Le Règlement Général sur la Protection des Données

Le RGPD

SOMMAIRE

I) APPLICATION GENERALE

1) QU'EST-CE QUE LE RGPD ?

RGPD signifie Règlement général sur la protection des données. Ce règlement de l'Union Européenne de 2016 est applicable à tous les Etats membres de l'UE, depuis le 25 mai 2018.

Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne…).

Le but de ce règlement est d'unifier la protection des données pour les individus au sein de l'UE mais aussi de responsabiliser les acteurs qui traitent les données personnelles.

2) QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

Une donnée personnelle se définit par **toute information se rapportant à une personne physique identifiée ou identifiable**. Une personne peut être identifiée directement (nom/prénom) ou indirectement (exemple : numéro de téléphone).

Le traitement de données personnelles est une opération ou ensemble d'opérations portant sur les données personnelles, quel que soit le procédé utilisé : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement.

Le traitement de données doit avoir un objectif, une finalité. Il n'est pas possible de collecter des données simplement *« au cas où cela serait utile un jour »*.

3) QUI EST CONCERNÉ PAR LE RGPD ?

Tout organisme, peu importe sa taille, son pays d'implantation et son activité, peut être concerné. Le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles, pour son compte ou non, dès lors :

- Soit qu'elle est établie sur le territoire de l'UE
- Soit que son activité cible directement des résidents européens.

4) QUELS SONT LES CHANGEMENTS DUS AU RGPD ?

Comme dit précédemment, le RGPD a pour but d'unifier le cadre juridique de l'ensemble des Etats membres de l'UE. Le RGPD étant un règlement européen, il est applicable à l'ensemble de l'Union sans nécessiter de transposition dans les différents Etats membres.

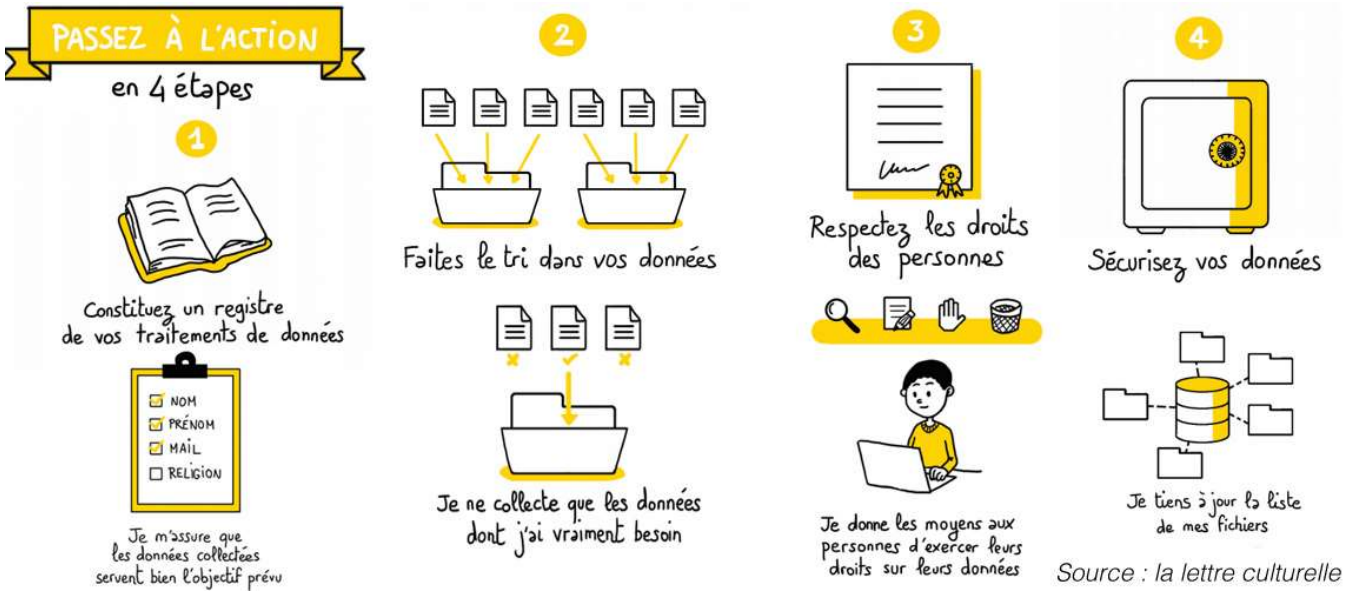
Ce règlement européen vise aussi à renforcer les droits des personnes et facilite l'exercice de ceux-ci notamment parce que l'expression du consentement est définie : les utilisateurs doivent être informés de l'usage de leurs données et doivent donner leur accord pour le traitement de leurs données ou pouvoir s'y opposer.

De nouveaux droits apparaissent dus au RGPD, notamment le droit à la portabilité des données. Ce droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable et le cas échéant de les transférer ensuite à un tiers. De plus, il existe un

droit à réparation des dommages matériels ou moraux ; cela signifie que toute personne, ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement, a le droit d'obtenir du responsable du traitement ou de son sous-traitant réparation du préjudice subi.

Le RPGD vise à responsabiliser les acteurs des traitements de données en uniformisant les obligations pesant sur les responsables de traitements et les sous-traitants.

Les acteurs de ce traitement de données ou sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement, les autorités de protection peuvent notamment : prononcer un avertissement, mettre en demeure l'entreprise, ordonner de satisfaire aux demandes d'exercice des droits des personnes.



Source : la lettre culturelle

II) APPLICATION POUR LES ASSOCIATIONS

1) EN TANT QU'ASSOCIATION ÊTES-VOUS CONCERNÉES ?

Oui, vous devez respecter le Règlement européen sur la protection des données applicable depuis le 25 mai 2018 si :

- **Vous collectez, stockez, utilisez des données à caractère personnel.** Dans ce cas, en tant qu'association, vous êtes « responsables de traitement. »
- **Vous traitez des données à caractère personnel pour le compte d'autres personnes morales.** Dans ce cas, vous êtes « sous-traitants ».

Pour être en norme vis-à-vis du RGPD, il faut que vous fassiez **une mise à jour de vos données** c'est-à-dire **trier les données que vous récoltez en repensant le cycle de vie des données au sein de votre association**.

Vous devez désormais vous demander :

- **Pourquoi collecter cette donnée ?**
- **En quoi celle-ci est-elle indispensable au bon fonctionnement de l'association ?**
- **Combien de temps avez-vous besoin de cette donnée ?**

2) LES OBLIGATIONS VIS-À-VIS DE LA CN!L

a) Tenir un registre de traitement de données

Ce registre des traitements des données est **un document relatant l'ensemble du détail de traitement des données au sein de votre association**.

Pour chaque traitement de donné, on doit retrouver plusieurs informations :

- Finalité du traitement
- Catégorie de données personnelles (nom, numéro, donnée de localisation, etc.)
- Objectifs poursuivis par ce traitement (enquête de satisfaction, gestion de recrutement, etc.)
- Les acteurs internes ou externes qui traitent ces données
- Les destinataires.

Pour chaque traitement, il s'agit de répondre aux questions :

Qui ?	Quoi ?	Où ?	Jusqu'à quand ?	Comment ?
Qui est responsable de la collecte des données ? Qui aura accès à vos données.	Préciser les données personnelles collectées exemple : nom, prénom et adresse	Où sont stockées les données ? Sur un Cloud ? En papier ? Sur un tableau Excel ?	Pour combien de temps les données sont-elles stockées ? Indiquez une date de fin.	Quelle est la méthode utilisée pour collecter les données ? Est-ce un Googleforms ? Un formulaire papier ?

b) Faire le tri dans les données

Le registre que vous allez faire va vous permettre de vous interroger sur les données dont votre association a réellement besoin et de supprimer les données inutiles. Moins de données collectées signifient moins de risques.

c) Respecter les droits des personnes

Il est désormais indispensable pour vous d'informer les personnes lors de toute collecte de données. **Le recueil du consentement doit être visible et explicite lors du recueil des données**. Vous devez notamment dire :

- Pourquoi vous collectez les données
- Ce qui vous autorise à collecter celles-ci
- Qui a accès aux données collectées
- Combien de temps vous allez stocker et conserver ces données.

Vous devez être capables de justifier votre récolte de données auprès des personnes désirant plus d'informations.

Vous devez aussi toujours permettre aux personnes d'exercer facilement leurs droits. N'oubliez pas que vos membres sont en droit d'accéder à toutes les données que vous conservez sur eux et qu'ils peuvent vous demandez de supprimer telle ou telle donnée.

Retrouver un exemple page 8 des mentions à indiquer lors d'une collecte de données.

d) Sécurisez vos données

En tant que détenteur de données personnelles, **vous êtes tenus d'assurer la sécurité de celles-ci. Instaurer des réflexes au sein de votre structure** est sans aucun doute le meilleur moyen d'assurer cette sécurité. Par exemple : changez votre mot de passe régulièrement, mettez à jour votre anti-virus.

Si vous êtes victime d'une violation de données personnelles, signalez-le à la CNIL dans les 72 heures suivant la fraude à cette adresse : https://www.cnil.fr/fr/plaintes

Si les risques sont importants, vous devez aussi informer les personnes concernées.

3) SE METTRE RAPIDEMENT AUX NORMES

a) Designer un pilote

La désignation d'un délégué à la protection des données (DPO) est obligatoire si vous êtes un organisme public ou une entreprise dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle ou à traiter à grande échelle des données dites « sensibles ou relatives à des condamnations pénales et infractions ».

En tant qu'association, vous n'êtes pas obligés de désigner un DPO, cependant il est fortement recommandé de désigner une personne disposant de relais internes, chargée de s'assurer de la mise en conformité au RPGD.

b) Inventorier et identifier les traitements de données

Pour cela, **réalisez une cartographie des données** grâce au registre des traitements de données. Cela sert à mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez. Vous trouverez un exemple en annexe page 9 à la fin de ce document.

c) Prioriser les actions à mener

Sur la base de votre registre, **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 libertés des personnes concernées.

d) Construire et mettre à jour certains documents pour prouver votre conformité au RGPD

De ce fait, vous pourrez anticiper un éventuel contrôle. **Cette documentation servira de preuve quant à la conformité de votre structure** aux différents principes et règles du RGPD.

4) LES SANCTIONS POSSIBLES

Le champ d'application du RGPD est virtuellement très large. A l'origine, le RGPD a surtout été mis en place pour encadrer les entreprises utilisant les données personnelles de leurs clients à des fins commerciales ou publicitaires.

L'intervention de l'autorité de contrôle est progressive en fonction de la gravité du manquement de l'entreprise à une des obligations découlant du RGPD. Les infractions sont sanctionnées graduellement et en fonction de leur gravité. Deux types de sanctions sont prévues : des **sanctions administratives et des sanctions pénales** qui peuvent être très lourdes : jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende.

Comme dit précédemment, les personnes concernées par les violations d'une disposition du RGPD peuvent demander le **versement de dommages et intérêts** du fait du préjudice subi.

De plus, l'image de l'entreprise due au non-respect du RGPD peut entrainer une perte de réputation de l'organisme.

Si le RGPD s'applique principalement pour les entreprises, **n'oubliez pas que vous êtes soumis à ce dernier et que vous pouvez faire l'objet d'un contrôle et être sanctionné en cas d'infraction**.

Exemple : L'Association pour le Développement des Foyers (ADEF) a dû le mois suivant l'application de la règlementation, payer une amende de 75 000 € à cause d'une faille de sécurité sur son site. Cette sanction exemplaire a notamment permis à la CNIL de renforcer le caractère dissuasif des amendes RGPD. **L'autorité administrative a démontré par la même occasion que cette nouvelle mesure concerne effectivement toutes les structures**.

5) LES BONS RÉFLEXES À ADOPTER

- **Ne collectez que les données vraiment nécessaires et pertinentes** pour votre association

- **Soyez transparent :** une information claire et complète constitue le socle de la confiance que vous lie avec les personnes dont vous traitez les données.

- **Pensez aux droits des personnes :** vous devez répondre dans les meilleurs délais aux demandes par rapport aux données.

- **Gardez la maîtrise des données :** le partage et la circulation des données personnelles doivent être encadrés et contractualisés afin de leur assurer une protection à tout moment

6) CE QUE VOUS DEVEZ FAIRE EN TANT QU'ASSOCIATION

En tant qu'association, **la conformité avec le RGPD consiste essentiellement à respecter les grandes lignes de la nouvelle réglementation, à travers le respect de la personne et l'amélioration de la sécurité des données**.

En cas de piratage ou de faille de sécurité majeure dans votre réseau, vous êtes tenus d'informer la ou les victimes et la CNIL sous 72h après la découverte du problème. ATTENTION : si l'anomalie non déclarée est constatée lors d'un contrôle, vous vous exposez à de lourdes sanctions.

Pour éviter un maximum les risques, il vaut mieux ne rassembler (et éventuellement ne stocker) que les informations pertinentes pour le projet en cours, par conséquent le traitement des donnés sera moins complexe.

Chaque citoyen a le droit de connaître la nature et la quantité de ses informations personnelles enregistrées sur une base de données. **Vous devez tout mettre en œuvre pour que l'utilisateur concerné puisse voir, récupérer ou effacer ses données collectées**.

Il est également indispensable de conserver toutes les pièces relatant le processus suivi par les données.

7) EXEMPLE DE MENTIONS À FAIRE APPARAITRE LORSQUE VOUS COLLECTEZ DES DONNÉES

Pour vous aider à informer les personnes dont vous traitez les données, voici un exemple de mentions de base à faire apparaître sur un formulaire de collecte de données.

L'année 2022 commence et nous avons décidé de mettre à jour notre fichier de liste d'adhérents. En effet, nous avons remarqué que quelques personnes n'avaient plus le même mail ou bien ne souhaitaient plus recevoir notre Newsletter. Merci donc de remplir ce formulaire afin que nous puissions mettre à jour notre base de données.

Données recueillies :

Les données suivantes sont recueillies avec votre accord : Nom, prénom, adresse mail, adresse postale, numéro de téléphone.

Finalités du traitement : ces données sont recueillies en vue de tenir à jour notre fichier d'adhérents et si vous le souhaitez (c'est-à-dire si vous avez coché la case l'acceptant), recevoir notre newsletter ; en aucun cas ces données ne seront cédées ou vendues à des tiers.

Responsable du traitement : Alain Daniel - alain.daniel@gmail.com

Destinataire des données : Alain Daniel, bénévole "communication" et Alice Dota, bénévole et présidente de l'association, ont accès à vos données dans le cadre de leurs missions respectives. Les membres du bureau ont accès à la liste des adhérents.

Droit d'accès et de rectification : vous pouvez, en vertu du Règlement européen sur la protection des données personnelles, en vigueur depuis le 25/05/2018, avoir accès aux données vous concernant ; vous pouvez demander leur rectification et leur suppression. Ces démarches s'effectuent auprès d'Alain Daniel, alain.daniel@gmail.com

Conservation des données : les données sont conservées jusqu'à un an après la fin de votre adhésion ou jusqu'à votre désabonnement à notre newsletter si cet abonnement se poursuit malgré votre non ré-adhésion.

Transmission des données à un tiers : Acceptez-vous que vos coordonnées soient transmises à notre partenaire, l'association « Cuisine du monde» ? (Merci de cocher la case oui ou non).

Acceptez-vous que vos données personnelles soient recueillies et conservées en vue de tenir à jour notre fichier adhérent ? (Merci de cocher la case oui ou non)

8) ANNEXE : RÉALISATION DE LA CARTOGRAPHIE DES DONNÉES