FICHE MÉMO RGPD à destination des réseaux d'AMAP

Des clés pour mettre son réseau en conformité avec le Règlement Général sur la Protection des Données

Le RGPD (*Règlement Général sur la Protection des Données*) consacre et renforce les principes de la loi Informatique et Libertés en vigueur depuis 1978 et accroît sensiblement les droit des citoyen.nes en leur donnant plus de maîtrise sur leur données et de responsabiliser davantage les entités qui traitent des données personnelles.

Tout organisme qui traite les données personnelles doit veiller au respect des textes tout au long du cycle de vie de la donnée. Pour assurer la conformité à tout instant, il est nécessaire que chaque réseau d'AMAP se dote de nouveaux outils. **Voici quelques clés pour mieux comprendre le RGPD et passer à l'action.**

Qui doit l'appliquer?

Ce nouveau règlement s'applique ***à toute organisation, publique et privée,*** quels que soient sa taille, son pays d'implantation et son activité: entreprises, associations, CE/CSE, syndicats… dès lors qu'elles traitent des données à caractère personnel.

Le RGPD concerne aussi les *sous-traitants* qui traitent des données personnelles pour le compte d'autres organismes.
Ainsi, si vous traitez ou collectez des données pour le compte d'une autre entité (entreprise, collectivité, association), vous avez des obligations spécifiques pour garantir la protection des données qui vous sont confiées.
Également, si vous transmettez des données à une autre entité pour les traiter soyez vigilant que ceux ci garantissent la protection des données qu'on lui a confiées.

À partir de quand?

Le Règlement général sur la protection des données est entré en application depuis le ***25 Mai 2018.***
À partir de cette date, tout traitement en infraction avec le RGPD peut déboucher sur des sanctions.

Quel interlocuteur?

En France, la ***CNIL*** (Commission Nationale de l'Informatique et des Libertés) est l'autorité chargée d'informer, de contrôler et veiller au respect de ces informations individuelles et personnelles traitées.
Son but principal est de renforcer le droit des usagers.

Cette fiche MÉMO est le fruit de mutualisations entre les équipes de plusieurs réseaux d'AMAP : Réseau des AMAP Hauts-de-France / Réseau des AMAP Ile de France / Réseau des AMAP Auvergne Rhône-Alpes / Les AMAP de Provence et MIRAMAP. Merci au Réseau des AMAP Hauts-de-France pour avoir été moteur de ce chantier.

PRINCIPALES NOTIONS À RETENIR

Donnée personnelle

Toute ***information identifiant une personne physique*** identifiée ou identifiable directement ou indirectement.

Exemples de données que l'on peut trouver dans nos réseaux:

Nom, prénom, sexe, mail, n° téléphone, adresse postale, n° sécu, diplômes, données RH, mail pro, fonction, salaires, charges, transactions commerciales, géo localisation, quotient familial, fichiers de donateurs, fichiers de salarié.e.s, listes d'e-mail pour envois de lettres d'information, fichiers de contacts…

Données personnelles sensibles

Informations qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale. Ce sont également le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Le RGPD **interdit** de recueillir et d'utiliser ces données. Sauf dans certains cas précis explicités dans l'article 9[1]. → Selon nous, les réseaux d'AMAP ne traitent pas de données personnelles sensibles.

Traitement des données personnelles

Opération, ou ensemble d'***opérations, effectuées*** ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel.

Exemples : Collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, la limitation, la destruction.

→ Un traitement de données doit avoir ***un objectif***, une finalité, c'est-à-dire que vous ne pouvez pas collecter ou traiter des données personnelles simplement au cas où cela vous serait utile un jour. A chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de votre activité professionnelle.

Exemples de finalité : gestion des recrutements, gestion des adhérents, émission bulletin de paye…

Responsable de traitement

Personne, société ou organisme qui décide de la création du traitement et détermine les finalités et les moyens de celui-ci, c'est à dire l'objectif et la façon de le réaliser.

→ C'est à ce **responsable** qu'il appartient de mettre en œuvre toutes les mesures techniques et organisationnelles appropriées pour démontrer que le ou les traitements dont il a la responsabilité sont effectués en conformité avec le RGPD.

Exemples : Collecte des données personnelles d'un salarié pour établir son contrat de travail; Utilisation des données personnelles des adhérents pour les convoquer à l'assemblée générale annuelle; Adresser par mail aux adhérents une lettre d'informations.

Sous-traitant

Toute personne physique ou morale qui traite des données à caractère personnel pour le compte du responsable de traitement dans le cadre d'un service ou d'une prestation.

Exemples : Prestataire informatique, Cabinet d'expertise comptable, banque…

→Les sous-traitants ont des obligations spécifiques pour garantir la protection des données personnelles qui nous lui confions concernant les données.

[1] https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article9

I. Comment mettre en œuvre le RGPD dans votre réseau d'AMAP ?

La CNIL qui est en charge de faire respecter le RGPD en France propose un certains nombres de conseils pour une bonne application du RGPD. Nous proposons de les mettre en œuvre dans nos réseaux d'AMAP. **Voici les 5 principales étapes et explications pour s'organiser[2].**

Étape n°1. Identifier et mandater un/des responsable/s de traitement

Si nos réseaux n'ont pas forcément besoin d'un *délégué à la protection des données* (« DPO » Data Protection Officer) comme dans de grandes entreprises, les personnes en charge du traitement des données ou du respect du RGPD peuvent être des administrateur.trices, un groupe de travail, le bureau… La responsabilité juridique restant la personne morale représentée par son conseil d'administration et ses représentants légaux.
→ En pratique ! Nous invitons chaque conseil d'administration de réseau d'AMAP à mandater un.e /des administrateur.trices référent.es et constituer un groupe de travail pour lancer et suivre le processus de mise en conformité de votre réseau au RGPD.

Étape n°2. Créer un recueil des traitements des données personnelles

Le fait de créer ce recueil permet par la suite de l'utiliser comme preuve que nos associations respectent le RGPD. En cas de contrôle de la CNIL, il est important de pouvoir montrer ce recueil même s'il n'est pas complètement finalisé.
La CNIL propose ***des modèles de recueils simplifiés*** : https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement
→En pratique ! Avant de se lancer dans la rédaction concrète du recueil, nous conseillons de faire la liste des activités qui génèrent du traitement de données personnelles. Chaque activité aura sa propre fiche (avec les mentions conseillées par la CNIL). L'ensemble de ses fiches constitue votre recueil des traitements des données personnelles.

Étape n°3. Faire le tri dans les données personnelles utilisées

Données strictement nécessaires, conservation limitée dans le temps, recueillir le consentement des personnes.

- Le RGPD est clair sur une obligation : « Les données à caractère personnel doivent être […], adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) » (art5. c).
  → Vérifiez quelles données sont strictement nécessaires aux activités de nos associations (le reste on le supprime).
- La CNIL conseille de créer des règles d'archivage en interne afin de supprimer au fur et à mesure du temps les données personnelles recueillies.
- Autre élément fondamental : le traitement des données personnelles n'est autorisé que si « la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques; » (art6. a).

[2] + d'infos : https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf; https://lemouvementassociatif.org/wp-content/uploads/2018/07/FAQ-Associations-et-RGPD.pdf

Étape n°4. Respecter les droits des personnes

Pour respecter les droits des personnes, il faut :

- **Informer et communiquer aux personnes physiques** → Créez des mentions d'information sur le ou les documents qui permettent au réseau d'AMAP de collecter des données OU donner un premier niveau d'information qui renvoie à une « politique de confidentialité » de l'association.
- **Formaliser un droit d'accès aux données personnelles** → Mentionnez que la personne à un droit d'accès, de rectification, de suppression de ses données. Conseil : avoir une boîte mail pour cela.

Autre élément important : les salarié.es des réseaux et les administrateur.trices sont potentiellement amenés à « traiter des données personnelles » particulières.
→ Il nous semble important que chaque contrat de travail contienne une clause de confidentialité (on peut rédiger un avenant) et que les administrateurs signent un document dans lequel ils autorisent que leurs données personnelles soient utilisées et une clause de confidentialité.

Étape n°5. Sécuriser les données

Votre réseau doit *garantir l'intégrité de votre patrimoine de données en minimisant les risques de pertes de données ou de piratage*. → Pour cette phase là, nous pensons que c'est surtout à chaque réseau d'AMAP de trouver ses moyens pour sécuriser les données.
Exemple d'actions possibles : mises à jour de vos antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes …

II. Cas particulier : les sous-traitants

En tant que « responsable de traitement », nos réseaux d'AMAP doivent pouvoir démontrer que nos sous-traitants respectent le RGPD.
→ Concrètement, établissez la liste des sous-traitants puis vérifiez si les contrats qui vous lient font mention du RGPD. Sinon, demandez-leur d'ajouter une mention RGPD au contrat (exemples sur le site de la CNIL. De nombreux sous-traitants ont crée des clauses comme les experts comptables….).

Une boîte à outils en constitution à destination des réseaux et des AMAP

Le groupe de travail rassemblant des membres de différents réseaux d'AMAP œuvre à créer progressivement d'une boite à outils à destination des AMAP et des réseaux d'AMAP :

- Pour **les réseaux d'AMAP**: avec des outils complémentaires à cette fiche mémo (ex : retours d'expérience des démarches mises en place dans certains réseaux, mentions d'information à inclure dans les bulletins d'adhésion, exemple de politiques de confidentialité, clauses pour les sous-traitants …)
- Pour **outiller les AMAP dans les territoires** afin de les appuyer dans leur démarche de mise en conformité avec le RGPD.

Plus d'informations → contactez le MIRAMAP ou allez sur miramap.org et amapartage.fr