Focus Thématique
GOUVERNANCE

Thématique
RGPD
(Règlement Général de Protection des Données)

Bonnes Pratiques de référence
3-31-32

Version de Novembre 2019

SOMMAIRE

De quoi parle-t-on ?

Ce réglement encadre le traitement des données personnelles sur le territoire de l'Union Européenne. Il est conçu pour renforcer les droits des personnes en matière de protection des données tout en rendant la législation sur la sécurité des données uniforme dans toute l'Union Européenne.

Le RGPD est-il applicable à une association ?

Cette réglementation s'applique à tous les acteurs économiques et sociaux ayant des activités de traitement ou de manipulation de données à caractère personnel concernant directement des citoyens européens. *On entend par traitement, toute activité de collecte, lecture, modification, stockage, etc., informatisée ou non*. Les entreprises sont bien évidemment concernées, mais également les associations, administrations, ou toutes autres entités collectant des données personnelles. I**l n'y a pas d'exemption pour les associations !**

Quelles sont les données considérées comme personnelles ?

Les « données à caractère personnel » sont définies comme toute information se rapportant à 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.

Attention, certaines données sont considérées comme **sensibles**, il s'agit en particulier de :

- l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale,
- les données concernant la santé ou l'orientation sexuelle,
- les données génétiques ou biométriques,
- les données d'infraction ou de condamnation pénale,

Dans le cas, le consentement explicite de la personne est obligatoire.

En tant qu'association, vous collectez et conservez une quantité importante de données personnelles. Des données bancaires aux données démographiques de vos contacts, les données personnelles sont au cœur de votre activité quotidienne, culturelle ou sociale. Ainsi, pour votre association, lorsque l'on parle de données personnelles, on inclut donc les informations sur vos membres, vos bénévoles, donateurs, employés, partenaires, et même vos contacts via votre site web.

Quels sont les principes fondamentaux de gestion des données personnelles ?

1. Le principe applicable aux données (Article 5 du règlement)

Les données à caractère personnel doivent être :
a) **traitées de manière licite, loyale et transparente** au regard de la personne concernée
b) **collectées pour des finalités déterminées, explicites et légitimes**, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;
c) **adéquates, pertinentes et limitées à ce qui est nécessaire** au regard des finalités pour lesquelles elles sont traitées ;

d) **exactes et, si nécessaire, tenues à jour** ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;
e) **conservées sous une forme permettant l'identification** des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
f) **traitées de façon à garantir une sécurité** appropriée des données à caractère personnel.

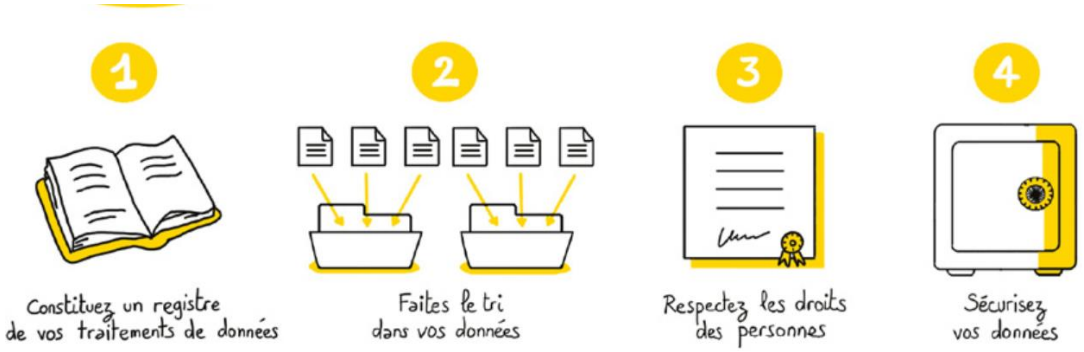
2. Le principe applicable aux traitements (Article 6 du règlement)

Le traitement n'est licite que si au moins une des conditions suivantes est remplie :
a) la personne concernée a **consenti au traitement** de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
b) le traitement est **nécessaire à l'exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
c) le traitement est **nécessaire au respect d'une obligation légale** à laquelle le responsable du traitement est soumis ;
d) le traitement est **nécessaire à la sauvegarde des intérêts vitaux de la personne** concernée ou d'une autre personne physique ;
e) le traitement est **nécessaire à l'exécution d'une mission d'intérêt public** ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
f) le traitement est **nécessaire aux fins des intérêts légitimes** poursuivis par le responsable du traitement ou par un tiers.

En pratique le consentement doit être :
● **librement donné** - la personne concernée doit disposer d'une véritable liberté de choix et être en mesure de refuser ou de retirer librement son consentement sans subir de préjudice ;
● **spécifique** - le traitement qu'ils acceptent doit être clair - quel marketing vont-ils recevoir ? De qui viendra-t-il ? Demander à quelqu'un d'accepter que ses coordonnées soient partagées avec des « tiers soigneusement sélectionnés » n'est pas suffisamment spécifique;
● **éclairé / informé** - si la personne ne comprend pas correctement comment ses données vont être utilisées, le consentement n'est pas valide. Vous devez préciser ce qu'ils acceptent, dans un langage qu'ils comprennent ;
● **univoque** - le consentement ne doit pas être détourné pour une autre utilisation.

Comment procéder ?

Nous vous conseillons de vous rendre sur le site de la CNIL qui propose une démarche très bien documentée en 4 étapes pour mettre en place un processus de traitement des données personnelles conforme au règlement européen.



Les droits des personnes concernées

Le RGPD donne aux personnes concernées plusieurs droits que vous devrez respecter.

Droit à l'information (Art 13 et 14)

En tant que *fundraiser*, si vous collectez des données auprès d'une personne physique (après un don par exemple), vous devrez lui communiquer la/les finalités du traitement et les droits dont elle dispose. Plus précisément quelles données collectées, leur durée de conservation, transmises à qui, et comment exercer ses droits d'accès et rectification. Il est important que la politique de confidentialité de votre association et celle relative à la protection des données soient facilement accessibles et mises à jour. Mettez un lien vers ces informations à chaque fois que des données sont recueillies, à partir de formulaires d'inscription en ligne ou de don en ligne par exemple.

Droit d'accès

Droit d'accès (Art 15) : la personne concernée a le droit d'obtenir de votre association la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès aux dites données à caractère personnel ainsi que certaines informations (telles que les finalités du traitement ; les catégories de données à caractère personnel concernées ; les destinataires auxquels les données à caractère personnel ont été ou seront communiquées, etc.). Formez vos volontaires à ce que ce genre de demandes soient considérées comme urgentes. Répondez dans un délai raisonnable et garder tout trace de communication.

Droit de rectification

Droit de rectification (Art 16) : la personne concernée a le droit d'obtenir, dans les meilleurs délais, que les données inexactes soient rectifiées, et que les données incomplètes soient complétées.

Droit à l'effacement

Droit à l'effacement (Art 17) : la personne concernée a le droit d'obtenir, dans les meilleurs délais, l'effacement de ses données, lorsqu'elle a retiré son consentement au traitement, lorsqu'elle s'y oppose, lorsque les données ne sont plus nécessaires au regard des finalités du traitement, lorsqu'elles ont fait l'objet d'un traitement illicite, ou lorsqu'elles doivent être effacées en vertu d'une obligation légale, sauf dans certains cas. Si votre association a rendu publiques les données, vous devrez informer les autres responsables du traitement qui les traitent qu'il faille effacer ces données ainsi que toutes reproductions de celles-ci

Droit à la limitation du traitement

Droit à la limitation du traitement (Art 18) : la personne concernée a le droit d'obtenir la limitation du traitement lorsqu'elle s'y est opposée, lorsqu'elle conteste l'exactitude des données, lorsque leur traitement est illicite, ou lorsqu'elle en a besoin pour la constatation, l'exercice ou la défense de ses droits en justice.

Droit à la portabilité

Droit à la portabilité (Art 20) : lorsque le traitement est fondé sur le consentement ou sur un contrat, et effectué à l'aide de procédés automatisés, la personne concernée a le droit de recevoir les données dans un format structuré, couramment utilisé, lisible par machine et interopérable, et de les transmettre à un autre responsable du traitement sans que le responsable du traitement initial y fasse obstacle.

Droit d'opposition

Droit d'opposition (Art 21) : la personne concernée a le droit de s'opposer à tout moment au traitement des données, lorsque celui-ci est nécessaire à l'exécution d'une mission d'intérêt public ou aux fins des intérêts légitimes du responsable du traitement. Elle peut également s'opposer au traitement fait à des fins de prospection. Votre *newsletter* doit par exemple permettre de se désinscrire.

Quand faut-il notifier ? hypothèse où une violation n'aura pas à être notifiée ?

Le règlement prévoit qu'en cas de violation, vous devrez notifier celle-ci à la CNIL dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance de la violation. Attention, si vous dépassez le délai de 72 heures, votre notification devra être accompagnée des motifs du retard.

Cependant, la violation n'a pas à être notifiée si celle-ci n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Votre notification doit comporter les éléments décrits ci-dessous. S'il vous est impossible de fournir toutes les informations en même temps, ces informations peuvent être communiquées de manière échelonnée.
a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
c) décrire les conséquences probables de la violation de données à caractère personnel ;
d) décrire les mesures prises, ou que le responsable du traitement propose de prendre, pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Le profilage est-il autorisé par le RGPD ?

Le RGPD n'impose pas d'interdiction généralisée sur le profilage et la prise de décision automatisée. Le RGPD indique ainsi qu'un traitement de ce type doit être assorti de garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée (donc il faut informer les donateurs de ce profilage) ainsi que le droit d'obtenir une intervention humaine (article 22), d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision.

Mon association est-elle obligée de tenir un registre des activités de traitement ?

Cette obligation ne s'applique qu'aux organismes de 250 employés et plus. Il est cependant conseillé de le mettre en place pour des raisons de clarté et de bonne gestion. Il est aussi important de tenir ce registre dans le cas d'organismes qui effectuent des traitements sur des données sensibles.

Pour aller dans le détail …

Vous trouverez toutes les informations utiles sur le site de la CNIL. En particulier :
https://www.cnil.fr/fr/comprendre-le-rgpd
https://www.cnil.fr/fr/rgpd-passer-a-laction
https://www.cnil.fr/fr/les-outils-de-la-conformite
https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles
https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence

Vous pouvez aussi prendre connaissance du guide conçu par 'France Générosité'
http://www.francegenerosites.org/memento-rgpd-decembre-2018/

LES BONNES PRATIQUES DE REFERENCE

Bonne Pratique 3 : L'entité établit une cartographie de ses parties prenantes internes et externes (bénévoles, personnes en mécénat de compétences, salariés, adhérents, donateurs et prospects, bénéficiaires, financeurs, …), en veillant à la protection des données à caractère personnel conformément à la règlementation en vigueur.

Bonne Pratique 31 : L'entité élabore collaborativement et met à jour la liste des principaux risques auxquels elle est confrontée à court et moyen terme. Elle en évalue la criticité en termes d'impact et de probabilité. Lorsqu'aucun changement n'est intervenu, la mise à jour est effectuée au minimum tous les 3 ans.

Bonne Pratique 32 : L'entité met en œuvre les plans d'actions, les procédures internes et les contrôles aptes à prévenir les principaux risques identifiés et à en réduire leurs impacts.