

De la bonne utilisation du règlement sur la protection des données

Depuis le 25 mai 2018, le règlement général sur la protection des données constitue le cadre réglementaire relatif à la protection des données personnelles, leur collecte, leur traitement et leur circulation. Les associations y sont contraintes comme toutes les autres organisations.

Dans le cadre de leur objet, les associations sont amenées à collecter beaucoup de données dont certaines sont dites sensibles. Le règlement général sur la protection des données (RGPD) ne se limite pas en effet aux données collectées dans un cadre commercial (vente, utilisation des données dans un objectif marketing...). Il concerne toutes les structures qui recueillent les « données personnelles » d'une personne physique. Les associations sont donc tenues de se conformer aux règles du RGPD.

LA CNIL VOUS GUIDE

La Commission nationale de l'informatique et des libertés (Cnil) a établi un guide d'utilisation du RGPD à destination des associations. Dans ce guide, dont la dernière version actualisée est parue cette année, elle définit avec des cas concrets les grands principes de protection des données personnelles issus du règlement. Des cas pratiques thématiques permettent aux associations de mieux évaluer leur degré d'attention dans la collecte et le traitement de ces données, et notamment de mettre en évidence les secteurs susceptibles de brasser des données sensibles (sport, médico-social, ONG, think tank et organisations politiques).

Le guide de la Cnil : s.42l.fr/CNIL-RGPD

Données personnelles et sensibles

Selon l'article 4 du RGPD, les données personnelles visent toute information se rapportant à une « personne physique identifiée ou identifiable ». Or, les associations sont amenées à collecter des données sur leurs membres, bénéficiaires, bénévoles, donateurs, etc. : fichiers d'adhérents, liste de donateurs auxquels sont adressés des reçus de dons, licenciés de clubs sportifs avec un certificat médical individuel, etc. Dès lors que ces données, quelles qu'elles soient (e-mail, numéro de téléphone, RIB, date de naissance, etc.), se rapportent à l'une de ces personnes, il s'agit de données personnelles protégées par le RGPD. Et ce même si ces données ne sont pas numériques !

En outre, parmi le million et demi d'associations en France, certaines sont par leur objet (culturel, politique, sportif, social, etc.) susceptibles de collecter des données dites sensibles : indications sur l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ou des données relatives à la santé ou à l'orientation sexuelle d'une personne. Or, le RGPD interdit de recueillir ou d'utiliser ces données, sauf dans certains cas précisés à son article 9 : si la personne a explicitement donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) ; ou si ces données concernent les adhérents d'une associa-

tion religieuse (type association loi 1905), politique, philosophique ou syndicale, lesquelles utilisent ces données sensibles « dans le cadre de leurs activités légitimes et moyennant les garanties appropriées ». En toute hypothèse, ces données ne peuvent être communiquées en dehors de l'organisme sans le consentement des personnes concernées.

Minimisation et cartographie des données

Les associations doivent limiter la collecte de données à celles qui leur sont strictement nécessaires. Pour cela, il leur est recommandé de faire le ménage dans ces données. Concrètement, elles doivent répertorier les données collectées et supprimer celles qui sont trop anciennes (datant de plus de trois ans), ou les données sensibles dont elles n'ont pas besoin. Une fois triées, les données doivent être rassemblées dans un ou plusieurs documents qui permettent à toute personne qui en ferait la demande, une suppression complète, une modification ou une extraction des données demandées. L'article 17 du RGPD prévoit en effet que toute personne peut demander l'effacement de ses données. Ce registre doit également recenser la provenance des données (événements, inscription mailing, etc.) et comment elles sont utilisées. Plus cette cartographie sera précise, mieux l'association pourra la maîtriser. Les associations doivent veiller à mettre continuellement à jour tous les documents

nt général



permettant de prouver leur conformité au RGPD. Enfin, il est fortement recommandé de créer un registre spécifique pour le suivi et la gestion des données sensibles.

Nommer un DPO

Afin de favoriser sa conformité au RGPD, il peut être judicieux de nommer, au sein de l'association, un délégué à la protection des données (ou DPO pour Data protection officer) qui aura notamment pour mission de contrôler la conformité au RGPD, de tenir à jour le registre des traitements, d'informer et conseiller les membres de l'association et, le cas échéant, de coopérer avec la Cnil (Commission nationale de l'informatique et des libertés). Cette fonction n'est pas obligatoire mais très recommandée si l'association traite un grand volume de données, surtout si certaines d'entre elles ont un caractère sensible.

Sanctions

Au même titre que les entreprises et les administrations, les associations peuvent

être contrôlées par la Cnil laquelle peut ainsi vérifier s'il y a des infractions au RGPD. À l'issue de ces contrôles, les associations peuvent être sanctionnées en cas d'infraction. Particulièrement dissuasives, ces pénalités peuvent atteindre les 20 millions d'euros (ou 4 % du chiffre d'affaires pour une structure d'envergure mondiale). La Cnil peut également les contraindre à limiter définitivement ou temporairement le traitement des données personnelles. Ces mesures peuvent faire l'objet d'une publication, ce qui peut avoir des conséquences désastreuses pour l'image de l'association.

Transmission de fichiers

À des fins de prospection caritative, les associations et autres organismes sans but lucratif peuvent se transmettre des fichiers contacts ou de donateurs. Cette prospection peut être faite par voie postale, appels téléphoniques ou électroniques (SMS, courriels, automates d'appels). Bien entendu, cette pratique est strictement encadrée. Les associations sont tenues d'informer les personnes

concernées (donateurs/abonnés à la newsletter) en leur permettant d'exercer leurs droits relatifs à la protection de leurs données. Elles devront être informées de l'utilisation des données collectées à des fins de prospection caritative, de leur possible transmission à des associations caritatives partenaires et de leur droit de s'opposer préalablement à chacune de ces utilisations. Afin de leur permettre d'exercer cette option, l'organisme doit leur proposer, sur le support permettant de collecter leurs données, de cocher une case avec une mention type : « Je m'oppose à ce que mes coordonnées postales et/ou mon adresse électronique soient transmises aux partenaires de l'association à des fins de prospection caritative par courrier postal et/ou par courrier électronique. »

Pierre Delicata, avocat

En savoir plus

- Le RGPD (Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016) : s.42l.fr/RGPD2016