les règles de sécurité ;
- Sensibilisant les collaborateurs ;
- S'entraînant sur la base de scénarii variés en impliquant l'ensemble des acteurs impactés.

10) Assurer un suivi et archiver

Le DPO procèdera à l'intégration des éléments finaux de la demande dans le registre des violations.

Le référent indiquera au service la clôture de l'incident.

Les éléments devront être **conservés en archive dix ans à compter de la clôture du dossier.**

5. Evaluation

Cette procédure sera évaluée lors de chaque violation de données, sinon annuellement.