LUSS
LIGUE DES USAGERS DES SERVICES DE SANTÉ

La fiche information a pour objectif d'éclairer les usagers et les associations de patients sur une thématique précise. Elle vise à les soutenir dans leurs actions.

FICHE INFORMATION N°5
RGPD - MAI 2018

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

La réglementation en matière de protection de la vie privée n'est pas nouvelle en Belgique. En effet, le cadre actuel est défini par la Directive UE 95/46 et celle-ci est transposée en droit belge par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Cette législation est abrogée par le Règlement 2016/679 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données[1]. Ce règlement se veut rassurant et sécurisant pour tous, il sera directement applicable dans chacun des États membres de l'Union européenne à partir du 25 mai 2018

À qui s'applique le RGPD ?

Le RGPD sera applicable à toute structure collectant des données personnelles, autant pour le secteur marchand que pour le secteur non marchand. L'Union européenne n'a pas limité ces nouvelles règles uniquement au secteur commercial, il sera bel et bien d'application pour toutes les organisations. L'UE a voulu faire valoir ces nouvelles règles pour tous ceux qui traitent des données[2]. Les personnes physiques qui conservent des données à des fins privées ne sont, bien entendu, pas soumises à ce règlement.

Principes

Traitement licite

Le traitement de données à caractère personnel ne sera licite que si l'une de ces conditions est remplie :

- Si la personne concernée a donné son consentement ;
- Si le traitement est nécessaire à l'exécution d'un contrat ;
- Si le traitement est exigé par une loi, un décret ou une ordonnance ;
- Si le traitement est nécessaire pour sauvegarder un intérêt vital ;
- Si le traitement est nécessaire pour exécuter une mission d'intérêt public ;
- Si le traitement est nécessaire pour réaliser un intérêt légitime du responsable.

Traitement loyal et transparent, collecte à des fins déterminées[3]

Celui qui collecte les données doit indiquer pourquoi il veut obtenir ces données. Il ne peut faire croire qu'il poursuit un but alors qu'il a l'intention de faire autre chose avec les données collectées. Il ne peut pas non plus agir à l'insu des personnes: elles doivent être informées de la manière dont leurs données seront utilisées.

Données collectées adéquates et pertinentes
Le but de la collecte doit bien être spécifié et les données demandées pertinentes au vu de cet objectif.

Par exemple
si on souhaite établir un fichier d'adresses pour l'envoi d'une newsletter, l'adresse mail sera pertinente mais pas une date de naissance ou un état civil.

Données sensibles
En principe, on n'a pas le droit de collecter certaines données dites sensibles, à savoir les données relatives à la race, aux opinions politiques, aux convictions religieuses et philosophiques, à l'appartenance syndicale, à la santé, à la vie sexuelle, à des suspicions, des poursuites ou des condamnations pénales ou administratives. Toutefois, des exceptions sont admises si les personnes ont donné leur consentement explicite ou dans le cadre de soins de santé ou de recherche scientifique.

Données exactes et tenues à jour
Le responsable du traitement doit veiller à ce que les données soient exactes et mises à jour si nécessaire. Il doit également prendre les mesures nécessaires pour corriger ou effacer les données inexactes ou incomplètes.

Durée de conservation des données
Les données personnelles ne doivent pas être conservées plus longtemps qu'il n'est nécessaire par rapport à l'objectif poursuivi. Il conviendra alors de les effacer ou de les rendre anonymes.

Sécurité des traitements & confidentialite
Le responsable du traitement doit veiller à ce que les personnes travaillant sous son autorité ne puissent avoir accès qu'aux données dont elles ont besoin pour exercer leurs fonctions. Il est important de protéger les données contre une curiosité malsaine (interne ou externe) et contre des manipulations non autorisées.

Droits des personnes

Droit à l'information
A partir du moment où l'on recueille des données sur des personnes, on doit informer ces personnes de ce que l'on compte en faire. On ne peut pas traiter de données à l'insu de ceux qu'elles concernent.

Droit à la curiosité
Chacun a le droit d'interroger tout responsable de traitement pour savoir s'il détient ou non des données le concernant. Le responsable doit alors confirmer ou non s'il détient des données, et si c'est le cas, préciser dans quel but, de quelles catégories de données et quels en sont les destinataires.

Droit d'accès
Chacun a le droit de recevoir, sous une forme intelligible, une copie des données faisant l'objet d'un traitement ainsi que toute information sur l'origine des données. Ce droit est exerçable par demande au responsable de traitement en faisant la preuve de son identité, par tout moyen de communication.

Droit de rectification
Toute personne peut faire rectifier des données inexactes qui se rapportent à lui, ou faire effacer ou interdire l'utilisation de données incomplètes ou non pertinentes (et ce sans aucun frais).

Droit d'opposition
Chacun peut s'opposer au traitement de ses données mais en invoquant des raisons sérieuses et légitimes. Dans le cas de marketing direct, l'opposition sera gratuite et sans aucune justification nécessaire.

Droit de na pas être soumis à une décision automatique
La loi interdit qu'une décision affectant une personne de manière significative soit prise sur le seul fondement d'un traitement

automatisé. Cette interdiction ne s'applique pas sir le traitement est fondé dans le cadre d'un contrat ou d'une disposition légale ou réglementaire.

Obligations du responsable de traitement

La loi prévoit une obligation de déclaration des traitements de données

Toutefois, les traitements suivants sont exemptés de déclaration :

- Traitement réalisé par une société pour la gestion du personnel
- Traitement réalisé par une fondation ou ASBL concernant ses membres, bienfaiteurs et contacts réguliers
- Traitement réalisé par les écoles et les établissements d'enseignement concernant leurs élèves et étudiants

Mesures techniques et organisationnelles - politique de protection des données

Les mesures de sécurité à mettre en œuvre sont de deux ordres : des mesures organisationnelles (limité le nombre de personnes ayant accès aux données, utilisation de mots de passe, locaux fermés, etc.) et des mesures techniques (anonymisation des données, chiffrement et encryptage, etc.).

établir un registre des activités de traitement

La loi prévoit une obligation de déclaration des traitements de données. Toutefois, les traitements suivants sont exemptés de déclaration :

- Traitement réalisé par une société pour la gestion du personnel
- Traitement réalisé par une fondation ou ASBL concernant ses membres, bienfaiteurs et contacts réguliers
- Traitement réalisé par les écoles et les établissements d'enseignement concernant leurs élèves et étudiants

Cependant, malgré la dispense de déclaration, le responsable de traitement doit tenir à la disposition de toute personne qui en fait la demande un registre des activités de traitement qui reprend :

- La dénomination du traitement
- La finalité ou les objectifs
- Les catégories de données traitées
- Les bases légales ou réglementaires
- Les destinataires à qui les données peuvent être fournies
- Les garanties entourant la communication de données à des tiers
- Les moyens d'information aux personnes dont les données sont traitées
- Les coordonnées d'un responsable auprès duquel les personnes concernées pourront exercer leurs droits
- Les catégories de données transmises à l'étranger, le pays de destination et les raisons permettant le transfert
- La période de validité des données
- Les mesures organisationnelles et techniques de sécurité

Obligation de signaler une violation ou fuite de données

En cas de violation de données ou de fuite de données, le responsable du traitement doit informer l'autorité de contrôle dont il dépend de la violation ou fuite et ce dans les 72 heures. Il existe une exception si la violation ou fuite ne représente pas de risque pour les droits et libertés des personnes concernées. Par ailleurs, si un tel risque existe, le responsable de traitement doit également informer les personnes concernées par cette violation ou fuite.

Exceptions

La loi ne s'applique pas dans le cadre d'activités exclusivement personnelles ou domestiques, comme la tenue d'un fichier d'adresses privé ou d'un agenda personnel électronique.

La loi peut s'appliquer de manière partielle dans le cadre de traitements à des fins journalistiques ou artistiques (afin de garantir un équilibre avec la liberté d'expression). Les traitements à des fins de sécurité publique bénéficient également d'exceptions partielles.

Quelques définitions

Données à caractère personnel

Toute information concernant une personne physique identifiée ou identifiable. Il peut s'agir du nom, d'une photographie, d'un numéro de téléphone, d'une empreinte digitale, d'un numéro de compte, etc. Même les informations qui se rapportent à la vie professionnelle ou publique sont considérées comme « données à caractère personnel ».

Traitement

Toute opération entièrement ou partiellement automatisée effectuée sur les données. Le sens du mot « opération » est très large, il peut s'agir de consultation, utilisation, modification, communication, etc. Attention, dans le cadre de traitement manuel, la loi s'applique également s'il s'agit de constituer un fichier accessible selon des critères spécifiques (classement, ordre alphabétique, etc.).

Responsable du traitement

Toute personne physique ou morale qui détermine les finalités et moyens du traitement des données. Les associations de fait ou les administrations publiques sont également concernées.

Autorité de contrôle

En Belgique, il s'agit de l'Autorité de Protection des Données (ancienne Commission Vie Privée)[4].

Références

1. S. Denooz, Règlement Général sur la Protection des données, Association des Établissements Sportifs, 2018.
2. S. Denooz, Règlement Général sur la Protection des données, Association des Établissements Sportifs, 2018.
3. Règlement Général européen de Protection des Données, APEF ASBL, consultable sur http://www.apefasbl.org.
4. Claeys & Engels, Traitement des données à caractère personnel : Nouvelle loi portant création de l'Autorité de protection des données, consulté sur https://www.gdprbelgium.be/fr/.

Pour plus de précisions, n'hésitez pas à contacter le référent RGPD de la LUSS, Mohamed Houssein, au 02/734.13.30 ou par mail ***rgpd@luss.be***

LUSS asbl
Avenue Sergent Vrithoff, 123
5000 Namur
luss@luss.be
081.74.44.28
081.74.47.25

Antenne Liège
Rue de la Station, 48
4032 Chênée
luss.liege@luss.be
04.247.30.57

Antenne Bruxelles
Rue Victor Oudart, 7
1030 Schaerbeek
luss.bruxelles@luss.be
02.734.13.30

INAMI culture.be Wallonie FÉDÉRATION WALLONIE-BRUXELLES