https://ressources.anap.fr/numerique/publication/2408-en-tant-que-structure-medico-sociale-suis-je-concerne-par-le-rgpd

Avis d'experts

En tant que structure sanitaire ou médico-sociale, suis-je concerné par le RGPD ?

Ce document s'adresse aux directeurs de structures sanitaires ou médico-sociales afin de leur permettre d'identifier :

- Les enjeux de la protection des données à caractère personnel ;
- Les actions à mettre en œuvre pour se conformer aux dispositions du règlement RGPD ;
- Les sources d'informations pour aller plus loin.

Cet avis d'expert a été rédigé par Dominique LORIOUX, directeur de la clinique La Parisière, expert numérique en santé à l'ANAP.

Le RGPD, le Règlement général sur la protection des données, est le règlement européen qui définit le cadre juridique applicable en matière de protection des données personnelles.

Que l'on soit professionnel du secteur privé, du secteur public, du secteur associatif, dès lors que l'on traite des données à caractère personnel, il convient de respecter les dispositions du RGPD.

Qu'est-ce qu'une donnée à caractère personnel ?

Le règlement européen définit une donnée à caractère personnel. Il s'agit d'une information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement[1].

Par exemple : un nom, une photo, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc.

Des informations qui, même très indirectement, permettent d'identifier une personne physique sont des données à caractère personnel, peu importe que ces informations soient confidentielles ou publiques.

De surcroit, dans le cadre de leurs missions, les structures médico-sociales sont amenées à traiter des données «sensibles» telles que des données de santé ou des appréciations sur les difficultés sociales des personnes. Le RGPD prévoit des règles spécifiques pour le traitement de ces données.

La notion large de traitement de données couvre tous les secteurs, y compris le secteur médico-social

Un «traitement de données personnelles» est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement)[2].

Cette notion de traitement est définie de manière très large dans le règlement européen.

Il peut s'agir d'un progiciel évolué pour gérer les ressources humaines ou la paie par exemple, d'un système de vidéosurveillance, d'un tableur dans un outil de bureautique standard (liste des adhérents à d'une association, liste des clients d'Établissement et service d'aide par le travail [ESAT], etc.)

Mais, cela peut aussi être un simple fichier papier organisé selon un plan de classement, des formulaires papier nominatifs ou des dossiers de candidatures classés par ordre alphabétique ou chronologique sont aussi des traitements de données personnelles.

Dès lors que l'outil permet de classer de l'information, même de manière simple, c'est un traitement de données.

A priori, l'ensemble de structures médico-sociales traite des données personnelles de leurs salariés, de leurs bénévoles et/ou de leurs bénéficiaires et, par conséquent, est soumis au RGPD et doit appliquer les dispositions prévues par le règlement.

En 2016, la CNIL avait pris en compte les spécificités du secteur médico-social en créant un régime d'autorisations uniques pour simplifier les formalités des organismes, œuvrant dans le champ de l'action sociale et médico-sociale. Avec l'entrée en application du RGPD, les autorisations uniques n'ont plus de valeur juridique. Le règlement européen repose désormais sur une logique de conformité, dont les acteurs sont responsables.

Dans ce contexte et dans l'attente de la production de référentiels RGPD, la CNIL a maintenu, sur son site internet, l'accès aux anciens textes afin de permettre aux responsables de traitement d'orienter leurs actions de mise en conformité au RGPD[3].

Principales dispositions du RGPD à mettre en œuvre

1. Documenter sa conformité

Chaque responsable de structure doit s'organiser pour vérifier qu'en interne, des procédures, des règles, ont été mises en œuvre afin que les données personnelles soient collectées et traitées conformément au cadre réglementaire.

En pratique, l'obligation de documenter va se traduire par la constitution d'un classeur et/ou d'un répertoire numérique dans lequel la structure va colliger toutes les diligences accomplies pour se conformer aux dispositions du RGPD. On y trouvera le registre des traitements de données, les analyses d'impact (analyse de risques), les procédures d'utilisation des outils informatiques, les actions mises en œuvre pour sécuriser les données, les contrats de prestations informatiques...

Dans tous les cas, le responsable de traitement des données doit mettre en place un mécanisme de définition des niveaux d'habilitation des différents utilisateurs et des moyens de contrôle des permissions d'accès aux données.

2. Information et Consentement des personnes pour le traitement des données personnelles

En principe, les professionnels des structures médico-sociales n'ont pas besoin de recueillir le consentement individuel des personnes pour collecter et conserver les données personnelles les concernant, dans la mesure où leur collecte et leur conservation sont nécessaires à la prise en charge sanitaire ou sociale des personnes concernées.

Néanmoins, il est important de préciser que ce consentement implicite principe ne s'applique qu'aux données utiles à la prise en charge de la personne. Les données doivent être adéquates, pertinentes et limitées à ce qui est strictement nécessaire au regard des finalités pour lesquelles elles sont traitées.

À défaut, il est nécessaire de recueillir le consentement exprès de la personne concernée ou celui de son représentant légal.

Dans tous les cas, les professionnels ont l'obligation de délivrer une information portant sur le traitement de données réalisé pour la prise en charge des personnes. À ce sujet, les directives de la CNIL, de l'ancien régime d'autorisations uniques, orientent sur ce qu'il convient d'effectuer :

« Le responsable du traitement doit informer les personnes concernées par le ou les traitements mis en œuvre par tout moyen approprié, dans un langage compréhensible et selon des modalités appropriées et adaptées à leur état.

L'information doit notamment porter sur l'identité du responsable de traitement, la finalité poursuivie par le traitement, les destinataires des données et les droits des personnes (droits d'opposition pour motifs légitimes, d'accès et de rectification).

Les personnes sont également informées du caractère obligatoire ou facultatif des réponses, ainsi que des conséquences éventuelles, à leur égard, d'un défaut de réponse ou de l'exercice de leur droit d'opposition.

Cette information doit notamment figurer sur les formulaires de collecte destinés aux personnes auprès desquelles les données sont collectées.

Les droits d'opposition, pour motifs légitimes, d'accès et de rectification s'exercent directement auprès du ou des services que le responsable de traitement doit impérativement désigner. » (2)

3. Obligation de notification des violations de données personnelles

L'article 33 du RGPD stipule qu'en cas de violation de données à caractère personnel, le responsable du traitement doit notifier la violation à la CNIL dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Le responsable de traitement doit également informer les personnes concernées, lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés, sous-entendu, lorsqu'il y a un vrai risque de réutilisation des informations détournées.

Il est conseillé de rédiger une procédure de notification des violations de données personnelles.

4. Désigner un Délégué à la Protection des Données (DPD ou, en anglais DPO, Data Protection Officer)

Le RGPD prévoit les cas où la désignation d'un Délégué à la Protection des Données est obligatoire.

Dans tous les cas, cette désignation est recommandée pour toutes les structures qui traitent des données sensibles. En effet, la mise en conformité au RGPD est un travail important qui nécessite d'être piloté par une personne spécifiquement formée qui va avoir un rôle de chef d'orchestre de la mise en conformité « Informatique et libertés ».

Le DPO est chargé notamment :

- d'informer et de conseiller le responsable de traitement et ses collaborateurs,
- documenter ou s'assurer que sont documentées (en lien avec le RSSI...) les politiques et les actions d'amélioration concernant la sécurité des traitements,
- de contrôler le respect du règlement et du droit national en matière de protection des données,
- d'être son point de contact de la CNIL.

Dans la pratique, le délégué est souvent chargé de constituer et de mettre à jour le registre des traitements.

Le DPO peut être interne ou externe, c'est-à-dire qu'il peut être salarié de la structure qui l'emploie ou être consultant externe. La désignation du délégué à la protection des données doit être effectuée officiellement auprès de la CNIL.

Conclusion

Les structures du secteur médico-social sont concernées par le RGPD au même titre que les autres établissements publics ou privés du secteur sanitaire.

Le RGPD a fortement accru le pouvoir de contrôle et de sanction de la CNIL qui peut désormais prononcer des amendes jusqu'à 20 millions d'euros, ou 4 % du chiffre d'affaires mondial d'une organisation. De plus, le responsable de traitement engage sa responsabilité sur le plan pénal. Les peines encourues vont de 1500 € d'amende jusqu'à 300 000 € d'amende et 5 ans d'emprisonnement.

Dès lors, le risque de non-conformité est nettement plus important qu'il ne l'était avant la date d'application du RGPD. Les responsables du secteur médico-social, qui traitent des données particulièrement sensibles, doivent prouver à tout moment leur bonne foi et leur engagement dans la démarche de conformité au RGPD.

Pour en savoir plus, consulter le site de la CNIL qui propose notamment un ensemble d'outils de mise en conformité avec le RGPD, en particulier une méthode en 6 étapes et un service d'information par téléphone pour les professionnels.

1. Site la CNIL www.cnil.fr « Comprendre le RGPD ».?
2. Site la CNIL www.cnil.fr « Comprendre le RGPD ».?
3. Site la CNIL www.cnil.fr « Des formalités simplifiées pour la sphère sociale et médico-sociale ».?

Ressources associées

KIT DE PRODUCTIONS
Kit RGPD

PERSONNE RESSOURCE

Wilfrid BENARD

PERSONNE RESSOURCE
Elise MORICHON

PERSONNE RESSOURCE
Gilles HERENGT

Glossaire

ANAP
CNIL
DPD
notification
personne
RGPD
risque