GUIDE PRATIQUE
Les associations et le Règlement Général sur la Protection des Données (RGDP ou GDPR)

Sophie Gioanni
VerticalSoft

Janvier 2018

ATTENTION : RESPONSABILITÉ DE L'ÉDITEUR

L'éditeur met à disposition des lecteurs un contenu informatif gratuit et s'assure en permanence de mettre les moyens à sa disposition pour s'assurer de la qualité du contenu. Ce document traite de l'environnement légal et réglementaire. Nous avons vérifié nos sources et citons d'une manière générale les textes du règlement sur lesquels nous nous appuyons. **Toutefois, il est de la responsabilité des lecteurs de s'assurer que les textes et régimes mentionnés dans les articles sont toujours bien en vigueur.**

Par ailleurs, aucune information dans ce document ne peut être considérée par les lecteurs comme un conseil, une consultation ou une recommandation. L'auteur n'étant pas habilité à fournir des consultations juridiques. Les lecteurs s'engagent donc à utiliser ces informations sous leur entière responsabilité et ne pourront pas tenir pour responsable l'éditeur du document de toute utilisation des informations fournies.

1- Introduction

L'objectif de ce document est de sensibiliser l'ensemble des salariés ou volontaires de votre association à la thématique de la protection des données personnelles. La protection des données est un sujet très important ; d'autant plus que Le GDPR (G*eneral Data Protection Regulation*), ou RGPD (Réglementation Générale sur la Protection des Données), est entré en vigueur le 25 mai 2016 et sera applicable à partir du 25 mai 2018. Ce nouveau règlement européen s'appliquera à toute entité qui collecte, traite et stocke des données personnelles dont l'utilisation peut directement ou indirectement identifier une personne, et donc s'appliquera aux associations et fondations.

La Réglementation Générale sur la Protection des Données est une nouvelle problématique pour tous les salariés et volontaires, et plus particulièrement pour ceux en charge de la levée des fonds, de par l'impact de cette réglementation pour l'association en cas de non respect.

La réglementation sur la protection des données présente certaines conditions qui permettent l'utilisation de données personnelles. Si vous souhaitez récolter et traiter des données sensibles comme celles relatives à la santé ou la sexualité, vous devrez remplir un ensemble de conditions supplémentaires. Vous devrez définir ce que vous faites des données personnelles que vous collectez, pourquoi vous êtes dans l'obligation de les collecter et, surtout, informer les personnes concernées de ce que vous faites avec leurs données et de leurs droits.

La protection des données n'est pas complexe mais elle requiert une certaine discipline de la part des associations et notamment des personnes dans le domaine du *fundraising*. De ce fait, cette réglementation n'est pas populaire dans cette discipline car elle freine sans doute certaines activités. Cependant, la non-conformité n'est pas une option ; la raison étant que les organismes qui ne respectent pas ces nouvelles obligations pourraient faire face à des pénalités et des amendes sévères. De plus, une perte de réputation serait désastreuse pour toute entité charitable.

2- Points clés à retenir

Si vous n'avez pas le temps de lire ce guide, voici les points clés à retenir :

Le GDPR est-il applicable à une association ?

L'objectif principal de cette nouvelle réglementation reste similaire à ce qui est actuellement en place : le GDPR est conçu pour renforcer les droits des consommateurs en matière de protection des données tout en rendant la législation sur la sécurité des données uniforme dans toute l'Union Européenne. Dès lors, cette nouvelle 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. Les entreprises sont bien évidemment concernées, mais également les associations, administrations, ou toutes autres entités collectant des données personnelles. Rappelez-vous : **il 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. 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, volontaires, donateurs, employés, partenaires, et même vos contacts via votre site web.

En quoi le GDPR diffère-t-il des réglementations existantes ?

Nous mentionnerons les quatre différences les plus importantes pour votre association entre l'ancienne et la nouvelle régulation :

1- Une portée géographique plus large : le GDPR étend la portée des lois sur la protection des données. À partir de mai 2018, si vous collectez des données auprès de ressortissants de l'Union Européenne, même si votre organisation est située en dehors de l'Union Européenne, cette réglementation s'appliquera à vous.

2- Sanctions : selon la nouvelle réglementation, l'amende maximale pour non-conformité peut atteindre 4 % du chiffre d'affaires global (ou 20 millions d'euros – le chiffre le plus élevé).

3- Consentement du consommateur : les organisations traitant des données personnelles doivent être claires et directes quant à la raison pour laquelle elles veulent collecter ces données. De plus, le règlement précise que ces traitements ne sont licites que si la personne concernée a donné son consentement de façon claire, indubitable et démontrable *a posteriori*. Enfin, les organisations doivent faire en sorte que les consommateurs puissent retirer leur consentement. Les obligations du GDPR supposent donc qu'une organisation doit à tout moment savoir de quelles données elle dispose, leur localisation, l'objectif de leur collecte et leur mode de gestion, stockage, sécurisation, transfert et effacement.

4- Obligation de signaler les violations de données : selon les termes de la nouvelle réglementation, les organisations seront tenues de signaler les violations de données à leurs autorités de surveillance dans les 72 heures suivant la découverte d'une violation. Donc, en

tant qu'association, vous devez être en mesure de déceler si l'intégrité de vos données a été compromise et y remédier promptement, tout en consignant et notifiant l'événement.

Le GDPR s'applique-t-il à mon association ou mon club sportif basé en France ?

Oui. Votre association est basée en France et collecte des données de ressortissants de l'Union Européenne.

Que dois-je faire en tant qu'association pour devenir conforme au GDPR ?

Premièrement, il est important de commencer dès maintenant. Vous devrez vous assurer que votre système actuel et que les procédures de contrôle existantes répondent aux exigences du GDPR. Effectuez un état des lieux des données collectées par votre association, de leur traitement, et des moyens de contrôle en place. Déterminez également les zones de risques vis-à-vis des exigences du GDPR.

Quelles actions concrètes mon association doit-elle prendre ?

- Si vous possédez un système existant, vérifiez que votre fournisseur actuel maîtrise GDPR et ses implications.
- Si vous pensez acheter un nouveau système, assurez-vous que le fournisseur est alerté de cette réglementation.
- Déterminez quelles sont les données personnelles que vous devez collecter. La nouvelle réglementation impose de ne collecter sur informatique que les données qui sont strictement nécessaires à vos objectifs. Évitez de collecter des données peu nécessaires et sensibles telles que données de santé, données relatives aux origines raciales ou ethniques.
- Décidez comment vous formulerez vos mentions légales et votre politique de confidentialité pour vous assurer qu'elles adhèrent à la nouvelle réglementation. Celles-ci devront comporter un certain nombre d'informations (identité de l'organisation, mention des droits des personnes au regard de leurs données, etc.).
- Assurez-vous de l'obtention du consentement explicite de vos utilisateurs et qu'ils comprennent pourquoi ces données sont collectées. Ce consentement pourra être retiré à tout moment par les individus le demandant. Ddonc, vous devrez pouvoir modifier ou effacer ces données si cela vous est demandé. Attention, vous devrez être en mesure de prouver le recueil de ce consentement le cas échéant (en cas de contrôle de la CNIL).
- Évaluez la sécurité de vos données et identifiez les améliorations nécessaires pour assurer la conformité aux nouvelles réglementations. N'oubliez pas qu'il y a de lourdes pénalités si vous ne respectez pas les nouvelles directives.

Que dois-je dire à mon *fundraiser* ?

1) Si un donateur ou une personne dont vous collectez les données personnelles ne comprend pas ce que vous faites avec celles-ci, la conséquence est que vous ne pouvez pas le faire. La même chose est vraie pour le consentement : si une personne ne comprend pas ce que vous faites, vous ne pouvez pas prétendre qu'elle y a consenti.

2) Vous ne pouvez pas assumer le consentement ; celui-ci doit être explicite. Le défaut de retrait n'est pas un consentement. Le silence n'est pas un consentement. Une case pré-cochée n'est pas un consentement. Il existe des règles spécifiques pour le consentement sur la méthode de communication de collecte de fonds et d'autres communications de marketing direct.

3) Le consentement n'est pas toujours nécessaire mais il reste le moyen le plus sûr pour votre association pour légitimer l'utilisation des données.

5) Attention, les bénévoles ne sont pas différents des employés et doivent être formés et équipés pour protéger les données. Il n'y a pas d'exemption de bénévolat.

6) Si vous faites sous-traiter vos données par une agence ou une société, vous êtes entièrement responsable de ce qu'ils font.

7) Les données personnelles disponibles dans le domaine public sont toujours des données personnelles et la protection des données s'applique toujours.

8) Les excuses suivantes ne vous sortiront pas d'affaire en cas de problème avec la CNIL :
• nous avons toujours travaillé de cette façon ;
• tout le monde le fait ;
• nous perdrons des donateurs si nous changeons notre façon de faire.

Ci-dessous, vous trouverez plus de détails sur les concepts du GDPR.

3- Le périmètre d’application du GDPR

Les règles et obligations du GDPR s’appliquent au traitement – automatisé ou non – des données à caractère personnel. Définissons chacun de ces éléments.

Définition des données à caractère personnel

La définition des données à caractère personnel est trouvée dans l'article 4 : il s’agit de toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; 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.

Les données personnelles sont donc des données concernant une personne physique identifiée ou identifiable (une personne physique est un individu plutôt qu'une personne morale comme une entreprise). L'information doit vous permettre d'identifier la personne, seule ou en combinaison avec d'autres informations disponibles. Si vous savez qui est la personne ou si elle peut déterminer qui elle est, le règlement s'applique à ce que vous faites et vous devrez vous conformer au GDPR. Par contre, si l'information est véritablement anonyme, c'est-à-dire que vous ne savez pas qui est l’individu, le règlement ne s'applique pas à ce que vous faites.

Qu’en est-il des données déjà dans le domaine public ?

Beaucoup de données personnelles sont dans le domaine public, telles que l'adresse ou le numéro de téléphone. Dans cette hypothèse, le règlement est-il applicable? la réponse est oui. En effet, le but de la réglementation sur la protection des données est de réguler et de contrôler la façon dont les données personnelles sont utilisées, plutôt que de seulement se préoccuper de leur sécurité. Certes, la sécurité de ces données est un élément puissant de la législation, mais ce n'est pas le seul. Les données du domaine public ne sont donc pas exemptées du GDPR. Si vous diffusez ou traitez des données personnelles qui sont déjà dans le domaine public, assurez-vous que la finalité du traitement que vous effectuez est compatible avec la finalité initiale du traitement effectué par la source publique.

Qu’en est-il des données sensibles ?

Le GDPR définit certaines informations comme des données sensibles : il s’agit d’informations concernant l’origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l’appartenance syndicale, la santé ou la vie sexuelle. Par principe, la collecte et le traitement de ces données sont interdits. Cependant, dans la mesure où la finalité du traitement l’exige (attention vous ne pourrez collecter ces données que si celles-ci sont absolument nécessaires à votre association), ne sont pas soumis à

cette interdiction :

- les traitements pour lesquels la personne concernée a donné son consentement exprès ;
- les traitements justifiés par un intérêt public après autorisation de la CNIL ou décret en Conseil d'État.

La collecte et le traitement de ces données doivent, dans ces hypothèses, être justifiés au cas par cas au regard des objectifs recherchés. Consultez un spécialiste sur ce point en cas de doute.

Ci-dessous une liste d'autres données à risque :

- données génétiques ;
- données relatives aux infractions pénales, aux condamnations, etc. ;
- données comportant des appréciations sur les difficultés sociales des personnes ;
- données biométriques ;
- données comprenant le numéro d'inscription des personnes (NIR) au répertoire national d'identification des personnes physiques (RNIPP), appelé encore numéro INSEE ou tout simplement numéro de sécurité sociale.

Qu'en est-il des données de santé?

Cette étude ne touchera pas à la question du traitement des données de santé car elle concerne très peu des associations avec lesquelles nous avons travaillé. Nous vous invitons à contacter la CNIL ou un conseiller pour plus de détails.

Définition du traitement

Selon l'article 4 du GDPR, le traitement se définit comme toute opération ou tout 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 telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Un traitement est donc présent, et vous êtes donc soumis au GDPR si vous procédez à une gestion de vos salariés ou de vos bénévoles ou de vos membres. Plus particulièrement dans le domaine du *fundraising*, la gestion de vos donateurs va entraîner l'application du GDPR. De même en est-il de l'utilisation de tout outil de fidélisation et de prospection (envoyer votre *newsletter* par exemple). Le fait que votre traitement soit manuel parce que vous n'avez pas de système informatique n'est pas une excuse. Ce traitement est soumis aux dispositions du règlement si ces données sont contenues ou appelées à figurer dans un fichier.

Certains traitements sont toutefois exclus de l'application du règlement. Aucune de ces exceptions ne concernent les associations mais elles sont énumérées ci-dessous :

- les traitements mis en œuvre dans le cadre d'une activité strictement personnelle ou

domestique, et donc sans lien avec une activité professionnelle ou commerciale. Les données de votre téléphone portable par exemple.

- les traitements mis en œuvre par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exaction de sanctions pénales.

- les traitements effectués dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union européenne, par exemple en matière de sécurité nationale.

- les traitements mis en œuvre par les États membres dans le cadre de leurs activités ayant trait à la politique étrangère et de sécurité commune de l'Union.

Définition du responsable de traitement

Le GDPR s'applique et donc prévoit des obligations à la charge des organismes responsables de traitement. Le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. Le fait que votre association sous-traite le traitement des données à un tiers ne vous exonère pas de votre responsabilité.

Mon association doit-elle être située en France ?

Le règlement s'applique aux traitements de données mis en œuvre dans le cadre de l'activité d'une association située sur le territoire de l'Union européenne, que l'entité en question dispose de la qualité de responsable de traitement ou de sous-traitant, et que le traitement ait lieu ou non dans l'Union européenne.

Attention, si votre association n'est pas établie dans l'Union européenne, alors le GDPR s'appliquera tout de même si les personnes dont les données sont traitées se trouvent sur le territoire d'un État membre de l'Union européenne et si le traitement est lié :

- soit à une offre de biens ou de services à destination desdites personnes concernées ;
- soit au suivi du comportement de ces personnes dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union européenne.

Les principes à respecter en matière de traitement des données à caractère personnel

Une fois établi que le GDPR est applicable à votre entité, quels sont les principes préalables applicables en matière de traitement des données à caractère personnel ?

Les 2 principes sont énumérés aux article 5 et 6 du règlement :
- le premier principe applicable aux données ;
- le deuxième principe applicable aux traitements.

Le premier 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.

Que doit faire mon association ?

Pour respecter ce premier principe, il vous faudra tenir une documentation interne complète, un registre plus précisément, sur les données personnelles, leurs traitements, et s'assurer que ces traitements respectent bien les nouvelles obligations légales. Votre association devra donc réaliser un état des lieux (autrement dit un audit). Dans ce registre, devront notamment être mentionnés :

- le nom et les coordonnées du responsable de traitement ;
- les différents traitements de données personnelles ;
- les catégories de données personnelles traitées ;
- les différentes catégories de personnes concernées ;
- les objectifs poursuivis par les opérations de traitements de données ;
- les acteurs (internes ou externes) qui traitent ces données (identification des sous-traitants éventuels) ;
- les flux de données en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne ;
- les durées de conservation ;
- la description générale des mesures de sécurité techniques et organisationnelles.

À partir de ce registre (voir plus loin pour les cas où le registre est obligatoire plutôt que conseillé), il sera plus aisé pour le responsable de traitement d'identifier les actions à mener en priorité pour mettre en conformité un traitement de données personnelles.

La définition des objectifs du traitement

Si vous ne pouvez pas décrire le but et la raison de la collecte de données, il vous sera

impossible de répondre aux questions clés telles que : quelles sont les données nécessaires (et celles superflues), combien de temps doit-on conserver ces données. Tout dépend du but pour lequel vous traitez les données.

Ces objectifs doivent être spécifiés, explicites et légitimes. Encore une fois, vous devez exposer clairement et sans ambigüité vos objectifs, et vous ne pouvez pas simplement dire « à fins de collecte de fonds », alors que cela pourrait couvrir une grande variété d'utilisations de données. La tâche consistant à identifier clairement vos objectifs dès le départ est l'une des choses les plus importantes à faire, et vous devez définir les « buts de la collecte de fonds » en détails.

Attention, si vous souhaitez utiliser les données dans un deuxième but, vous aurez besoin d'un argument convaincant que ce que vous faites n'est pas en conflit avec l'objectif initial. Si on peut dire qu'il est incompatible avec le but initial, vous êtes en contravention avec le règlement et ne pourrez pas utiliser les données.

Vos objectifs peuvent prendre les formes suivantes :

a) nous voulons maintenir une liste de personnes qui nous ont déjà fait un don afin que nous puissions les contacter pour leur demander de le faire à nouveau ;
b) nous voulons maintenir une liste de personnes qui nous ont explicitement dit qu'elles ne veulent plus nous contacter ;
c) nous voulons utiliser (a) pour rechercher la situation financière des donateurs en utilisant des sources publiques pour déterminer quel type de communication leur faire parvenir ;
d) nous voulons utiliser (a) pour faire des recherches sur les antécédents financiers du donateur, et nous voulons payer une entreprise pour faire la recherche pour nous ;
e) nous voulons acheter des données d'un tiers pour nous assurer que (b) est à jour ;
f) nous voulons acheter des données d'un tiers pour créer une liste de personnes qui ne font pas partie de notre liste de donateurs actuels, afin que nous puissions les contacter et leur demander de faire un don pour la première fois.

Le deuxième principe applicable aux traitements

Article 6 du règlement

1. 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.

Les conditions du traitement

Ce deuxième principe vous force à analyser si le traitement est légal. Il y a donc six conditions pour justifier le traitement des données à caractère personnel, figurant dans l'article 6 du GDPR. Vous devez satisfaire l'un d'eux. Attention, si vous ne pouvez pas justifier l'une de ces conditions, vous êtes en violation du règlement.

La plupart des ces conditions ne s'appliqueront pas à la levée des fonds dans les associations.

- **Contrats** - il est peu probable qu'il y ait une sorte de contrat entre votre association et un donateur / donateur potentiel. Attention, si un prospect a payé pour un événement sponsorisé par votre association, vous ne serez pas en mesure de faire du marketing juste parce que la personne a acheté ce billet.
- **Obligation légale** - non applicable aux associations.
- **Les intérêts vitaux** - non applicable aux associations (il s'agit des situations de vie ou de mort).
- **Fonctions officielles / administration de la justice / intérêt public** - non applicable aux associations (s'applique à l'administration de la justice).
- **L'intérêt légitime** - l'intérêt légitime du responsable de traitement à mettre en œuvre le traitement prévaut-il sur l'intérêt de la personne concernée à ce que ses données ne soient pas traitées dans le cadre dudit traitement ? C'est un argument difficile à prouver. Dans le contexte de la levée des fonds, peut-on faire l'évaluation de la situation financière d'une personne concernée, son âge, sa propension à donner ? Ceci n'est probablement pas nécessaire pour administrer un don, certainement pas pour justifier une demande de nouveau don.

Le consentement

Le consentement est défini à l'article 7 du règlement. Le consentement de la personne concernée est défini comme toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement. Attention, si le consentement est le fondement de votre traitement, alors votre association devra être en mesure de prouver que la personne concernée a effectivement consenti à l'opération de traitement.

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.

Le consentement et le *opt-in/opt-out* ?

Attention, vous ne pouvez pas assumer le consentement. Beaucoup d'organisations utilisent des cases pré-cochées (et si la personne oublie de cocher, elle est supposée avoir consenti). Cela n'est pas autorisé par le GDPR. Nous conseillons plutôt de faire apparaître une case à cocher pour mettre la question hors de doute.

Donc a ne pas faire :
• décochez cette case (case pré-cochée) ;
• cochez cette case si vous ne souhaitez pas recevoir de marketing (en particulier si le marketing est courriel ou texte) ;
• texte STOP
• en nous donnant vos coordonnées pour [chose sans rapport], vous acceptez de recevoir des courriels.

Le consentement peut-il être implicite?

Non, le consentement doit être explicite. Si un donateur a acheté un billet de tombola ou a fait un don, il n'y a aucune implication du consentement pour le marketing, la collecte de fonds supplémentaire ou quoi que ce soit d'autre. Le consentement nécessite une acceptation positive.

Combien de temps dure le consentement?

Il semble qu'il n'y ait pas de limite de temps pour le consentement, mais il peut être raisonnable de revoir et actualiser le consentement, s'il y a lieu. La vraie limite de la durée du consentement est ce que vous dites à la personne concernée lors de la collecte. Si vous donnez à l'individu l'impression qu'il consent pour une campagne à durée limitée, son consentement prend fin lorsque la campagne est terminée. Si vous persuadez la personne d'opter pour une relation à long terme, le consentement dure une période de temps potentiellement plus longue. Le facteur crucial est la possibilité de se désinscrire (voir plus loin).

Comment obtenir les consentements explicites ?

1- Rédigez un texte de demande de consentement. Le texte doit être clair et facilement compréhensible pour tout le monde.

Par exemple :

« En faisant ce don (en remplissant ce formulaire, etc.), vous acceptez que Association XYZ mémorise et utilise vos données personnelles collectées dans ce formulaire dans le but d'améliorer votre expérience et vos interactions avec elle. En l'occurrence, vous autorisez

Association XYZ à communiquer occasionnellement avec vous si elle le juge nécessaire afin de vous apporter des informations complémentaires sur ses projets et appels à dons via les coordonnées collectées dans le formulaire.

Afin de protéger la confidentialité de vos données personnelles, Association XYZ s'engage à ne pas divulguer, ne pas transmettre, ni partager vos données personnelles avec d'autres entités, entreprises ou organismes, quels qu'ils soient, conformément au Règlement Général de Protection des Données de 2018 sur la protection des données personnelles et à notre politique de protection des données »

2- Demandez clairement et activement le consentement sur vos formulaires.
Ajoutez une case vide que l'utilisateur devra cocher afin de démontrer qu'il a donné son consentement explicite.

3- Si possible, ajoutez un mécanisme de « double *opt-in* » afin de pouvoir prouver le consentement explicite de vos contacts.
Le « double *Opt-in* » consiste à demander une confirmation par courriel à chaque personne concernée qui a rempli un formulaire sur votre site web. Afin de valider leur consentement, ils devront alors cliquer sur un lien dans le courriel de confirmation.

Que se passe-t-il si vous n'avez pas de preuve historique du consentement ?

Nous parlons ici du cas où une personne est dans votre base de données mais vous ne pouvez pas être certain qu'elle a opté pour le marketing ou l'appel à dons ? Pouvez-vous la contacter par courriel pour lui demander si elle consent toujours à recevoir du marketing ? **Ce point n'est pas clair**. Il est possible d'envoyer un seul et unique courriel aux personnes dont vous avez légitimement obtenu les données en disant : « Nous pensons avoir reçu votre consentement pour vous envoyer du marketing (de nouveaux appels à dons, etc.), pouvez-vous nous confirmer que nous avons raison ? Cependant, certains pays, comme le Royaume-Uni, considèrent que d'envoyer un courriel pour demander le consentement à recevoir du marketing est en lui-même un courriel de marketing, et donc interdit.

Le problème du profilage et de la recherche dans le *fundraising*

Il est très courant pour les associations de faire des recherches sur des personnes qui, par exemple, ont déjà fait un don. L'idée étant qu'une fois ces donateurs sélectionnés et classifiés, il est possible de créer des campagnes d'appel à dons plus ciblées et donc plus efficaces. Ce profilage est-il autorisé par le Règlement Européen sur la Protection des Données (RGPD ou GDPR) ?

Qu'est-ce que le *profiling* ou le profilage ?

Le RGDP ou GDPR définit à l'article 4 le profilage comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la

situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique».

Le profilage, ou *profiling* en anglais, est très courant surtout dans les pays anglo-saxons. Il est généralement utilisé par des sociétés qui analysent le « profil de consommation » de chaque client ou prospect, avant de décider d'une stratégie de marketing. Grâce à ce profilage, la société est à même d'adapter sa communication et donc de bâtir la meilleure offre commerciale.

Le problème du profilage et de la recherche dans le *fundraising*

Le profilage a rapidement été adopté par les associations cherchant à établir une image plus complète de leurs donateurs, elles aussi, pour rendre leur communication et donc leurs appels à dons plus efficaces.

Le profilage est-il autorisé par le RGDP ou GDPR ?

Il est important de souligner que 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 concernée ?

Potentiellement oui. Cela dépend des pratiques de *fundraising* de votre association. Pour une clarification des pratiques autorisées, il est intéressant de regarder la situation au Royaume-Uni ou l'association *British Heart Foundation* s'est vue infliger une amende de 18 000 GBP pour avoir enfreint la loi sur la protection des données. L'association avait ciblé de nouveaux donneurs pour ses campagnes d'appel à dons en rassemblant des renseignements personnels obtenus de sources publiques et en échangeant des renseignements personnels avec d'autres associations afin de créer une base de données de donateurs. Le régulateur anglais a déclaré que les donateurs n'étaient pas informés de ces pratiques et étaient donc incapables de donner leur consentement (ou d'objecter).

Le régulateur anglais, appelé l' Office of the Information Commissioner(OIC) affirme dans son blog qu'il reconnaît que le profilage peut être « un outil puissant pour les organismes caritatifs et peut bénéficier aux individus, à l'économie et à la société en général ». Cependant, l'OIC souligne le fait que le profilage peut aussi parfois avoir « des effets significatifs et préjudiciables sur les personnes ».

Que doit faire mon *fundraiser* ?

L'OIC a récemment publié un document sur le profilage qui peut être utilisé aussi pour les associations (nous n'avons pas trouvé un tel document pour la CNIL, mais l'avis d'un autre régulateur soumis au RGPD peut être intéressant). Le point essentiel pour les associations et les *fundraisers* est d'examiner **quelle sera leur base juridique pour le traitement dans**

le contexte du profilage, et documenter cela conformément aux exigences du RGPD.

En tant que *fundraiser*, vous pouvez vous baser sur **le consentement** comme fondement juridique du profilage de vos donateurs. Rappelez-vous que ce consentement doit être donné librement, qu'il doit être spécifique, renseigné et sans ambiguïté. Donc, vos mentions légales et votre politique de confidentialité doit être claire sur le profilage.

D'autres bases légales que votre association peut utiliser pour le profilage incluent le traitement étant :

- nécessaire à l'exécution d'un contrat ; ou
- nécessaires aux fins des intérêts légitimes poursuivis par votre association.

Cependant, vous devrez être en mesure de démontrer que le profilage est nécessaire pour atteindre cet objectif plutôt que simplement utile. Il sera bien plus difficile de prouver que le profilage est nécessaire (car en réalité il est plutôt utile pour vous), et il est probablement sage de se baser sur le consentement des donateurs et donc de leur information.

Il est intéressant de noter que l' « *Institute of Fundraising* », a publié sur son site Web une réponse à cette étude, et indique que la grande majorité des associations utilisent des données publiques pour effectuer le profilage afin d'identifier de nouveaux donateurs potentiels et pour s'assurer que leurs communications avec les donateurs existants sont adaptées. Selon l'IoF, cela implique une intervention humaine plutôt que des « processus automatisés », du GDPR, et donc devrait bénéficier d'un traitement différent.

Que doit faire mon association ?

Vos mentions légales sur la confidentialité des données doit contenir des références claires sur les points suivants :

• partage de données avec une autre organisation (que les données soient vendues ou échangées gratuitement) ;
• recherche, indépendamment du fait que les données proviennent du domaine public ou d'une source accessible au public. Par recherche, on entend essayer de trouver des informations sur la situation financière d'une personne, ses biens, ses dons antérieurs ou sa propension à donner ;
• tout autre profilage, recherche ou sélection, qui peut inclure l'âge, les intérêts, la santé, ou des évaluations éthiques ou similaires ;
• acquérir des données de tiers - cela inclut les détails des donateurs potentiels, l'acquisition de données pour étayer les dossiers de donneurs existants ou potentiels.

Doit-on tenir un registre des traitements ?

L'une des nouvelles obligations phares du règlement est la tenue d'un registre des activités de traitement (art. 30 GDPR). Cette obligation s'applique-t-elle aux associations?

Qu'est ce qu'un registre ?

Un registre n'est autre qu'un fichier qui comporte toutes les informations importantes pour

prouver le respect du GDPR. Ainsi, ce dernier comporte (voir Article 30 pour plus de détails : nous présentons ici un résumé de cet article) :
a) le nom et les coordonnées du responsable du traitement ;
b) les finalités du traitement ;
c) une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées ;
e) les délais prévus pour l'effacement des différentes catégories de données ;
f) une description générale des mesures de sécurité techniques et organisationnelles. Et toute information en ce qui concerne les sous-traitants.

A qui s'applique l'obligation de tenir un registre des activités de traitement ?

Cette obligation ne s'applique qu'aux organismes de 250 employés et plus.

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

Probablement pas, mais attention, le fait que vous ayez moins 250 salariés ne signifie pas forcément une totale exonération. En effet, les organismes qui effectuent des traitements sensibles de façon non occasionnelle ou qui concernent certaines catégories de personnes ou des données relatives à des condamnations pénales et à des infractions doivent aussi se plier à l'exercice. Probablement, votre association n'est donc pas concernée. Mais elle peut, si elle le désire et pour des raisons de clarté, tenir ce registre.

Exemple de registre de la CNIL

Tenir un tel registre peut vous permettre de cartographier vos données et de vous assurer que vous êtes en conformité avec le règlement. Vous pouvez cliquer sur le modele-de-registre-GDPR ou le télécharger directement du site de la CNIL.

Données personnelles sensibles (catégories spéciales GDPR)

Une complication supplémentaire survient si vous utilisez des données personnelles définies comme sensibles ou spéciales. Les catégories de données sensibles sont l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou d'autres croyances de même nature, l'appartenance à un syndicat, la santé ou la condition physique ou mentale ; la vie sexuelle, la commission ou la prétendue commission par la personne concernée de toute infraction ; ou toute procédure pour une infraction en cours. Si vous souhaitez utiliser des données sensibles dans le cadre de votre campagne de levée de fonds, vous devrez respecter les conditions supplémentaires à l'article 9 du GDPR.

Mon association peut elle « acheter » une liste de donateurs ?

Oui mais il y a un risque. Une société qui partage ou vend des données est un traiteur de données, et vous en devenez le traiteur une fois que vous les achetez. Vous ne pouvez pas invoquer l'innocence ou l'ignorance s'il s'avère que les données ont été volées ou que le fournisseur a déformé les objectifs pour lesquels il a été obtenu. Même si le fournisseur vous ment (« *opt-in* » et « pleinement accepté » sont deux mensonges à surveiller), une fois que

vous traitez les données, vous êtes responsable de ce traitement. Si le vendeur vous a dit que les sujets ont consenti et que cela s'avère être un mensonge, si vous n'avez pas obtenu la preuve du consentement avant d'avoir acheté les données, vous pouvez être sanctionné.

Gardez une liste de personnes qui ne donnent pas leur consentement

Gardez la liste de toutes les personnes qui vous ont dit qu'elles ne veulent pas être contactées par votre organisation.

Les droits des personnes concernées

Le GDPR donne aux personnes concernées plusieurs droit que vous devrez respecter :

Droit à l'information (Art 13 et 14)

On a parlé un peu de ce droit plus haut. 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. 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 auxdites 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.

4- 6 conseils pour se préparer

1- Désignez un responsable de la conformité au règlement européen GDPR

Première étape essentielle, désignez au sein de votre organisation la personne qui sera responsable de mettre en place les mesures de conformité. Cette personne est à distinguer d'un délégué à la protection des données dont la désignation est obligatoire en 2018 dans trois cas limités.

Faut-il désigner un délégué à la protection des données (DPO) ?

Le délégué à la protection des données est au cœur du nouveau règlement européen. Le règlement européen sur la protection des données pose les règles applicables à la désignation, à la fonction et aux missions du DPO, sous peine de sanctions.

Qui est le DPO?

Le délégué à la protection des données est une évolution du « correspondant informatique et libertés (CIL) ». Le délégué est la personne qui a pour mission de veiller à ce qu'un organisme protège convenablement les données à caractère personnel des individus, conformément à la législation en vigueur.

Fonctions du DPO

Le DPO aura pour mission de conseiller votre association et ses salariés sur les règles applicables. Notamment, il sera là pour contrôler le respect du règlement et pour coopérer avec la CNIL.

Mon association doit-elle désigner un délégué à la protection des données ?

Selon le règlement, un DPO doit être désigné lorsque :
- les activités de base de votre association consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
- les activités de base de votre association consistent en un traitement à grande échelle de catégories particulières de données dites « sensibles » ou relatives à des condamnations pénales et infractions.

A l'exclusion de ces deux cas bien précis et particuliers, votre association n'aura pas l'obligation de nommer un délégué à la protection des données. Par contre, il est conseillé de désigner au sein de votre organisation une personne qui pourra être responsable de s'informer des obligations auxquelles votre association est potentiellement assujettie, de contrôler le respect du règlement et d'informer votre organe de direction des possibles changements à faire.

2- Effectuez un état des lieux des données récoltées par votre association

Afin de comprendre l'impact de la nouvelle réglementation, vous devrez analyser :

1- les données personnelles que vous récoltez. Les données personnelles sont définies par le règlement comme : « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; 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 ». Si vous êtes une association, vous collectez probablement des données personnelles telles que le nom, l'adresse, l'âge (pour les clubs sportifs), etc. ;

2- ce que vous faites de ces données personnelles (quel « traitement » au sens du règlement faites-vous ?) ;

3- vos objectifs poursuivis par les opérations de traitements de données (connaître vos membres, mieux les servir ? leur offrir des cours par tranche d'âge ?) ;

4- vos systèmes : si vous possédez un système existant, vérifiez que votre fournisseur actuel maîtrise GDPR et ses implications. Où les données sont elles stockées ? Qui y a accès ? Quelle est la sécurité ? Etc. Si vous pensez acheter un nouveau système,

assurez-vous que le fournisseur soit alerté de cette réglementation ;

5- où vont vos données ? : attention à d'éventuels transferts de données hors de l'Union européenne.

3- Une fois un état des lieux effectué, établissez les actions à mener pour être en conformité avec le règlement européen GDPR

Assurez-vous d'établir un calendrier stricte puisque le GDPR ou RGPD sera applicable à partir du 25 mai 2018. Les actions suivantes peuvent être prises quelles que soient les conclusions de votre analyse :

1- Une fois que vous avez déterminé quelles sont les données personnelles que vous devez collecter pour faire fonctionner votre association, évitez de collectez les informations superflues. Si votre objectif est de recenser vos membres, collectez des données nécessaires et évitez celles peu nécessaires et sensibles telles que données de santé, données relatives aux origines raciales ou ethniques.

2- Rédigez vos mentions légales pour vous assurer qu'elles adhèrent à la nouvelle réglementation. Celles-ci devront comporter un certain nombre d'informations que vous pouvez retrouver dans les articles 12, 13 et 14 du règlement.

3- Assurez-vous de l'obtention du consentement explicite de vos membres ou adhérents et qu'ils comprennent pourquoi ces données sont collectées. Concrètement, votre contrat d'adhésion devra comporter des mentions relatives aux données personnelles. Même votre formulaire de contact en ligne devra comporter des mentions (renvoi vers les mentions légales par exemple). Attention, vous devrez être en mesure de prouver le recueil de ce consentement le cas échéant (en cas de contrôle de la CNIL).

4- Rappelez-vous que vos membres peuvent retirer leur consentement à tout moment dès qu'ils le demandent. Donc, votre système de gestion devra permettre la modification ou la possibilité d'effacer les données si cela vous est demandé.

5- Si vous possédez un système existant, vérifiez que votre fournisseur actuel maîtrise GDPR et ses implications.

6- Assurez-vous de la sécurité des données. Ou sont-elles stockées ? par qui ? qui y a accès ?

4- Pour les grandes associations : réalisez une analyse d'impact sur la protection des données

La CNIL peut vous donner de nombreuses informations sur ce type d'analyse qui est une pratique recommandée pour s'assurer que votre traitement est conforme au RGPD et

respectueux de la vie privée. Une analyse d'impact est parfois obligatoire pour les traitements présentant un risque élevé pour les droits et libertés des personnes physiques. La CNIL met à disposition un logiciel libre PIA pour ceux qui désirent utiliser un tel outil.

5- Informez vos employés / volontaires

Assurez-vous que tout le monde dans votre association est sensibilisé à cette réglementation. Pour nombre d'associations, la collecte de données se fera via un système informatique. Votre système devra vous permettre de recueillir le consentement et de garder les informations de façon sécurisée. Pour les associations qui utilisent du papier, les devoirs d'information sont les mêmes et le consentement doit être similairement éclairé et recueilli par votre organisme.

6- Conservez les documents nécessaires

Étape évidente mais parfois négligée : conservez tous les documents qui prouvent que vous êtes en conformité avec le règlement. Gardez la preuve des consentements recueillis (soit sous forme papier soit dans votre système informatique). Documentez les règles internes que vous avez mises en place en cas de violation du règlement.

4- Que dois-je faire si mon association a commis une violation ?

Quelle sécurité devez-vous assurer ?

Selon l'article 32 du RGPD, votre association doit mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris, entre autres et selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Assurez-vous que votre système actuel ou le système de gestion des données que vous entendez utiliser est suffisamment sécurisé. Un bon CRM est probablement recommandé.

Qu'entend-on par violation de données à caractère personnel ?

L'article 4 du RGPD définit la violation de données à caractère personnel comme une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte,

l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Votre association peut donc se trouver dans un des 3 scénarios suivants :

- violations de confidentialité : c'est le cas où il y a eu divulgation des données avec un accès à des données personnelles accidentelle ou non-autorisée ;
- violations de disponibilité : c'est à dire en cas de perte ou de destruction de données personnelles accidentelle ou non-autorisée ;
- violations d'intégrité : c'est à dire en cas d'altération ou de modification de données personnelles accidentelle ou non-autorisée.

Que faire en cas de violations des données de votre association ?

Premièrement, ne pas paniquer. Alertez immédiatement les responsables de votre association. Assurez-vous de mettre en place immédiatement des mesures pour minimiser l'impact de la violation. Vous devrez ensuite notifier l'autorité responsable et parfois les personnes concernées.

Quand faut-il notifier ? quelles sont les hypothèses 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.

Mon association doit-elle communiquer cette violation a ses membres ou donateurs concernés ?

Potentiellement, oui. Indépendamment de votre obligation légale, vous devrez évaluer votre risque de réputation et décider si vous voulez communiquer à vos contacts ou donateurs que leurs données ont été accidentellement dévoilées.

Le règlement prévoit que lorsqu'une violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, votre association devra en général communiquer ladite violation à la personne concernée dans les meilleurs délais (il existe quelques exceptions notamment si votre association avait pris des mesures pour rendre les informations incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement). Vous devrez décrire clairement la nature de la violation et les mesures prises pour y remédier.

CONCLUSION

Nous espérons que ce guide pourra aider les associations. Nous aidons les associations à mieux se gérer en utilisant les nouvelles technologies. Nous ne sommes donc pas des professionnels juridiques. À ce titre, en cas de doute, il est toujours recommandé de consulter son conseiller juridique.

Si vous avez remarqué une erreur ou une correction à apporter, merci de nous aider à améliorer ce document en adressant un courriel (contact@verticalsoft.com).

ATTENTION : RESPONSABILITÉ DE L'ÉDITEUR

L'éditeur met à disposition des lecteurs un contenu informatif gratuit et s'assure en permanence de mettre les moyens à sa disposition pour s'assurer de la qualité du contenu. Ce document traite de l'environnement légal et réglementaire. Nous avons vérifié nos sources et citons d'une manière générale les textes du règlement sur lesquels nous nous appuyons. **Toutefois, il est de la responsabilité des lecteurs de s'assurer que les textes et régimes mentionnés dans les articles sont toujours bien en vigueur.**

Par ailleurs, aucune information dans ce document ne peut être considérée par les lecteurs comme un conseil, une consultation ou une recommandation ; l'auteur n'étant pas habilité à fournir des consultations juridiques. Les lecteurs s'engagent donc à utiliser ces informations sous leur entière responsabilité et ne pourront pas tenir pour responsable l'éditeur du document de toute utilisation des informations fournies.