RÈGLEMENT RGPD

DES CLÉS
POUR LA MISE EN CONFORMITÉ

DANS CE DOCUMENT, VOUS TROUVEREZ :

- LES **INFORMATIONS ESSENTIELLES** SUR LE RÈGLEMENT
- LES **6 GRANDS PRINCIPES** QUI RÉGISSENT LE RÈGLEMENT
- UNE **FAQ**
- LES **10 RÈGLES** À METTRE EN PLACE POUR VOUS METTRE EN CONFORMITÉ
- **4 CHECKLIST** POUR PASSER À L'ACTION :

  √ CHECKLIST GÉNÉRALE : **RGPD ET ORGANISATION**

  √ CHECKLIST **COMMUNICATION EXTERNE**

  √ CHECKLIST **GESTION DE DONNÉES EN RELATION AVEC LES ACTIVITÉS DE L'ORGANISATION**

  √ CHECKLIST **SÉCURITÉ INFORMATIQUE**

Cercle de Coopération
des ONGD DU LUXEMBOURG

Suite à l'entrée en vigueur du règlement RGPD et aux réflexions menées conjointement avec ses membres, le Cercle de Coopération des ONGD est en mesure de vous proposer ce document **« RÈGLEMENT RGPD - DES CLÉS POUR LA MISE EN CONFORMITÉ »** comme outil de mise en pratique du règlement RGPD pour le secteur ONG.

Pour toute question liée à cette thématique, merci d'adresser votre demande à fx.dupret@cercle.lu

Réalisation : François-Xavier Dupret - fx.dupret@cercle.lu
Mise en forme : Camille Lassignardie - camille.lassignardie@cercle.lu

Publication : Octobre 2018

Cercle de Coopération des ONGD
1-7 rue Saint Ulric
L-2651 Luxembourg

cercle.lu

INTRODUCTION

LE RGPD, C'EST QUOI AU JUSTE ?

Le Règlement Général sur la Protection des Données (RGPD) est un règlement européen entré en vigueur le 25 mai 2018. Il s'attache à renforcer les droits des personnes physiques en référence au traitement de leurs données à caractère personnel. Afin de se conformer à ce règlement, toutes les associations qui traitent des données personnelles sont soumises à un certain nombre d'obligations.

QU'EST-CE QU'UNE DONNÉE À CARACTÈRE PERSONNEL ?

Toute information se rapportant à une personne physique identifiée ou identifiable : est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (article 4 RGPD).

Toutes les ONG récoltent, utilisent et conservent des données personnelles en relation avec les membres, les donateurs, le personnel de l'ONG, les bénévoles, les fournisseurs, ... Ces données peuvent être le nom, le prénom, le lieu de naissance, la date de naissance, l'adresse e-mail professionnelle ou personnelle,...

Certaines ONG conservent des données personnelles sensibles. Les données personnelles sensibles sont celles qui concernent la race, la religion, la santé, l'orientation sexuelle, les opinions politiques. Uniquement les personnes physiques sont visées par le règlement, sont donc exclues les données des organisations et généralement des personnes morales.

Le RGPD est applicable à toutes les associations : De ce fait toute association doit être en mesure de prouver qu'elle a mis en œuvre des mesures pour assurer la mise en conformité de son organisation au nouveau règlement.

OÙ TROUVER LES INFORMATIONS GENERALES ET UNE PRESENTATION RÈGLEMENT ?

La Commission Nationale pour la Protection des Données (CNPD) a préparé une page thématique pour les personnes qui désirent s'informer sur le RGPD.

La CNPD a publié également un guide pour le monde associatif. Assurez-vous de lire ce document et de le partager avec vos collègues et responsables de votre ONG.

LA MISE EN ŒUVRE DE LA RGPD AU LUXEMBOURG

La CNPD est responsable du contrôle de la mise en œuvre de la RGPD au Luxembourg.

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES
1, avenue du Rock'n'Roll
Tél. : (+352) 26 10 60 -1
Contact par email

QUELLES SONT VOS OBLIGATIONS ?

Théoriquement toutes les organisations et les entreprises devaient être en conformité à partir du 25 mai 2018. Dans les faits, beaucoup d'organisations et d'entreprises n'ont pas pu respecter ce délai.

En ce qui concerne le secteur associatif, la CNPD est consciente du défi de la mise en conformité et que cela ne peut pas être fait du jour au lendemain. Néanmoins, la mise en conformité doit être une priorité et toute organisation doit pouvoir démontrer qu'elle a un plan d'action pour se mettre en règle et que des procédures sont mises en œuvre afin d'être le plus vite possible en conformité avec le règlement.

LES 6 PRINCIPES

Afin de se mettre en conformité, votre ONG doit appliquer les 6 principes du RGPD :

LICÉITÉ, LOYAUTÉ ET TRANSPARENCE

Les organisations doivent s'assurer que leurs pratiques de collecte des données sont légitimes et qu'elles ne cachent rien aux personnes concernées. Afin de continuer à collecter les données en toute légitimité, vous vous devez d'avoir une bonne connaissance du RGPD et en particulier sur le consentement valide. Soyez respectueux des engagements que vous prenez envers avec les personnes concernées dans votre politique de confidentialité. Informez-vous bien sur le type de données collectées ainsi que les raisons pour lesquelles vous les collectez.

LIMITATION DES FINALITÉS

Les ONG ne doivent collecter les données personnelles qu'à des fins spécifiques qui doivent être précisées dans votre politique de confidentialité. Indiquez clairement quelles sont ces raisons et ne conservez ces données que pour la durée nécessaire au traitement.

MINIMISATION DES DONNÉES

Les ONG ne peuvent traiter les données personnelles que si cela est nécessaire aux finalités spécifiques pour lesquelles elles ont été collectées. Tachez de récolter le minimum d'information nécessaire.

EXACTITUDE DES DONNÉES

Le RGPD indique dans son règlement que « toutes les mesures raisonnables doivent être prises » afin de supprimer ou de modifier les données inexactes ou incomplètes. Les personnes concernées ont le droit de demander à ce que les données inexactes ou incomplètes soient effacées ou modifiées dans un délai de 30 jours.

LIMITATION DE LA CONSERVATION

Les organisations doivent supprimer les données personnelles lorsqu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées. Les données personnelles ne peuvent pas être conservées indéfiniment sans s'assurer d'un renouvellement du consentement de la personne intéressée.

INTÉGRITÉ ET CONFIDENTIALITÉ

Les données personnelles doivent « être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées ». Ce point concerne surtout les conditions de conservation des données personnelles et la sécurité informatique.

COMMENT GÉRER LES LISTES DE CONTACTS ET LES LISTES D'ENVOIS ?

Doit-on avoir un consentement positif « opt-in » pour tous nos envois de newsletter ou appels aux dons ?

◢ **Pour les listes de contact** que vous aviez avant l'entrée en vigueur de la RGPD : vous n'êtes pas obligé de demander un renouvellement du consentement positif mais vous devez vous assurer que les destinataires aient la possibilité de se désinscrire ou de contacter sans difficulté votre organisation pour effacer leurs données si elles le désirent.

◢ **Pour toutes les données collectées après le 25 mai 2018,** il est demandé un consentement positif à l'exception des courriers postaux toutes boites.

◢ Il est obligatoire de recueillir une autorisation explicite et transparente **pour vos envois vers vos donateurs ou membres**. Ce consentement doit être obtenu pour chaque type de traitement et l'utilisation finale des données récoltées, l'abonné doit avoir le choix. **Par exemple :** Un consentement est nécessaire pour l'envoi d'une newsletter, un second pour l'envoi de matériel pour une campagne de récolte de fonds, un troisième pour les invitations à des évènements.

Qu'entend-t-on par consentement positif ?

Le RGPD défini le consentement positif de la manière suivante. « Le consentement doit être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale »

Ce consentement doit pouvoir être retiré aussi simplement qu'il a été donné.

Il faut donc idéalement pour chaque contact :

- mettre en place un mécanisme de recueil du consentement « opt-in » et de rétractation « opt-out » ;
- préciser les principales caractéristiques du traitement (objet, finalité, durée, etc.) afin que la personne sache clairement à quoi elle consent ;
- démontrer avoir obtenu le consentement de la personne ;
- consigner et conserver la charge de la preuve du consentement dans le registre des activités de traitement (date, heure, etc.) ou en l'absence de ce dernier, tout autre support aisément consultable par l'autorité de contrôle me dispensant du consentement exprès.

COMMENT GÉRER LES DROITS À L'IMAGE ?

Le RGPD considère qu'une photographie d'une personne est une donnée à caractère personnel.

En règle générale avant de prendre une photo ou une vidéo d'une personne, vous devez lui demander son autorisation mais cela ne veut pas dire qu'elle consent à la publication ou à la diffusion de ces images. Il y a donc deux consentements distincts à prendre en compte de l'utilisation de son image.

La question du droit à l'image qui comprend le droit de publication et de prise de vue sont complexes. De nombreux facteurs interviennent pour analyser la légalité de la publication d'une photo sans consentement explicite.

Afin d'être certain de ne pas enfreindre les lois et règlements, il est préférable de prendre les mesures suivantes :

- Avertir les participants que vous allez prendre des photos pendant un événement et que vous allez éventuellement utiliser les photos.

- Recueillir le consentement des participants pour la prise de photo et la publication ultérieure. Pour ce faire vous pouvez une liste de présence avec une case à cocher qui autorise la publication de photos pour pouvoir prouver le consentement par la suite.

- Pour les photographies en milieu scolaire ou les photographies de mineurs, il faut le consentement des représentants légaux. Il faut donc prévoir un formulaire type qui sera signé par les représentants légaux. En milieu scolaire, il faut analyser avec l'établissement scolaire qu'elles sont les accords signés en relation avec le droit à l'image avec les représentants légaux lors d'activités organisées par des organisations tierces.

- Si vous n'avez pas de consentement explicite pour la publication ou si vous avez des doutes, il est préférable de flouter les visages des personnes qui peuvent être reconnues sur la photo.

Qu'en est-il des photos provenant des projets ?

En principe, d'un point de vue éthique, il faut appliquer les mêmes mesures avec la prise de photographie lors des visites sur le terrain. D'un point de vue légal, il convient également de se référer aux lois nationales en vigueur.

Afin de vous éclairer sur ce sujet vous pouvez vous référer aux documents publiés :

Le Règlement Général sur la Protection des Données : Le droit à l'image. (CNPD, 2018)

Fiche pratique relative à l'utilisation de photos ou vidéos en milieu scolaire. (CNPD, 2018)

Le guide illustré : Code de conduite en matière de message et images. (Dochas & Cercle de Coopération, 2017)

COMMENT GÉRER LES DONNÉES PERSONNELLES LIÉES À L'ADMINISTRATION DE L'ORGANISATION ET LA GESTION DU PERSONNEL ?

Pour la gestion quotidienne de l'organisation beaucoup de données sont collectées et traitées. Il peut s'agir de la gestion des cotisations des membres, de la gestion du personnel, des données concernant des fournisseurs ou des données personnelles enregistrées dans les logiciels de gestion financière. Les 6 principes de la RGPD s'appliquent également ici.

Les données liées au personnel

Concrètement, il faut tacher de traiter avec précaution les données liées au personnel surtout les données qui peuvent être sensibles comme les certificats pour les absences, les commentaires et évaluations.

La durée de garde des données relatives à un employé doit être limitée dans le temps. Les données doivent être détruites après le départ d'un employé. Certaines données peuvent être gardées jusque 3 ans pour des raisons administratives ou de gestion et certaines jusque 10 ans quand elles sont indispensables pour un audit financier ultérieur. Ici également le principe de minimisation ou d'anonymisation des données prévaut.

Au sein de l'organisation les données relatives au personnel doivent être sécurisées et les autorisations d'accès limitées au maximum. Les employés doivent pouvoir avoir accès à l'information les concernant.

Si des personnes vous envoient des CV lors de procédures d'embauche, il faut demander leur autorisation pour les garder. Sans autorisation préalable, il faut supprimer les CV de votre base de données.

Les données personnelles en relation avec le travail sur le terrain (données des bénéficiaires ou partenaires) tombent-elle sous le coup de la RGPD ?

Toute donnée qui est traitée sur le sol européen est soumise à la RGPD. Les ONG sont donc responsables de traiter de la même manière les données provenant des pays partenaires et les données collectée au Luxembourg.

Dans la mesure du possible, déléguez la gestion de ces informations à votre partenaire. Si vous avez besoin de cette information pour des rapports ou des comptes rendus vers les donateurs et les bailleurs de fonds, tachez de minimiser les données et de les anonymiser quand cela est possible.

Il est important également de sensibiliser votre partenaire sur la gestion des données personnelles et de vous assurer que les lois en vigueur dans leur pays soient respectées.

COMMENT S'ASSURER QUE LES SOUS-TRAITANTS RESPECTENT LE RGPD ?

Les ONG confient des fichiers contenant des données personnelles à des fournisseurs pour la prestation de certains services. Ce peut être une liste d'adresse pour un imprimeur qui envoie les documents, des fichiers envoyés à un auditeur, l'hébergeur de votre site internet, vos service de cloud ou des services de partage de fichiers. Il est de votre responsabilité de vous assurer que ces données seront gardées et traitées en conformité avec le RGPD pour cela les mesures suivantes sont à considérer :

- Choisir des sous-traitants de confiance
- Choisir des sous-traitants basés en Europe ou qui s'engagent à se soumettre au RGPD européen
- Faire signer une contrat avec le sous-traitant

Le RGPD impose que les relations entre responsable de traitement et sous-traitant de données soient strictement encadrées et formalisées dans un contrat écrit. Ce contrat doit contenir un certain nombre de mentions et de clauses obligatoires parmi lesquelles on compte une clause autorisant le responsable de traitement à auditer la manière avec laquelle le sous-traitant traite les données pour son compte ou encore une clause organisant l'accès du personnel du sous-traitant aux données.

Voici le lien vers un contrat-type

COMMENT ASSURER LA SÉCURITÉ DES DONNÉES PERSONNELLES ?

La sécurité des données personnelles se réfère principalement à la manière dont sont sécurisés vos bases de données au sein de votre réseau informatique et vos ordinateurs.

Pour plus d'information vous pouvez vous rérérer au document de la CNIL, France. Ce document contient une procédure en 17 étapes pour améliorer la sécurité informatique dans votre organisation.

La checklist «Sécurité informatique» se base sur ce document.

QUE FAIRE EN CAS DE VIOLATION DE DONNÉES ?

Si vous pensez que votre site ou votre base de données a été piratée ou si vous avez perdu un ordinateur, vous devez notifier à la CNPD dans les 72 heures qui suivent le moment du constat. Si l'attaque ou la perte est susceptible d'entrainer un risque pour les droits et les libertés des personnes présentes dans la base de données vous devez également les avertir.

Pour en savoir plus sur la violation des donnés

Accès aux formulaires de notification de violation de données de la CNPD

10 RÈGLES POUR LA MISE EN CONFORMITÉ RGPD

10. INFORMER LA CNPD EN CAS DE PERTE OU DE VIOLATION DE DONNÉES

1. FAIRE UN INVENTAIRE
de tous les traitements et des données traitées ainsi que de leurs objectifs.
Besoin d'aide ? Cliquez ici.

2. FAIRE RÉGULIÈREMENT LE MÉNAGE DANS LES BASES DE DONNÉES EXISTANTES
et supprimer les entrées et les informations qui ne sont plus nécessaires ou que la loi vous interdit de garder. Prévoir dans votre calendrier une fonction de rappel périodique.

3. RÉDIGER UNE POLITIQUE DE CONFIDENTIALITÉ ET DE PROTECTION DE LA VIE PRIVÉE POUR VOTRE ORGANISATION
Cliquez ici pour voir l'exemple proposé par le responsable RGPD de la Caritas.

4. RÉDIGER UN MANUEL DE PROCÉDURES POUR ASSURER LA CONFORMITÉ DE VOTRE ORGANISATION À LA RGPD
Besoin de pistes ? Cliquez ici.

5. TRAITER LES DONNÉES ENREGISTRÉES DE MANIÈRE LOYALE ET TRANSPARENTE
conformément à la politique de confidentialité de votre organisation.

6. INFORMER CLAIREMENT LES PERSONNES CONCERNÉES PAR LES DONNÉES
et leur donner la possibilité de se désinscrire ou de modifier leurs données.

7. PRÊTER ATTENTION AU DROIT À L'IMAGE.

8. DÉSIGNER UNE PERSONNE RESPONSABLE
de la protection des données et de la vie privée en interne pour l'organisation.

9. RÉALISER UN DIAGNOSTIC DE LA SÉCURITÉ INFORMATIQUE
de l'organisation et prendre les mesures nécessaires.

Cercle de Coopération des ONGD du Luxembourg

CHECKLIST GÉNÉRALE « RGPD ET ORGANISATION »

	Mesures mises en place	Périodicité / Reste à faire	Commentaires
1. Notre organisation dispose d'une politique de confidentialité Voir le modèle			
2. Nous avons désigné un responsable de la protection des données			
3. Notre organisation dispose d'un registre de traitement des données Voir le modèle			
4. Notre organisation dispose d'un manuel de procédure interne pour la protection des données Document de référence			
5. Notre organisation s'assure de la sécurité des données Voir checklist «Sécurité informatique»			
6. Nous veillons à ce que les sous-traitants respectent le RGPD Voir la FAQ			
7. Le personnel de notre organisation connait et respecte les procédures de mise en conformité au RGPD			

CHECKLIST « COMMUNICATION EXTERNE » 1/2

	Mesures mises en place	Périodicité / Reste à faire	Commentaires
1. Mise en conformité des bases de données			
Les bases de données de contact et des membres ont été analysées, l'information actualisée et si nécessaire les contacts ont été supprimés			
L'information contenue dans la base de donnée a été minimisée			
L'information contenue dans la base de donnée est vérifiée et actualisée régulièrement			
2. Mise en conformité des procédures de collecte de données			
Lors des événements publics, des formulaires de manifestation d'intérêt avec un mécanisme de recueil de consentement sont disponibles			
Tous nos envois vers l'extérieur contiennent l'information nécessaire pour se désinscrire			
Tous nos envois contiennent une adresse de contact en relation avec le traitement des données personnelles			
Tous les envois, contiennent un lien vers la politique de confidentialité de notre organisation			
Nous veillons au droit à l'image lors de l'utilisation des photos pour nos publications et site web Voir la FAQ			

CHECKLIST « COMMUNICATION EXTERNE » 2/2

	Mesures mises en place	Périodicité / Reste à faire	Commentaires
3. Mise en conformité du site web			
Une page en lien avec la politique de confidentialité est facilement accessible pour le visiteur			
La collecte de données pour la newsletter contient l'information sur le traitement des données et un lien vers la politique de confidentialité et une personne de contact			
Les formulaires pour la récolte de données ont été adaptés			
Les photos ou information concernant des personnes sont publiées avec le consentement valide des personnes			
Les utilisateurs du site ont la possibilité d'accepter ou de refuser la pose des cookies?			
Les utilisateurs sont conscients de l'utilisation de cookies et de la collecte de données qui est effectuée			
La demande de consentement pour le traitement des cookies est renouvellée tous les 13 mois			

CHECKLIST « GESTION DE DONNÉES EN RELATION AVEC LES ACTIVITÉS DE L'ORGANISATION

	Mesures mises en place	Périodicité / Reste à faire	Commentaires
1. Gestion des données du personnel			
L'information concernant les employés est supprimée le plus tôt possible après le départ des employés			
2. Information des pays partenaires			
Nous avons inclus l'information concernant les données personnelles provenant des projets dans notre registre des données			
Nous supprimons les informations lorsque les projets sont clôturés			
Nous déléguons au maximum le traitement des données des projets à nos partenaires			
Nous veillons à ce que nos partenaires respectent les règlements nationaux des pays concernant la protection des données			
Nos partenaires sont sensibilisés à la protection des données personnelles			

CHECKLIST « SÉCURITÉ INFORMATIQUE »

EN VOUS BASANT SUR LE DOCUMENT « LA SÉCURITÉ DES DONNÉES PERSONNELLES » DE LA CNIL VOUS POUVEZ METTRE EN PLACE LES MESURES DE SÉCURITÉ POUR PRÉSERVER LES DONNÉES PERSONNELLES EN VOTRE POSSESSION.

	Mesures mises en place	Périodicité / Reste à faire	Commentaires
1. Sensibilisation des membres de votre organisation			
2. Authentification des utilisateurs			
3. Gestion des droits d'accès			
4. Tracer les accès et gérer les incidents liés à des accès non autorisés			
5. Sécurisation des postes de travail			
6. Sécurisation de l'informatique mobile			
7. Protection du réseau informatique interne			
8. Sécurisation des serveurs			
9. Sécurisation des sites web			
10. Sauvegarde et continuation de l'activité			
11. Archivage de manière sécurisée			
12. Encadrer la maintenance et la destruction des données			
13. Gérer la sous traitance			
14. Sécuriser les échange avec d'autres organisations			
15. Protéger les locaux			
16. Encadrer les développements informatiques			