

FICHE MÉMO RGPD à destination des AMAP

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



De quoi parle-t-on ?

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

Tout organisme qui traite des 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 AMAP construise sa propre politique de confidentialité et se dote de nouveaux outils, notamment d'un registre des traitements des données personnelles.**

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, dès lors qu'elle traite des données à caractère personnel.

Le RGPD concerne aussi les partenaires qui traitent des données personnelles pour le compte d'autres organismes.

Ainsi, si vous transmettez des données à une autre entité pour les traiter (réseau régional d'AMAP par exemple), pensez à échanger avec elle sur sa politique de protection des données.

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 de veiller au respect de ces informations individuelles et personnelles traitées. Son but principal est de renforcer le droit des usagers.

► PRINCIPALES NOTIONS À RETENIR

Donnée personnelle

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

Exemples : nom, prénom, sexe, mail, téléphone, adresse postale, e-mail pour envois de lettres d'information, fichier de contacts...

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, limitation, destruction.

→ Un traitement de données doit avoir **un objectif**, une finalité, c'est-à-dire qu'**on ne peut pas collecter ou traiter des données personnelles simplement au cas où cela 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 l'activité.

Exemples de finalité : gestion des adhésions, envoi de lettres d'informations, envoi de contrats...

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 **démontrer que les traitements dont il a la responsabilité sont effectués en conformité avec le RGPD**.

Exemples : utilisation des données personnelles des adhérents pour les convoquer à l'assemblée générale annuelle, leur adresser par mail une lettre d'informations, leur envoyer les contrats.

Prestataire, partenaire, 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, banque...

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

I. Comment mettre en œuvre le RGPD dans votre groupe AMAP ?

La CNIL qui est en charge de faire respecter le RGPD en France propose un certain nombre de conseils pour une bonne application du RGPD. **Voici les 5 principales étapes et explications pour s'organiser**¹.

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

Les personnes en charge du traitement des données ou du respect du RGPD peuvent être un membre du conseil d'administration du groupe AMAP, un groupe de travail, le bureau...

→ **En pratique !** Nous invitons chaque groupe AMAP à mandater un.e /des administrateur.trices référent.es pour s'assurer du bon respect du RGPD en son sein.

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

Le fait de créer ce registre 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 registre.

La CNIL propose **des modèles de recueils simplifiés** (vous pouvez les trouver sur le [site de la CNIL](#) ; voir également la fiche pratique RGPD). Chaque activité qui génère du traitement de données personnelles aura sa propre fiche (avec les mentions conseillées par la CNIL). L'ensemble de ses fiches constitue votre registre des traitements des données personnelles.

→ **En pratique !** Avant de se lancer dans la rédaction concrète du registre, nous conseillons de faire la liste des activités qui génèrent du traitement de données personnelles : fichier Excel de gestion des adhérents, logiciel ou site internet permettant de gérer les listes d'adhérents, liste mails, envoi de lettres d'informations, etc.

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).

¹Plus 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>

- ▶ La CNIL conseille de créer des règles d'archivage 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).

Étape n°4. Respecter les droits des personnes

Pour respecter les droits des personnes, il faut :

- **Informé et communiquer aux personnes physiques** → Créez des mentions d'information sur le ou les documents qui permettent au groupe AMAP de collecter des données OU donnez 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 a un droit d'accès, de rectification, de suppression de ses données. Conseil : avoir une boîte mail pour cela.

Étape n°5. Sécuriser les données

Le groupe AMAP doit *garantir l'intégrité du patrimoine de données en minimisant les risques de pertes de données ou de piratage.* → C'est donc à chaque groupe AMAP de trouver les moyens pour sécuriser ses 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...

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 une boîte à outils à destination des AMAP et des réseaux d'AMAP :

- Pour **les réseaux d'AMAP** afin de les appuyer dans leur démarche de mise en conformité avec le RGPD.
- Pour **outiller les groupes AMAP** avec des outils complémentaires à cette fiche mémo : déjà disponibles ou à paraître : Fiche pratique (contenant des exemples de mentions d'information à inclure dans les bulletins d'adhésion, exemple de politiques de confidentialité, ...) ; fiche outil « Jeu pour se lancer » ; modèle de recueil...

Plus d'informations : miramap.org et amapartage.fr

Auteur.es :

Cette fiche mémo est le fruit d'échanges entre 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 / Réseaux des AMAP de Haute Normandie et MIRAMAP.

