

**POLITIQUE
GÉNÉRALE DE
GESTION DES
DONNÉES À
CARACTÈRE
PERSONNEL**



POLITIQUE GÉNÉRALE DE GESTION DES DONNÉES À CARACTÈRE PERSONNEL

Liste des mesures techniques et organisationnelles de la **Centre Intercommunal d'Action Sociale** de Thiers Dore et Montagne et relatives à la protection des données à caractère personnel

En référence au RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 et la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée.

Nom du responsable du traitement : Tony BERNARD, Président

Nom du référent opérationnel : Nathalie SERGERE

Centre Intercommunal d'Action Sociale de Thiers Dore et Montagne

Délégué à la protection des données :

ADIT63

24 rue Saint Esprit

63000 CLERMONT FERRAND

Délégué référent : Alain LAGRU

dpo.adit63@puy-de-dome.fr

04 73 42 22 46

Politique générale de gestion des données à caractère personnel

2

Date d'entrée en vigueur de la présente politique : 01 avril 2020

SOMMAIRE

1.	CONTEXTE.....	1
2.	COMITÉ INFORMATIQUE ET LIBERTÉS.....	2
2.1.	Objectifs	2
2.2.	Composition du comité « Informatique et libertés »	2
2.3.	Responsabilités du comité.....	2
2.4.	Référent opérationnel à la protection des données.....	2
2.5.	Fréquence des comités.....	2
2.6.	Procédure de gestion des demandes des personnes concernées.....	3
3.	GÉRER LE REGISTRE DES TRAITEMENTS.....	3
3.1.	Objectifs	3
3.2.	Tenue du registre des traitements.....	4
4.	GÉRER LES SOUS-TRAITANTS DE DCP	4
4.1.	Objectifs	4
4.2.	Conformité des contrats de sous-traitance	4
5.	GÉRER LES MESURES DE SÉCURITÉ	4
5.1.	Objectifs	4
5.2.	Recommandations en matière de mesures de sécurité	4
5.3.	Liste des mesures de sécurité opérationnelles.....	4
6.	GÉRER LES VIOLATIONS DE DONNÉES.....	4
6.1.	Objectifs	4
6.2.	Définition de la violation de données à caractère personnel	5
6.3.	Procédure à suivre en cas de violation de données.....	5
6.4.	Contenu de la notification de violation de données	5
7.	PILOTER LA MISE EN CONFORMITÉ.....	5
7.1.	Objectifs	5
7.2.	Production du rapport annuel.....	5
7.3.	Patrimoine documentaire à valeur de preuve.....	5
7.4.	Veille juridique.....	6

Politique générale de gestion des données à caractère personnel

1

CONTEXTE

La présente politique décrit les mesures techniques et organisationnelles qui permettent à la **(Centre Intercommunal d'Action Sociale** de Thiers Dore et Montagne

de respecter dans le temps les exigences du règlement européen et de pouvoir le démontrer. Le tableau ci-dessus présente une synthèse de la politique générale de gestion des données à caractère personnel

Politique générale de gestion des données à caractère personnel		
6 Domaines de mesures	12 Objectifs	14 Règles
Comité informatique et libertés	Définir, mettre en oeuvre et réexaminer les mesures techniques et organisationnelles de la présente politique	Composition du comité "Informatique et libertés" Responsabilités du comité
	S'assurer que l'ensemble des agents est sensibilisé à la protection des données	Référent opérationnel à la protection des données Fréquence des comités
	Répondre aux demandes des personnes concernées	Procédure de gestion des demandes des personnes concernées
Gérer le registre des traitements	Disposer d'un registre des activités de traitement à jour S'assurer que les mesures de conformité des traitements de DCP sont effectivement prises en compte en cas de traitement ultérieurs	Tenue du registre des traitements
Gérer les sous-traitants de DCP	S'assurer de la conformité des contrats de sous-traitance	Conformité des contrats de sous-traitance Tenue du registre des sous-traitants
Gérer les mesures de sécurité	Etablir, mettre en œuvre et réexaminer les mesures de sécurité nécessaires pour empêcher la violation de données	Liste des mesures de sécurité opérationnelles
Gérer les violations de données	Identifier les cas de violation de données	Procédure à suivre en cas de violation de données
	Informers la CNIL et Soliris en cas de violation de données	Contenu de la notification de violation de données
Piloter la mise en conformité	Produire un rapport annuel	Production du rapport annuel
	Tenir à jour le patrimoine documentaire attaché à la protection des données	Patrimoine documentaire à valeur de preuve
	Assurer une veille réglementaire	La lettre d'information du service DPD de Soliris

Figure 1 : Politique générale de gestion des données à caractères personnel

COMITÉ INFORMATIQUE ET LIBERTÉS

Objectifs

- Définir, mettre en œuvre et réexaminer les mesures techniques et organisationnelles de la présente politique
- S'assurer que l'ensemble des agents est sensibilisé à la protection des données
- Répondre aux demandes des personnes concernées

Composition du comité « Informatique et libertés »

- Tony BERNARD, Président, et agissant en tant que responsable du traitement
- Nathalie SERGERE, Secrétaire général et des Assemblée agissant en tant référent opérationnel à la protection des données
- Monsieur Alain LAGRU, délégué référent, agissant en tant que représentant de l'ADIT63, DPO personne morale, mutualisé

Responsabilités du comité

- Il organise et fournit les ressources nécessaires à la mise en œuvre, au fonctionnement et au réexamen des présentes mesures techniques et organisationnelles
- Il s'assure que les agents de la collectivité sont régulièrement sensibilisés à la protection des données
- Il produit et valide un rapport annuel relatif aux actions de la collectivité en matière de protection des données à caractère personnel
- Il définit et tient à jour la procédure de gestion des demandes des personnes concernées
- Il nomme son représentant opérationnel

Référent opérationnel à la protection des données

Le comité est représenté par Nathalie SERGERE qui interagit avec le service délégué à la protection des données de l'ADIT63.

Le référent réalise ou s'assure que les actions prises par le comité en matière de protection des données sont réalisées.

Fréquence des comités

Le comité se réunit 1 fois par an ou lorsque la situation l'exige.

L'agenda type d'un comité est le suivant :

- Rapport annuel
- Révision des mesures
- Révision de la politique

Procédure de gestion des demandes des personnes concernées

Pour exercer ses droits, la personne concernée doit adresser un formulaire à Nathalie SERGERE, accompagné de la photocopie d'un titre d'identité comportant sa signature, à l'adresse postale suivante : **Centre Intercommunal d'Action Sociale** de Thiers Dore et Montagne , 47 avenue du Général de Gaulle, 63 300 THIERS

ou à l'adresse de courrier électronique contact@cias-tdm.fr Le formulaire est disponible sur demande en mairie.

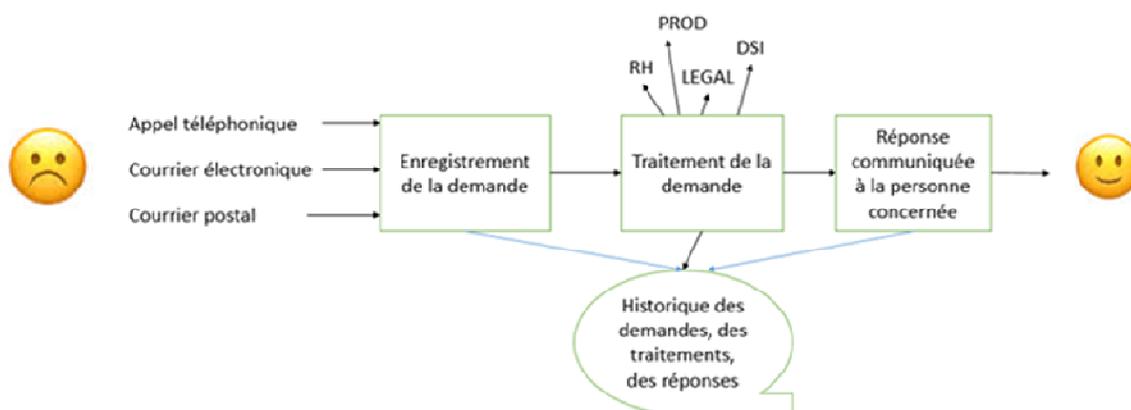


Figure 2 : Le schéma ci-dessus représente la procédure de gestion des demandes

Chaque demande est recensée dans un registre tenu à jour par Nathalie SERGERE

GÉRER LE REGISTRE DES TRAITEMENTS

Objectifs

- Disposer d'un registre des activités de traitement à jour
- S'assurer que les mesures de conformité des traitements de DCP sont effectivement prises en compte en cas de traitements ultérieurs

Politique générale de gestion des données à caractère personnel

4

Tenue du registre des traitements

La tenue et mise à jour du registre des traitements est réalisé par Nathalie SERGERE
L'ensemble des agents est informé de ses obligations à signaler tout nouveau traitement ou tout traitement ultérieur de données à caractère personnel

GÉRER LES SOUS-TRAITANTS DE DCP

Objectifs

- S'assurer de la conformité des contrats de sous-traitance

Conformité des contrats de sous-traitance

LA LISTE DES SOUS-TRAITANTS DE DCP AINSI QUE LE NIVEAU DE CONFORMITE DE CES CONTRATS EST TENU A JOUR. CETTE LISTE EST TENUE ET MISE A JOUR PAR NATHALIE SERGERE GÉRER LES MESURES DE SÉCURITÉ

Objectifs

- Etablir, mettre en œuvre et réexaminer les mesures de sécurité nécessaire pour empêcher la violation de données

Recommandations en matière de mesures de sécurité

Il est recommandé les 7 mesures minimales de sécurité suivantes :

- L'accès physique aux locaux contenant des équipements numériques est contrôlé
- Tous les équipements sont protégés par un antivirus
- L'accès au réseau informatique depuis l'extérieur est unique et protégé par un pare-feu
- Les utilisateurs en situation de mobilité sont sensibilisés au vol des équipements portables
- Les données à caractère personnel sont sauvegardées
- Il existe des sauvegardes externalisées
- Les mots de passe sont tenus secrets

Liste des mesures de sécurité opérationnelles

Il existe un document qui liste l'ensemble des mesures de sécurité sur les données à caractère personnel de la collectivité.

Cette liste est tenue et mise à jour par Nathalie SERGERE

GÉRER LES VIOLATIONS DE DONNÉES

Objectifs

- Informer la CNIL et le service DPO de l'ADIT63 en cas de violations de données

Politique générale de gestion des données à caractère personnel

5

Définition de la violation de données à caractère personnel

Il est rappelé les 3 cas principaux de violations de données :

- Accès illégitime aux DCP
- Modification non désirée des DCP
- Perte définitive de DCP

Procédure à suivre en cas de violation de données

A moins que la violation ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes, le responsable du traitement ou le référent opérationnel en informe l'ADIT63 (et éventuellement la CNIL) dans les meilleurs délais et si possible dans les 72 heures de la connaissance de la violation.

Chaque violation de données est enregistrée dans un registre qui y est tenu par Nathalie SERGERE.

Contenu de la notification de violation de données

La notification doit comprendre les informations suivantes :

- Nombre approximatif de personnes concernées
- Mesures prises pour remédier à la violation
- Nom et coordonnées du délégué ou d'un autre point de contact
- Conséquences potentielles pour les personnes concernées
- Mesures prises pour y remédier ou atténuer les conséquences
-

PILOTER LA MISE EN CONFORMITÉ

Objectifs

- Produire un rapport annuel
- Tenir à jour le patrimoine documentaire attaché à la protection des données
- Assurer une veille réglementaire

Production du rapport annuel

Le rapport annuel est généré par Nathalie SERGERE (avec Madis) qui le transmet pour signature auprès de son responsable du traitement.

Patrimoine documentaire à valeur de preuve

Il a été établi une liste minimale de 8 documents opposables en cas de sollicitations de la CNIL ou de poursuite par une personne concernée :

- Politique générale de gestion des données à caractère personnel
- Politique de protection des données à caractère personnel

Politique générale de gestion des données à caractère personnel

6

- Déclaration du DPO ADIT63 à la CNIL
- Registre des traitements
- Liste des mesures de sécurité
- Contrats de sous-traitance
- Attestation de formation ou de sensibilisation au règlement
- Rapport annuel

Veille juridique

Afin de maintenir des connaissances minimales en matière de protection de données, un membre du comité Informatique et Liberté sera abonné à la lettre d'information RGPD du service DPO de l'ADIT63

Politique générale de gestion des données à caractère personnel



NOTES :