Le REGLEMENT GENERAL RELATIF A LA PROTECTION DES DONNEES (RGPD) vous concerne…

En bref

25 mai 2018 : le règlement européen sur la protection des données (RGPD) entrera en vigueur et s'appliquera à tous les organismes et tous les secteurs d'activités.

Selon les informations que le Groupe de travail de la Fédération[1] a pu récolter (formation Socialware et contacts avec juristes), très peu d'asbl seront prêtes à cette date et ce n'est probablement pas le plus important.

Ce qui est par contre essentiel pour le 25 mai, c'est que la structure soit conscientisée sur ce que le RGPD entend apporter comme améliorations à la protection des données des personnes et que chacun se mette au travail pour préparer la mise en conformité. Le RGPD insiste davantage sur l'obligation de documentation du responsable du traitement[2] comme preuve de sa responsabilité.

Le RGPD a pour objectif de renforcer les droits des citoyens en matière de protection et du traitement de leurs données personnelles. En d'autres termes, les données personnelles comme le terme l'indique, appartiennent à la personne et PAS aux travailleurs d'une maison médicale ou aux gouvernements, à la FMM, etc.

- ⇨ Le secteur de la santé, les maisons médicales, la Fédération des maisons médicales et les intergroupes sont d'autant plus concernés et impactés que nous traitons chacun des données de santé à caractère personnel et sensible. Pour cette raison, toutes les nouveautés du RGPD vont s'appliquer à nos structures, nous ne faisons partie d'aucune exception.
- ⇨ C'est donc une opportunité pour revoir l'ensemble de notre/votre politique de protection des données.

Un nouveau cadre juridique

Les 4 grandes idées phares de ce RGPD :

Renforcement des droits des personnes	**Obligation pour les compagnies/asbl,…**
Renforcement de la sécurité des données	**Renforcement des sanctions**

[1] GT : Mano Carton, Marie-Agnès Broze, Marie Marganne, Julie Atérianus, Aurélie Feller, Nicola Iezzi
[2] Voir point définitions

Le RGPD renforce les droits des personnes :

Chaque personne, dont nous traitons les données personnelles a :

- *Le droit d'être informée* : à partir du moment où l'on recueille des données sur des personnes (travailleurs, patients, etc.), on doit informer ces personnes de ce que l'on compte en faire. On ne peut pas traiter de données à l'insu des sujets. Ni pour autre chose que le traitement communiqué.
- *Le droit de rectification* : toute personne peut faire rectifier des données inexactes la concernant, ou faire effacer ou interdire l'utilisation de données incomplètes ou non pertinentes.
- *Le droit d'opposition* : chacun peut s'opposer au traitement de ses données mais en invoquant des raisons sérieuses et légitimes.
- *Le 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 simple demande au responsable de traitement en faisant la preuve de son identité.

Ce qui implique de nouvelles obligations légales :

- Garder une traçabilité des données
- Ecrire et implémenter les nouvelles procédures nécessaires à la mise en conformité
- Respecter les règles du renforcement des droits des personnes
- Augmenter les niveaux de sécurité

Le règlement renforce la sécurité des données :

- À terme, un nouveau règlement interne (de l'asbl) pour la Protection de la Vie Privée (déclaration d'intention, politique interne/règlement de travail, etc.) devra être écrit conformément au RGPD.
- Les nouveaux contrats avec des sous-traitants seront conformes et les contrats existants revus.
- Des précisions seront à apporter dans les consentements (par exemple la durée de conservation des données devra être stipulée, traduction si nécessaire, etc.).
- Un registre de traitement de données devra être tenu.
- Un « Délégué à la protection des données » - DPO devra être désigné.
- Un registre des fuites de données et/ou autres violations au RGPD sera constitué.

Il prévoit des sanctions en cas de non-respect :

- Impact financier important : amende jusqu'à 4% du chiffre d'affaire ou 20 millions d'euros, mais également des procédures de saisies et d'exécution forcée.

Un Plan d'action…

Le GT a essayé de vous proposer ci-dessous un plan d'action que vous pouvez dès à présent mettre en œuvre et qui nécessite une implication de TOUTE l'équipe, la désignation d'un référent RGPD (voir plus bas) et d'un Délégué à la Protection des Données (DPO). C'est bien une proposition avec les informations dont nous disposons actuellement. Chaque maison médicale est bien entendu libre de fonctionner comme elle le souhaite et de continuer à s'informer par ailleurs.

Remarque : Vous trouverez en annexe un fichier de documents qui nous ont été fournis par Socialware. Nous nous en sommes inspirés pour vous proposer la suite et y ferons référence par moment. Les exemples de contrats, règlements…qui se trouvent dans ce fichier ont été fournis par le cabinet Sirius. Ils peuvent être utilisés et adaptés à votre situation.

Se mettre en conformité en 5 étapes

⇨ En préalable à ces étapes, nous vous conseillons de **choisir un référent RGPD** dans votre maison médicale. Selon le GT, cette personne pourrait être en charge de :

- Sensibiliser son équipe avec l'aide des outils en annexe
- Aider chaque membre de l'équipe à identifier et décrire les flux de données à caractère personnel qu'il traite.
- Remplir le registre des traitements (voir annexe)
- Etre la personne de référence pour toute interaction avec le DPO
- Etre la personne de référence pour centraliser les fuites de données et en faire rapport à l'Autorité compétente.

⇨ **L'identification d'un DPO** devrait également se faire avant d'amorcer l'ensemble de la mise en conformité. Néanmoins, du côté de la Fédération nous n'avons pas de piste à vous proposer pour le moment. De plus, nous devons encore éclaircir la nécessité d'avoir ou non un DPO par MM ou si un DPO pour un ensemble de MM est suffisant.
Nous allons continuer à nous pencher sur la question.
Parallèlement, vous pouvez vous mettre en recherche de votre côté, seul ou via les IG. De plus, l'absence de DPO ne vous empêche absolument pas de commencer le travail de mise en conformité selon les étapes citées ci-dessous. Pour rappel : A la date du 25 mai votre asbl ne doit pas être en conformité totale mais bien avoir commencé le travail et pouvoir le prouver aux instances de contrôle !

I. Première étape : Information

L'objectif de cette étape est que chaque personne de l'équipe se conscientise au nouveau règlement, en mesure les enjeux et les objectifs. C'est la responsabilité de chacun avec l'aide du référent RGPD de votre équipe.

⇨ ***Pistes*** **:** Dès à présent, prendre connaissance de ce document et des outils proposés en annexe. En discuter en équipe et ne pas hésiter à déposer vos questions/demandes au GT de la Fédération via l'adresse : service.etude@fmm.be

Remarque : en fonction des questions/remarques déposées, la FMM, en collaboration avec les IG évaluera avec le futur DPO, la nécessité d'apporter d'autres réponses aux maisons médicales.

II. Deuxième étape : Faire l'inventaire des données à caractère personnel que vous traitez

Cette étape doit permettre d'aboutir à la tenue d'un registre des traitements de données :
Ce document identifie et décrit tous les traitements de données réalisés au sein de votre maison médicale (et constitue un des documents obligatoires à produire).

⇨ **Pistes** :

- Le référent aide chaque membre de l'équipe à identifier et décrire les flux de données à caractère personnel qu'il traite.
- A ce stade, on peut déjà identifier certains manquements potentiels. Cela aidera le référent avec l'aide du DPO à effectuer l'analyse d'impact (qui constitue un des autres documents obligatoires à produire) qui consistera à s'assurer que des mesures de protection sont en place et adéquates pour chaque traitement de données : Contrats à revoir ? Consentements à refaire ? Le traitement repose-t-il bien sur une base légale ?...

  Exemples :

  Le consentement des patients de maisons médicales pour le traitement de leurs données au niveau de la Fédération doit comporter la mention de durée de conservation des données.
  De plus, il doit être compréhensible par tous => Traduit dans différentes langues.
  Pas le cas actuellement => PAS CONFORME AU RGPD

  Session de Pricare qui reste ouverte dans une maison médicale alors que l'utilisateur principal est en réunion pour plusieurs heures => PAS CONFORME AU RGPD

- Le référent, une fois les flux de données identifiés, doit remplir un registre de données (nous vous proposons un exemple rempli par Socialware en annexe). A ce stade, le référent peut déjà remplir les colonnes bleues du registre (qui représentent l'analyse de flux).

III. Troisième étape : Se mettre au travail avec le DPO « délégué à la protection des données ».

Comme expliqué ci-dessus, cette étape ne pourra se faire que si vous avez déjà identifié un DPO.
En attendant, passez aux étapes suivantes et voyez dans quelle mesure vous pouvez continuer à progresser sans l'aide du DPO.

Selon le RGPD, les missions du DPO sont les suivantes :

- Informer et conseiller le responsable du traitement ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du RGPD ;
- Contrôler le respect du RGPD ;
- Dispenser des conseils ;
- Coopérer/être le point de contact avec l'autorité de contrôle.

Remarque : Dans les documents en annexe, vous trouverez également un document reprenant le profil type d'un DPO ainsi que ses fonctions et son statut.

IV. Quatrième étape : la mise en conformité

Sur base du travail fait par l'équipe dans l'identification des flux des données à caractère personnel (voir deuxième étape) et de la collaboration avec le DPO

⇨ le référent peut à présent remplir les colonnes vertes du registre que nous proposons d'utiliser, en intégrant les règles de mise en conformité suivantes telles que décrites dans le RGPD et dont une définition vous est donnée dans le registre :

a. **Un traitement licite :**
   Le traitement de données à caractère personnel doit être licite et donc reposer sur un des 6 fondements légaux suivants :
   - Obligation légale
   - Obligation contractuelle
   - Autorité publique
   - Intérêts légitimes
   - Intérêts vitaux
   - Consentement

b. **Un traitement loyal et transparent**
c. **Des données exactes et tenues à jour**
d. **Une durée de conservation des données :** Cette durée doit être justifiable.
e. **Des mesures de sécurité des traitements et la confidentialité**

V. Cinquième étape : documenter la mise en conformité

Les documents à produire servent tant d'outils à la mise en conformité et donc à l'amélioration des processus internes que de preuve en cas de contrôle.

⇨ **Les 7 documents sont les suivants** :

1. Le registre des données
2. L'analyse d'impact (DPIA)
3. Le registre des violations

Vous êtes désormais dans l'obligation de signaler toute violation ou fuite de données.
« *En cas de violation 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.* »
L'autorité de contrôle est l'Autorité de Protection des Données (ancienne Commission Vie Privée).
Une fuite de données va de la perte d'une clé USB contenant les fiches de salaires ou des données patients à une demande de rançon suite à un piratage informatique. Les procédures en cas de fuite de données (limiter impact de la fuite ; prévenir les personnes concernées ; prévenir l'autorité de contrôle…) doivent inclure le maximum de scénarios possible.

4. La déclaration d'intention
5. La politique interne revue en fonction du RGPD

Le règlement interne (à l'asbl) relatif à la protection de la vie privée ou règlement relatif à la protection de la vie privée de ses travailleurs
définit la manière dont vos collaborateurs doivent appréhender les données à caractère personnel dont ils prennent conscience dans le cadre de l'exécution de leur travail.

6. Le recueil des consentements
7. La preuve de vérification des contrats

Quelques définitions :

Données à caractère personnel	Toute information se rapportant à une personne physique identifiée ou identifiable; 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.
Traitement de données	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 tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.
Responsable du traitement	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.
Délégué à la protection des données (DPO)	Le DPO contrôle les traitements de données au sein de l'organisation. Mission d'information; mission de conseil; mission de contrôle en interne.
Sous-traitant	La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.
Destinataire	La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers.
Tiers	Une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.