Délibération n° 2019-0018 /AT/APDP du 30 décembre 2019

Portant Autorisation de traitement des données de santé des utilisateurs de la plateforme KEA Medicals

L'Autorité de Protection des Données Personnelles (APDP), réunie en séance plénière, sous la présidence de monsieur Etienne Marie FIFATIN ;

Etant également présents, les Conseillers :

- BIO TCHANE MAMADOU Ismath
- BENON Nicolas ;
- YEKPE Guy-Lambert ;
- ABOU SEYDOU Amouda ;
- MADODE Onésime
- OKE Soumanou ;
- LEKOYO Imourane.

Vu la loi n° 90-32 du 11 décembre 1990 portant Constitution de la République du Bénin ;

Vu la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin ;

Vu le décret n° 2015-533 du 06 novembre 2015 portant nomination des membres de l'Autorité de Protection des Données Personnelles (APDP) précédemment, Commission Nationale de l'Informatique et des Libertés (CNIL), deuxième mandature ;

Vu le décret n° 2016-513 du 24 août 2016 portant nomination de Madame Félicité AHOUANDOGBO née TALON en qualité de Commissaire du Gouvernement près l'APDP précédemment, Commission Nationale de l'Informatique et des Libertés (CNIL) ;

Vu le décret n° 2016-606 du 26 septembre 2016 modifiant le décret n° 2015-533 du 06 novembre 2015 portant nomination des membres de l'APDP précédemment Commission Nationale de l'Informatique et des Libertés (CNIL), deuxième mandature ;

Vu le règlement intérieur de l'Autorité de Protection des Données Personnelles en date du 25 janvier 2019 ;

Vu la lettre en date du 19 septembre 2019 par laquelle la Directrice Générale de l'entreprise KEA Medicals a sollicité une autorisation de l'Autorité de Protection des Données Personnelles (APDP), aux fins de traitement automatisé des données de santé des usagers de la plateforme KEA Medicals ;

Vu le rapport du Conseiller Imourane LEKOYO de l'Autorité de Protection des Données Personnelles ;

Après en avoir délibéré en présence du Commissaire du Gouvernement madame Félicité AHOUANDOGBO née TALON qui a fait ses observations ;

IL EST EXPOSÉ CE QUI SUIT :

I- Objet de la demande d'autorisation et responsable du traitement

1-1 . Objet

Par lettre en date du 19 septembre 2019, la Directrice Générale de KEA Medicals, sollicite auprès de l'Autorité de Protection des Données Personnelles, une autorisation aux fins de traitement des données de santé des utilisateurs de la plateforme de santé ''KEA Medicals.

1-2 . Responsable du traitement

Est considéré comme responsable de traitement, aux termes des dispositions de l'article 1er du livre préliminaire de la loi n° 2017-20 du 20 avril 2018 :

*« **Toute personne physique ou morale, l'autorité publique, le service ou tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités et les moyens** ».*

En l'espèce, le Responsable de traitement est la Directrice Générale de KEA Medicals.

II-Examen de la demande d'autorisation du traitement

2-1 Recevabilité

Au regard des dispositions des articles 380 et 407 de la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, la demande est recevable.

2-2 Finalités

Aux termes des dispositions de l'article 383 de la loi n° 2017-20 du 20 avril 2018 portant code du numérique:

« Les données à caractère personnel doivent être :

collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables ».

Le traitement a pour finalités de :

- Faciliter la remontée de l'historique médicale des patients à partir de l'identité médicale universelle (IMU) ;
- Améliorer la prise en charge des patients ;
- Optimiser le service offert aux usagers.

L'Autorité estime que les finalités existent, qu'elles sont explicites, légitimes et non frauduleuses.

2-3 . Droits des personnes concernées

2.3.1- Droit à l'information préalable et respect du principe de consentement et de légitimité

➢ **Droit à l'information préalable**

Aux termes des dispositions de l'article 415 de la loi portant code du numérique en République du Bénin, le responsable du traitement ou son représentant doit fournir à la personne dont les données font l'objet d'un traitement au plus tard lors de la collecte et quels que soient les moyens et supports employés, toutes les informations liées au traitement.

L'Autorité note, au regard du formulaire renseigné par le requérant que les personnes concernées bénéficient du droit à l'information préalable sur la base de mentions légales sur formulaire et sur site internet.

➢ **Respect du Principe de consentement et de légitimité**

Conformément aux dispositions des articles 389 alinéa 1er, 390 et 415 points 8 et 10 de la loi n° 2017-20 du 20 avril 2018 portant code du numérique, le consentement des personnes concernées est requis.

L'Autorité note que le requérant a prévu et garanti le respect du principe de consentement préalable et de légitimité aux personnes concernées par le traitement.

2.3.2- Droit d'accès

Aux termes des dispositions de l'article 437 du code du numérique, *« **Toute personne physique dont les données à caractère personnel font l'objet d'un traitement peut demander au responsable de ce traitement :***

1- ***les informations permettant de connaître et de contester le traitement de ses données à caractère personnel ;***

2- ***la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de traitement, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées ;***

3- ***la communication sous forme intelligible des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;***

… ».

L'Autorité relève que le droit d'accès des abonnés à leurs données personnelles est assuré par KEA Medicals. Ce droit s'exerce via le site internet de KEA Medicals.

La communication des informations demandées par les adhérents en cas d'exercice du droit d'accès par le requérant est immédiate.

Cette mesure est conforme à la loi.

2.3.3- Droit à la portabilité des données et droit à l'oubli

- **Droit à la portabilité des données**

Conformément aux dispositions de l'article 438 du code du numérique :

« Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle… ».

L'APDP note que ce droit est garanti aux usagers de la plateforme ''KEA Medicals''.

L'Autorité en prend acte

- **Droit à l'oubli**

Conformément aux dispositions de l'article 443 du code du numérique, lorsque le responsable du traitement a rendu publiques les données à caractère personnel, il prend toutes les mesures raisonnables, y compris les mesures techniques, en ce qui concerne les données publiées sous

sa responsabilité, en vue d'informer les tiers qui traitent lesdites données, qu'une personne concernée leur demande d'effacer tout lien vers ces données à caractère personnel.

KEA Medicals indique que ce droit est assuré aux utilisateurs de sa plateforme.

L'Autorité en prend acte.

2.3.4 Droit d'opposition

L'article 440 du code du numérique dispose en substance que l'exercice du droit d'opposition se fait sur demande écrite, datée, signée et adressée au responsable du traitement ou à son représentant par voie postale ou électronique.

Le droit d'opposition est assuré aux personnes concernées par le traitement.

Cependant, le délai de réponse ne saurait excéder les trente (30) jours qui suivent la réception de la demande adressée au responsable du traitement, conformément aux dispositions de l'article précité.

2.3.5 Droit de rectification et de suppression

Conformément aux dispositions de l'article 441 de la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, l'exercice du droit de rectification et de suppression par les personnes concernées doit être assuré par le requérant.

Le requérant indique que les droits de rectification et de suppression sont garantis aux utilisateurs de la plateforme. Il précise s'agissant spécifiquement de l'exercice du droit de suppression, qu'il procède dans les quarante-huit (48) heures qui suivent la réception de la demande à une suppression temporaire et au bout de trois (03) mois à une suppression définitive des données.

L'Autorité rappelle au requérant qu'en cas d'exercice de ce droit, le délai de suppression définitif des données ne doit excéder quarante-cinq (45) jours conformément aux dispositions du code du numérique.

2-4 Proportionnalité

Conformément aux dispositions de l'article 383-4 du code du numérique :

« Les données collectées doivent être :

… ;

*4- **adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées** ;*

… ».

En l'espèce, les personnes concernées par le traitement sont les utilisateurs de la plateforme ''KEA Medicals''.

Les catégories de données à collecter sont de deux (02) ordres. Il s'agit des :

1. **données alphanumériques** : *nom et prénoms, numéro de téléphone, date et lieu de naissance ;*

2. **données sensibles :** informations sensibles de 2 ordres **:**

- **informations sensibles de niveau 1 :** antécédents médicaux (diabète, *hypertension, ulcère*) et résumé de consultation des diagnostics de base (paludisme, *fièvre typhoïde*) ;

- **informations sensibles de niveau 2 :** informations et diagnostics sensibles (*sérologie VIH, cancer*).

L'APDP considère que les catégories de données qui font l'objet du traitement sont adéquates, pertinentes et non excessives au regard des finalités poursuivies.

2-5 Durée de conservation des données collectées

Le requérant précise que les données collectées sont conservées aussi longtemps que l'utilisateur est abonné à la plateforme KEA Medicals sauf en cas de demande expresse de suppression manifestée par l'abonné. Dans ce cas, les données le concernant sont supprimées définitivement au bout de trois (03) mois.

En cas de décès, les données sont archivées aux fins de statistiques et/ou de recherche scientifique.

L'Autorité en prend acte et recommande au requérant qu'en cas de décès que les données des patients soient conservées sous anonymat pour une durée n'excédant pas dix (10) ans.

En cas d'une conservation des données au-delà des 10 ans ou d'utilisation des données (non anonymisées) des patients à d'autres fins, le requérant devra introduire auprès de l'Autorité une nouvelle demande d'Autorisation.

2-6 Traitement des données de santé

L'article 394 du code du numérique dispose en substance que le traitement des données sensibles telles que les données de santé est interdit. Cependant, l'interdiction ne s'applique pas dans certains cas particuliers prévus aux points 1-15 de l'article précité.

Le requérant indique que la plateforme met en relation des hôpitaux, des médecins et des patients utilisateurs de ladite plateforme.

Les informations de santé communiquées par les utilisateurs sont consignées et enregistrées sur leurs propres terminaux mobiles (smartphones).

''KEA Medicals'' précise également que le traitement est effectué sous la supervision d'un professionnel de santé conformément aux dispositions de l'article 394.7 du code du numérique.

De même, le requérant indique qu'il appartient à ses adhérents, de fournir eux-mêmes les informations de santé les concernant au professionnel de santé via la plateforme KEA Medicals.

L'Autorité estime que le traitement des données de santé est justifié au regard des dispositions de l'article 394 du code du numérique.

2-7 TRANSFERT DE DONNEES

Le requérant indique que les données de santé anonymisées ne permettant pas l'identification des utilisateurs de la plateforme KEA MEDICALS, peuvent être transférées à des organismes publics ou autres à des fins d'enquêtes et/ou de statistique.

L'autorité en prend acte.

2-8 Sécurité

- **Sécurité physique des locaux abritant les équipements**

Le serveur est hébergé dans un Data Center aux Etats-Unis d'Amérique plus précisément à News-York chez un opérateur de données de santé dénommé ''Océan Digital''. Il est protégé selon les normes internationales requises.

- **Sécurité logique des données**

À l'analyse, l'Autorité note que le traitement des données est effectué via la plateforme (www.keamedical.net). Chaque usager de la plateforme dispose d'un identifiant unique de connexion (login et mot de passe).

Les données collectées par ''Kea Medicals'' ne sont pas stockées sur des serveurs locaux, mais sur un serveur distant basé aux USA. La sécurité physique des locaux abritant la base de données des patients est donc assurée par l'hébergeur de la plateforme.

Un accord de confidentialité a été dûment établi pour garantir la confidentialité des données. Aussi, une authentification est-elle requise pour l'accès aux données qui sont chiffrées sur le serveur.

Des niveaux d'accès sont donnés à travers la mise en place d'un système de gestion des droits et autorisations.

En cas d'indisponibilité du serveur de base de données hébergé aux USA, les données pourront être immédiatement disponibles à travers un service de réplication des données basé en Angleterre.

Le requérant dispose d'un système de collecte des logs pour constater à postériori l'identité des personnes ayant eu accès aux données.

Le traitement déclaré est soumis à une politique de sécurité applicable au traitement.

Eu égard à toutes ces différentes dispositions et procédures mises en œuvre, l'Autorité constate que les mesures de sécurité (physique et logique) sont satisfaisantes.

Par ces motifs et après en avoir délibéré conformément à la loi,

1. **enjoint à KEA Medicals d'avoir à :**

   - **notifier aux internautes de sa plateforme l'utilisation de cookies sur son site internet www.keamedicals.net dès l'accès au site internet ;**

   - **conserver les données des personnes concernées par le traitement pendant un délai n'excédant pas la durée nécessaire à l'atteinte des finalités pour lesquelles elles sont collectées ou traitées, conformément aux dispositions de l'article 383 point 6 du code du numérique ;**

   - **respecter les dispositions de l'article 441 qui dispose entre autres qu'en cas d'exercice du droit de suppression, le délai de réponse ne saurait excéder les quarante-cinq (45) jours qui suivent la réception de la demande adressée au responsable du traitement, conformément aux dispositions de l'article précité.**

2. **Recommande au requérant de :**
   - **indiquer aux utilisateurs de la plateforme les modalités d'exercice des droits d'accès, d'opposition, de rectification et de suppression ;**

   - **préciser aux utilisateurs les différentes voies d'exercice de ces différents droits conformément aux dispositions des articles 437, 440 et 441 du code du numérique.**

3. **Rappelle au requérant que :**
   - **le traitement déclaré ne saurait être détourné de ses finalités ;**

- **un rapport annuel d'activités en application des dispositions de l'article 387, dernier alinéa du code du numérique doit être adressé à l'APDP ;**

- **sa responsabilité est entièrement engagée, en cas d'atteinte aux données personnelles hébergées à l'étranger.**

Sous réserve de ce qui précède,

KEA Medicals est autorisé à mettre en œuvre le traitement des données envisagé.

Conformément aux dispositions des articles 462 et 489 de la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, l'APDP se réserve le droit de procéder à des contrôles aux fins de s'assurer du respect par le requérant des termes et conditions de la présente autorisation.

Ladite autorisation est valable pour une durée maximale de deux (2) ans à compter de sa date de notification.

Le Président,

Etienne Marie FIFATIN