Politique de protection des données à caractère personnel

Politique de protection des données à caractère personnel

Le respect de la vie privée et de la protection des données à caractère personnel constitue un facteur de confiance, et une valeur à laquelle tient particulièrement AURAL, en s'attachant également au respect des libertés et droits fondamentaux de chacun.

La présente politique de protection des données à caractère personnel témoigne des engagements mis en œuvre AURAL dans le cadre de ses activités de dialyse, d'Hospitalisation à domicile (HAD), et de formation pour une utilisation responsable des données personnelles. Cette politique est en lien étroit avec la Politique de sécurité du système d'information d'AURAL.

Article 1 – Le traitement des données à caractère personnel

AURAL respecte pour le traitement des données à caractère personnel les principes et obligations relatives à la protection des données à caractère personnel pour les patients pris en charge, les partenaires et sous-traitant, ainsi que ses salariés, conformément au Règlement (UE) 2016/179 relatif à la protection des données à caractère personnel, ainsi qu'à la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et à la Loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique.

Article 1.1 – le domaine

Le traitement de données, selon le Règlement européen général relatif à la protection des données à caractère personnel « RGPD » concerne le traitement de données à caractère personnel automatisé en tout ou en partie, ainsi que le traitement non automatisé, de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Avec le RGPD, le législateur européen souhaite renforcer les droits des personnes, responsabiliser les acteurs traitant des données, renforcer la coopération entre les autorités de protection des données. Le traitement des données personnelles n'est pas interdit, mais est encadré pour éviter toutes dérives.

Article1.2 – les données personnelles

Une donnée à caractère personnel est définie comme toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement. C'est-à-dire : le nom, le prénom, la date de naissance, l'adresse postale ou électronique, la photo, l'adresse IP, le numéro de sécurité sociale, le numéro de téléphone, les habitudes de consommation etc.

Parmi les données personnelles, il y a la catégorie des données dites « sensibles ». Celles-ci regroupent toutes les données personnelles concernant l'origine raciale/ethnique, les opinions politiques/religieuses, l'appartenance syndicale, les données génétiques/biométriques, les données de santé, les données concernant la vie /orientation sexuelle.
Les données personnelles sensibles doivent donc être protégées par AURAL. Ce sont précisément les données à caractère personnel relative à la santé physique ou mentale d'une personne, y compris la prestation de services de soins de santé, qui relève de l'information sur l'état de santé de cette personne.

Concernant le traitement des données, il s'agit de toute opération ou tout ensemble d'opération effectuées ou non à l'aide de procédés automatisés appliqués à des données. C'est-à-dire les

Politique de protection des données à caractère personnel

fichiers de patients/salariés, vidéosurveillance, code d'accès, annuaire interne, logs de serveurs etc.

Article 2 – Le délégué à la protection des données (DPO)

Afin de préserver la vie privée et la protection des données à caractère personnel de tous, AURAL avait désigné un Correspondant Informatique et Libertés (CIL), qui exerce ses missions pour l'ensemble d'AURAL.
Suite aux évolutions législatives, et par volonté de se mettre en conformité avec le règlement européen, AURAL a désigné depuis mars 2018 une déléguée à la protection des données personnelles (ou DPO, c'est-à-dire Data Protection Officer). Un plan d'action a été rédigé pour le déploiement des obligations du RGPD à AURAL.

Un DPO est un gage de confiance et de transparence. Il est un interlocuteur spécialisé dans la protection des données personnelles, chargé de veiller à la préservation de la vie privée et à la bonne application des règles de protection des données personnelles, ainsi qu'un interlocuteur privilégié de la Commission Nationale de l'Informatique et des Libertés (CNIL), et de toutes personnes concernées par une collecte ou un traitement de données à caractère personnel.

Il a pour rôles et missions de/d':

- Informer, conseiller, sensibiliser, et former le responsable du traitement et leurs employés
- Contrôler le respect du règlement et du droit national en matière de protection des données
- Conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données personnelles
- Coopérer avec l'autorité de contrôle (CNIL), et les services dédiés
- Tenir un registre des traitements
- Auditer la conformité
- Assurer la protection des données dans tout projet et collaborer avec les relais
- Faire appliquer les politiques et procédures
- Tenir une documentation prouvant la conformité
- Mettre en place des mesures de sécurité adaptées au risque
- Intervenir en cas d'incident de sécurité pour les données

La DPO d'AURAL est joignable par courrier au : 5, Rue Henri Bergson - CS 30038 - 67087 STRASBOURG Cedex, ou par courriel à DPO@aural.asso.fr.

Article 3 - Registre du traitement des données :

Avec les évolutions législatives, le régime de déclaration préalable auprès de la CNIL pour les traitements de données a évolué vers une obligation de constituer un registre regroupant tous les types de traitement de données personnelles réalisés par AURAL. Ce registre permet à AURAL de communiquer en toute transparence sur les données traitées, ainsi que sur leur utilisation. Ce registre doit être accessible aux salariés et aux patients ou à nos partenaires sur demande. Une version papier et informatique du registre est disponible auprès du DPO. Une cartographie des traitements a préalablement été rédigée, et figure dans Ennov (LIS/014).

Politique de protection des données à caractère personnel

Article 4 – Principes et droits applicables à la protection des données personnelles à AURAL

AURAL traite les données personnelles dans le respect des lois et réglementations en vigueur, et notamment du Règlement (UE) 2016/179 relatif à la protection des données à caractère personnel, ainsi qu'à la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et à la Loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique.
Le traitement des données tel que prévu par le Règlement européen doit répondre à 5 grands principes :

- la légitimité du traitement
- la transparence du traitement,
- la proportion et la pertinence du traitement,
- une durée de conservation limitée,
- la confidentialité et la sécurité des données.

Les personnes concernées ont également des droits concernant leurs données, qui sont respectées à AURAL.

Article 4.1- *Finalité déterminée, explicite et légitime du traitement :*

Les données personnelles sont collectées pour des objectifs précis (finalités), portés à la connaissance des personnes concernées. Ces données ne peuvent être utilisées ultérieurement de manière incompatible avec ces finalités. L'ensemble des finalités de traitement des données à caractère personnel d'AURAL est regroupé dans le registre des traitements.

Ces données sont collectées loyalement : aucune collecte n'est effectuée à l'insu des personnes et sans qu'elles en soient informées.

En effet, des documents de consentement au traitement de leurs données personnelles sont remis aux patients de Dialyse et d'HAD dès leur admission (Le document pour la dialyse se nomme « Consentement des patients au traitement de leurs données à caractère personnel »).

Les salariés d'AURAL reçoivent une note d'information sur le traitement de leurs données personnelles, ainsi que sur le système de badge qui permet de déterminer le temps de travail effectif lors de leur premier jour à AURAL.

Les partenaires d'AURAL (notamment les professionnels libéraux, stagiaires ou formateurs de l'organisme de formation, ou encore les répondants à un marché public) reçoivent également une information sur le traitement de leurs données personnelles.

Ces documents permettent aux personnes concernées d'avoir une information détaillées sur les finalités, les destinataires des données, la durée de conservation, leurs droits et leurs moyens de contact de la DPO d'AURAL.

Article 4.2 - *Proportion et pertinence des données collectées :*

Les données personnelles collectées sont strictement nécessaires à l'objectif poursuivi par la collecte. AURAL s'attache à minimiser les données collectées, à les tenir exactes et à jour en facilitant les droits des personnes concernées.

Politique de protection des données à caractère personnel

Article 4.3 - *Durée de conservation limitée des données à caractère personnel :*

Les données à caractère personnel sont conservées pendant une durée limitée qui n'excède pas la durée nécessaire aux finalités de collecte.
Les délais de conservation des données sont portés à la connaissance des personnes, et varient selon la nature des données, la finalité des traitements, ou les exigences légales ou réglementaires. En effet, pour les durées de conservations, AURAL est notamment soumis au Code de la santé publique, au Code de la sécurité sociale, ou encore au Code du travail.

Article 4.4 - *Confidentialité / Sécurité des données :*

Concernant la sécurité informatique des données personnelles traitées, une Politique de Protection des Systèmes d'Information (PSSI), en étroit lien avec la politique de protection des données, est mise en œuvre, adaptée à la nature des données traitées et aux activités de l'association. Elle est disponible dans Ennov (POL/005), et mise à jour régulièrement.
Des mesures de sécurité physiques, logiques et organisationnelles appropriées sont prévues pour garantir la confidentialité des données, et notamment éviter tout accès non autorisé. Par exemple, dans le cadre des générateurs de dialyse, certains sont dit « connectés » ; le prestataire réalise la maintenance du logiciel des générateurs dans un pays hors-Union européenne, et cela figure dans le document de consentement spécifique remis aux patients. De plus, un contrat d'hébergeur de données de santé a été signé avec le prestataire.

AURAL exige également de tout sous-traitant qu'il présente des garanties appropriées pour assurer la sécurité et la confidentialité des données personnelles. Une Charte d'accès et d'usage du système d'information AURAL par un tiers existe depuis 2017, et doit être signée par chaque intervenant extérieur à AURAL.

Des données à caractère personnel peuvent faire l'objet de transferts vers des pays situés dans l'Union Européenne ou hors de l'Union Européenne. Si tel était le cas, les personnes concernées en sont précisément informées, et des mesures spécifiques sont prises pour encadrer ces transferts.

Article 4.5 - *Droits des personnes :*

Tous les moyens nécessaires à garantir l'effectivité des droits des personnes sur leurs données personnelles sont mis en œuvre.
Une information claire et complète sur les traitements de données mis en œuvre, facilement accessible et compréhensible par tous.
Un accès facilité aux informations : toute personne dispose de droits sur les données la concernant, qu'elle peut exercer à tout moment et gratuitement, en justifiant de son identité. Ainsi, les personnes peuvent accéder à leurs données personnelles, et dans certains cas les faire rectifier, supprimer ou s'opposer à leur traitement.
L'exercice de ces droits (droit d'accès, droit de rectification, droit à l'effacement/oubli, droit d'opposition, droit à la limitation du traitement, droit à la portabilité, directive anticipées concernant les données personnelles) est facilité en remplissant un formulaire de demande, mais aussi grâce aux demandes par courriel ou possibles par tout autre moyen (courrier etc.) selon les modalités portées à la connaissance des personnes. Ces demandes sont adressées au DPO.

Politique de protection des données à caractère personnel

Le délai de réponse aux demandes concernant les données à caractère personnel est d'un mois, ou de deux, compte-tenu de la complexité de la demande ou du nombre de demande.

Une procédure décrit la gestion des demandes d'exercice des droits d'accès aux données personnelles, et une autre procédure décrit la gestion des violations de données personnelles possédées par AURAL sur les patients, salariés ou toutes autres personnes en lien avec AURAL

Article 5 - Suivi de la Politique de Protection des Données Personnelles

Cette politique, accessible à tous sur le site internet d'AURAL et dans Ennov pour les salariés, est actualisée régulièrement par notre DPO pour prendre en compte les évolutions législatives et réglementaires, et tout changement dans l'organisation ou les activités d'AURAL.

Politique de protection des données à caractère personnel

Documents de référence :

- ✓ Règlement (UE) 2016/179 relatif à la protection des données à caractère personnel,
- ✓ Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles,
- ✓ Loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés,
- ✓ Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

Documents associés : CONS/044 - 01 - Note d'information sur la protection des données personnelles des salariés, CONS/045 - 01 - Note d'information sur la protection des données personnelles des candidats, FORM/074 - 08 - Acceptation du patient, FORM/482 - 02 - Consentement des patients en dialyse au traitement de leurs données personnelles et de santé, FORM/487 - 01 - Demande d'accès aux données personnelles, LIS/014 - 01 - Cartographie des traitements des données personnelles à AURAL, POL/005 - 01 - Politique de sécurité du système d'information

Définitions et abréviations :

- ✓ **Traitement de données à caractère personnel** : toute opération ou tout ensemble d'opération effectuées ou non à l'aide de procédés automatisés appliqués à des données. Ex : fichiers patients/salariés, vidéosurveillance, code d'accès, annuaire interne, logs de serveurs…
- ✓ **Données à caractère personnel** : toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement. Ex : nom, prénom; date de naissance, adresse postale ou électronique, photo, adresse IP, numéro de sécu, numéro de téléphone, habitudes de consommation …

- ✓ **Données sensibles** : origine raciale/ethnique, opinions politiques/religieuses, appartenance syndicale, données génétiques/biométriques, données de santé, données concernant la vie /orientation sexuelle.

- ✓ **Violation de données à caractère personnel** : vous avez mis en œuvre un traitement de données personnelles. Ces données ont fait l'objet d'une violation (faille de sécurité, fuite de données, perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite).

- ✓ **DPO :** Data Protection Officer ou en français délégué à la protection des données Personnelles

- ✓ **CNIL** : Commission nationale de l'informatique et des libertés ; Elle a pour mission générale de veiller à ce que l'informatique ne porte atteinte ni au droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Dans l'univers numérique, la CNIL est le régulateur des données personnelles.

Politique de protection des données à caractère personnel

- ✓ **Responsable de traitement de données** : est en principe la personne, l'autorité publique, la société ou l'organisme qui détermine les finalités et les moyens de ce fichier, qui décide de sa création. En pratique, il s'agit généralement de la personne morale (entreprise, collectivité, etc.) incarnée par son représentant légal (président, maire, etc.). C'est lui qui doit accomplir, lorsque cela est nécessaire, les formalités déclaratives auprès de la CNIL.

Signataires :

Rédaction : Alexandra BARBARA (Chargée des affaires générales)
Vérification service qualité : Sophie QUERE (Responsable QHSE)
Vérification : Rebecca DANTONIO (Directrice adjointe), Pierre SCHAAL (Directeur)
Approbation :