Annexe 1 : Le traitement des données par un produit innovant

LE PRODUIT INNOVANT TRAITE DES DONNÉES À CARACTÈRE PERSONNEL

Définition des données à caractère personnel

Les données à caractère personnel présentent **deux spécificités**:

- **Leur fonction:**
Ce sont des informations permettant d'identifier une personne physique c'est-à-dire de la distinguer d'autrui.

- **Leur objet:**
Ce sont des informations directement nominatives (noms) ou indirectement nominatives (adresse IP) relatives à une personne physique.

> *Loi « Informatique et libertés », art. 2 modifié*

Définition d'un traitement

Toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé: collecte, enregistrement, organisation, conservation, adaptation ou modification, extraction, consultation, utilisation, communication par transmission, diffusion ou tout autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction.

=> Loi « Informatique et libertés », art. 2 modifié

Définition du responsable de traitement

Sauf désignation expresse par des dispositions législatives ou règlementaires, le responsable de traitement est la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.

=> Loi « Informatique et libertés », art. 3-I modifié

Définition de la finalité d'un traitement de donnée de santé

Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime.

> *Loi « Informatique et libertés », art. 6 al 2 modifié*

Votre produit innovant traite des données à caractère personnel

Vos obligations en tant que responsable de traitement

Une obligation procédurale:
- Vous devez préalablement déclarer vos traitements auprès de la CNIL.
- En fonction de la finalité du traitement, vous devez choisir un des six régimes déclaratifs précisés dans la loi « Informatique et libertés ».

Ex : régime de la déclaration normale pour un fichier concernant la vie privée ou les libertés individuelles des personnes (fichiers de clients).

=> Loi « Informatique et Libertés », art. 23, 24,25, 26 et 27 modifiés

Trois obligations spécifiques:

1- Obligation d'information :
Vous devez délivrer 8 éléments cumulatifs à la personne dont les données sont collectées. (ex : informer la personne sur les destinataires des données).

2- Obligation de sécurité:
Vous devez préserver la sécurité des données et éviter leur divulgation à des tiers par l'adoption de mesures physiques et/ou techniques appropriées.

3- Durée de conservation limitée des données à caractère personnel:
Vous devez définir une durée à l'issue de laquelle les données seront détruites ou archivées. Les données ne peuvent être conservées au-delà de cette durée qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques.

> *Loi « Informatique et Libertés », art. 32-I, 34 et 36 modifiés*

Le respect des droits de la personne

La personne dont vous collectez et traitez les données à caractère personnel a des droits que vous devez respecter:

- **Le consentement:** un traitement de données à caractère personnel doit avoir reçu le consentement de la personne physique concernée.
- **Le droit d'opposition:** toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.
- **Le droit d'accès:** toute personne physique a le droit d'interroger le responsable de traitement en vue d'obtenir des informations relatives aux finalités du traitement ou la communication des données qui la concernent.
- **Le droit de rectification:** toute personne physique a le droit d'exiger du responsable de traitement qu'il rectifie, complète, verrouille ou efface les données inexactes ou incomplètes la concernant.

> *Loi « Informatique et Libertés », art. 7, 38, 39-I et 40-I modifiés*

LE PRODUIT INNOVANT TRAITE DES DONNÉES DE SANTÉ

Définition des données de santé

Les données de santé présentent **deux spécificités :**

- **Leur cadre :**
Ces données sont collectées auprès d'un professionnel de santé au cours d'une activité de soins réalisée *in situ* ou à distance (télémédecine).

- **Leur objet:**
Elles portent sur l'état de santé physique et/ou mental d'un individu.

Par principe

Les traitements de données de santé sont interdits.

Par exception

Sept traitements de données de santé exclus du champ de cette interdiction

- Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf disposition contraire prévue par la loi ;
- Les traitements nécessaires à la sauvegarde de la vie humaine ;
- Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel ;
- Les traitements réalisés par l'Institut national de la statistique et des études économiques ;
- Les traitements nécessaires à la recherche, aux études et évaluations dans la domaine de la santé ;
- Les données de santé qui sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation ;
- Les traitements justifiés par l'intérêt public et autorisés par la CNIL.

Sont interdits les traitements de données de santé poursuivant une finalité commerciale.

> *Loi « Informatique et libertés », art. 8-II, 8-III et 8-IV modifiés*

Votre produit innovant poursuit un des sept traitements susmentionnés

Vos obligations en tant que responsable de traitement

Une obligation procédurale:
- Vous devez préalablement déclarer vos traitements auprès de la CNIL.
- En fonction de la finalité du traitement, vous devez choisir un des six régimes déclaratifs précisés dans la loi « Informatique et libertés ».

Ex: régime de l'autorisation préalable pour un traitement impliquant un partage de données de santé (dossier médical partagé)

=> Loi « Informatique et Libertés », art. 23, 24, 25, 2627 modifiés

Trois obligations spécifiques:

1- Obligation d'information :
Vous devez délivrer 8 éléments cumulatifs à la personne dont les données sont collectées. (ex: informer la personne sur les destinataires des données).

2- Obligation de sécurité:
Vous devez préserver la sécurité des données et éviter leur divulgation à des tiers par l'adoption de mesures physiques et/ou techniques appropriées. Cette obligation est renforcée pour les données de santé.

3- Durée de conservation limitée des données de santé:
Vous devez définir une durée à l'issue de laquelle les données seront détruites ou archivées. Les données ne peuvent être conservées au-delà de cette durée qu'en vue d'être traités à des fins historiques, statistiques ou scientifiques.

> *Loi « Informatique et Libertés », art. 32-I, 34 et 36 modifiés*

Le respect des droits de la personne

La personne dont vous collectez et traitez les données de santé a des droits que vous devez respecter:

- **Le consentement :** toute personne physique doit préalablement donner son consentement au traitement de ses données de santé.
- **Le droit d'opposition :** toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données de santé la concernant fassent l'objet d'un traitement.
- **Le droit d'accès :** toute personne physique a le droit d'accéder à ses données de santé directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet.
- **Le droit de rectification** : toute personne physique a le droit d'exiger du responsable de traitement qu'il rectifie, complète, verrouille ou efface les données de santé inexactes ou incomplètes la concernant.

> *Loi « Informatique et Libertés », art. 38, 43 et 40-I modifiés*