

## Le médecin et le « R.G.P.D. »

### 1. Qu'est-ce que c'est ?

**R.G.P.D.** = *Règlement Général sur la Protection des Données*  
(ou *General Data Protection Regulation*)

C'est la législation européenne (n° 2016/679) la plus importante depuis une vingtaine d'années en ce qui concerne la protection des données à caractère personnel, ce texte accentuant davantage, par rapport à la législation antérieure<sup>1</sup>, les notions :

- de transparence : quelle utilisation est faite de nos données personnelles ?
- et de contrôle : comment pouvons-nous agir en vue d'une utilisation proportionnée de ces données ?

Cette législation est notamment applicable aux entreprises >> depuis l'entrée en vigueur du Livre XX au sein du Code de Droit Economique en cours d'année 2018, un médecin exerçant son activité professionnelle est une entreprise, et doit donc se conformer aux normes édictées par le RGPD.

### 2. Les notions clés

Est une *donnée à caractère personnel* : *toute information concernant une personne physique* identifiée ou identifiable (nom, prénom, adresse IP, adresse électronique, numéro de téléphone, etc., même si de nature professionnelle).

▷ Ceci **ne concerne donc pas** les **données** relatives aux **personnes morales**.

Est un *traitement de données à caractère personnel* : *la collecte, l'enregistrement, la conservation, l'organisation, la diffusion, la transmission (etc.) de données personnelles*.

Il s'agit de tout traitement automatisé ou non automatisé mais contenu dans un fichier.

---

<sup>1</sup> Notamment, la directive européenne n° 95/46/CE du 24 octobre 1995.

### **3. Quels sont les principes généraux du RGPD ?**

Le Règlement impose le *respect de différents principes* lors du traitement des données personnelles, notamment pour éviter les excès :

**Principe de loyauté et de transparence** : communication à la personne concernée d'*informations claires, précises et exprimées simplement* quant aux modalités de traitement des données.

**Principe de licéité (finalité)** : pour être licite, un traitement doit :

- soit être *fondé sur le consentement* préalable libre, informé, univoque et spécifique ;
- soit être *fondé sur une obligation légale* du responsable du traitement ;
- soit être *nécessaire* à l'exécution d'un *contrat* ;
- soit être *nécessaire* aux fins des *intérêts légitimes* du responsable du traitement (*équilibre des intérêts*).

**Principe de responsabilité (dit « accountability »)** : le responsable du traitement doit prouver que *chaque traitement est conforme* au RGPD.

**Principe de proportionnalité** : le traitement des données personnelles doit répondre à une *finalité précise, expresse*, et demeurer *proportionnel* à ladite finalité.

**Principe de pertinence et de minimisation** : seules les données *strictement nécessaires* peuvent être traitées.

**Principe d'intégrité et de confidentialité** : mise en place de dispositifs et procédures de *sécurité*, tant du côté du responsable du traitement que de ses sous-traitants.

**Principe de conservation limitée** : la *durée de conservation* doit être justifiée par la finalité du traitement.  
Les données qui ne sont *plus utilisées* doivent être *supprimées*.



Quant à ce dernier principe, les normes déontologiques médicales demeurent d'application → le dossier médical, contenant nécessairement diverses données personnelles, doit être conservé pendant 30 ans après le dernier contact avec le patient.

#### **4. Quid des données particulièrement sensibles ?**

Sont considérées comme des *données sensibles* (article 9 du Règlement) les données qui révèlent l'origine raciale, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, **les données relatives à la santé**, la vie sexuelle ou l'orientation sexuelle, etc.

Le *traitement* de telles données est par principe *interdit* par le RGPD.

L'article 9 prévoit toutefois une série d'*exceptions* à cette interdiction, dont une *à portée médicale* (cf. article 9, 2. h)):

« (...) *le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé (...)* ».

Un médecin peut donc bien sûr continuer à créer et alimenter ses dossiers médicaux comme auparavant, sans crainte de contrevenir aux normes européennes.

#### **5. Le consentement**

Toute personne physique doit donc désormais être en mesure, *préalablement et expressément*, de consentir au traitement de ses données à caractère personnel.

Est appelé « *responsable de traitement* » (« RT ») toute personne amenée à traiter une donnée à caractère personnel, d'une manière ou d'une autre.

*Un médecin endosse donc le rôle de RT vis-à-vis de ses patients.*

- Le RT doit obtenir de ses patients un consentement préalable libre, informé, univoque et spécifique en vue du traitement des données à caractère personnel (exemple : collecte en vue de la constitution du dossier médical).
- Ce consentement peut être obtenu une seule fois pour une ou plusieurs finalités spécifiques.
- Le cas échéant, la charge de la preuve incombe au responsable de traitement.
- Si un traitement est prévu pour d'autres usages ou questions, il faut obtenir un consentement spécifique.



- Chacun a la possibilité de retirer son consentement à tout moment, et aussi simplement qu'au moment où il l'a donné.



Si la personne physique concernée est *obligée de consentir* à un traitement de données qui n'est pas nécessaire pour bénéficier de prestations ou de la fourniture d'un service, *le consentement n'est pas considéré comme libre*.

## **6. Les droits des personnes concernées par le traitement de leurs données personnelles**

Les personnes physiques faisant l'objet d'un traitement quel qu'il soit de certaines de leurs données personnelles disposent de certains *droits spécifiques*, qu'ils peuvent exercer au titre de contrôle et de vérification du respect des principes légaux du RGPD, en accord avec la notion de renforcement de la protection voulue par le législateur.

AVANT LE TRAITEMENT	PENDANT LE TRAITEMENT	APRES LE TRAITEMENT
<ul style="list-style-type: none"><li>➤ Transparence des informations sur le traitement et sa finalité</li><li>➤ Consentement libre, spécifique et informé de la personne sur les données traitées</li></ul>	<ul style="list-style-type: none"><li>➤ Le droit de demander des informations au RT</li><li>➤ Le droit de retirer son consentement : droit de s'opposer à tous les traitements ou à un traitement particulier</li><li>➤ Le droit d'accéder à ses données personnelles et à toutes informations supposées être disponibles avant le traitement (finalité de traitement, DPO, ...)</li><li>➤ Le droit de rectifier ses données</li></ul>	<ul style="list-style-type: none"><li>➤ Le droit d'obtenir la suppression des données conservées qui ne sont plus nécessaires au regard de la finalité</li><li>➤ Le droit à la portabilité</li><li>➤ Le droit de demander le transfert de ses données vers un autre responsable de traitement</li></ul>



A noter :

- L'*exercice des droits* précité est en principe *gratuit* (sauf en cas d'exercice manifestement infondé ou excessif).  
En cas d'exercice de ces droits, le responsable de traitement concerné dispose d'un délai d'un mois pour répondre.
- Ce délai peut être prolongé de deux mois en cas de complexité du cas, ou en raison d'un nombre élevé de demandes.
- Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande.
- Si la demande parvient sous une forme électronique, les informations doivent être fournies par voie électronique lorsque cela est possible.
- La personne concernée est toutefois en droit de déterminer la forme de la réponse (électronique, courrier postal...).
- A défaut de réponse dans le mois, le RT informe dans ce délai les motifs de son inaction et la possibilité d'introduire une réclamation auprès de l'autorité de contrôle et de former un recours.

## **7. Les autres obligations**

- Obligation de démontrer la conformité du traitement au RGPD, dans la durée... → d'où la *nécessité de mettre en place un « registre des activités de traitement »*.

Généralement sous forme de tableau (Excel ou autre format) comprenant des métadonnées, votre registre contiendra toutes vos sources d'acquisition de données personnelles, et pour chacune de ces données, ses différents traitements (cf. point 8).

- Ceci augmente nécessairement le *degré de responsabilité des sous-traitants du médecin* (exemple : la société éditrice de son logiciel médical, son prestataire informatique, etc.) ainsi que la responsabilité, le cas échéant, dans le chef du *responsable de traitement* désigné au sein d'une structure plus importante (clinique, hôpital, etc.).

Au sein de structures plus importantes, est désigné un « DPO » (« *Data Protection Officer* ») qui aura notamment la charge de l'établissement du registre des activités de traitement ainsi que la responsabilité de veiller à ce que les traitements effectués au sein de l'institution, association, société, etc., soient conformes aux normes européennes.



- Conséquences à réfléchir également sur l'*organisation* au sein de votre cabinet ou entre membres d'une association, d'une maison médicale, etc. : que faire en cas de fuite des données (fuite informatique, perte ou vol d'un ordinateur portable, d'un GSM, d'une mallette professionnelle, etc.) ?

Pour toutes ces raisons, *il est recommandé que les médecins ou groupes de médecins prennent le temps de revoir leur organisation professionnelle et s'adaptent en conséquence* :


*Nécessité d'initier un audit* « vie privée » quant au traitement des données à caractère personnel (recensement des différents traitements qui surviennent dans le cadre de la pratique professionnelle quotidienne), puis :



*Identifier les traitements* de données, fixer les finalités poursuivies par ces traitements, déterminer la durée et les modes de conservation, puis :



*Mettre en place le registre* des activités de traitements, adapter le cas échéant ses contrats fournisseurs / prestataires, former son personnel en conséquence, etc.

 *Nommer un DPO n'est pas requis si le médecin concerné ne pratique aucun traitement à grande échelle (généralement applicable aux structures de type hôpital, de par le volume des données personnelles que ces structures sont amenées à traiter.*

## **8. Le registre des activités de traitements**

Pourquoi établir ce registre ?

- Identifier la *localisation des traitements* et ceux qui les réalisent ;
- *Inventaire et description* de *chaque traitement* réalisé ;
- *Description de la méthode* de mise à jour des données ;
- Le registre doit être à *disposition de l'autorité* de contrôle.

Le RGPD impose à tous les responsables de traitements de mettre en œuvre une large gamme de mesures afin de réduire les risques de violation.

Ceci signifie pour le responsable :

- Mettre en place des moyens techniques pour sécuriser les données à caractère personnel contre les risques de perte, de vol, de divulgation et tout autre risque ;
- Fournir une documentation claire et précise de toutes les mesures et procédures utiles pour assurer la protection de données ;
- Garantir que les cocontractants et prestataires répondent aux obligations du RGPD et sont responsables de cette conformité ;
- Détailler les mesures techniques dans le registre des traitements qui est à la disposition de l'autorité de protection ;
- Notification obligatoire à l'autorité compétente et information immédiate des personnes concernées en cas de risque d'atteinte à la protection des données.

## **9. Quels sont les risques encourus en cas de non-conformité ?**

En cas de *manquement au RGPD*, la sanction peut être lourde (en théorie) :

- Peuvent être infligées par l'autorité de contrôle des *amendes* correspondant à une somme comprise entre 2 et 4 % du chiffre d'affaires → caractère dissuasif recherché : les entreprises doivent préférer consacrer des budgets à la mise en conformité plutôt que risquer des sanctions financières.

Mais également, au-delà des sanctions financières éventuelles :

- Réparation du préjudice subi par la personne physique concernée ou pour toute personne ayant subi un dommage du fait de cette violation des normes du RGPD (dommage matériel ou moral) ;
- Tout RT ayant participé au traitement peut être considéré responsable du dommage causé par le traitement constituant une violation du RGPD (de même que ses sous-traitants ou prestataires éventuels).



## 10. Informations et liens utiles



Cette évolution des normes engendrera nécessairement son lot de démarchage commercial voire d'arnaques ou tentatives d'arnaques auprès des entreprises, et notamment des médecins, certains esprits malintentionnés pouvant jouer sur la crainte des entreprises de se voir appliquer des amendes excessives à défaut de conformité aux normes du RGPD, pouvant également miser sur un manque de connaissances en la matière, etc.

Si la majorité de ces démarchages peuvent être légitimes et de bonne foi, il semble plus prudent d'examiner avec attention, et suffisamment de recul, toute offre qui vous parviendrait en ce sens.

En aucun cas le RGPD ne prévoit l'application spontanée d'amendes sans qu'aucun contact avec l'entreprise concernée n'ait été pris au préalable.

Une telle finalité ne serait que l'aboutissement de procédures menées auparavant par l'autorité de contrôle, dont l'entreprise aurait de toute façon été informée.

En cas de doute, il semble sage de solliciter l'avis de confrères qui utiliseraient déjà, le cas échéant, les services de sociétés professionnelles pour la tenue de leurs registres de traitements, ou auraient éventuellement déjà été victimes de ces tentatives de « hameçonnage ».

De même, l'avis de votre Conseil provincial peut toujours être sollicité : <https://www.ombbw.be/fr/contact>

Le Conseil national de l'Ordre des médecins peut également être contacté pour toute demande relative au RGPD : <https://www.ordomedic.be>, et particulièrement sa juriste en la matière, Madame Audrey VAN SCHAREN ([privacy@ordomedic.be](mailto:privacy@ordomedic.be)).

\* \*  
\*

Votre « *nouveau* » *Code de déontologie médicale*, en vigueur depuis le 3 mai 2018 (<https://www.ordomedic.be/fr/code-2018/contenu/>), soit antérieur à l'entrée en vigueur du règlement européen, a couvert cette problématique en son *article 27* : « Le **médecin respecte la finalité et la proportionnalité** en matière de traitement de données à caractère personnel relatives à la santé. À la demande du patient ou avec son accord, le médecin transmet les informations et éléments pertinents à un autre professionnel de santé ».





En d'autres termes, le médecin est invité à tenir à jour ses *dossiers médicaux* en veillant, plus encore qu'auparavant, à la *pertinence diagnostique et thérapeutique des informations* qui y sont *consignées*.

\* \*  
\*

Les dates-clés du RGPD :

- Date d'adoption du texte par le Parlement Européen : 27 avril 2016 (J.O.U.E. : 4 mai 2016).
- Entrée en vigueur du RGPD : 24 mai 2016.
- ***Depuis le 25 mai 2018, tous les traitements réalisés doivent être conformes au RGPD.***
- La directive 95/46/CE (législation antérieure en la matière) a été abrogée par le RGPD.

\* \*  
\*

Liens utiles :

Le texte du Règlement Européen : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

L'autorité de contrôle belge : <https://www.autoriteprotectiondonnees.be/>

Les informations fournies par le SPF Economie : <https://economie.fgov.be/fr/themes/line/securite-de-linformation/protection-des-donnees>

L'avis du Conseil national de l'Ordre des médecins sur le sujet : <https://www.ordomedic.be/fr/avis/conseil/reglement-sur-la-securisation-des-donnees-privees-rgpd>