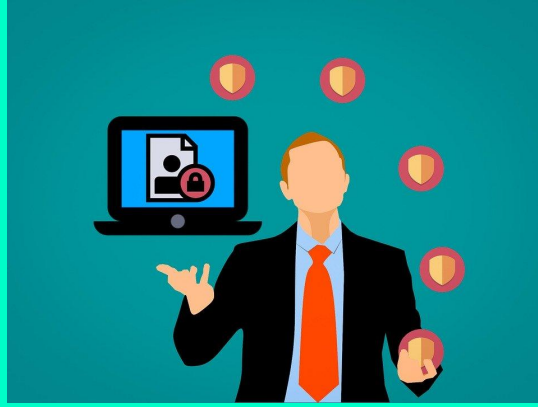
RGPD ET ASSOCIATION POUR WEBASSOC

Retour d'expérience de la mise en conformité du RGPD dans une association - MME HAMRA Rana Co-fondatrice Humanity Diaspo ONG

Définition et rôle du RGPD

- **Qu’est-ce que le RGPD?**
  Le RGPD signifie : «Règlement Général sur la Protection des Données»
- **A quoi sert le RGPD?**
  Le RGPD encadre le traitement des données personnelles sur le territoire de l’Union européenne.

Définition et rôle du RGPD



° A qui s’applique le RGPD et depuis quand?

Le RGPD s’applique depuis le 25 Mai 2018, à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :

- ❏ qu’elle est établie sur le territoire de l’Union européenne ;
- ❏ que son activité cible directement des résidents européens

Contexte Européen et données personnelles

DÉFINITION D'UNE DONNÉE PERSONNELLE

Une « donnée personnelle est: « toute information se rapportant à une personne physique identifiée ou identifiable »

CONTEXTE EUROPÉEN

L’UE a souhaité:

- **réglementer** l’utilisation des données des utilisateurs notamment à cause des abus des GAFAM **Google, Apple, Facebook, Amazon et Microsoft**
  - **uniformiser** une loi pour restaurer la confiance des utilisateurs
  - **garantir** le respect de la vie privée des utilisateurs

IDENTIFICATION DES PERSONNES ET DONNÉES

Une personne peut être identifiée:

- **directement:** nom, prénom
- **indirectement:** par un identifiant, un numéro de téléphone, une donnée biométrique,génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image

L'identification d'une personne physique peut être réalisée :

- **à partir d'une seule donnée** (exemple : numéro de sécurité sociale, ADN)
- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, et militant dans telle association).

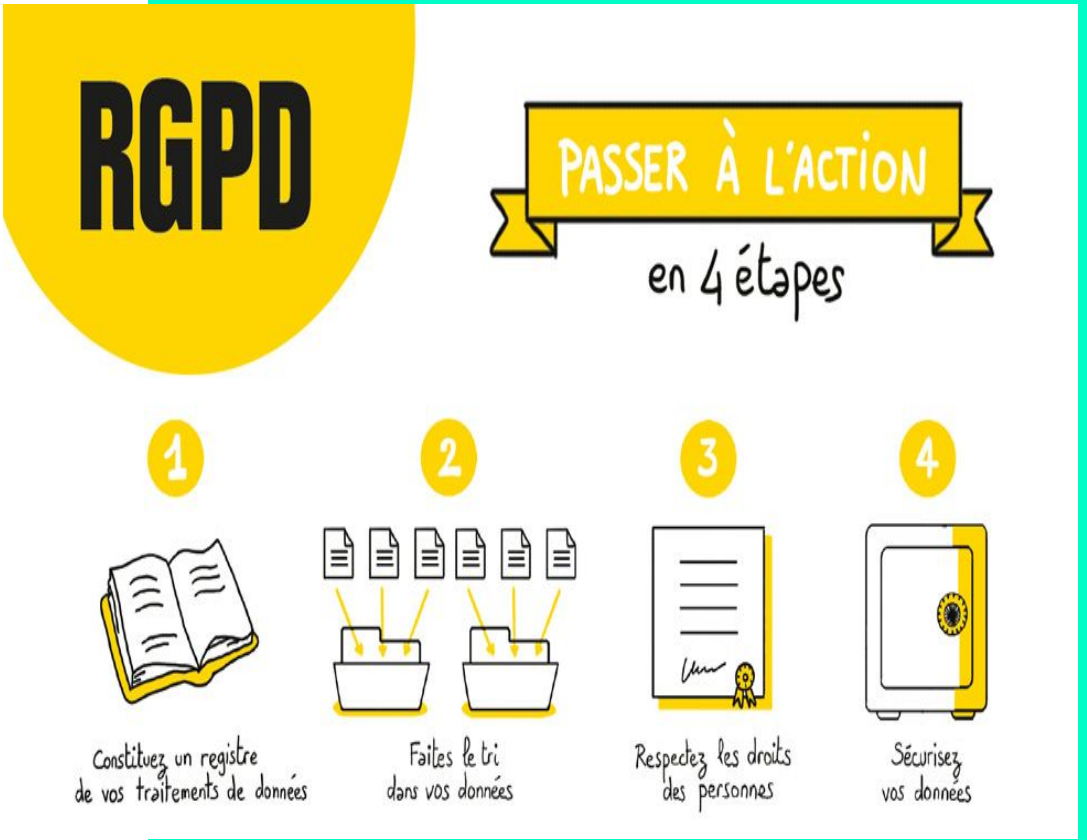
CNIL ET RGPD

CNIL - Commission Nationale de l'Informatique et des Libertés

- Elle est **chargée de veiller à la protection des données personnelles** contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés.
- Ainsi, elle est **chargée de veiller à ce que l'informatique soit au service du citoyen** et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.
- La CNIL est une **autorité administrative indépendante**, c'est-à-dire un organisme public qui agit au nom de l'Etat, sans être placé sous l'autorité du gouvernement ou d'un ministre.
- Elle a un rôle d'alerte, de conseil et d'information vers tous les publics **mais dispose également d'un pouvoir de contrôle et de sanction.**

LA CNIL VEILLE À FAIRE RESPECTER LA RGPD

en préconisant de suivre ces différentes étapes...



-Mise en pratique-
Bilan sur les data collectées

Commencer par faire le point sur comment et où vous collectez des données?

- la plupart du temps pour les associations il s'agira de collecter des informations concernant **leurs adhérents, leurs bénévoles, leurs donateur.rice.s**
- Ces **données pourront être physiques ou informatiques**
- Par le biais de **formulaire en ligne** par exemple sur votre site web pour devenir adhérent ou bénévole ou **bien sur une plateforme gérée par un sous-traitant** de type Hello asso si vous collectez des dons ou des adhésions en ligne

Mise en pratique et constitution du registre des traitements de données

Définir qui a accès à ces données dans votre structure?

- **L'équipe communication pour les newsletters,** les emailings etc…
- **Le service donateur** pour les campagnes de dons et relances etc…
- **Le responsable des bénévoles**, pour les formulaires en ligne pour inscription des bénévoles
- **Le service en charge des adhésions** etc…
- Le responsable des partenariats pour **les partenaires professionnels**
- **Un DPO a-t-il été nommé?**
- **Important:** les anciens membres du bureau ou salariés non plus à y avoir accès!

Mise en pratique

Pourquoi faire un tri?

- Le tri va **permettre de créer un processus: de sélection, gestion et utilisation des données.**
- Quelle activités ou actions dans ma structure génèrent de la captation de données?
- Dans quels cadres je les ai obtenues?
- Est-il nécessaire de les garder et dans quels buts?

Important: un bénévole ou adhérent qui n’est plus actif depuis des années ne doit plus figurer dans vos données!

Mise en pratique

Avez-vous obtenu le consentement des propriétaires de ces données?

Vous avez **le devoir d'informer vos adhérents, bénévoles, donateurs, bénéficiaires** du traitement que vous faites de leurs données:

- ❏ par les **droits d'accès et de rectification** des données dans vos mentions légales sur votres site web
- ❏ dans vos **newsletters** le lien de désinscription doit être affiché et accessible
- ❏ pour les cookies sur votre site web, les **utilisateurs doivent disposer d'une possibilité de choisir de ne pas être tracés** lorsqu'ils visitent votre site web

Important: Si votre base de données a été piratée les personnes et la CNIL doivent être informées dans les 72H

Mise en pratique

Les associations sont- elles à l'abris des cybers attaques, des piratages? Non!

- Prévoir un mécanisme de **verrouillage automatique de session**
- Installer un **« pare-feu »** (*« firewall »*) logiciel
- Utiliser des **antivirus régulièrement mis à jour** et prévoir une politique de **mise à jour régulière des logiciels**
- Configurer les logiciels pour que les **mises à jour de sécurité se fassent automatiquement** dès que cela est possible.
- **Favoriser le stockage des données des utilisateurs sur un espace de stockage** régulièrement sauvegardé accessible via le réseau de l'organisme

Important: La CNIL considère que ces précautions sont élémentaires

Sanctions :(

Les sanctions pénales

Les sanctions peuvent aller d'une amende jusqu'à une peine d'emprisonnement et les deux peuvent être cumulatifs.

Ex: Art. 226-21 CODE Pénal

Le **fait, par toute personne détentrice de données à caractère personnel** à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, **de détourner ces informations de leur finalité** telle que définie par la disposition législative,..., **est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.**

Rassurez-vous, les associations ne sont pas la cible des contrôles néanmoins rien ne les dispense de respecter la loi et la mise en conformité peut se faire au fur et à mesure.

Source: CNIL.FR