Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DJEPVA – Bureau du développement de la vie associative

FICHE PRATIQUE :

Le RGPD (Règlement général sur la protection des données) et son application aux associations

Un dispositif qui se veut moins contraignant sur le plan administratif mais qui est assorti d'une responsabilité accrue.

LES TEXTES

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;
- libre circulation de ces données (règlement (UE) 2016/679)
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée.

Le RGPD est une règlementation européenne obligatoire qui refond et renforce les droits et la protection des données à caractère personnel des personnes physiques.

Ce nouveau règlement européen entré en vigueur le 25 mai 2018 s'applique aux traitements de données personnelles, réalisés sur support informatique (logiciels, sites web…), mais également sur support papier.
Le RGPD s'applique à toutes les associations, quelle que soit leur taille, leur structure et leur domaine d'activité.

Le RGPD a pour objectif de moderniser le cadre européen de la protection des données à caractère personnel afin de prendre en compte les avancées technologiques et d'harmoniser les législations des États membres de l'Union européenne.

Avec le RGPD, la responsabilité des organismes se trouve renforcée : ceux-ci devront à tout moment assurer une protection optimale des données et être en mesure de démontrer la conformité de leur traitement, ce qui implique de documenter cette conformité.

Au système déclaratif actuel à la Commission nationale de l'informatique et des libertés (CNIL), le Règlement substitue une démarche responsable (dite « accountability ») selon laquelle un organisme responsable de traitement doit être en mesure de démontrer à son autorité de contrôle qu'il se conforme à ses obligations en matière de protection des données personnelles.

Le responsable de traitement ne sera plus soumis au système de formalités préalables à la mise en œuvre des traitements tel qu'il figure aujourd'hui dans la loi du 6 janvier 1978 modifiée.

En pratique, le principe de responsabilité impliquera que le responsable d'un traitement de données personnelles adopte des mesures techniques et organisationnelles garantissant le respect de la réglementation. Ces mesures devront être adaptées en tenant compte de plusieurs éléments factuels tels que la nature du traitement de données mis en œuvre, le contexte, la portée, les finalités du traitement et le devoir d'information aux personnes concernées.

La loi relative à la protection des données personnelles va prochainement modifier la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés aux fins de l'adapter à ces nouvelles règles.

NOTIONS CLÉS

Une donnée personnelle est toute information permettant d'identifier une personne directement (nom, prénom, etc.) ou indirectement (numéro de sécurité sociale, numéro de téléphone, etc.).

La notion de « traitement » couvre toute opération ou ensemble d'opérations effectuées sur des données : collecte, enregistrement, conservation, modification, communication par transmission. Cette notion désigne également le moyen à l'appui duquel les données sont traitées. (l'outil de traitement : il peut s'agir, par exemple, d'un « tableau Excel », d'une base de données créée grâce au logiciel « métier » de l'organisme, d'un dispositif de de géolocalisation).
Le traitement de données personnelles peut être automatisé ou non (par exemple un dossier professionnel sous format papier est un traitement de données personnelles).

La notion de fichier recouvre « tout ensemble stable et structuré de données accessibles selon des critères déterminés », c'est-à-dire organisé de telle sorte qu'il permet un accès aisé aux données (ce peut être des dossiers papier classés par ordre alphabétique ou chronologique).

La notion de responsable de traitement renvoie à la personne physique ou morale qui détermine les finalités et les moyens du traitement et sur laquelle reposent les obligations prévues par la loi. En général, le responsable de traitement est la personne morale d'un organisme incarnée par son représentant légal.
Le sous-traitant est celui qui traite des données à caractère personnel pour le compte du responsable de traitement.

LES PRINCIPES QUE DOIVENT RESPECTER LES TRAITEMENTS

Les données à caractère personnel ne peuvent être recueillies et traitées que pour une finalité déterminée, explicite et légitime, correspondant aux objectifs poursuivis par le responsable du traitement.

Le caractère licite d'un traitement est respecté si au moins l'une des conditions, ci-après, est satisfaite :

- La personne a consenti au traitement ;
- Le traitement est nécessaire à l'exécution d'un contrat ;
- Le traitement est nécessaire au respect d'une obligation légale ;
- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ;
- Le traitement est nécessaire aux fins des intérêts légitimes (et privés) poursuivis par le responsable du traitement ou par un tiers.

Seules les informations adéquates, pertinentes et nécessaires à la finalité du traitement peuvent faire l'objet d'un traitement.

Une durée de conservation doit être établie en fonction de la finalité de chaque fichier.
Les données contenues dans les fichiers ne peuvent être consultées que par les personnes habilitées à y accéder en raison de leurs missions.

Le consentement de la personne concernée par le traitement doit être obtenu.
Le responsable du traitement doit toujours pouvoir être en mesure de démontrer que la personne a donné son consentement, du moins dans les cas où ce recueil était nécessaire.

La CNIL sera compétente pour surveiller l'application du présent règlement, afin de protéger les libertés et droits fondamentaux des personnes physiques.

LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Quel que soit la taille de la structure et ses activités, la désignation d'un délégué à la protection des données (DPO) est fortement recommandée. Elle permet en effet de confier à un « chef d'orchestre » l'identification et la coordination des actions à mener en matière de protection des données personnelles. Les organismes peuvent désigner un délégué interne ou externe à leur structure. Le délégué à la protection des données peut par ailleurs être mutualisé, c'est-à-dire désigné par et pour plusieurs organismes sous certaines conditions.

Le délégué doit être désigné « sur la base de ses qualités professionnelles et, en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir [ses] missions » (article 37.5 du règlement européen).

Le délégué à la protection des données est principalement chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- de contrôler le respect du règlement et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci (voir question ci-après).

Les missions du délégué couvrent l'ensemble des traitements mis en œuvre par l'organisme qui l'a désigné.

Pour mener son action, il doit disposer des ressources nécessaires à la réalisation de ses tâches. Sa ou ses structures doivent à cet effet :

- lui permettre d'agir de manière indépendante (exemples : positionnement hiérarchique adéquat, absence de sanction pour l'exercice de ses missions) ;
- lui faciliter l'accès aux données et aux opérations de traitement (exemple : accès facilité aux autres services de l'organisme) ;
- veiller à l'absence de conflit d'intérêts.

Le délégué n'est pas personnellement responsable en cas de non-conformité de son ou de ses organismes avec le règlement.
En savoir plus : Lignes directrices concernant les délégués à la protection des données (DPD)

LE REGISTRE DES ACTIVITÉS DE TRAITEMENT

En contrepartie de la suppression des formalités déclaratives, le RGPD prévoit l'instauration d'un registre des activités de traitement qui doit être tenu par le responsable de traitement.

Cette obligation ne s'impose pas aux entreprises comptant moins de 250 salariés, sauf si le traitement que l'entreprise effectue est susceptible de comporter un risque au regard des droits et des libertés des personnes concernées ou s'il n'est pas occasionnel (exemple : gestion de paie, fichiers d'adhérents), ou encore s'il porte notamment sur des données sensibles, ou sur des données se rapportant à des condamnations et des infractions pénales.

En pratique, les dérogations à la tenue d'un registre sont donc limitées.
Pour en savoir plus et disposer d'un modèle de registre : https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

LES DROITS DES PERSONNES - LE DROIT À L'INFORMATION

Le RGPD renforce le droit à l'information des personnes concernées par les traitements de données à caractère personnel. Elles doivent disposer d'une information concise, compréhensible par tous et aisément accessible. Ces informations peuvent être fournies par tous moyens. L'article 13 du RGPD exige que soient communiquées les informations suivantes :

- les coordonnées du responsable du traitement et, le cas échéant, celles du représentant du responsable du traitement ;
- le cas échéant, les coordonnées du délégué à la protection des données ;
- les finalités du traitement auquel sont destinées les données à caractère personnel ;
- la base juridique du traitement ;
- les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers lorsque ces intérêts légitimes sont la condition pour que le traitement de données soit licite ;
- le fait, le cas échéant, que le responsable de traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ;
- le cas échéant, l'existence ou l'absence d'une décision d'adéquation rendue par la CNIL, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ;
- la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
- l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;
- lorsque le traitement est fondé sur le consentement de la personne concernée, l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
- le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;
- l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareil cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Ces informations doivent être communiquées au moment où les données sont collectées. Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité.

Des exemples de mentions types sont disponibles sur le site internet de la CNIL : https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation

Pour en savoir plus : https://www.cnil.fr/fr/respecter-les-droits-des-personnes

LE DROIT D'OPPOSITION, DE COMMUNICATION

Toute personne peut s'opposer, pour un motif légitime, à ce que des données la concernant soient traitées, sauf si le traitement concerné présente un caractère obligatoire.

Par ailleurs, toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel notamment pour :

- savoir si des données qui la concernent y figurent ou non ;
- obtenir la communication des données qui la concernent sous une forme compréhensible, d'une part, et de toutes les informations disponibles quant à leurs origines, d'autre part ;
- obtenir des informations sur la finalité du traitement, les données collectées et les destinataires.

Les personnes concernées par un traitement peuvent obtenir du responsable du traitement une copie des données à caractère personnel leur appartenant. L'article 20 du RGPD exige que ces données soient remises dans un format structuré, couramment utilisé et lisible par machine. Le RGPD n'impose aucune recommandation quant au format des données à caractère personnel à fournir :
L'article 17 du RGPD prévoit par ailleurs le droit à l'effacement ou « droit à l'oubli ». Les personnes concernées ont le droit d'obtenir du responsable du traitement, dans les meilleurs délais, l'effacement des données à caractère personnel les concernant.

MÉTHODOLOGIE DE MISE EN CONFORMITÉ

La CNIL a développé une méthodologie en six étapes afin de faciliter la mise en conformité des responsables de traitements.
Ces six étapes correspondent à :

- La désignation d'un pilote ;
- La cartographie des traitements de données à caractère personnel, recenser ses fichiers ;
- La priorisation des actions à mener ;
- La gestion des risques ;
- L'organisation des processus en interne ;
- La documentation de la conformité.

Pour en savoir plus : https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf