



REGLEMENT EUROPEEN SUR LA PROTECTION DES DONNEES

QUELS ENJEUX POUR LE RADIOLOGUE ?

Formation présentée par Me Thibaud VIDAL – Associé du Cabinet VIDAL Avocats

Paris - Aix en Provence - Marseille



Notre objectif : votre Résultat



REGLEMENT EUROPEEN SUR LA PROTECTION DES DONNEES

QUELS ENJEUX POUR LE RADIOLOGUE ?

*Intervention de Me Thibaud VIDAL
Exerçant des missions de DPO
(délégué à la protection des données)*

Associé Fondateur

GSM : 06.66.68.68.62

Mail : tv@vidalavocats.com

Comment le RGPD modifie-t-il les obligations du radiologue en matière de protection des données ?

Comment le RGPD modifie-t-il les obligations du radiologue en matière de protection des données ?

I. La modification du système de protection des données traitées par le radiologue

A. Apports et renforcements des droits relatifs à la protection des données ayant trait à la santé

- 1 - Le renforcement des droits des patients
- 2 - Le principe de responsabilité
- 3 - *Privacy by design, Privacy by default*

B. L'articulation entre obligations légales du professionnel de santé et le RGPD

- 1- La confrontation entre l'obligation de conservation des données du radiologue et le droit à l'oubli de la personne concernée.
- 2- La dérogation à l'obligation de recherche du consentement du patient par le radiologue.

II. La mise en conformité du radiologue au règlement

A. Les étapes nécessaires à accomplir pour garantir le respect du règlement

- 1- La création d'un registre des activités de traitement
- 2- La mise en place d'un système de sécurité spécifique

B. Les contrats de service pour l'accompagnement du radiologue

- 1- La mise en place d'un délégué à la protection des données ou DPO
- 2- La mise en place éventuelle d'un contrat de sous-traitance

INTRODUCTION

INTRODUCTION - Dans quelle mesure le radiologue doit-il se sentir concerné par le règlement européen pour la protection des données ?

1. Présentation exhaustive du règlement :

- Qu'est-ce que le RGPD ?
- Date de mise en application

2. Pourquoi le radiologue doit-il se sentir particulièrement concerné par le RGPD ?

- Il traite des données personnelles quotidiennement (*données concernant la santé des personnes*).
- Il traite des données caractérisées comme « sensibles »
- Il s'expose à des sanctions importantes en cas de non-conformité au règlement.

1. Présentation du règlement



Qu'est-ce que le RGPD ?

Le RGPD (règlement général à la protection des données) est le nouveau texte de loi venant harmoniser **le système de protection des données**.

Le RGPD offre aux personnes concernées par le traitement de leurs données personnelles, une **transparence** et des **droits sur leurs données** dont ils ne bénéficiaient pas forcément.

Par ailleurs, le nouveau règlement **permet une responsabilisation accrue des responsables de traitement de données** et prévoit de lourdes sanctions.

Date d'application

Dès le 25 mai 2018 en France !

2. Pourquoi le radiologue est-il particulièrement concerné par le RGPD ? (1/3)

Le traitement de données de santé

Le radiologue dans l'exécution de ses fonctions est amené à traiter principalement des données relatives à la santé des personnes

Le RGPD apporte une définition des données de santé : « *l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée.* »

Il s'agit donc des informations collectées :

- soit lors de l'inscription de la personne concernée dans le service de soin;
- soit des informations collectées lors des prestations de soin.

2. Pourquoi le radiologue est-il particulièrement concerné par le RGPD ? (2/3)

Le traitement de données dites « sensibles »

Les données de santé sont considérées comme des données sensibles. Du fait de leur statut, le traitement de ces données est par nature illicite.

Toutefois, une dérogation est délivrée par l'article 9.3 du RGPD si elles sont traitées par un professionnel de santé soumis à obligation de secret professionnel.

Le radiologue traite donc ces données en toute légalité.

Elles doivent cependant faire l'objet d'une protection spécifique car le contexte dans lequel elles sont traitées peut engendrer des risques pour les droits et libertés des personnes concernées.

2. Pourquoi le radiologue est-il particulièrement concerné par le RGPD ? (3/3)

Les sanctions applicables :

Au même titre que toute entreprise responsable de traitement de données à caractère personnel, les radiologues sont susceptibles de faire l'objet de sanction par la CNIL en cas de manquement aux obligations de conformité du règlement :

- **Infractions graves : 4% du CA ou 4 millions d'euros**
- **Infractions légères : 2% du CA ou 2 millions d'euros**

Le montant de l'amende devra être effectif, proportionné et dissuasif et à ce titre, il est susceptible d'être réajusté par l'autorité nationale de contrôle.

Ces amendes font suite à une procédure de contrôle et mises en demeure et de l'intention de frauder ou non par le responsable du traitement.

PARTIE I.A

La modification du système de protection des données traitées par le radiologue

Apports et renforcements des droits relatifs à la protection des données ayant trait à la santé

I.A - Apports et renforcements des droits relatifs à la protection des données ayant trait à la santé (1/2)

1. Le renforcement des droits des patients

Le règlement européen vient renforcer ces droits par le biais de nouvelles dispositions et l'apparition de sanctions plus importantes pour les professionnels qui ne les respecteraient pas.

- **Le droit d'accès aux données collectées** : Le patient a le droit d'obtenir de la part du radiologue la confirmation que des données le concernant sont ou ne sont pas traitées, et, si elles le sont, peut demander au professionnel de santé un accès auxdites données.
- **Le droit de rectification** : Le patient, lorsqu'il estime que les informations personnelles le concernant n'ont pas été délivrées avec exactitude peut demander au radiologue que ce dernier les rectifie.
- **Le droit à la portabilité des données (nouveau)** : par le biais de ce droit, chaque patient est dans la mesure de demande à un radiologue de transférer ses données à l'un de ses confrères.
- **Droit à la transparence**: Le radiologue prend des mesures afin de fournir toutes les informations concernant le traitement des données et notamment les droits dont bénéficient leurs patients. Ces informations sont délivrées de manière « claire » et « accessible » afin que notamment, les enfants eux-mêmes puissent comprendre.

I.A - Apports et renforcements des droits relatifs à la protection des données ayant trait à la santé (2/2)

2. Principe de Responsabilité renforcée (nouveau)

Un des principaux objectifs du règlement est de créer une responsabilisation accrue du responsable du traitement.

A ce titre, le radiologue se doit de créer un contrôle en interne des données qu'il traite.

L'autorité de contrôle (la CNIL pour tous les radiologues exerçant en France), sera à même d'exercer des contrôles à tout moment afin de vérifier la conformité du professionnel au Règlement.

Si le professionnel de santé n'est pas en conformité avec le règlement au jour du contrôle, il s'expose à faire l'objet d'une des sanctions déjà évoquées.

Le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au règlement.

3. Privacy by design, Privacy by default (nouveau)

Privacy by design : Obligation de mettre en place des mesures techniques et opérationnelles afin de prévenir tout risque.

Privacy by default : Obligation de garantir, par défaut, le meilleur système de protection des données.

PARTIE I.B

Le RGPD vient modifier le système de protection des données sensibles traitées par le radiologue.

L'articulation entre obligations légales du professionnel de santé et le RGPD

I.B - L'articulation entre les obligations légales du radiologue et le RGPD (1/2)

1. Confrontation entre obligation de conservation des données du radiologue et le droit à l'oubli de la personne concernée.

RAPPEL : Au titre de ses obligations légales, le professionnel de santé respecte une durée de conservation des données médicales de 10 ans.

Les clichés de même que les comptes rendus radios font partie intégrante du dossier médical.

Le règlement prévoit un droit à l'oubli (effacement des données) profitant à la personne concernée par le traitement de données.

Il existe toutefois des dérogations à cette disposition

Aux termes de cet article, le radiologue pourra passer outre cette disposition au titre du respect des obligations légales délivrées par le code de la santé publique en la matière.

La conservation des données médicales par le radiologue est donc justifiée.

I.B - L'articulation entre les obligations légales du radiologue et le RGPD (2/2)

2. La dérogation à l'obligation de recherche du consentement du patient par le radiologue.

De manière générale, le responsable du traitement doit rechercher le consentement de la personne concernée pour que le traitement soit licite.

Deux cas de figure se présentent au radiologue dans le cadre de ses fonctions :

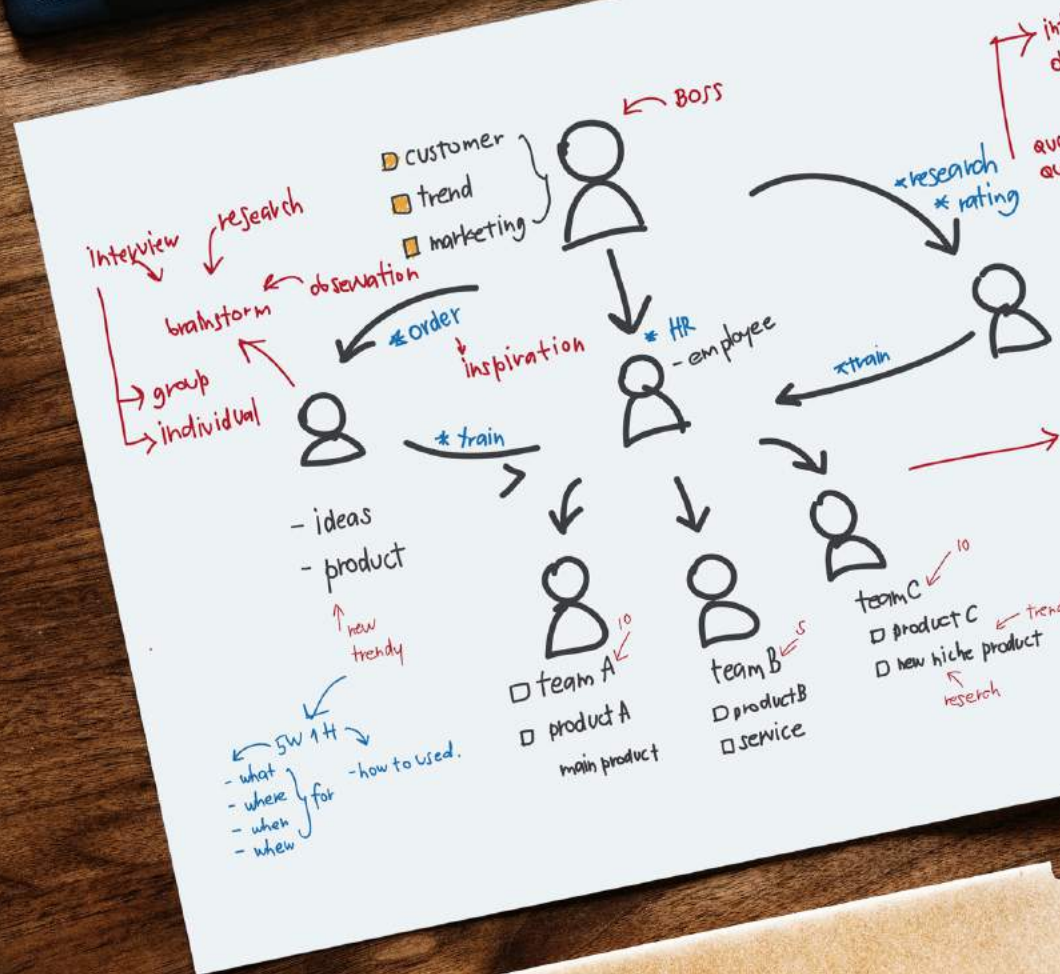
- En présence de données relatives à la santé : du fait de son obligation au secret professionnel, le radiologue **peut passer outre le consentement de la personne** pour traiter des données.
- En présence de données qui ne sont pas relatives à la santé : le consentement doit être relevé auprès de la personne (exemple; orientation sexuelle ...), sauf si il est nécessaire aux fins des intérêts légitimes poursuivis par le radiologue.

Conclusion: le radiologue peut se passer du consentement de la personne concernée et n'a pas vocation à soumettre un formulaire pour le traitement des données au patient.

Ce que le radiologue doit **retenir** :

1. Les données sensibles doivent faire l'objet d'une protection particulière.
2. Le radiologue doit mettre en place un système de sécurité des données formalisé et opérationnel.
3. Le simple fait de ne pas être en conformité constitue une infraction au regard de l'autorité nationale de contrôle (RGPD)

Dans moins de 2 mois,
votre système de sécurité des données ne doit plus
comporter de failles et doit répondre à toutes les
exigences du règlement.



PARTIE II.A

Vers une mise en conformité du radiologue au RGPD

*Les étapes nécessaires pour
garantir le respect du règlement*



II.A - Les étapes nécessaires à accomplir pour garantir le respect du règlement (1/2)

1. Etablissement d'un registre des données (pas de forme particulière)

- Pour cartographier vos données et leur traitement: voir <https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles>)
- Le registre des données peut être un tableau Excel informatique: voir le modèle de registre sur le lien précédent.

En qualité de responsable du traitement, le radiologue doit veiller à établir un registre comprenant :

- **Le nom et les coordonnées du ou des radiologues responsable(s) du traitement des données** (représentant légal et le cas échéant le délégué à la protection des données).
- **Les finalités du traitement** : traitement médical du patient
- **Une description des catégories de personnes concernées** : (patients, médecins, fournisseurs) et des catégories de données à caractère personnel (identité, des données de localisation, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale; santé)
- **Les flux**: les catégories de destinataires auxquels les données ont été ou seront communiquées (patients, médecins)
- **Une description générale des mesures de sécurité techniques et organisationnelles mises en place. (identifier les acteurs internes ou externes**: prestataires et décrire précisément le parcours des données et leur sécurisation).
- **Les délais prévus pour l'effacement des différentes catégories de données** (se référer aux obligations de conservation prévues par l'article L1142-28 du CSP) (10 années)

II.A - Les étapes nécessaires à accomplir pour garantir le respect du règlement (2/2)

2. Etablissement d'un système de sécurité spécifique

Du fait de la sensibilité des données qu'il traite, le radiologue va voir son obligation de sécurité renforcée. Il sera donc tout particulièrement concerné par la mise en place d'un système de sécurité adéquat afin de protéger les données récupérées auprès des patients.

Cette obligation de sécurité passe par la mise en œuvre de « mesures techniques et organisationnelles appropriées » évoquées à l'article 32 du RGPD. A titre d'exemple il peut être conseillé au radiologue de mettre en œuvre :

- Un mécanisme d'anonymisation ou de chiffrement des données de santé récupérées;
- Des moyens permettant de garantir l'entière confidentialité et intégrité des données (ex : pouvoir contrôler où, quand et par qui les données ont été consultées);
- Des moyens permettant de rendre à nouveau disponibles les données récupérées en cas d'incident;
- La mise en place d'une procédure permettant d'analyser l'efficacité de toutes ces mesures de sécurité des données.

En cas de violation du système de sécurité, et aux termes des articles 33 et 34 du règlement, le radiologue doit en faire état à l'autorité de contrôle (CNIL) et aux patients concernés.

PARTIE II.B

Vers une mise en conformité du radiologue au RGPD

*Les contrats de services en vue de
l'accompagnement du radiologue*



II.B - Les contrats de services en vue de l'accompagnement du radiologue

1. La nomination d'un délégué à la protection des données ou DPO

La nomination d'un délégué à la protection des données évoquée à l'article 37 du RGPD est obligatoire dans des cas de traitement de données à grande échelle ce qui ne correspond pas au Radiologue.

Du fait de la sensibilité des données qu'il traite et du travail spécifique que représente la mise en conformité au règlement, il est très fortement conseillé au radiologue de désigner un DPO.

Ce dernier aura un rôle de conseil en interne, en soutenant le radiologue dans sa démarche de mise en conformité au règlement, et en externe pour communiquer avec l'autorité de contrôle. En toute logique, il est possible de faire appel à un DPO commun pour plusieurs radiologues par le biais d'un contrat de service.

En vertu de l'article 37 du règlement, le délégué à la protection des données est notamment désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données.

II.B - Les contrats de services en vue de l'accompagnement du radiologue

2. La mise en place éventuelle d'un contrat de sous-traitance

Est ici évoqué le cas de figure où le radiologue fait appel à un sous-traitant dans le cadre de ses fonctions. Le sous-traitant sera lui-même amené à traiter les données sensibles conservées par le radiologue.

Ex type : *Le radiologue fait appel à une société d'archivage afin de stocker les données qu'il collecte et envers lesquels il dispose d'une obligation de conservation. Ce sous-traitant aura donc à respecter les règles de conservation et de protection des données.*

Les contrats de sous-traitance (nécessaires pour encadrer ce type de relations) sont très strictement encadrés par le RGPD qui leur consacre l'intégralité de l'article 28 du règlement.

Le radiologue devra notamment s'assurer que le sous-traitant dispose de « garanties suffisantes » pour répondre à la nécessaire sécurité des données traitées.

Au même titre que le radiologue, tout sous-traitant sera responsable du respect du règlement européen à la protection des données.

En définitive :

Ce qu'il est important de retenir en vue pour/après le 25 Mai 2018

- Le RGPD apporte de nouvelles obligations auxquelles le radiologue doit impérativement se conformer.
- Les sanctions prévues en cas de non-respect du règlement sont applicables au 25 Mai 2018 - Une période de tolérance sera observée si il apparaît que le radiologue est entré dans une démarche de mise en conformité.
- Afin de se mettre en conformité au règlement le radiologue devra :
 - cartographier les données et créer un registre des données intégrant les informations obligatoires,
 - Mettre en place un système de sécurité de données renforcé (anonymisation ...),
- Le radiologue pourra se faire assister par un DPO et conclure des contrats d'assistance

Notre cœur de clientèle

PROFESSIONNELS DE SANTE - PHARMACIES - BIOLOGIE MEDICALE
CLINIQUES - SYNDICATS CATEGORIELS



Nos compétences

DELEGUE A LA PROTECTION DES DONNEES (DPO)
ACCOMPAGNEMENT CNIL

DEFENSE DES PROFESSIONNELS DE SANTE:
CONTRÔLE D'ACTIVITE - INDU (LITIGES AVEC
ASSURANCE MALADIE)
DISCIPLINAIRES
RESTRUCTURATION JURIDIQUE DE GROUPES ET
DROIT DES SOCIETES
CONTENTIEUX COMMERCIAL ET IMMOBILIER



Notre équipe vous accompagne dans tous vos projets

La philosophie du cabinet VIDAL Avocats : apporter du résultat et de la plus-value à ses clients.

L'engagement : mettre tous les moyens en œuvre pour atteindre l'objectif fixé en proposant des solutions innovantes et concrètes.



REGLEMENT EUROPEEN SUR LA PROTECTION DES DONNEES

QUELS ENJEUX POUR LE RADIOLOGUE ?

Formation présentée en partenariat entre l'association FORCO FMC et le cabinet VIDAL Avocats

