# Comment respecter les droits des personnes dont les données de santé sont traitées ?

Les personnes dont les données font l'objet d'un traitement bénéficient de **droits sur leurs données**, définis par la loi Informatique et Libertés du 6 janvier 1978 (Loi IFL) et encore renforcés par le nouveau Règlement européen relatifs à la protection des données personnelles (RGPD). Pour le responsable de traitement (RT), ce sont autant d'obligations qui s'imposent, dès le stade de la conception de l'outil à l'origine de la collecte, afin de garantir leur mise en œuvre effective.

## Les droits maintenus par le Règlement européen

### ✓ Droit d'information [Article 32 Loi IFL] – [Article 13 RGPD]

Les personnes concernées doivent être informées, préalablement à la collecte de leurs données, sur les modalités du traitement, et notamment sur l'identité du RT, la finalité poursuivie par le traitement, le caractère obligatoire ou facultatif des réponses et des conséquences en cas de défaut de réponse, les destinataires des données, les droits des personnes concernées, ainsi que les transferts de données.

Le RGPD **renforce ce droit** en ajoutant notamment à la liste des informations à fournir la période de conservation des données (lorsque cela est possible), le droit à la portabilité des données, le droit d'introduire une réclamation auprès d'une autorité de contrôle.

**En pratique,** ces informations pourront être délivrées par le RT sur les **supports** suivants :

- Le formulaire de collecte
- Les CGU d'un site internet
- Le panneau d'information pour une vidéosurveillance.

### ✓ Droit d'accès [Article 39 Loi IFL] – [Article 15 RGPD]

La personne concernée doit pouvoir interroger le RT pour savoir s'il détient des informations la concernant et dans l'affirmative se les faire communiquer au moyen d'une copie fidèle.

Le RT est tenu de répondre favorablement à la personne qui aura fait cette demande d'accès et qui justifie de son identité, sauf à en démontrer le caractère abusif ou en cas de demandes répétées.

***En matière de santé**, en vertu de l'article L. 1111-7 du Code de la santé publique, le patient a accès aux informations formalisées qui ont contribué à l'élaboration et au suivi du diagnostic et du traitement ou d'un acte de prévention, telles que les résultats d'examen, les comptes rendus de consultation, d'intervention, d'hospitalisation, etc.*

**En pratique,** le RT doit prévoir des **procédures** pour l'exercice effectif de ce droit. Exemples :

- Prévoir la possibilité d'extraire du fichier les données relatives à la personne pour lui en adresser une copie.
- Prévoir une possibilité d'accès aux données à distance par la personne elle-même, sans que le RT n'ait à intervenir.
- Informer la personne sur les modalités d'exercice (courrier AR, adresse de la personne auprès de qui doit être formulée la demande.)
- La réponse du RT doit intervenir au plus tard dans les deux mois suivants la demande.
- Les frais de délivrance sont à la charge du demandeur (il ne peut excéder le coût de reproduction et d'envoi).

✓ **Droit de rectification** [Article 40 Loi IFL] – [Article 16 RGPD]

Ce droit permet à la personne concernée de demander au RT de compléter, rectifier ou actualiser des informations la concernant lorsque celles-ci sont erronées, inexactes, incomplètes ou périmées.

**En pratique,** le RT met à la disposition de ses utilisateurs une **adresse mail et/ou postale** pour qu'ils formulent leur demande. La rectification doit intervenir dans les deux mois de la demande.

✓ **Droit d'opposition** [Article 38 Loi IFL] – [Article 21 RGPD]

Au sens de la loi IFL, toute personne de s'opposer, pour des **motifs légitimes**, au traitement de ses données, sauf si celui-ci répond à une obligation légale (ex : services fiscaux, services de police).

Dans le RGPD, le droit d'opposition est cependant moins large, il ne peut s'appliquer que lorsque les données sont traitées à des fins de profilage, de recherche scientifique ou historique ou de statistiques, ou encore lorsque ce traitement est nécessaire à l'exécution d'une mission d'intérêt public dont est investi le RT ou aux fins des intérêts légitimes poursuivis par le RT.

➔ Cette limitation au droit d'opposition est cependant compensée par la nouvelle possibilité pour la personne concernée de **retirer son consentement au traitement à tout moment**.

Le RT a deux mois pour répondre à cette demande. Il ne pourra la refuser que s'il justifie de l'existence de motifs impérieux et légitimes primant sur les intérêts et les droits et libertés de la personne.

**En pratique,** le RT peut mettre en place les **outils de conformité** suivants :

- Sur le formulaire de collecte, une **case à cocher** permet à l'utilisateur de refuser un traitement (ex : refus de communication de ses données à des partenaires aux fins de publicité).
- Sur une application, un **réglage** permet aux utilisateurs de s'opposer à tout moment au traitement de certaines de ses données personnelles (ex : géolocalisation).
- Une **adresse mail et/ou postale** peut être communiquée aux utilisateurs pour qu'ils informent le RT qu'ils ne souhaitent plus apparaître dans un fichier.

✓ **Le droit à la limitation du traitement** [Article 40 Loi IFL] – [Article 18 RGPD]

Ce droit d'opposition particulier, permet à la personne de demander au RT un verrouillage **temporaire** de ses données : le RT ne pourra alors plus traiter les données concernées pendant un temps défini. Selon le RGPD, la limitation du traitement consiste en un marquage des données enregistrées, en vue d'empêcher leur traitement futur, sauf pour leur conservation ou consentement de la personne.

Ce verrouillage peut être demandé :

- Lorsque les données en question sont inexactes, incomplètes, équivoques, périmées ;
- Lorsque leur collecte, utilisation, communication ou conservation est interdite ;
- Lorsque les données ne sont plus nécessaires à la réalisation des finalités du traitement ;
- Pendant la période nécessaire à l'examen, par le RT, du bien-fondé d'une demande d'opposition.

**En pratique,** le RT peut mettre en place les **outils de conformité** suivants :

- Déplacer temporairement les données sélectionnées vers un autre fichier ;
- Rendre les données sélectionnées inaccessibles aux utilisateurs ;
- Retirer temporairement les données publiées d'un site internet.

## Innovations européennes

✓ **Le droit de consentir de manière explicite au traitement et de retirer son consentement à tout moment** [Articles 6.1.a et 7.3 RGPD]

**En pratique,** le RT peut mettre en place les **outils de conformité** suivants :

- Sur une application, un **réglage** permettant aux utilisateurs de retirer leur consentement à tout moment.
- Une **adresse mail et/ou postale** peut être communiquée aux utilisateurs pour avertir le RT qu'ils souhaitent retirer leur consentement.

✓ **Le droit à l'oubli numérique** [Article 17 RGPD] **et à l'effacement des données** [Article 40 Loi IFL]

La loi IFL octroie déjà à la personne concernée le droit de demander au RT l'effacement de ses données personnelles lorsqu'elles sont inexactes, incomplètes, équivoques ou périmées, lorsque la collecte de ces données est interdite, ou encore lorsque la durée de conservation nécessaire à la réalisation des finalités du traitement a été atteinte.

Le RGPD va plus loin et consacre un véritable **droit à l'oubli** permettant à la personne d'obtenir du RT dans les meilleurs délais l'effacement de données la concernant lorsque :

- Les données ne sont **plus nécessaires** au regard des finalités pour lesquelles elles sont traitées ;
- La personne **retire son consentement** au traitement ou exerce son droit d'opposition ;
- Le traitement **est illicite** ;
- L'effacement est nécessaire en vertu d'une **obligation légale**.

Le RT a également l'obligation de prendre des mesures raisonnables pour informer les autres RT qui traitent les données dont l'effacement a été demandé, de procéder eux-mêmes à l'effacement de tout lien vers ou copie de ces données.

**En pratique,** le RT peut mettre en place les **outils de conformité** suivants :

- Réglage permettant de retirer son consentement au traitement.
- Mécanisme automatique d'effacement des données en cas de retrait du consentement ou d'expiration de la durée de conservation.
- Le RT peut mettre à la disposition des utilisateurs une **adresse mail et/ou postale ou un formulaire** leur permettant de demander à ce que leurs données soient effacées.

✓ **Le droit à la portabilité des données** [Article 20 RGPD]

Nouveauté du RGPD, ce droit d'accès amélioré permet à la personne concernée de recevoir les données qu'elle a fourni au RT dans un format couramment utilisé et lisible par une machine afin qu'elle en reprenne le contrôle et puisse notamment les transmettre à un autre RT.

Le RT doit ainsi garantir l'interopérabilité du traitement notamment pour permettre à l'utilisateur d'un produit ou service de changer de prestataire/fournisseur.

Lorsque cela est techniquement possible, la personne pourra même exiger de transmettre **directement** les données en question au responsable de traitement destinataire.

> *NB : Ce droit ne peut être mis en œuvre que lorsque le traitement est fondé sur le consentement de la personne ou sur un contrat entre le RT et la personne.*

**En pratique,** le RT peut mettre en place les **outils de conformité** suivants :

- Une fonctionnalité pour **extraire les informations** pertinentes de leur base de données.
- Un outil permettant la communication sécurisée des données extraites au RT destinataire ou à la personne concernée.
- Un accord entre les RT sur la façon dont ils souhaitent réaliser cette portabilité (supports, standard, etc.).

✓ **Le droit d'être informé en cas de piratage de ses données** [Article 34 RGPD]

Ce droit est le corollaire de l'obligation du RT de notifier aux autorités et aux personnes concernées les éventuelles failles de sécurité impactant les données traitées. Il n'est cependant pas illimité puisque seules les violations de données susceptibles d'exposer les personnes à un **risque élevé** à leurs droits et libertés doivent être notifiées (Voir notre fiche « ***La sécurité et la confidentialité des données de santé, quelles obligations ?*** »).

***NB :*** **Réclamation** [Article 77 RGPD] **& Recours juridictionnel** [Article 79 RGPD]

En cas de non-respect par le RT de la règlementation européenne en vigueur, les personnes concernées disposent de droits d'action renforcés :

- La réclamation auprès d'une autorité de contrôle ;
- Le droit à un recours juridictionnel effectif contre un RT ou un sous-traitant.