# À partir de mai 2018, toutes les entreprises qui collectent **des données personnelles** devront respecter Le GDPR.

## Le GDPR, c'est quoi ?

Le GDPR, General Data Protection Regulation (règlement général sur la protection des données), est une nouvelle législation européenne sur la protection de la vie privée qui entrera en vigueur en mai 2018.

## Qui est concerné par cette législation ?

**Toutes les entreprises et organisations basées en Europe**, qui collectent des données* sur les citoyens, indépendamment de leur présence physique dans le pays concerné. « Toutes », indépendamment de leur taille (PME. grandes entreprises, micro entreprises) ou de leur forme juridique (asbl, SA, etc.).

## Pourquoi est-ce important ?

En cas de non-respect, les amendes seront très élevées.

## Quelques concepts clés qu'il faut maîtriser

**Deux types de données : données personnelles et données sensibles.**

***DONNÉES PERSONNELLES**

*"Toute information se rapportant à une personne physique identifiée ou identifiable, 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"*

Par exemple, une adresse courriel (mail), un N° de téléphone, un N° de registre national ou de carte de crédit pourraient tous être considérés comme des informations sur une personne identifiable.

**Attention** : la détention d'une adresse courriel professionnelle du type al@appl.be ainsi qu'un N° de téléphone personnel, peuvent suffire pour identifier la personne liée au suffixe al. Dès lors, l'adresse professionnelle ainsi que le N° de téléphone devront être considérés comme des données personnelles.

Sources ; APB, Spot it, eugdpr.org, retis.be, efficy.com,

***DONNÉES SENSIBLES :**

*"Certaines données personnelles sont plus sensibles que d'autres. Il s'agit, par exemple, d'informations relatives à la race, la santé, les opinions politiques, les convictions religieuses ou philosophiques, l'affiliation à un syndicat, les préférences sexuelles ou le passé judiciaire. Ces données ne peuvent être ni collectées, ni enregistrées, ni même demandées[1]."*

[1]. un cadre est fixé pour les professionnels de la santé.

# Quels sont les grands principes de cette législation ?

**PRINCIPE I : LICEITÉ ET TRANSPARENCE**

Si les données sont utilisées, leur utilisation doit répondre à une base légale et doit être justifiée avec une finalité **en accord avec la personne concernée**, titulaire de ces données. (transparence et établissement de conditions générales)

**PRINCIPE II : CONSENTEMENT**

Le consentement est défini comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».*

Cela signifie aussi que la personne peut, à tout moment, retirer son consentement, et ce, sans conditions.

**PRINCIPE III : LE DROIT À L'OUBLI ET À L'ACCÈS DE SES DONNÉES**

*"La personne a le droit de demander l'effacement et la suppression de ses données personnelles."* C'est à dire que votre client/prospect dont vous possédez des données peut vous écrire et vous demander de supprimer ses données personnelles.

*"Les organisations peuvent refuser de supprimer les données pour des raisons particulières, telles que pour exercer le droit de liberté d'expression et d'information, pour se conformer avec une obligation légale pour la réalisation d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ; pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public et pour l'exercice ou la défense de droits en justice. "*

Les clients/prospects peuvent transférer facilement les données d'un prestataire à un autre.

Sources ; APB, Spot it, eugdpr.org, retis.be, efficy.com,

Par exemple, si votre client décide de s'affilier dans une autre organisation, il aura parfaitement le droit de vous demander de transférer toutes ses informations vers l'autre organisation.

**PRINCIPE IV: LIMITATION DES FINALITÉS**

Il faut impérativement s'assurer que *les données encodées et sauvées sont utilisées à des fins explicites, spécifiques, légitimes pour aucun autre objectif que celui mentionné de manière publique et transparente.* ***Les données doivent être utilisées de manière sécurisée.***
*Les organisations devraient donner la priorité à la minimisation des données, aux restrictions d'utilisation et à la non-distribution des données à d'autres personnes sans une vérification des intérêts. Ce principe peut être contraire au concept de « big data »."*

**PRINCIPE V: EXACTITUDE DES DONNÉES**

Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour. Toutes les mesures raisonnables doivent être prises pour que les données qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder.

**PRINCIPE VI: INTÉGRITÉ ET CONFIDENTIALITÉ**

*« Les données doivent être utilisées de manière sécurisée »*

**PRINCIPE VI : RESPONSABILITÉ**

*"Le responsable du traitement des données doit être capable de démontrer que les prescrits du RGPD sont respectés."*

**PRINCIPE VIII : AUTOMATISATION**

*"Les personnes ont le droit de ne pas être soumises à des décisions automatisées. Les organisations seront obligées d'assurer qu'un individu obtienne une intervention humaine, puisse exprimer son point de vue, reçoive une explication et conteste la décision*

## Le GDPR et vos Unions

Aux vues des éléments énoncés ci-dessus, vous comprendrez très rapidement la nécessité pour vos Unions de respecter cette réglementation.

Sources ; APB, Spot it, eugdpr.org, retis.be, efficy.com,

**Au niveau tarification et communication** (données personnels et sensibles), l'APPL vous contactera et vous communiquera les démarches à entreprendre.
**Au niveau communication et sécurisation de vos données patients** (personnelles et sensibles) au sein de l'officine, vos maisons de soft devront aussi être impliquées.

## Quelques premiers conseils :

- Le mail ou le courriel n'est pas une voie de communication sécurisée. NE COMMUNIQUEZ PLUS DE **DONNEES SENSIBLES** PAR COURRIEL (CPAS, ….).

- Dans le cadre d'une demande de communication de données « patients » (données personnelles et sensibles), dans un 1er temps nous vous conseillons :
    - De mentionner la requête du patient sur le document renfermant les données personnelles et/ou sensibles (liste des médicaments) : « à la demande du patient » et de faire signer le patient.
    - Ne prenez pas la responsabilité d'envoyer ce document renfermant des données personnelles et/ou sensibles par courriel. Remettez le document directement au patient.
    - Le traitement des données DPP et ASSURpharma est sécurisé : Flux (single message)

- Ne prenez pas la responsabilité de communiquer des données personnels ou sensibles à des tiers.

- Ne communiquez pas d'informations (publicité ou promotions, rappel de vaccination, ….) à vos patients par leurs données personnelles (courriel ou envoi postal) sans les avoir préalablement avertis de l'utilisation de leurs données personnelles dans le cadre d'une communication, même s'il s'agit de vos propres patients.

- Lors de vos échanges de courriel entre pharmaciens (rôle de garde, congés, indisponibilités produits, …) **MENTIONNEZ tous vos destinataires en Cci (copie cachée)**. Pour rappel :
    - **Le courriel n'est pas sécurisé**
    - **En SIMPLE Copie (Cc) non cachée, vous transférez d'office toutes les adresses de vos confrères (données personnelles) à TOUS vos destinataires et lecteurs du message adressé**.

**Ces premiers conseils ne sont pas exhaustifs**, nous reviendrons vers vous rapidement pour vous guider dans cette nouvelle réglementation.

Cordialement, Michel Kohl

Sources ; APB, Spot it, eugdpr.org, retis.be, efficy.com,