Règlement général européen sur la protection des données à caractère personnel (RGPD)

Quels impacts et obligations pour les collectivités territoriales?

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Programme de la réunion

- Présentation du cadre juridique
- Le RGPD en quelques questions
- Le délégué à la protection des données
- Les DPO en Haute-Savoie
- Comment mettre en œuvre le RGPD ?
- Références et documents utiles
- Echanges/Questions
- Proposition d'accompagnement Adm74

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Présentation du cadre juridique

Un cadre juridique vieux de 40 ans marqué par un renforcement constant du niveau de protection

➢ **La loi « Informatique et Libertés » du 6 janvier 1978 : apparition des grands principes de protection des données**

- **Modifiée en 2004** sous l'impulsion des évolutions technologiques et de la directive européenne du 24 octobre 1995
- **Enrichie en 2016** par les dispositions de la loi pour une République numérique d'octobre 2016
- **Modifiée en dernier lieu en juin 2018 :** loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles

➢ **Le règlement européen du 27 avril 2016, applicable à compter du 25 mai 2018 : avènement de l'ère de la gouvernance des données personnelles**

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Présentation du cadre juridique

UNION EUROPÉENNE

Pourquoi un règlement alors qu'on avait déjà la loi Informatique et Libertés?

- **Cadre juridique pas totalement respecté**

- **Hétérogénéité des cadres juridiques et volonté d'unifier les législations nationales** (mais avec la possibilité de garder certaines spécificités nationales).

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

- **Volonté de renforcer les droits des personnes en matière de protection des données face à l'augmentation importante du volume des données et à l'absence de maîtrise de ces données :**
  - droit à l'information
  - droit d'accès
  - droit de rectification
  - droit d'opposition

  Droits renforcés
  - droit à l'effacement
  - *droit à la portabilité des données*
  - *droit au déréférencement*

  Nouveaux droits

  Délai pour répondre = 1 mois

- **Volonté de responsabiliser les responsables de traitement de données : changement de logique et d'outils**

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

Qu'est ce qu'une donnée à caractère personnel ?

Art. 4 §1 du RGPD

Toute information relative à une personne physique susceptible d'être identifiée, directement (nom, prénom, photo, etc.) ou indirectement (numéro de sécurité sociale, plaque d'immatriculation, etc.).

Exemples : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, des coordonnées bancaires, des données de géolocalisation, etc.

Peu importe que ces informations soient confidentielles ou publiques.

A noter : pour que ces données ne soient plus considérées comme personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la personne concernée : noms masqués, visages floutés, etc.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

Un traitement de données à caractère personnel, c'est quoi ?

➢ C'est **toute opération portant sur des données personnelles, quel que soit le procédé utilisé :** enregistrer, organiser, conserver/héberger, modifier, rapprocher avec d'autres données, transmettre, etc. des données personnelles.

➢ **Des fichiers mais pas seulement :** un traitement n'est pas uniquement un fichier, une base de données ou un tableau Excel. Il peut s'agir aussi d'une installation de vidéosurveillance, d'un système de paiement par carte bancaire ou de reconnaissance biométrique, d'une application pour smartphone, etc.

➢ **Informatisés mais pas uniquement :** un traitement de données à caractère personnel peut être informatisé ou non. Un fichier papier organisé selon un plan de classement, des formulaires papiers nominatifs ou des dossiers de candidatures classés par ordre alphabétique ou chronologique sont aussi des traitements de données personnelles.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

Article 9 RGPD

Une donnée sensible, c'est quoi ?

C'est une **information qui révèle les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle d'une personne physique.**

NB : NIR (n° de sécurité sociale) = donnée sensible

La loi interdit de recueillir et d'utiliser ces données, sauf dans certains cas précis et notamment :

- Si la personne concernée a donné son **consentement exprès** (écrit, clair et explicite)
- Si ces données sont nécessaires dans un **but médical** ou pour la recherche dans le domaine de la santé ;
- Si leur utilisation est justifiée par l'**intérêt public et autorisée par la CNIL** ;
- Si elles concernent les **membres ou adhérents d'une association** ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

Pourquoi entend-on beaucoup parler du RGPD?

- **Application depuis le 25 mai 2018**

- **Nouveau cadre unifié au niveau européen prévoyant le renforcement des droits des personnes**

- **Renforcement des sanctions**

- **Triple changement pour les responsables de fichiers et leurs sous-traitants** :
  - changement de culture: **logique de responsabilisation des organismes**
  - changement d'outils (registre des traitements, analyses d'impact…)
  - changement de gouvernance (DPO)

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

Dans quelle mesure les droits des personnes sont-ils renforcés ?

Principes généraux du RGPD :

- **licéité** : base juridique du traitement de données?

Plusieurs bases juridiques possibles :

- ✓ consentement
- ✓ exécution d'un contrat
- ✓ respect d'une obligation légale (ordures ménagères)
- ✓ sauvegarde des intérêts vitaux (interventions médicales d'urgence)
- ✓ intérêt public ou exercice de l'autorité publique (organisation d'un évènement)
- ✓ intérêts légitimes poursuivis par le responsable de traitement (newsletter)

Attention : **renforcement du consentement**

- **limitation des finalités**

Exemple : données de l'Etat civil ne peuvent pas être utilisées pour déclarer une naissance ou un mariage dans le bulletin municipal

- **minimisation des données**

Exemple : recueillir la nationalité pour inscrire les enfants au centre de loisirs n'est pas justifié

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

- **exactitude des données**

Attention aux bases de données dont les données ne sont jamais supprimées ou actualisées.
En cas de données inexactes, obligation de les rectifier ou de les effacer au plus vite.

- **limitation de la conservation des données**

La durée de conservation doit être **définie par le responsable du fichier, sauf si un texte impose une durée précise** (*ex : listes électorales = 3 ans ; vidéosurveillance = 1 mois ; gestion du personnel = 5 ans à compter du départ du salarié*).
Cette durée va dépendre de la nature des données et des objectifs poursuivis (conservation des données le temps nécessaire à l'accomplissement de l'objectif poursuivi lors de leur collecte).
A l'issue de cette période, 3 options :

-supprimer les données
-archiver les données (archives intermédiaires/définitives)
-anonymiser les données

- **intégrité et confidentialité**

Les traitements doivent faire l'objet de mesures de sécurité techniques et opérationnelles (sécurité physique + informatique).
Voir Guide de la CNIL sur la sécurité des données personnelles.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

Principes dont le responsable de traitement doit être en mesure de prouver le respect.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

Art. 83 RGPD

Quelles sanctions en cas de non respect du RGPD ?

Le montant des amendes administratives est déterminé en fonction :

-de la nature, la gravité et la durée de la violation du RGPD

-de la nature, la portée ou la finalité du traitement concerné

-du nombre de personnes concernées affectées et du niveau de dommage subi

Amende maximale

20 millions d'euros ou pour une entreprise **4% du chiffre d'affaires annuel mondial total** de l'exercice précédent

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

Un changement de culture d'abord…

Avant le 25 mai 2018

Régime de déclaration ou d'autorisation préalable auprès de la CNIL.

La CNIL doit prouver la non-conformité des organismes aux règles relatives à la protection des données.

CNIL.

Après le 25 mai 2018

Disparition des formalités préalables.

Logique de responsabilisation et de conformité continue

Les organismes doivent être en mesure de prouver leur conformité au RGPD.
Chaque responsable de traitement devra s'assurer de sa conformité à tout moment, de manière continue tout au long de la vie du traitement de données.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

Nouveau !

La responsabilité du sous-traitant

Art. 4 §8 RGPD

Sous-traitant : personne physique ou morale, autorité publique, service ou autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Art. 26 RGPD

Tout le monde sera comptable du respect des principes posés par le RGPD : **les responsables de traitement mais aussi leurs sous-traitants,** tels que par exemple les fournisseurs de logiciels et de plateformes pour les collectivités.

→ **responsabilité conjointe du traitement**

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

Un changement d'outils ensuite…

-Registre des traitements

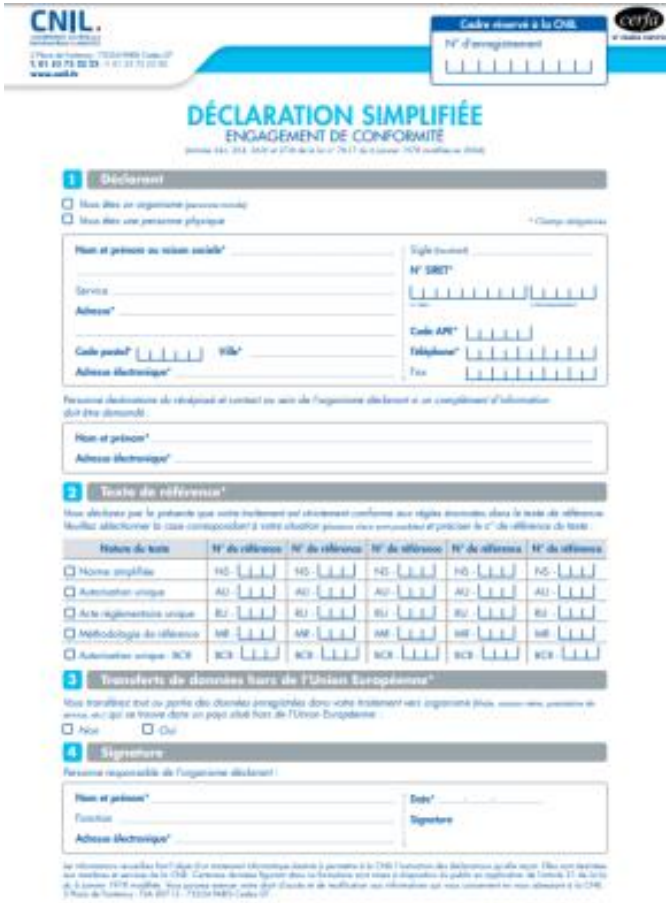
-Sécurisation des données et des traitements

-Etudes d'impact sur la protection des données (*Privacy Impact Assessment ou PIA*)

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

Au revoir les formalités CNIL !


CNIL.

Cadre réservé à la CNIL

N° d'enregistrement

cerfa

DÉCLARATION SIMPLIFIÉE

ENGAGEMENT DE CONFORMITÉ

1 Déclarant

Nom et prénom ou raison sociale*

Sigle

N° SIRET*

Service

Adresse*

Code APE*

Code postal* Ville*

Téléphone*

Adresse électronique*

Fax

Nom et prénom*

Adresse électronique*

2 Texte de référence*

Nature du texte | N° de référence | N° de référence | N° de référence | N° de référence | N° de référence

Norme simplifiée | NS

Autorisation unique | AU

Acte réglementaire unique | RU

Méthodologie de référence | MR

Autorisation unique - BCR | BCR

3 Transferts de données hors de l'Union Européenne*

Non Oui

4 Signature

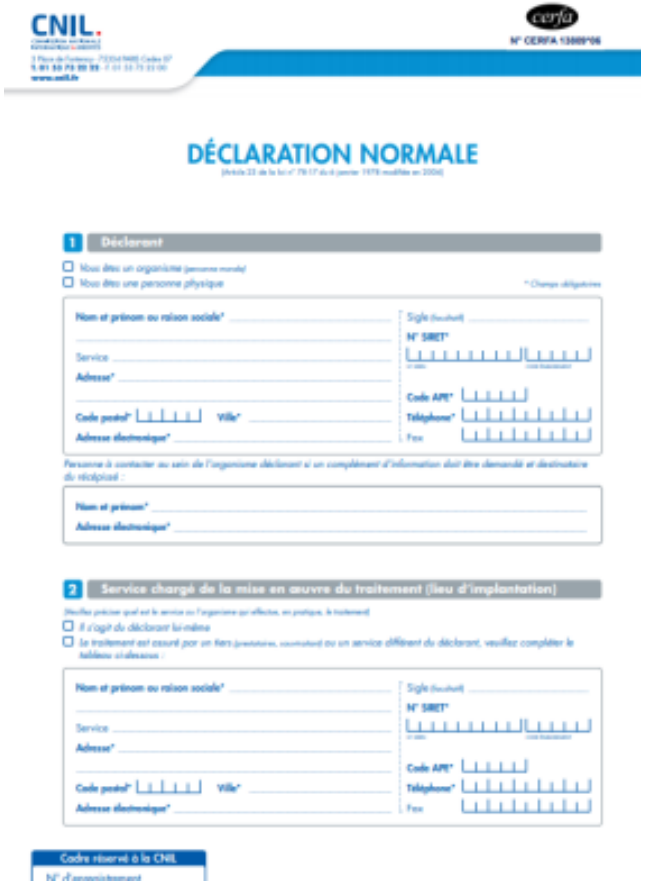
Nom et prénom*

Date*

Fonction

Signature

Adresse électronique*


CNIL.

cerfa

N° CERFA 13980*06

DÉCLARATION NORMALE

1 Déclarant

Nous êtes un organisme

Nous êtes une personne physique

* Champs obligatoires

Nom et prénom ou raison sociale*

Sigle

N° SIRET*

Service

Adresse*

Code APE*

Code postal* Ville*

Téléphone*

Adresse électronique*

Fax

Personne à contacter au sein de l'organisme déclarant si un complément d'information doit être demandé et destinataire du récépissé :

Nom et prénom*

Adresse électronique*

2 Service chargé de la mise en œuvre du traitement (lieu d'implantation)

Veuillez préciser quel est le service ou l'organisme qui effectue, en pratique, le traitement

Il s'agit du déclarant lui-même

Le traitement est assuré par un tiers (prestataire, sous-traitant) ou un service différent du déclarant, veuillez compléter le tableau ci-dessous :

Nom et prénom ou raison sociale*

Sigle

N° SIRET*

Service

Adresse*

Code APE*

Code postal* Ville*

Téléphone*

Adresse électronique*

Fax

Cadre réservé à la CNIL

N° d'enregistrement

Adm74

ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Art. 30 RGPD

§1 et 2

§4

§3

§1

Voilà le Registre des traitements !

- Principal outil permettant de prouver le respect des obligations imposées par le RGPD
- Obligation pour le responsable de traitement et pour le sous-traitant
- Doit être mis à disposition de l'autorité de contrôle (CNIL) sur demande
- Forme écrite (y compris électronique)
- Contenu :
  - Nom et coordonnées du responsable du traitement (et du DPO)
  - Finalités du traitement
  - Description des catégories de personnes concernées et données personnelles
  - Catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées
  - Transferts de données personnelles vers un pays tiers
  - Si possible : délais prévus pour l'effacement des différentes catégories de données et description générale des mesures de sécurité techniques et organisationnelles

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Modèle de Registre de traitement (format excel)

Autres modèles et formats sur le site de la CNIL :

https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

Identification du traitement				Acteurs	Finalité du traitement	Transferts hors UE ?	Données sensibles ?
Nom / sigle	N° / REF	Date de création	Dernière mise à jour	Responsable du traitement	Finalité principale	Oui /non	Oui/non

Fiche de registre ref-000

Description du traitement	
Nom / sigle	
N° / REF	ref-000
Date de création	
Mise à jour	

Acteurs	Nom	Adresse	CP	Ville	Pays	Tel
Responsable du traitement						
Délégué à la protection des données						
Représentant						
Responsable(s) conjoint(s)						

Finalité(s) du traitement effectué	
Finalité principale	
Sous-finalité 1	
Sous-finalité 2	
Sous-finalité 3	
Sous-finalité 4	
Sous-finalité 5	

Mesures de sécurité	
Mesures de sécurité techniques	
Mesures de sécurité organisationnelles	

Catégories de données personnelles concernées	Description	Délai d'effacement
Etat civil, identité, données d'identification, images...		
Vie personnelle (habitudes de vie, situation familiale, etc.)		
Informations d'ordre économique et financier (revenus, situation financière,		
Données de connexion (adress IP, logs, etc.)		
Données de localisation (déplacements, données GPS, GSM, etc.)		

Données sensibles	Description	Délai d'effacement
Données révèlant l'origine raciale ou ethnique		
Données révèlant les opinions politiques		

Registre des activités de traitement de [Nom de l'organisme]

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	*Ex : NOM prénom du responsable légal* *Adresse* *CP VILLE* *Téléphone* *Adresse de messagerie*
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	*Ex : NOM prénom du DPO* *Société (si DPO externe)* *Adresse* *CP VILLE* *Téléphone* *Adresse de messagerie*

Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités (exemples)
Activité 1	*Etat-civil*
Activité 2	*Elections*
Activité 3	
Activité 4	
Activité 5	
Activité 6	
Activité 7	
Activité 8	
Activité 9	

Vous devrez créer et tenir à jour une fiche de registre par activité. Le modèle de fiche de registre est disponible sur la page suivante.

Composition du document

Une première page du registre recense les informations communes à toutes vos activités de traitement.

Les coordonnées de votre organisme.

Les coordonnées du délégué à la protection des données (DPO) si vous en disposez.

La liste des activités de votre organisme impliquant le traitement de données personnelles (liste des traitements par finalité principales : état civil, élections, RH, marchés publics, scolaire/périscolaire, gestion des fournisseurs, voirie, collecte et traitement des déchets, gestion des bibliothèques, action sociale, formation du personnel et des élus, police municipale, circulation et stationnement, etc.).

Pour chaque activité recensée, vous devrez créer et tenir à jour une fiche de registre.

C'est l'adition du sommaire et de toutes les fiches de traitement qui constituent le REGISTRE DES TRAITEMENTS.

Fiche de registre de l'activité 1

(Reprise de l'activité 1 de la liste des activités)

Date de création de la fiche	
Date de dernière mise à jour de la fiche	
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	
Nom du logiciel ou de l'application *(si pertinent)*	

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.

Tenue des registres d'État-civil ; Enregistrement des PACS ; Gestion des avis de mention ;
Hébergement des données

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. Officiers d'Etat civil (Maire et adjoints) 2. Agents d'Etat civil 3. Administrés

Catégories de données collectées

Listez les différentes données traitées

[X] Etat-civil, identité, données d'identification, images *(nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*

.....

[X] Vie personnelle *(habitudes de vie, situation familiale, etc.)*

.....

[X] Vie professionnelle *(CV, situation professionnelles, scolarité, formation, distinctions, diplômes, etc.)*

.....

[ ] Informations d'ordre économique et financier *(revenus, situation financière, données bancaires, etc.)*

.....

[ ] Données de connexion *(adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)*

.....

[ ] Données de localisation *(déplacements, données GPS, GSM, ...)*

.....

[ ] Internet *(cookies, traceurs, données de navigation, mesures d'audience, ...)*

.....

[ ] Autres catégories de données *(précisez)* :

.....

.....

.....

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

[X] Oui [ ] Non

Si oui, lesquelles ? : Personnes sous tutelle ou curatelle (non systématique)

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

Base active (ou archivage courant) : 100 ans
Archive définitive : intérêt historique

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

(exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.)

1. Services concernés ;

Organismes externes

(Exemples : filiales, partenaires, etc.)

1. Notaires 2. Autre collectivité locale française
3 TGI 4. Administrés ;

Sous-traitants

(Exemples : hébergeurs, prestataires et maintenance informatiques, etc.)

1. Maintenance (ADM74) 2.

3 Google (Google Doc) 4. .....

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

[X] Oui [ ] Non

Si oui, vers quel(s) pays : Etats-Unis : garanti par l'adhésion au Privacy Shield (25 septembre 2018)

Mesures de sécurité

Décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

Volet sécurité

[X] Contrôle d'accès des utilisateurs

Physique : Clés – Alarme – Fermetures des bureaux – Archives avec accès restreint

Informatique : Profils (administrateur / utilisateur / invité) ; Mdp robuste (12 caractère ; 1 caractère spécial, etc.) ; Gestion des droits (lecture / modification) ;

[ ] Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs)*, les données enregistrées *(exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation :

Voir le prestataire

[X] Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures :

Anti-virus ; Firewall ;

[X] Sauvegarde des données

Décrivez les modalités :

Voir le prestataire

[ ] Chiffrement des données

Décrivez les mesures (*exemple : site accessible en https, utilisation de TLS, etc.)* :

.....

.....

[X] Contrôle des sous-traitants

Décrivez les modalités :

Contrat avec le sous-traitant (clause article 28)

[ ] Autres mesures :

Responsable du Traitement

Dénomination sociale	Nom/Prénom/Coordonnées du Représentant légal	Nom/Prénom/Coordonnées du Représentant légal
Ex : RGPD SOCIETY *Forme juridique : S.A.* *Adresse du siège social : 3 rue du Pin – 75000 PARIS* *Capital social : 100 000 €* *N°RCS et Ville : 123 456 789 – Paris*	*Ex : Monsieur Stéphane Dupont – PDG* *01 XX XX XX XX* *stephane.dupont@rgpdsociety.fr*	*Ex : Madame Valérie Richard* *01 XX XX XX XX* *valérie.richard@dpo.fr*

Activité de Traitement

Catégories de traitements effectués par XXXXXXXX pour le compte du CLIENT	Instruction donnée à XXXXXXXX pour effectuer le traitement Oui/Non	Exigences article 28 RGPD					Exigences article 30.2 RGP
		Objet du traitement	Finalité du traitement	Durée du traitement	Type de donnée	Catégorie de personnes concernées	Description générale des mesures techniques et organisationnelles mises en place par le XXXXXXXX pour assurer la sécurité du traitement
Catégorie 1 Transmission au Client	*A compléter*	*A compléter*	Exécution par XXXXXXXX des prestations définies dans le contrat d'infogérance	Egale à la durée du contrat d'infogérance	*Ex : données de santé, base commerciale, base RH, ….*	*A compléter*	*A compléter par le ST*
Catégorie 2 Accès donné au Client	*A compléter*	*A compléter*	Exécution par XXXXXXXX des prestations définies dans le contrat d'infogérance	Egale à la durée du contrat d'infogérance		*A compléter*	*A compléter par le ST*
Catégorie 3 Transmission au Tiers	*A compléter*	*A compléter*	Exécution par XXXXXXXX des prestations définies dans le contrat d'infogérance	Egale à la durée du contrat d'infogérance		*A compléter*	*A compléter par le ST*
Catégorie 4 Accès donné au Tiers	*A compléter*	*A compléter*	Exécution par XXXXXXXX des prestations définies dans le contrat d'infogérance	Egale à la durée du contrat d'infogérance		*A compléter*	*A compléter par le ST*
Catégorie 5 Structuration	*A compléter*	*A compléter*	Exécution par XXXXXXXX des prestations définies dans le contrat d'infogérance	Egale à la durée du contrat d'infogérance		*A compléter*	*A compléter par le ST*
Catégorie 6 Stockage	*A compléter*	*A compléter*	Exécution par XXXXXXXX des prestations définies dans le contrat d'infogérance	Egale à la durée du contrat d'infogérance		*A compléter*	*A compléter par le ST*
Catégorie 7 Consultation	*A compléter*	*A compléter*	Exécution par XXXXXXXX des prestations définies dans le contrat d'infogérance	Egale à la durée du contrat d'infogérance		*A compléter*	*A compléter par le ST*

Le règlement général sur la protection des données en quelques questions

METHODOLOGIE POUR CONSTITUER LE REGISTRE DES TRAITEMENTS

1- Faire l'inventaire des traitements de données dans la collectivité via un questionnaire adressé à l'ensemble des services de la collectivité

Traitez-vous des données personnelles ?

Dans quels buts ?

Qui sont les personnes concernées ? *(ex : administrés, fonctionnaires, etc.)*

Quelles données utilisez-vous ?

Etat-civil, identité, données d'identification, images

Vie personnelle *(habitudes de vie, situation familiale, etc.)*

Vie professionnelle *(CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)*

Informations économiques *(Revenus, situation financière, données bancaires, etc.)*

Données sensibles *(données judicaires, infractions, opinions politiques, religion, etc.)*

Qui vous communique ces données ? *(les personnes directement concernées)*

Qui a accès à ces informations ?

Communiquez-vous ces informations à d'autres services ?

Communiquez-vous ces informations en tout ou partie à des sous-traitants ?

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

2- Remplir les fiches de traitement

Fiche de registre de l'activité 1 (scolaire et périscolaire)

(Reprise de l'activité 1 de la liste des activités)

Date de création de la fiche	**06/09/2018**
Date de dernière mise à jour de la fiche	-
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	-
Nom du logiciel ou de l'application *(si pertinent)*	**3D OUEST (SaaS)** **SERVEUR** **OUTLOOK / ORANGE / ETC.**

Objectifs poursuivis (POURQUOI)

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.

Gestion des inscriptions (fiche d'inscription/formulaire en ligne) ; Gestion des présences (école ; garderie ; cantine) ; Recensement des effectifs (élèves et intervenants) ; Facturation ; Prévention des risques liés aux allergies ; (établissement des grilles de tarif) ; Etablissement des statistiques

Catégories de personnes concernées (QUI ?)

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. Familles 2. Élèves
3 Intervenants 4. Personnel scolaire

Catégories de données collectées (QUOI, QUELLES DONNÉES)

Listez les différentes données traitées

[X] Etat-civil, identité, données d'identification, images *(nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*

[X] Vie personnelle *(habitudes de vie, situation familiale, etc.)*
Situation matrimoniale, Quotient familiale

[X] Vie professionnelle *(CV, situation professionnelles, scolarité, formation, distinctions, diplômes, etc.)*

.....

[X] Informations d'ordre économique et financier *(revenus, situation financière, données bancaires, etc.)*

.....

[X] Données de connexion *(adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)*
Plateforme inscription en ligne

[ ] Données de localisation *(déplacements, données GPS, GSM, ...)*

.....

[X] Internet *(cookies, traceurs, données de navigation, mesures d'audience, ...)*
Google analytics

[ ] Autres catégories de données *(précisez)* :

.....

.....

.....

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

[X] Oui [ ] Non

Si oui, lesquelles ? : Allergies ; régime alimentaire ;

Durées de conservation des catégories de données (COMBIEN DE TEMPS ?)

Combien de temps conservez-vous ces informations ?

..... [ ] jours [ ] mois [ ] ans

[X] Autre durée :

Papiers : Année scolaire puis archivage (le temps de scolarité de l'élève)
Numérique : Le temps de scolarité de l'élève puis archivage numérique
Messagerie : Ad vitam aeternam (tant que c'est pas saturé)

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

3- Déterminer les mesures de sécurité

- Mesures de sécurité physiques
- Mesures de sécurité informatiques

4- Déterminer la durée du conservation

- durée justifiée au regard des finalités
- texte de loi pour les obligations légales

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

Art. 32 RGPD

Sécurisation des données et des traitements

La protection des données personnelles nécessite de prendre des « ***mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque*** ».

Guide de la CNIL de la protection des données personnelles : https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

Guide qui rappelle les précautions élémentaires qui devraient être mises en œuvre de façon systématique.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Évaluer le niveau de sécurité des données personnelles de votre organisme

Avez-vous pensé à ?

Fiche		Mesure	
1	Sensibiliser les utilisateurs	Informez et sensibilisez les personnes manipulant les données	☐
		Rédigez une charte informatique et lui donner une force contraignante	☐
2	Authentifier les utilisateurs	Définissez un identifiant (*login*) unique à chaque utilisateur	☐
		Adoptez une politique de mot de passe utilisateur conforme à nos recommandations	☐
		Obligez l'utilisateur à changer son mot de passe après réinitialisation	
		Limitez le nombre de tentatives d'accès à un compte	
3	Gérer les habilitations	Définissez des profils d'habilitation	☐
		Supprimez les permissions d'accès obsolètes	☐
		Réaliser une revue annuelle des habilitations	☐
4	Tracer les accès et gérer les incidents	Prévoyez un système de journalisation	☐
		Informez les utilisateurs de la mi… …stème de journalisation	☐
		Protégez les équipement… …on et les informations journalisées	☐
		Prévoyez les pr… …es notifications de violation de données à caractère personnel	☐
5	Sécuriser les postes de travail	Pré… …ure de verrouillage automatique de session	☐
		U… …antivirus régulièrement mis à jour	☐
		Installez un « pare-feu » (*firewall*) logiciel	☐
		Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	☐
6	Sécuriser l'informatique mobile	Prévoyez des moyens de chiffrement des équipements mobiles	☐
		Faites des sauvegardes ou synchronisations régulières des données	☐
		Exigez un secret pour le déverrouillage des smartphones	☐
7	Protéger le réseau informatique interne	Limitez les flux réseau au strict nécessaire	☐
		Sécurisez les accès distants des appareils informatiques nomades par VPN	☐
		Mettez en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi	☐

17 points de contrôle recommandés par la CNIL

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

8	Sécuriser les serveurs	Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées	☐
		Installez sans délai les mises à jour critiques	☐
		Assurez une disponibilité des données	☐
9	Sécuriser les sites web	Utilisez le protocole TLS et vérifiez sa mise en œuvre	☐
		Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les url	☐
		Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu	☐
		Mettez un bandeau de consentement pour les *cookies* non nécessaires au service	☐
10	Sauvegarder et prévoir la continuité d'activité	Effectuez des sauvegardes régulières	☐
		Stockez les supports de sauvegarde dans un endroit sûr	☐
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	☐
		Prévoyez et testez régulièrement la continuité d'activité	☐
11	Archiver de manière sécurisée	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	
		Détruisez les archives obsolètes de manière sécurisée	
12	Encadrer la maintenance et la destruction des données	Enregistrez les interventions de maintenance dans une main courante	☐
		Encadrez par un responsable de l'organisme les interventions par d	☐
		Effacez les données de tout matériel avant sa mise au rebut	☐
13	Gérer la sous-traitance	Prévoyez une clause spécifique dans les contrats des so	☐
		Prévoyez les conditions de restitution et de destru ées	☐
		Assurez-vous de l'effectivité des garanties p de sécurité, visites, etc.)	☐
14	Sécuriser les échanges avec d'autres organismes	Chiffrez les données avant leur envoi	☐
		Assurez-vous qu'il s'agit du bo	☐
		Transmettez le secret lo stinct et via un canal différent	☐
15	Protéger les locaux	Restreignez les ac au moyen de portes verrouillées	☐
		Installez des ntrusion et vérifiez-les périodiquement	☐
16	Encadrer les développements informatiques	Proposez d tres respectueux de la vie privée aux utilisateurs finaux	☐
		Évitez les zones de commentaires ou encadrez-les strictement	☐
		Testez sur des données fictives ou anonymisées	☐
17	Utiliser des fonctions cryptographiques	Utilisez des algorithmes, des logiciels et des bibliothèques reconnues	☐
		Conservez les secrets et les clés cryptographiques de manière sécurisée	☐

https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

RGPD
Art. 33

Art. 34

Notification des violations de données personnelles

- **Auprès de la CNIL**

Dans les meilleurs délais possibles et au plus tard 72h après avoir pris connaissance de la violation

NB : même obligation pour le sous-traitant, mais notification à faire au responsable de traitement.

- **Auprès de la personne concernée par la violation des données**, si cette violation est susceptible d'engendrer un risque élevé pour ses droits et libertés :
  - Notification dans les meilleurs délais.
  - Si cela exige des efforts disproportionnés : communication publique ou autre mesure permettant aux personnes concernées d'être informées.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le règlement général sur la protection des données en quelques questions

Art. 35 RGPD

Analyses d'impact relatives à la protection des données

*(Data protection impact assessment ou **DPIA**, plus connue sous le nom de Privacy Impact Assessment ou **PIA** avant le RGPD)*

Par qui ?

Le responsable de traitement.

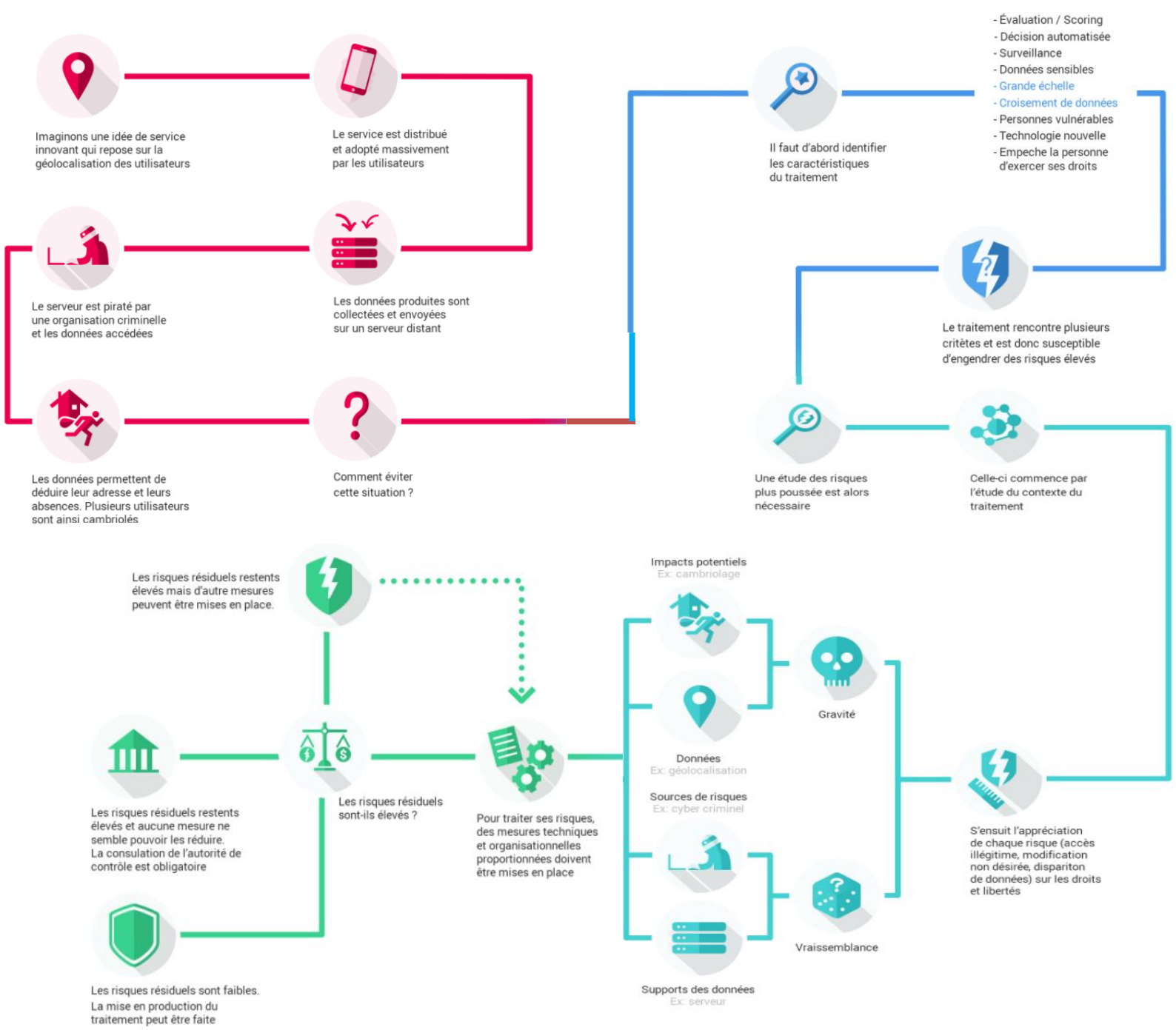
Quand ?

L'analyse d'impact est obligatoire lorsqu'un type de traitement (en particulier par le recours à des nouvelles technologies) est susceptible d'engendrer un **risque élevé pour les droits et libertés** des personnes physiques.

Quelles conséquences?

Si l'analyse d'impact révèle l'existence d'un risque élevé, il convient de consulter la CNIL.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE


Imaginons une idée de service innovant qui repose sur la géolocalisation des utilisateurs
Le service est distribué et adopté massivement par les utilisateurs
Le serveur est piraté par une organisation criminelle et les données accédées
Les données produites sont collectées et envoyées sur un serveur distant
Les données permettent de déduire leur adresse et leurs absences. Plusieurs utilisateurs sont ainsi cambriolés
Comment éviter cette situation ?
Il faut d'abord identifier les caractéristiques du traitement
- Évaluation / Scoring
- Décision automatisée
- Surveillance
- Données sensibles
- Grande échelle
- Croisement de données
- Personnes vulnérables
- Technologie nouvelle
- Empeche la personne d'exercer ses droits
Le traitement rencontre plusieurs critètes et est donc susceptible d'engendrer des risques élevés
Une étude des risques plus poussée est alors nécessaire
Celle-ci commence par l'étude du contexte du traitement
Impacts potentiels
Ex: cambriolage
Données
Ex: géolocalisation
Sources de risques
Ex: cyber criminel
Supports des données
Ex: serveur
Gravité
Vraissemblance
S'ensuit l'appréciation de chaque risque (accès illégitime, modification non désirée, dispariton de données) sur les droits et libertés
Pour traiter ses risques, des mesures techniques et organisationnelles proportionnées doivent être mises en place
Les risques résiduels sont-ils élevés ?
Les risques résiduels restents élevés mais d'autre mesures peuvent être mises en place.
Les risques résiduels restents élevés et aucune mesure ne semble pouvoir les réduire. La consulation de l'autorité de contrôle est obligatoire
Les risques résiduels sont faibles. La mise en production du traitement peut être faite

Le règlement général sur la protection des données en quelques questions

Un changement de gouvernance…

Depuis le 25 mai 2018, l'ensemble des organismes et autorités publics, et donc, l'ensemble des collectivités territoriales ont l'obligation de désigner un **délégué à la protection des données (DPD ou DPO pour *Data Protection Officer*).**

Successeur du **correspondant informatique et libertés (CIL)**

- ✓ fonction introduite en 2004
- ✓ désignation facultative pour les collectivités
- ✓ seulement 2% des communes en France ont désigné un CIL

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le délégué à la protection des données

Art. 37 RGPD

Article 37 RGPD - Désignation du délégué à la protection des données

1.Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque:

a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;

b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées;

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

2.Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement.

3.Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.

4.Dans les cas autres que ceux visés au paragraphe 1, le responsable du traitement ou le sous-traitant ou les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent désigner ou, si le droit de l'Union ou le droit d'un État membre l'exige, sont tenus de désigner un délégué à la protection des données. Le délégué à la protection des données peut agir pour ces associations et autres organismes représentant des responsables du traitement ou des sous-traitants.

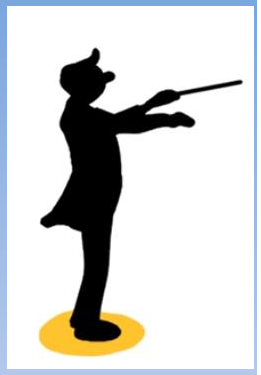
5.Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39.

6.Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

7.Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le délégué à la protection des données



Art. 39 §1 RGPD

Missions du délégué

- **contrôler le respect du RGPD** et du droit national en matière de protection des données
- **conseiller la collectivité sur la réalisation d'analyses d'impact** relatives à la protection des données et en vérifier l'exécution
- **informer et conseiller le responsable de traitement** de la collectivité ou le sous-traitant, ainsi que les agents
- **diffuser une culture Informatique & Libertés** au sein de la collectivité
- **coopérer avec la CNIL et être le point de contact** de celle-ci
- Dans l'exercice de ces missions, le délégué devra être à l'abri des conflits d'intérêts, rendre compte directement au niveau le plus élevé de la hiérarchie et bénéficier d'une liberté certaine dans les actions qu'il décidera d'entreprendre.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le délégué à la protection des données

CNIL.

DPO = chef d'orchestre de la démarche permanente et dynamique de mise en conformité de la collectivité

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le délégué à la protection des données

Expertise et moyens du DPO

La collectivité devra s'assurer qu'il dispose **d'un niveau d'expertise et de moyens suffisants pour exercer son rôle de façon efficace**.

Art. 37 §5 RGPD

Ainsi, le délégué devra :

- être désigné sur la base de ses connaissances spécialisées du droit et des pratiques en matière de protection des données (**exigence de qualification mais pas de profil type**)
- être associé en temps utile et de manière appropriée à l'ensemble des questions Informatique & Libertés

Art. 38 RGPD

- bénéficier des ressources et formations nécessaires pour mener à bien ses missions.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le délégué à la protection des données

Art. 38 §3 RGPD

Indépendance et protection du DPO

DPO ne doit recevoir **aucune instruction** en ce qui concerne l'exercice de ses missions.

> *« De tels délégués à la protection des données, qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance » (extrait du considérant n° 97 du RGPD).*

Pas de sanction possible du fait de l'accomplissement de ses missions de délégué.

Art. 24 §1 RGPD : Responsabilité du responsable de traitement

Art. 28 RGPD : responsabilité du sous- traitant

Responsabilité du DPO

Pas de transfert possible de la responsabilité incombant au responsable de traitement ou au sous-traitant au profit du DPO : **le DPO ne peut être tenu responsable en cas de non respect des dispositions du RGPD**.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le délégué à la protection des données

Attention au conflit d'intérêts !

Un DPO ne peut être « juge et partie » : le DPO ne peut occuper une fonction ou un rôle au sein de la collectivité qui le conduit à déterminer les finalités et les moyens du traitement de données.

Art. 38 §6 RGPD

Appréciation de l'existence éventuelle d'un conflit d'intérêts étudiée au **cas par cas**.

Exemple : on ne peut pas être à la fois DPO et

- élu dans la collectivité (maire, adjoint)
  Les conseillers municipaux sans délégation pourraient assumer cette fonction à titre bénévole
- DGS
  Débat à propos des secrétaires de mairie
- directeur financier
- responsable du service informatique
- Etc.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le délégué à la protection des données

Désignation du DPO en ligne sur le site de la CNIL

https://www.cnil.fr/fr/designez-en-ligne-votre-delegue-la-protection-des-donnees-aupres-de-la-cnil

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le délégué à la protection des données

Formulaire de déclaration en ligne: https://www.cnil.fr/designation-dpo

*Avant de **désigner en ligne** votre délégué à la protection des données, vérifiez qu'il dispose du statut, des compétences et des moyens nécessaires à l'exercice de ses missions.*

Assurez-vous en particulier que ces 3 conditions sont réunies :

1. LE DPO DÉTIENT LES COMPÉTENCES REQUISES

Cela suppose :

- une expertise juridique et technique en matière de protection des données personnelles ;
- une bonne connaissance du secteur d'activité, de l'organisation interne, en particulier des opérations de traitements, des systèmes d'information, des besoins en matière de protection et de sécurité des données.

Ces compétences peuvent être acquises, par exemple, à l'occasion de formations adaptées à son profil.

> En savoir plus

2. LE DPO DISPOSE DE MOYENS SUFFISANTS

Cela implique en particulier pour le DPO de :

- disposer du temps suffisant pour exercer ses missions ;
- bénéficier de moyens matériels et humains adéquats ;
- pouvoir accéder aux informations utiles ;
- être associé en amont des projets impliquant des données personnelles ;
- être facilement joignable par les personnes concernées.

> En savoir plus

3. LE DPO A LA CAPACITÉ D'AGIR EN TOUTE INDÉPENDANCE

Cela signifie :

- ne pas être en situation de conflit d'intérêt en cas de cumul de sa fonction de DPO avec une autre fonction ;
- pouvoir rendre compte de son action au plus haut niveau de la direction de l'organisme ;
- ne pas être sanctionné pour l'exercice de ses missions de DPO
- ne pas recevoir d'instruction dans le cadre de l'exercice de ses missions de DPO.

> En savoir plus

Vous répondez à ces prérequis ?

Commencez votre désignation

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le délégué à la protection des données

Art. 37 §3 et 37 §6 RGPD

Mutualisation, DPO interne ou externalisation ?

Art. 37 §3 RGPD – MUTUALISATION

« Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, ***un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes*** *de ce type, compte tenu de leur structure organisationnelle et de leur taille ».*

Art. 37 §6 RGPD – DPO INTERNE OU EXTERNE

« Le délégué à la protection des données peut être un ***membre du personnel*** *du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un* ***contrat de service*** *».*

Dans le cas du recours à un prestataire extérieur, il est fortement conseillé de désigner, au sein de la collectivité, une personne qui fera office de contact principal du prestataire.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

DAGC/DIT/DCJD

Le délégué à la protection des données (DPD) : missions et désignation

Désignation obligatoire d'un délégué à la protection des données (DPD) dans chaque commune et intercommunalité depuis le 25 mai 2018

En interne

- en transformant le poste du correspondant informatique et libertés (CIL), quand celui-ci est déjà existant, en DPD
- en attribuant les missions du DPD à un agent déjà en poste
- en créant l'emploi de DPD au tableau des effectifs.

Par le biais de la coopération

- en ayant recours, par convention entre communes et communautés à la mise à disposition d'un agent ou à la prestation de services
- en créant un service commun
- en bénéficiant des services du DPD d'un syndicat dédié.

Par le biais de l'externalisation

- en conventionnant avec le centre de gestion
- en s'assurant les services d'un prestataire privé.

NOTE A CONSULTER SUR LE SITE DE L'AMF : www.amf.asso.fr

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Le délégué à la protection des données

Alors, DPO interne ou externe?

	DPO INTERNE	DPO EXTERNE
AVANTAGES	• Bonne connaissance de l'entreprise et de ses rouages. • Bonne connaissance de ses interlocuteurs • Informé « à la source » • Peut réagir « sur-le-champ »	• Indépendant • Absence de conflit d'intérêts • Coûts maitrisés • Disponible immédiatement (pas de formation) • Expertise assurée • Disponible « à la carte » • Renforts disponibles • Remplacement facilité (relation contractuelle libre)
INCONVÉNIENTS	• Temps partiel ingérable • Climat tendu lors de sa désignation • Indépendance difficilement applicable • Risques importants de conflit d'intérêts • Coût partiel incontrôlable • Formation nécessaire • Remplacement risqué juridiquement	• Temps d'adaptation aux rouages de l'entreprise • Coût « à l'heure » plus élevé

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Les DPO en Haute-Savoie

- DPO mutualisés entre plusieurs communes
- DPO mutualisés à l'échelle d'une communauté de communes/d'agglomération
- DPO internes :
  - responsables commande publique
  - responsables communication
  - informaticiens
  - secrétaires de mairie
  - agents d'accueil
  - juristes
  - chargés de mission
  - etc.
- DPO externalisés

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Comment mettre en œuvre le RGPD ?

Se préparer en 6 étapes

https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

Désigner un pilote

Cartographier vos traitements de données personnelles

Prioriser les actions

Gérer les risques

Organiser les processus internes

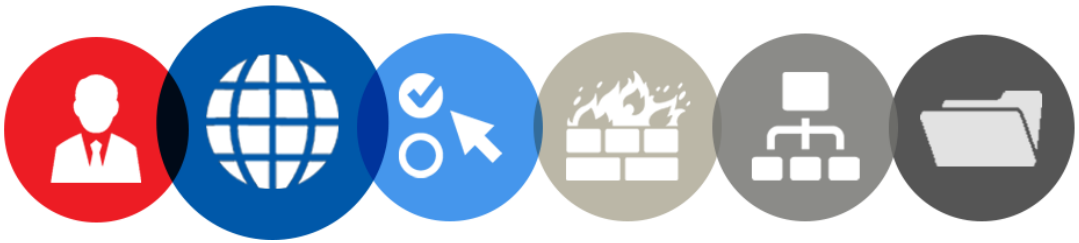
Documenter la conformité

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Comment mettre en œuvre le RGPD ?

ETAPE
1
DÉSIGNER UN PILOTE

Désignation obligatoire d'un DPO pour tous les organismes publics



Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

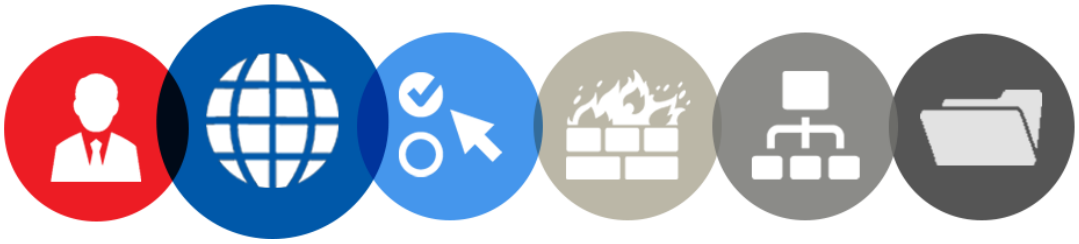
Comment mettre en œuvre le RGPD ?

ETAPE 2
CARTOGRAPHIER

Cartographier vos traitements de données personnelles

Recenser de façon précise les traitements de données personnelles que vous mettez en œuvre.

<u>Outil :</u> registre des traitements de données



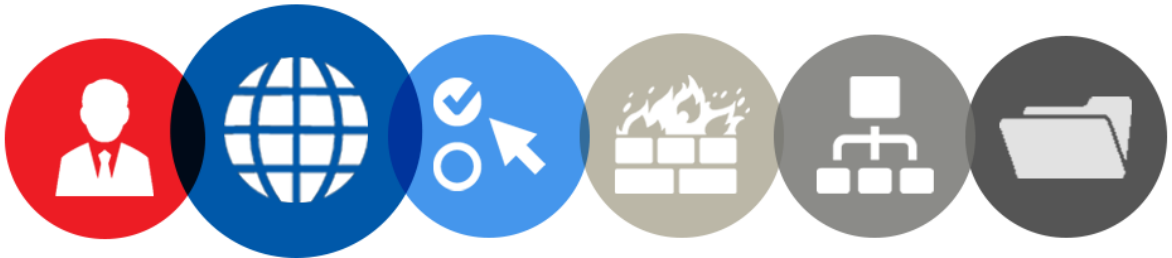
Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Comment mettre en œuvre le RGPD ?

ETAPE
3
PRIORISER

Sur la base du registre des traitements, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

<u>Outils :</u> Guide de la sécurité des données personnelles et guide du sous-traitant



Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Comment mettre en œuvre le RGPD ?

ETAPE
4
GÉRER LES RISQUES

https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données.

<u>Outil :</u> logiciel open source PIA facilite la conduite et la formalisation d'analyses d'impact sur la protection des données telles que prévues par le RGPD.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Comment mettre en œuvre le RGPD ?

Pour garantir un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la protection des données à tout moment, 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 demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

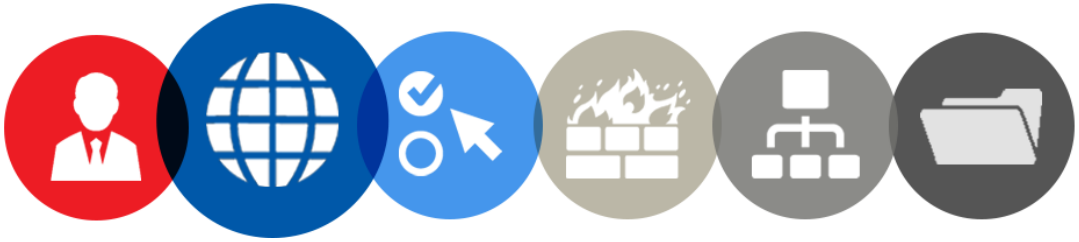
<u>Outil à venir</u> : téléservice de notification de violations de données personnelles.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Comment mettre en œuvre le RGPD ?

ETAPE
6
DOCUMENTER

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.



Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Références et documents utiles

-Site de la CNIL :

- RGPD : se préparer en 6 étapes : https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes
- Guide CNIL de la sécurité des données personnelles : https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles
- RGPD : Guide du sous-traitant : https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants
- Collectivités territoriales : les principes clés de la protection des données personnelles : https://www.cnil.fr/fr/collectivites-territoriales/les-principes-cles-de-la-protection-des-donnees
- En quoi les collectivités territoriales sont-elles impactées par le règlement européen sur la protection des données ? - 11/07/2017 : https://www.cnil.fr/fr/RGPD-quel-impact-pour-les-collectivites-territoriales
- Lignes directrices édictées par le G29 (groupe des CNIL européennes) : https://www.cnil.fr/fr/reglement-europeen/lignes-directrices
- Modèle de registre de traitement des données : https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles
- Texte du RGPD du 27 avril 2016 : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

-Ouvrage : *Protection des données personnelles : se mettre en conformité d'ici le 25 mai 2018* - Editions législatives – 2017

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Echanges/Questions

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DATA

Proposition d'accompagnement/Formation RGPD

Règlement Général sur la Protection des Données

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DATA

POUR LES « PETITES COLLECTIVITES »

Accompagnement/formation mutualisé

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

Accompagnement/formation mutualisé sur plusieurs collectivités

OPTIMEX DATA

2 journées en groupes de 6 à 8 participants (6 à 8 collectivités maximum, soit un participant par collectivité)
+ 1 jour d'audit individuel, dans la collectivité

Suite individuelle par collectivité – à voir en direct avec Optimex Data

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

TARIFS

PROPOSITION PACK ADM74 (3 jours dont un audit d'une journée sur site):

- **Une journée de formation en groupe** pour évoquer le RGPD et ce que la mairie doit mettre en place dans la collectivité pour s'y conformer
- **Une journée d'audit informatique** dans la collectivité (individualisé - sur site)
- **Une dernière journée en groupe** pour faire le point (suite à l'audit) et voir le plan d'action à mettre en place

TOTAL POUR LES 3 JOURS : 1 500 euros TTC / collectivité (une personne par collectivité pour les journées de formation)

OPTIONS A VOIR EN DIRECT AVEC NOS PARTENAIRES

-Option validation individuelle des traitements : 1 jour sur site = 850 € HT (+ frais de déplacement : forfait de 70 euros HT)

-Option DPO externalisé/an: 1 jour réparti sur l'année = 850 € HT/an (engagement 2 ans minimum – contrat de service).

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DATA

JOUR 1 - Détail de la journée de formation groupée - Matin: Découverte et Sensibilisation

A. Présentation des ateliers de formation
   a) Les intervenants
   b) Les participants
   c) La méthodologie

B. Introduction à la protection des données personnelles
   a) Contexte et cadre légal
   b) Principes et obligations du RGPD – Règlement Général sur la Protection des Données
   c) Missions et pouvoirs de la CNIL

C. Besoins et compétences des collectivités participantes
   a) Identification des compétences gérées
   b) Identification des données personnelles traités
   c) Identification des personnes concernées

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DATA

Jour 1 - Détail de la journée de formation groupée - Après-midi : Inventaire

A. Les bases pour identifier les traitements de données
   a) Définitions et terminologie du RGPD
   b) Les exigences du RGPD

B. La méthode d'inventaire des traitements
   a) Cartographie des traitements
   b) Registre des traitements
   c) Outils de la CNIL

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DATA

JOUR 2 – Audit sécurité dans la collectivité (sur site)

- Intervention sur site pour réaliser l'audit de sécurité

- Dans le cadre de la mise en conformité au RGPD d'un système d'information, à l'issue de la cartographie des traitements (étape 2 du RGPD), il est nécessaire de réaliser un audit informatique qui va permettre d'identifier :

    1. Les vulnérabilités du système informatique et des réseaux, des flux et stockage de données.
    2. Définir les bonnes pratiques dont les recommandations ANSSI applicables.
    3. Proposer un plan d'action, avec priorisation.

=> Le résultat de cet audit se traduit par un rapport, remonté au DPO, qui peut alors prioriser les actions de mise en conformité (étape 3 du RGPD "prioriser les actions").

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DATA

JOUR 2 – DETAIL DE L'AUDIT DE SECURITE

=> Mix entre les 17 points de contrôles de la CNIL et les 50 points du CIGREF

1. Sensibiliser les utilisateurs
2. Authentifier les utilisateurs
3. Gérer les habilitations
4. Tracer les accès et gérer les incidents
5. Sécuriser les postes de travail
6. Sécuriser l'informatique mobile
7. Protéger le réseau informatique interne
8. Sécuriser les serveurs
9. Sécuriser les sites web

10. Sauvegarder et prévoir la continuité d'activité
11. Archiver de manière sécurisée
12. Encadrer la maintenance et la destruction des données
13. Gérer la sous-traitance
14. Sécuriser les échanges avec d'autres organismes
15. Protéger les locaux
16. Encadrer les développements informatiques
17. Utiliser des fonctions cryptographiques

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DATA

JOUR 3 - Détail de la journée de formation groupée – Matin : Plan d'actions

A. Check-list des points de contrôle
   a) Actions prioritaires à mener
   b) Procédures à mettre en place
   c) Analyse d'impact (PIA)

B. Outils de la CNIL
   a) Présentation
   b) Méthodologie
   c) Cas pratiques

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DA

JOUR 3 - Détail de la journée de formation groupée – Après-midi : Conclusion et feuille de route

A. Feuille de route
   a) Gestion des situations à risques
   b) Gestion des priorités
   c) Les exigences du RGPD

B. Nomination du DPO – Data Protection Officer
   a) Obligations et exigences du RGPD
   b) Missions du DPO
   c) Outils de la CNIL

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

6 SESSIONS

-**Session 1** : **27/6/18 et 13/09/18** *(achevée)*
-**Session 2** : **9/07/18 et 24/09/18** *(achevée)*
-**Session 3** : **6/09/18 et 5/11/18** *(en cours)*
-**Session 4** : **11/12/18 et 29/01/19** *(quelques places encore disponibles)*
-**Session 5** : **14/11/2019 et 11/03/2019**
-**Session 6** : **4/02/2019 et 8/04/2019**

La date des audits sur site (Jour 2) seront vus directement entre la collectivité et notre partenaire COVATEAM.

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DATA

POUR LES « PLUS GRANDES COLLECTIVITES »

Accompagnement/formation Spécifique

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

Accompagnement spécifique pour une collectivité de taille et aux besoins plus importants

DIAGNOSTIC RGPD « AVANT DE SE LANCER »

Permet de définir
Les besoins
et la façon
d'aborder
RGPD

Sur site, Forfait 950 €HT

AUDIT RGPD + **AUDIT SÉCURITÉ**

Devis personnalisé

OU

SI DPO INTERNE

=> FORMATION AU MÉTIER DE DPO POUR LA PERSONNE RÉFÉRENTE EN INTERNE

=> ACCOMPAGNEMENT DU DPO INTERNE DANS LA MISE EN PLACE DE SES MISSIONS

SI DPO EXTERNALISÉ

=> Formation au règlement européen pour le relais en interne

Devis personnalisé

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DATA

Détail Diagnostic RGPD « Avant de se Lancer »
1 journée sur site = Forfait 950 € HT

- Matin 30 minutes : présentation rapide RGPD aux participants: DG, DRH, DGS, DSI…(toutes les personnes ressources sur cette question)
- Matin 2h30: atelier Questionnaire collectif en deux phases:
    - autour de la gouvernance et des métiers de la collectivité
    - autour du système d'information
- Après-midi: rédaction du document de synthèse et des préconisations d'actions
- Après-midi pendant 1heure: présentation des résultats, des préconisations, restitution des documents de synthèse, décisions autour du plan d'action.

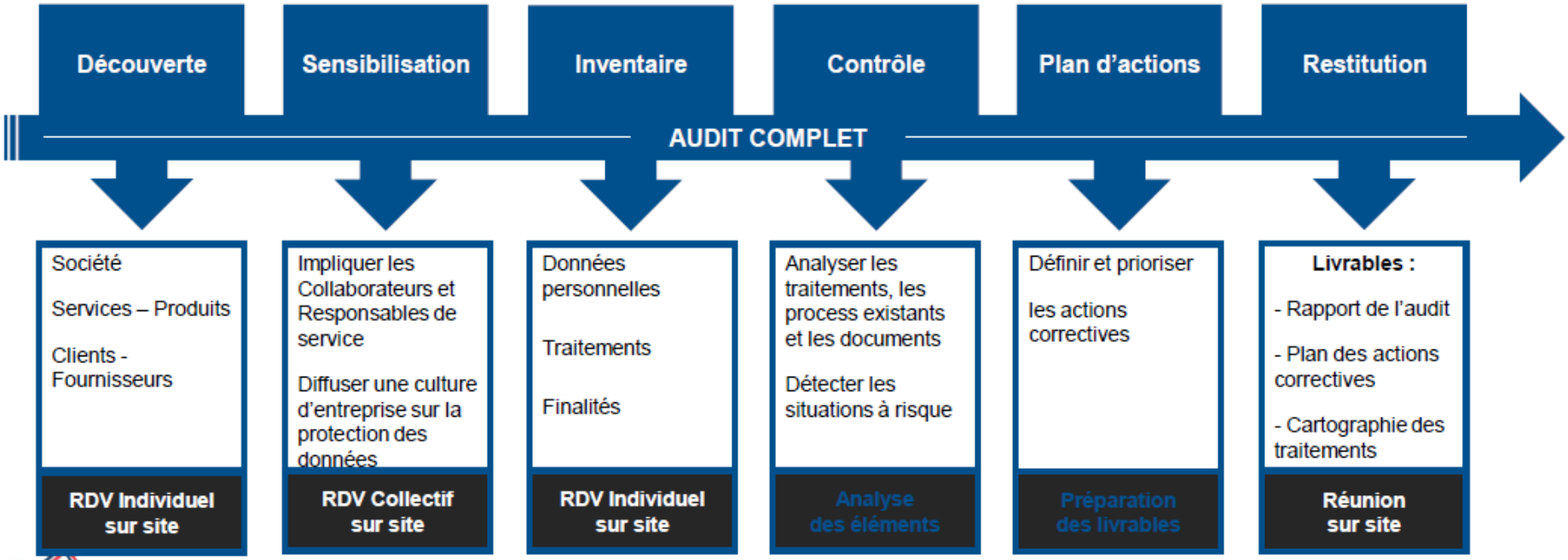
Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DATA

Détail AUDIT RGPD: Temps à définir en fonction du Diagnostic



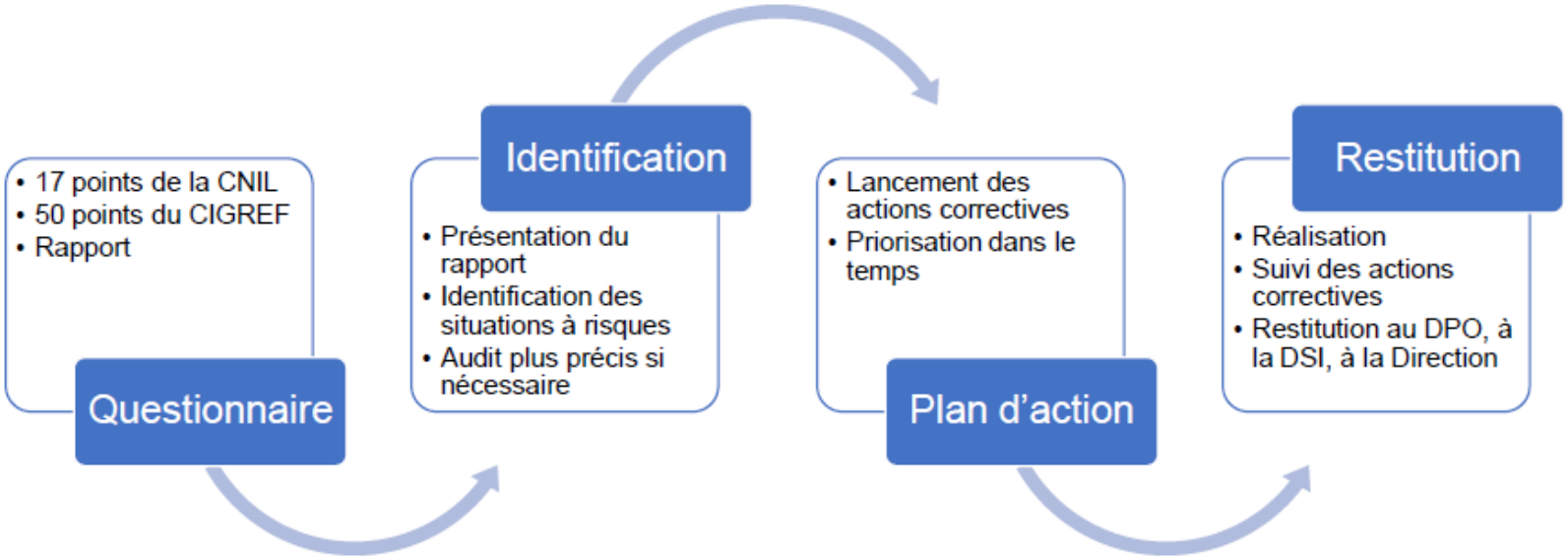
Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DATA

Détail AUDIT SECURITE du SYSTÈME d'INFORMATION: Temps à définir en fonction du Diagnostic



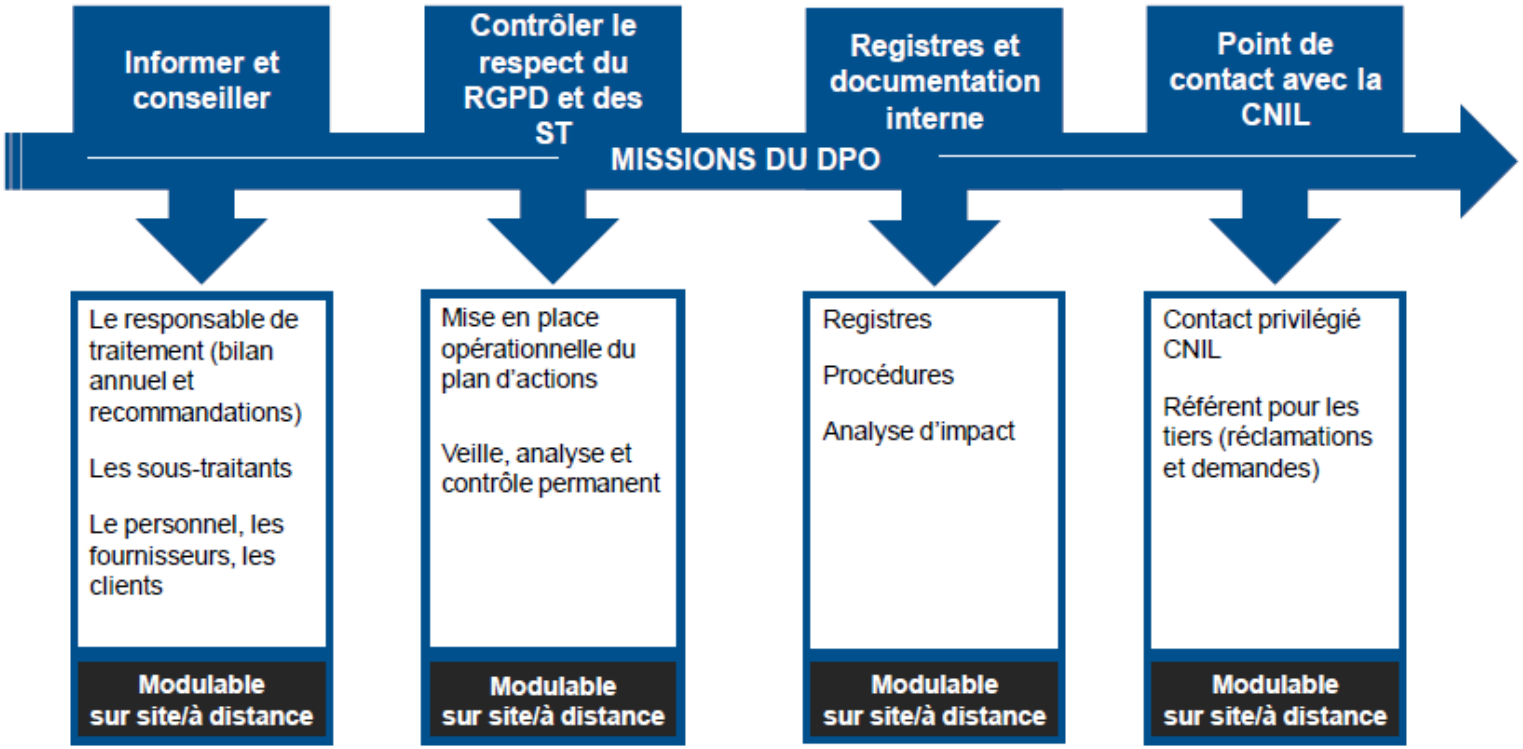
Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DATA

Détail MISSION d'ACCOMPAGNEMENT DPO EXTERNALISE: Temps à définir en fonction du Besoin



Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE

ACCOMPAGNEMENT PROPOSE PAR L'ADM74 EN PARTENARIAT AVEC COVATEAM ET OPTIMEX DATA

COVATEAM

OPTIMEX DATA

CONTACT Adm74 :

Lauriane MOUNIER-FARAUT - Directrice
lmounier@maires74.asso.fr
Tél: 04 50 51 47 05
Port. : 06 37 01 29 40

CONTACTS PARTENAIRES :

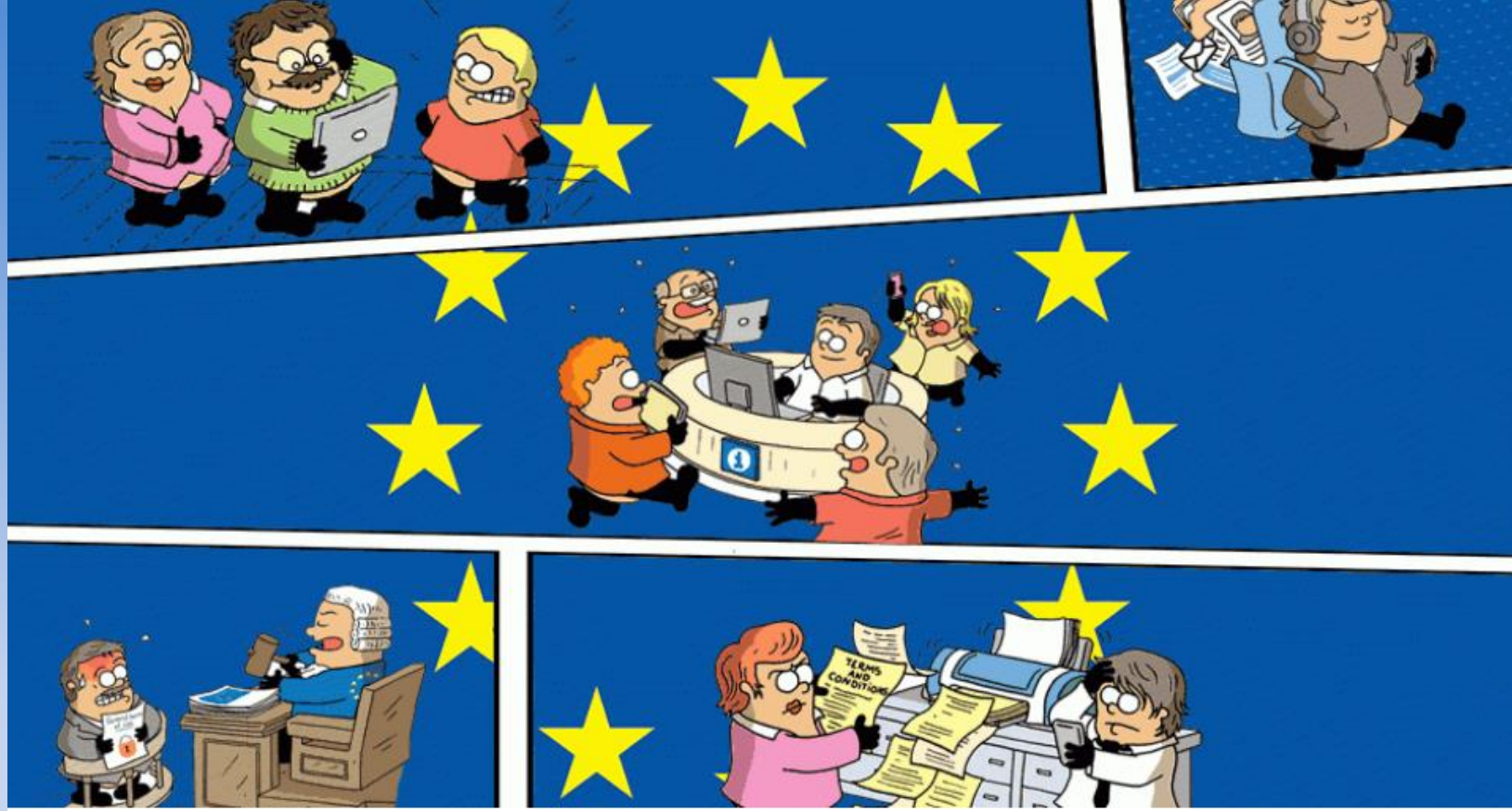
COVATEAM

Tél. : 04 58 00 30 33
Philippe Dujardin
E-mail : philippe.dujardin@covateam.com
Site Internet : www.covateam.com

OPTIMEX DATA

Tél. : 09 71 16 15 42
Sandrine Rieussec
E-mail : sandrine@optimex-data.fr
Site Internet : www.optimex-data.fr

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE



MERCI DE VOTRE ATTENTION

Adm74
ASSOCIATION DES MAIRES DE HAUTE-SAVOIE