République du Bénin

Fraternité - Justice - Travail

RAPPORT D'ACTIVITÉS

2019

AUTORITE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

RAPPORT D'ACTIVITÉS

2019

Prévu par l'article 481 de la loi n°2017-20 du 20 avril 2018 portant code du numérique en République du Bénin.

SOMMAIRE

Pages

PARTIE - II

Le nouvel environnement juridique de l'APDP : Le délégué à la protection des données personnelles (DPD)

PARTIE - III

La problématique de la vidéosurveillance

PARTIE - IV

Annexe

MOT DU PRESIDENT

Etienne Marie FIFATIN

Président de l'APDP

La loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, en son article 481 fait obligation au Président de l'Autorité de Protection des Données à caractère Personnel (APDP) de rendre compte chaque année de l'exécution de sa mission. À ce titre, il adresse à la fin de l'année au Président de la République, au Président de l'Assemblée nationale ainsi qu'à tous les ministères et autres institutions de l'État un rapport d'activités.

En substance, ce rapport dresse le bilan des actions menées au regard des missions et des objectifs définis au plan de travail annuel. Il présente les délibérations dont l'impact social apparaît assez important. Les préoccupations liées au fonctionnement des structures de l'Institution ne sont pas occultées.

Plus particulièrement, le rapport de 2019 lève le voile sur l'une des avancées majeures du code du numérique à savoir le délégué à la protection des données personnelles et aborde également les préoccupations liées à l'installation des systèmes de vidéosurveillance.

En 2019, plusieurs actions menées ont eu pour objectifs de faire connaître davantage l'Institution aussi bien par les personnes physiques que morales. Les acteurs de l'APDP se sont en effet investis dans l'information, la formation, l'accompagnement des responsables de traitement, la sensibilisation des populations sur la protection des données personnelles et de la vie privée.

S'agissant de la formation, dans le cadre d'une convention de partenariat conclue avec la Chambre de Commerce et d'Industrie du Bénin (CCIB), une dizaine de séances a été organisée au profit des opérateurs économiques de plusieurs secteurs d'activités.

Dans la même dynamique, l'association des photographes professionnels des départements de l'Atlantique et du Littoral a bénéficié d'un atelier de formation sur la protection des données personnelles relativement à leurs activités.

Au titre de l'accompagnement, les conseillers de l'APDP et les collaborateurs de l'Institution ont constamment apporté leur

appui aux administrations centrales et territoriales, aux entreprises publiques et privées, aux organismes internationaux et aux organisations non gouvernementales (ONG) à l'occasion de l'accomplissement des formalités requises pour se conformer aux exigences du code du numérique.

Dans le souci de son rayonnement et forte de l'expérience acquise depuis 2010, l'APDP a participé à diverses rencontres et manifestations régionales et internationales.

Les membres de l'Institution sont pleinement conscients que des défis majeurs restent encore à relever. Aussi, œuvrent-ils constamment à l'amélioration des résultats. En témoignent les statistiques sur le nombre de sessions organisées et de décisions rendues au cours de l'année de référence.

Il importe de souligner que l'année 2019 a connu le renforcement des structures de gestion financière à travers la mise en place des organes de passation et de contrôle des marchés publics.

Du point de vue du fonctionnement de l'administration, un Directeur des Affaires Administratives et de la Logistique et un Conseiller Technique aux Affaires Juridiques auprès du Président de l'Autorité ont été nommés.

Au titre des perspectives, nous entendons poursuivre la sensibilisation des populations en général et, en particulier, la jeunesse qui s'adonne sans discernement à la diffusion des données personnelles même les plus sensibles sur les réseaux sociaux.

Par ailleurs, l'APDP entend renforcer sa mission de contrôle de traitements des données personnelles par les responsables de structures publiques et privées.

Je saisis cette opportunité pour remercier Madame et Messieurs les conseillers de la deuxième mandature pour leur détermination, leur engagement à donner le meilleur d'eux mêmes afin que l'APDP devienne l'une des institutions les plus performantes de la République.

À Madame le Commissaire du Gouvernement près l'APDP, j'exprime ma profonde reconnaissance pour son dynamisme et son esprit d'initiative grâce auxquels une collaboration fructueuse s'est instaurée aussi bien avec la Présidence de la République qu'avec d'autres administrations publiques.

Enfin, j'adresse toute ma gratitude au personnel technique, administratif et de soutien qui accomplit au quotidien un travail remarquable avec pour motivation, la volonté de contribuer à l'accomplissement de la mission républicaine de protection des données personnelles et de la vie privée, un maillon essentiel de l'État de droit.

Je voudrais adresser plus particulièrement mes sincères remerciements au Ministre d'État, Secrétaire Général de la Présidence de la République, pour son accompagnement inestimable.

J'exprime ma plus haute reconnaissance au Chef de l'État pour son implication personnelle dans le vote et la promulgation du code du numérique dont plusieurs dispositions ont renforcé les prérogatives de l'APDP dans la protection des données personnelles et de la vie privée au Bénin.

Le Président de l'APDP

Etienne Marie FIFATIN

LES PRINCIPAUX ACTEURS

L'Autorité de Protection des Données à caractère Personnel (APDP) est composée de onze (11) membres issus de différents secteurs socio-professionnels ainsi que le prévoit l'article 464 de la loi 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin.

Le bureau

Etienne Marie FIFATIN

Président de l'APDP

Amouda ABOU SEYDOU

Vice-président

Imourane LEKOYO

Secrétaire du Bureau

Les Conseillers

Nicolas BENON

Conseiller

Soumanou OKE

Conseiller

Wally M. ZOUMAROU

Conseiller

Onésime MADODE

Conseiller

Guy-lambert YEKPE

Conseiller

Ismath BIO-TCHANE

Conseillère

Commissaire du Gouvernement près l'APDP

Félicité AHOUANDOGBO TALON

Secrétaire Général

Ambroise Djima ZINSOU

PARTIE - I

LES ACTIVITÉS DE l'APDP AU COURS DE L'ANNÉE 2019

Les activités de l'APDP en 2019 ont porté notamment sur la visibilité de l'Institution à travers l'organisation et l'animation de diverses séances de sensibilisation au profit des populations, la formation, l'appui conseil et l'accompagnement des responsables de traitement, l'organisation des sessions plénières, la participation à divers ateliers et séminaires.

L'APDP a en outre pris part à plusieurs rencontres aux plans national, régional et international.

I. Les activités de régulation

Au 31 décembre 2019, l'APDP a rendu au total quatre-vingt-onze (91) décisions relatives aux demandes d'autorisation et aux déclarations. Elle a donné quatre (04) avis et traité quelques plaintes.

A. Les autorisations

Au nombre des autorisations, on peut retenir :

1- Autorisation de traitement des données alphanumériques et biométriques des usagers de la Direction Générale de la Police Républicaine aux fins d'établissement de passeports et de cartes de séjour sécurisés par la Direction de l'Émigration et de l'Immigration

Le Directeur Général de la Police Républicaine (DGPR) a sollicité de l'APDP, une autorisation de collecte et de traitement par la Direction de l'Émigration et de l'Immigration (DEI) des données personnelles de ses usagers-clients, aux fins d'établissement des titres de voyages et des cartes de séjour sécurisés.

Le traitement a été autorisé par l'APDP.

2- Autorisation de collecte et de traitement électronique de données à caractère personnel dans le cadre de l'utilisation de l'application santé « Dis-moi Doc »

Le Directeur Exécutif des Opérations de ARRIAUZ SERVICES SANTE a adressé à l'APDP, une demande d'autorisation aux fins de traitement automatisé des données de santé des utilisateurs de l'application « Dis-moi Doc ».

Le traitement a pour but de rendre plus accessibles aux populations, les services de santé offerts par les professionnels de la santé en République du Bénin.

Ladite autorisation a été accordée au responsable de traitement par l'APDP.

3- Autorisation de transfert des données alphanumériques et biométriques extraites de la base de données du Recensement Administratif à Vocation d'Identification de la Population (RAVIP) pour l'établissement des cartes d'identité nationales biométriques au profit des plus démunis

Conformément aux dispositions de la loi 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, le Régisseur Général de l'Agence Nationale de Traitement (ANT) a sollicité de l'Autorité de Protection des Données Personnelles (APDP), une autorisation aux fins de transfert des données alphanumériques et biométriques extraites de la base de données du Recensement Administratif à Vocation d'Identification de la Population (RAVIP).

La finalité poursuivie à travers le traitement envisagé est l'établissement de nouvelles cartes d'identité nationales biométriques au profit de la catégorie sociale des personnes les plus démunies de la population béninoise.

Sous réserve des injonctions faites et de la prise en compte des recommandations, l'ANT a été autorisée à procéder au traitement envisagé.

4- Autorisation d'interconnexion de la base de données clients des abonnés de MTN Mobile Money-Bénin SA avec celles de ses partenaires financiers

Le Directeur Général de MTN Mobile Money-Bénin SA a sollicité une autorisation de l'APDP aux fins de partage de données à caractère personnel avec des institutions financières partenaires.

La finalité poursuivie à travers le traitement est de s'assurer de l'identité du client avant la fourniture du service par les partenaires financiers interconnectés à la base de MTN Mobile Money-Bénin SA.

MTN Mobile Money-Bénin SA a été autorisé par l'Autorité à effectuer l'interconnexion envisagée.

5- Autorisation de collecte et de traitement de données alphanumériques et de santé sur l'application « GOMEDICAL »

Le Directeur Général de la Société GOMEDICAL a sollicité une autorisation auprès de l'APDP aux fins de procéder à la collecte et au traitement de données alphanumériques et de santé sur l'application « GOMEDICAL ».

Les finalités poursuivies à travers le traitement sont d'une part, d'offrir un meilleur mécanisme de prise de

rendez-vous entre les patients et les médecins et d'autre part, permettre la gestion efficace des données médicales du patient de même que la maîtrise de l'emploi du temps du médecin traitant.

L'APDP a autorisé le requérant à mettre en œuvre le traitement envisagé. Des recommandations portant sur la limitation de la durée de conservation des données personnelles et la mise en place des mesures visant à garantir la confidentialité desdites données ont été également faites par l'Autorité.

6- Autorisation de traitement et de transfert de données alphanumériques à partir du site web https://vraimanagertpe.com

Monsieur Aboua Hermann AGOSSA a demandé une autorisation aux fins de procéder d'une part, au traitement de données alphanumériques sur le site **https://vraimanagertpe.com** hébergé en France puis d'autre part, de transférer lesdites données vers la société **« GetResponse »** sise en Pologne et chargée du marketing et de la campagne e-mailing auprès des usagers.

Au regard de la particularité des traitements envisagés et notamment des questions qu'ils soulèvent, l'APDP a fait droit en partie à la requête. Elle a en effet :

- Autorisé le promoteur du site web **https://vraimanagertpe.com** à mettre en œuvre le traitement conformément aux finalités déclarées ;

- Autorisé le transfert vers la Pologne des données personnelles portant sur les nom, prénoms et e-mail ;

- Mais interdit le transfert des données bancaires et de géolocalisation des prospects et clients vers son sous-traitant « **GetResponse** » en Pologne.

7- Autorisation de traitement des données de santé des utilisateurs de la plateforme KEA Medicals

La Directrice Générale de KEA Medicals a sollicité une autorisation auprès de l'APDP aux fins de traitement des données de santé des utilisateurs de la plateforme de santé « **KEA Medicals** ».

A l'issue de l'examen en plénière de la requête, « **KEA Medicals** » a été autorisée à mettre en œuvre le traitement objet de la requête sous réserve de la mise en œuvre des injonctions qui font obligation au requérant de :

- Notifier aux internautes l'utilisation de cookies sur le site internet www.keamedicals.net dès l'accès audit site ;

- 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 383.6 du code du numérique ;

- Respecter des dispositions du code du numérique relatif au délai de réponse imparti au responsable de traitement en cas d'exercice du droit de suppression par la personne concernée par le traitement (les utilisateurs de la plateforme).

8- Autorisation de collecte et de transfert de données personnelles par Société Générale Bénin (SGB) dans le cadre du recensement des cadeaux et repas d'affaires en vue de la lutte contre la corruption et le trafic d'influence.

Le Directeur Général Adjoint de Société Générale Bénin a sollicité de l'APDP une autorisation aux fins de collecte et de transfert des données personnelles alphanumériques de ses collaborateurs, clients, prospects, fournisseurs et tiers, dans le cadre du recensement des cadeaux et repas d'affaires.

La finalité poursuivie à travers le traitement envisagé est la lutte contre la corruption par le recensement des cadeaux, invitations à des repas d'entreprise et la collecte des données personnelles des collaborateurs, clients, prospects, fournisseurs, tiers et ceci, à partir de l'application « **Gifts Events Meals Solutions** » (GEMS).

Société Générale Bénin a été autorisée à procéder au traitement des données personnelles objet de sa requête.

9- Autorisation de collecte, de traitement et de transfert de données alphanumériques, biométriques et de santé des assurés de Atlantique Assurances Bénin IARDT

La Directrice Générale de la compagnie d'assurances Atlantique Assurances Bénin IARDT a sollicité une autorisation de l'Autorité de Protection des Données Personnelles (APDP) aux fins de collecte, de traitement et de transfert des données alphanumériques, biométriques et de santé de ses assurés vers le Maroc.

Le traitement envisagé a pour finalités d'une part, la gestion des contrats d'assurances et d'autre part, la remise d'une carte contenant les empreintes digitales des personnes concernées par le traitement dans le cadre du contrôle de leurs soins.

L'APDP a autorisé la mise en œuvre du traitement déclaré sous réserve de la prise en compte par le déclarant des recommandations faites.

B. Les déclarations

L'APDP a été saisie de soixante-douze (72) dossiers de déclarations auxquelles suite a été donnée. Quelques unes méritent d'être signalées :

1- Déclaration de traitement de données à caractère personnel par le système de vidéosurveillance de la Direction Générale de la Police Républicaine (RD n° 012-2019/APDP/Pt/SG/DAJC/SA du 15 mars 2019)

Le Directeur Général de la Police Républicaine a déclaré à l'APDP, un traitement de données à caractère personnel portant sur les images enregistrées par les caméras de vidéosurveillance installées à l'**Aéroport International Cardinal Bernadin GANTIN** de Cotonou (130 caméras).

Un récépissé de déclaration a été délivré au requérant.

2- Déclaration du site web de l'Agence Béninoise du Service Universel des Communications Électroniques et de la Poste (ABSU-CEP) (RD n° 013/APDP/Pt/SG/DAJC/SA du 1er avril 2019)

Le Directeur Général de l'Agence Béninoise du Service Universel des Communications Électroniques et de la Poste (ABSU-CEP) a saisi l'Autorité d'une déclaration de traitement de données à caractère personnel sur son site web dénommé **www.absucep.bj.**

Un récépissé de déclaration a été délivré au requérant. Toutefois, des injonctions et des recommandations lui ont été faites.

3- Déclaration de traitement des données à caractère personnel des avocats inscrits au Barreau du Bénin (RD n° 019-2019/APDP/Pt/SG/DAJC/SA du 29 avril 2019)

Le **Bâtonnier de l'Ordre des Avocats du Bénin** a déclaré à l'Autorité de Protection des Données à caractère Personnel (APDP), un traitement portant sur les données personnelles des avocats inscrits au Barreau du Bénin.

L'Autorité a pris acte de la déclaration du requérant à travers la délivrance d'un récépissé de déclaration.

4- Déclaration de traitement de données personnelles via une application mobile (RD n° 025/APDP/Pt/SG/DAJC/SA du 17 juin 2019)

Le Directeur Général de la Société IROKOLAB a déclaré à l'Autorité de Protection des Données à caractère Personnel qu'il procède au traitement de données à caractère personnel des avocats du barreau du Bénin en vue de leur mise en réseau et de la facilitation de la communication entre eux à partir de son application mobile dénommée : **BaroMaître**.

Un récépissé de déclaration a été délivré à charge pour le requérant de notifier à l'APDP, dans un délai de deux (02) mois, l'engagement à se conformer aux injonctions et aux recommandations.

5- Déclaration de la base de données des candidats aux élections présidentielles (RD n° 030-2019/APDP/Pt/SG/DAJC/SA du 23 juillet 2019)

Le Président de la **Commission Électorale Nationale Autonome** (**CENA**), agissant au nom et pour le compte de ladite Commission, a déclaré à l'Autorité de Protection des Données à caractère Personnel qu'il procède au traitement des données à caractère personnel des candidats aux élections présidentielles.

L'Autorité a pris acte de la déclaration du Président de la **CENA**, en lui délivrant un récépissé de déclaration.

6- Déclaration de traitement sur site web de BGFI Bank Bénin (RD n° 058/APDP/Pt/SG/DAJC/SA du 05 décembre 2019)

Le Directeur Général de **BGFI Bank Bénin** a déclaré à l'APDP, le traitement de données à caractère personnel de ses clients sur le site web **benin.groupebgfibank.com**.

Un récépissé de déclaration a été délivré sous réserve du respect par **BGFI Bank** des injonctions portant sur :

- La limitation de la durée de conservation des données personnelles et l'exploitation des cookies dans un délai n'excédant pas celui nécessaire à l'atteinte des finalités du traitement ;
- La garantie des droits des personnes concernées par le traitement (droits d'accès, de rectification et de suppression, droit à l'oubli conformément au code du numérique).

7- Déclaration de traitement de données personnelles par le système de vidéosurveillance de l'hôtel GOLDEN TULIP – LE DIPLOMATE (RD n° 065/APDP/Pt/SG/DAJC/SA du 06 décembre 2019)

Conformément à la loi n° 2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin, le Directeur Général de la **Société West Africaine pour l'Investissement** (**SOWAFI)** a déclaré à l'APDP un traitement de données à caractère personnel portant sur les images enregistrées par le système de vidéosurveillance (32 caméras) de l'hôtel **GOLDEN TULIP – LE DIPLOMATE**.

Le système de vidéosurveillance installé ayant entre autres pour finalités la surveillance des salariés de l'hôtel, l'APDP a rappelé à travers le récépissé de déclaration délivré que le responsable de traitement est tenu de respecter les dispositions de l'article 3.2 de la « **Délibération n° 2016-008/RE/CNIL du 09 novembre 2016 portant conditions de mise en place et d'utilisation d'un système de vidéosurveillance** ». Lesdites dispositions sont relatives aux règles applicables lorsque le système de vidéosurveillance est installé sur les lieux de travail.

En effet, des paragraphes 1, 2 et 3 de l'article précité, il ressort que :

Paragraphe 1er : « le recours à la vidéosurveillance sur les lieux de travail par les entreprises ou organismes privés ou par les administrations publiques doit répondre à un besoin de sécurité ».

Paragraphe 2 : « la vidéosurveillance ne doit pas avoir pour but la surveillance délibérée et systématique du personnel, de la qualité et de la quantité de travail individuel sur les lieux de travail ».

Paragraphe 3 : « Ce type de système ne peut non plus visionner les accès aux toilettes ou aux vestiaires ».

8- Déclaration de traitement de données personnelles par le système de vidéosurveillance de United Bank for Africa (UBA) du Bénin (RD n° 069/APDP/Pt/SG/DAJC/SA du 07 décembre 2019)

Le Directeur Général de United Bank for Africa (UBA) du Bénin, a déclaré à l'Autorité de Protection des Données à caractère Personnel, un traitement de données personnelles portant sur les images enregistrées par le système de vidéosurveillance (220 caméras) installé au siège et dans les agences de ladite banque.

Un récépissé de déclaration a été délivré à charge pour le requérant de notifier à l'APDP, dans un délai de deux (02) mois, l'engagement à se conformer aux injonctions et aux recommandations.

9- Déclaration de la base de données des clients de la société Bénin Control (RD n° 063-2019/APDP/Pt/SG/DAJC/SA du 08 décembre 2019)

Le Directeur Général de la société **BENIN CONTROL** a saisi l'Autorité de Protection des Données à caractère Personnel, d'une déclaration relative au traitement des données personnelles de ses clients dans le cadre de l'exécution des activités métiers de ladite société.

Un récépissé de déclaration a été délivré à charge pour le requérant de notifier à l'APDP, dans un délai de deux (02) mois, l'engagement à se conformer aux injonctions et aux recommandations.

C. Les plaintes

Plaintes pour piratage de compte Facebook et Whatsapp

L'APDP a reçu au cours de l'année 2019 plusieurs plaintes suite à la violation des comptes Facebook et / ou Whatsapp de certains usagers par des individus malintentionnés.

A l'issue de l'instruction des dossiers, les plaintes revêtant un caractère cybercriminel ont été transmises à l'Office Central de Répression de la Cybercriminalité (OCRC) aux fins de poursuite éventuelle.

Néanmoins, certaines plaintes ont donné lieu à un règlement amiable au niveau de l'APDP.

D. Les avis

Au nombre des avis émis par l'Autorité, on peut citer :

1- Avis de l'Autorité de Protection de Données Personnelles sur le projet de décret portant intégration des grands facturiers à la plateforme électronique de partage des informations sur le crédit en République du Bénin

Conformément aux dispositions de l'article 411 du code du numérique, l'Autorité a été appelée à émettre son avis sur une requête à elle adressée par le Ministère de l'Économie et des Finances (MEF). Le projet

de décret était relatif à l'intégration des grands facturiers sur la plateforme électronique de partage des informations sur le crédit en République du Bénin.

Un avis a été émis par l'APDP conformément aux dispositions du code du numérique.

2- Avis de l'Autorité de Protection de Données Personnelles sur la transmission à la CENA par l'ANT de la LEPI en format électronique

L'Agence Nationale de Traitement (ANT) a sollicité l'avis de l'APDP sur une demande que lui a adressée la Commission Électorale Nationale Autonome (CENA) en vue d'obtenir la transmission en format électronique de la Liste Électorale Permanente Informatisée (LEPI).

L'avis de l'APDP a été émis conformément aux dispositions du code du numérique.

3- Avis de l'Autorité de Protection des Données Personnelles (APDP) sur la demande d'autorisation du Directeur Général de la Police Républicaine (DGPR) aux fins de collecte et de traitement de données alphanumériques et biométriques dans le cadre de la mise en place du système central de contrôle aux frontières

Le Secrétaire Général du Gouvernement a saisi l'Autorité de Protection des Données Personnelles (APDP), aux fins d'avis au sujet de la requête du Directeur Général de la Police Républicaine relative à la collecte et au traitement de données alphanumériques et biométriques, dans le cadre de la mise en place du Système Central de Contrôle aux frontières.

L'APDP a également émis à ce sujet un avis conformément au code du numérique.

II. Les activités au plan international

En vue du renforcement des capacités des cadres de l'APDP, un voyage d'étude et d'immersion a été organisé du 14 au 20 avril 2019 à la Commission de protection des Données Personnelles (CDP) du Sénégal. Une délégation de trois personnes (deux juristes et un informaticien) conduite par un conseiller a effectué cette mission dont les acquis sont d'une grande utilité pour l'APDP. Elle a permis aux cadres de l'APDP de s'imprégner de l'expérience de la Commission de protection des Données Personnelles (CDP) du Sénégal ;

Participation de l'APDP à Accra au Ghana, du 24 au 27 juin 2019 à la conférence internationale sur la protection des données personnelles et à la réunion du Réseau africain des Autorités de Protection des Données Personnelles (RAPDP) ;

- Participation en septembre 2019 à Dakar au Sénégal à l'Assemblée générale de l'AFAPDP et à la réunion des autorités membres du RAPDP ;

- Participation à Tirana (Albanie) du 21 au 25 octobre 2019 à la Conférence Internationale des Commissaires à la Protection de la vie privée ;

- Participation en décembre 2019 à Rabat (Maroc) à la réunion du groupe technique sur la gestion des identités , mis sur pied par le RAPDP ;

III. Les rencontres, sensibilisations et autres actions de visibilité au plan national

Au plan national, l'APDP a été très sollicitée par les organismes publics et privés. À ce titre, elle a participé à plusieurs ateliers et forums de discussions relatifs au numérique, à la cybersécurité et à la protection des données personnelles organisés par des structures telles que : l'Agence pour le Développement du Numérique (ADN), l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), l'Agence des Services et Systèmes d'Information (ASSI), le Ministère du Numérique et de la Digitalisation (MND), le réseau mobile MTN, l'Association Nationale des Professionnels en Gestion des Ressources Humaines (ANPGRH) et autres associations professionnelles.

En outre, l'APDP a initié des activités d'information, d'éducation et de communication. On peut citer entre autres :

- Conférence débats sur la protection des données personnelles et de la vie privée au Ministère des Affaires Sociales et de la Microfinance ;

- Conférence débats sur la protection des données personnelles et de la vie privée à l'Université de Parakou ;

- Séance d'informations sur les réseaux sociaux et la protection des données personnelles au profit des membres de la Conférence Administrative Départementale (CAD) des Préfectures de Cotonou et d'Allada ;

- Séances d'informations aux Collèges d'Enseignement Général (CEG) de Gbégamey et de Sainte Rita (Cotonou), à l'occasion de la Fête du Droit et des Avocats francophone, les 20 et 29 mars 2019 ;

- Conférence débats sur la protection des données personnelles sur les réseaux sociaux au profit des jeunes scouts de la commune d'Abomey-Calavi ;

- Formation au profit de l'association des photographes professionnels du département du Littoral. Près de trois cents (300) photographes réunis ont été sensibilisés sur le droit à l'image, à l'occasion de la commémoration de la Journée Internationale de la protection des données personnelles ;

- Tournée d'information, de contrôle et de sensibilisation sur les conditions de collecte et de traitement des données à caractère personnel dans les préfectures, mairies, hôpitaux, supermarchés et hôtels des départements de l'Ouémé-plateau et Zou-Collines ;

- Signature d'une convention de partenariat avec la Chambre de Commerce et d'Industrie du Bénin (CCIB), pour la formation de tous les opérateurs économiques des divers secteurs d'activités. Dans ce cadre, sept (07) séances de formation ont été organisées ;

- Conférence débats au profit de l'Association Nationale des Professionnels de la Gestion des Ressources Humaines (ANPGRH) sur les responsabilités des entreprises en matière de protection des données personnelles dans les relations professionnelles ;
- Saisine de tous les ministères et mairies pour la désignation de délégués à la protection des données personnelles.
- En vue d'amener les responsables de traitement à se conformer aux prescriptions du code du numérique, l'APDP a pris diverses initiatives dont notamment des lettres adressées à tous les ministères ainsi qu'aux établissements bancaires, aux compagnies d'assurances et aux complexes hôteliers pour l'accomplissement de formalités préalables ;

Ces initiatives ont porté leurs fruits puisque les appels à déclaration ont été suivis de nombreuses requêtes de mise en conformité.

L'Autorité a également participé à des débats télévisés et interviews sur les chaines de télévision et de radiodiffusions nationales.

Enfin l'APDP a reçu en audience à son siège, plusieurs délégations nationales et internationales avec lesquelles elle a eu des échanges sur plusieurs sujets qui ont trait à des projets intéressant les données personnelles. Il y a lieu de rappeler quelques unes de ces rencontres avec les organismes et structures ci-après :

- La Police républicaine, la CENA, le CNSR;
- Le représentant de Facebook Afrique ;

- L'ENABEL BENIN (ex Coopération Technique Belge) ;

- La Banque Mondiale dans le cadre de la mise en œuvre du projet WURI (création d'une plateforme pour l'identification des populations);

IV. Le fonctionnement de l'APDP

A. La tenue des sessions plénières

En 2019, l'APDP a organisé vingt (20) sessions plénières, dont une session extraordinaire délocalisée à Possotomè, les 24 et 25 janvier 2019 au cours de laquelle son nouveau règlement intérieur a été adopté.

B. L'adoption d'un nouveau règlement intérieur

Le 25 janvier 2019, l'APDP a adopté un nouveau règlement intérieur pour tenir compte du nouvel environnement de protection des données personnelles, induisant la mise en place d'un cadre de travail permettant d'atteindre de meilleurs résultats.

C. L'acquisition des biens et services

En 2019, il a été acquis des mobiliers de bureau, ordinateurs, onduleurs, régulateurs et imprimantes ainsi que des fournitures de bureau. Il s'agit de :

- Mobiliers de bureaux pour directeurs et cadres (7 ensembles tables + fauteuils et des chaises visiteurs pour la salle de réunion) ;
- Deux (02) ordinateurs portatifs au profit de deux conseillers ;
- Six (06) onduleurs au profit d'agents de l'APDP ;
- Quatre (04) régulateurs au profit des agents ;
- Cinq (05) imprimantes au profit des conseillers et des agents.

Les prestations suivantes ont été exécutées :

- Contrat pour la prise en charge de l'assurance maladie des conseillers et du personnel ;
- Contrat de prestation pour le gardiennage et l'entretien des locaux de l'APDP ;
- Contrat de prestation pour la fourniture d'internet à haut débit ;
- Contrat de prestation pour la maintenance des copieurs de l'APDP ;
- Edition de divers documents (code du numérique, règlement intérieur, régime financier, manuel de procédures, etc.) ;
- Réalisation des badges au profit des conseillers et des agents.

D. Les autres réalisations

On peut citer :

- L'animation et la mise à jour régulière du site web de l'APDP ;
- La numérisation et l'archivage des rapports d'instruction, des récépissés et des délibérations ;
- La mise en place de Windows Servers 2016 pour la gestion de fichiers et la sauvegarde électronique des documents ;
- L'acquisition des outils de maintenance du parc informatique.

E. Le point d'exécution du budget

L'Autorité de Protection des Données à caractère Personnel a obtenu de l'État une subvention au titre de l'année 2019 d'un montant de trois cent cinquante-quatre millions trois cent cinquante-deux mille (354 352 000) FCFA. Cette subvention constitue exclusivement les ressources utilisées par l'Autorité toute l'année 2019.

Au 31 décembre 2019, le budget a été exécuté à hauteur de trois cent vingt-huit millions quatre cent quatre-vingt-six mille cinq cent quatre-vingt-dix (328 486 590) FCFA, soit un taux d'exécution de 92,70%, base ordonnancement.

Il convient de signaler que les salaires, les primes et les dotations en carburant qui constituent les éléments de charges du personnel ont été régulièrement payés aux conseillers et aux agents.

Le taux de consommation des crédits alloués aurait pu être amélioré si certaines contraintes n'avaient pas empêché la tenue de la deuxième session délocalisée inscrite au PTA et qui devait se pencher sur d'importantes questions touchant à la vie de l'Institution. Cette activité est reportée en 2020.

Les différentes rubriques du budget se présentent ainsi qu'il suit :

RUBRIQUE	PREVISIONS	REALISATION	"TAUX D'EXECUTION (%)"
DEPENSES DU PERSONNEL	242 898 908	240 814 179	99,14
ACHATS DES BIENS ET SERVICES	90 361 492	68 399 521	75,70
ACQUISITIONS DES EQUIPEMENTS	21 091 600	19 272 890	91,38
TOTAL	354 352 000	328 486 520	92,70

F. Les difficultés

Les difficultés rencontrées sont surtout d'ordre budgétaire. La subvention allouée à l'APDP étant insuffisante, les ressources affectées aux missions de sensibilisation n'ont pas permis à l'APDP d'atteindre pleinement ses objectifs au cours de l'année 2019.

Il y a aussi l'insuffisance de personnel qualifié, ce qui oblige l'autorité à recourir aux services de stagiaires professionnels.

G. Les perspectives

En termes de perspectives, l'APDP envisage :

- L'organisation d'un atelier de formation des Directeurs de l'Informatique et du Préarchivage des ministères (DIP) et des délégués à la protection des données personnelles et de la vie privée des ministères et autres structures privées;
- La poursuite des diverses actions de sensibilisation sur le contenu du code du numérique ;
- L'organisation des missions de contrôle des traitements de données personnelles mis en œuvre par différentes structures ;
- Le renforcement des capacités du personnel sur les techniques d'instruction des requêtes et la rédaction administrative.

PARTIE - II

LE NOUVEL ENVIRONNEMENT JURIDIQUE DE L'APDP :

Le délégué à la protection des données personnelles (DPD)

I. Historique du délégué à la protection des données personnelles

En matière de protection des données personnelles, la France fait partie des premiers États à adopter une loi sur les données personnelles et la protection de la vie privée. Dans cette loi qui date de 1978, il est prévu la désignation d'un «Correspondant Informatique et Libertés» (CIL) de la Commission Nationale de l'Informatique et Liberté (CNIL).

Le CIL est chargé de veiller au respect de la loi Informatique et Libertés au sein de l'entreprise. La désignation du CIL est facultative et la CNIL publie la liste des organismes privés et publics qui souhaitent s'engager dans une démarche de conformité par cette désignation.

Au sein de l'organisme auquel il est lié, le CIL veille au respect des dispositions de la loi de 1978 et alerte sur les éventuels risques de sécurité. Il est le point focal de la CNIL.

Avec l'entrée en application le 25 mai 2018 dans l'espace européen, du Règlement Général sur la Protection des Données (RGPD), les compétences de cet organe sont désormais plus étendues. Il est devenu un acteur central pour conseiller et faciliter la mise en conformité des entreprises et prend désormais le nom de Délégué à la Protection des Données (DPD) ou Data Protection Officer (DPO).

Au Bénin, la loi 2009-09 du 22 mai 2009 portant protection des données à caractère personnel, abrogée, était restée muette sur la notion de délégué à la protection des données personnelles. Ce n'est qu'avec l'avènement du code du numérique que cette notion y a été intégrée en raison du nouvel environnement juridique béninois.

II. Le code du numérique et le délégué à la protection des données personnelles

La loi 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin a apporté des innovations majeures en matière de protection de données personnelles.

Au nombre de ces innovations, on note l'institution du Délégué à la Protection des Données personnelles (DPD) qui est la personne chargée de mettre en œuvre les actions tendant à la protection des données au sein d'une organisation. Il est le point focal de l'APDP.

A. L'obligation de désigner un délégué à la protection des données personnelles (DPD)

La désignation d'un Délégué s'impose au responsable de traitement et au sous-traitant dans trois (3) cas de figures qui peuvent être résumés comme suit :

1- si le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;

2- si les activités de base de la structure consistent à réaliser des opérations de traitement qui, de part leur nature, leur portée et / ou leur finalité, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;

3- si la structure effectue des activités l'emmenant à traiter à une échelle importante des données personnelles soumises à des régimes particuliers tels que les données sensibles ou les données à caractère personnel relatives aux condamnations pénales et aux mesures de sureté.

Par ailleurs, en fonction de leur taille ou de leur structure organisationnelle, plusieurs organismes publics et / ou sous- traitants peuvent s'associer et désigner un seul délégué à la protection des données. Ce dernier doit être facilement joignable.

Du point de vue du profil, le DPD est désigné sur la base de ses qualités professionnelles et en particulier, de ses connaissances du droit, des pratiques en matière de protection des données et de sa capacité à accomplir des missions spécifiques prévues par le législateur. Il est soumis au secret professionnel ou à l'obligation de confidentialité en ce qui concerne l'exercice de ses missions.

Le DPD peut être un membre du personnel de la structure du responsable de traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

B. La fonction du délégué à la protection des données personnelles

Le Délégué à la protection des données jouant un rôle primordial dans la structure ou l'organisation où il est désigné, il revient au responsable de traitement et au sous-traitant de veiller à ce qu'il soit associé d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données à caractère personnel. De même, il doit être mis à sa disposition les ressources nécessaires pour exercer ses missions, faciliter son accès aux données à caractère personnel ainsi qu'aux opérations de traitement.

Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données ne reçoive aucune instruction dans le cadre des missions qui lui sont confiées. Il ne peut être relevé de ses fonctions par le responsable du traitement ou le sous-traitant dans l'exercice de ses missions.

Il adresse directement ses rapports au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant.

Le Délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veille à ce que ses missions et tâches n'entraînent pas de conflit d'intérêts.

Les personnes concernées par le traitement peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confèrent les dispositions du code du numérique.

C. Les missions du délégué à la protection des données personnelles

Le législateur béninois a énuméré de façon non exhaustive les missions dévolues au délégué à la protection des données. Il s'agit de :

- Informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent ;

- Contrôler le respect des dispositions du code du numérique en matière de protection des données et des règles internes de la structure du responsable de traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;

- Dispenser des conseils sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et en vérifier l'exécution ;

- Coopérer avec l'Autorité de Protection des Données Personnelles (APDP);

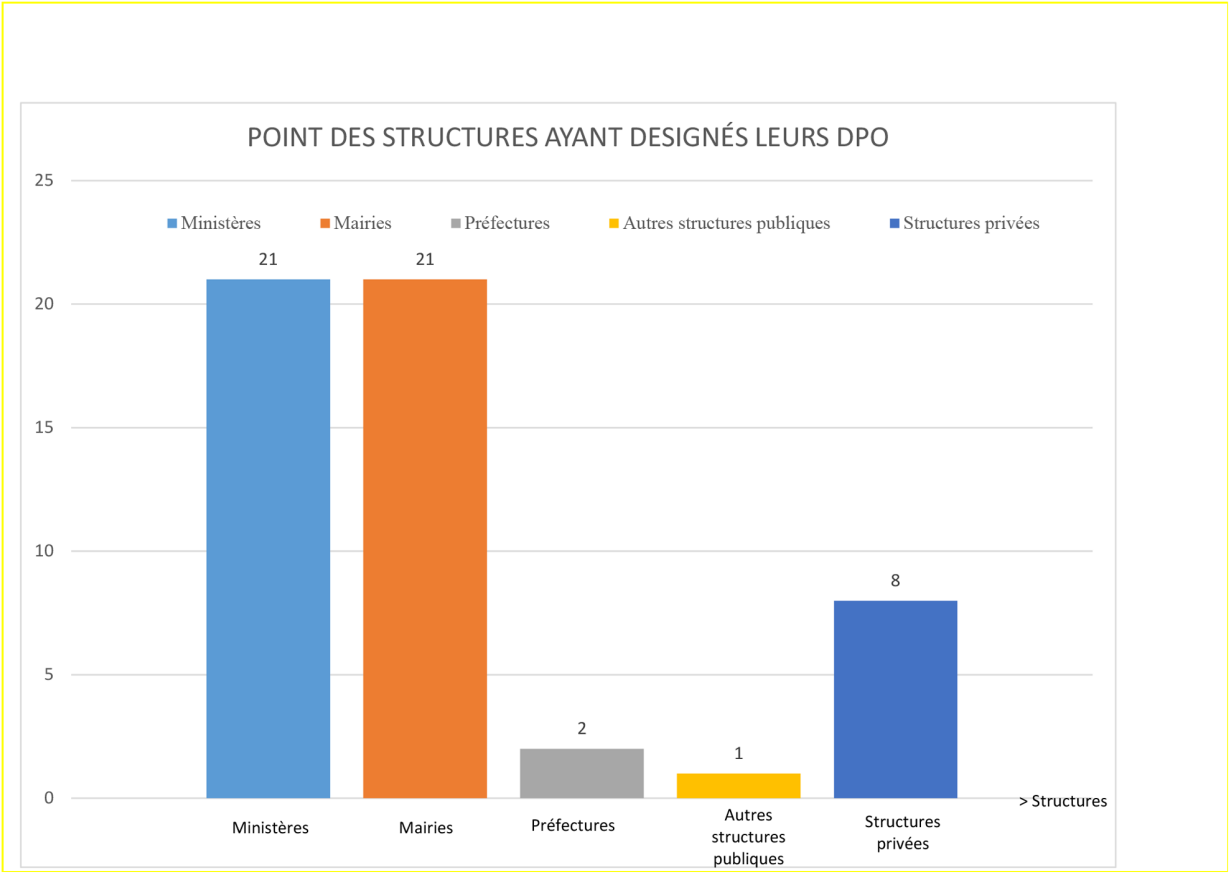
- Faire office de point focal pour l'Autorité sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 429 du code du numérique et mener des consultations, le cas échéant, sur tous autres sujets.

Le Délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, des risques associés aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

D. L'APDP dans la dynamique de formation des délégués à la protection des données personnelles

En 2019, l'APDP s'est également fixée pour objectifs la sensibilisation des institutions publiques et privées pour la désignation des délégués à la protection des données personnelles. Un programme de formation et de renforcement de capacité des délégués désignés a été élaboré.

Le point des structures impactées par cette activité se présente comme suit :



N° D'ORDRE	STRUCTURES
	MINISTERES
1	Ministère de l'Economie Numérique et de la Communication
2	Ministère du Travail et de la Fonction Publique (MTFP)
3	Ministère de l'Enseignement Supérieur et de la Recherche scientifique
4	Ministère du cadre de vie et du développement durable
5	Ministère de la santé
6	Ministère de la Décentralisation et de la Gouvernance locale
7	Ministère de la justice et de la législation
8	Ministère de l'Economie et des Finances
9	Ministère des Enseignements Maternel et Primaire
10	Ministère des Affaires Sociales et de la Microfinance
11	Ministère de l'Agriculture, de l'Elevage et de la Pêche
12	Ministère de l'Eau et des Mines
13	Ministère des petites et moyennes entreprises et de la promotion de l'emploi
14	Ministère des infrastructures et des transports
15	Ministère de l'Energie
16	Ministère de la défense Nationale
17	Ministère des Affaires Etrangères et de la Coopération
18	Ministère d'Etat chargé du plan et du Développement
19	Ministère de l'Industrie et du Commerce
20	Ministère de l'Intérieur et de la Sécurité Publique
21	Ministère de la Communication et de la Poste


MAIRIE DE COTONOU
RÉPUBLIQUE DU BÉNIN
AUTORITÉ DE PROTECTION DES DONNÉES
À CARACTÈRE PERSONNEL (A. P. D. P.)
RÉPUBLIQUE DU BÉNIN
DEPARTEMENT DE L OUEME
HOTEL DE VILLE
HOTEL DE VILLE
BEMBEREKE

N° D'ORDRE	STRUCTURES
MAIRIES ET PREFECTURES	
1	Mairie de Cotonou
2	Mairie de Toviklin
3	Mairie de Kérou
4	Mairie de Kouandé
5	Mairie de OUASSA PEHUNCO
6	Mairie de ZOGBODOMEY
7	Mairie de Bembéréké
08	Préfecture de Cotonou
09	Préfecture de Porto-novo
10	Mairie d'Ifangni
11	Mairie de Sèmè-Kpodji
12	Mairie de Grand-Popo
13	Mairie d'Adjohoun
14	Mairie de Comé
15	Mairie de Kétou
16	Mairie de Zè
17	Mairie de Djidja
18	Mairie d'Adjarra
19	Mairie de Gogounou
20	Mairie de Bantè
21	Mairie de Sakété
22	Mairie de Grand-Popo
23	Mairie de BOPA
AUTRES STRUCTURES PUBLIQUES	
01	CENA
STRUCTURES PRIVEES	
01	SPACETEL BENIN S.A
02	SAHAM Assurances Vies + SAHAM Assurances IARD
03	Bank Of Africa Bénin (BOA-Bénin)
04	BGFI Bank
05	ETISALAT Bénin S.A.
06	BAIC (Banque Africaine pour l'Industrie et le Commerce)
07	Société de Financement et de Participation (SFP)
08	ECOBANK

PARTIE - III

LA PROBLÉMATIQUE DE LA VIDÉOSURVEILLANCE

De nos jours, le souci du renforcement de la sécurité des biens et des personnes conduit de plus en plus à l'installation des systèmes de vidéosurveillance aussi bien sur les lieux de travail que dans les espaces publics. Cette technique de captation d'images et de sons permet de collecter et d'enregistrer les données personnelles de tout usager se retrouvant dans son champ visuel. En principe, un tel enregistrement porte atteinte à la protection des données personnelles et de la vie privée.

La nécessité de concilier les exigences de la sécurité publique et / ou privée et la protection des données personnelles et de la vie privée a entrainé la réglementation de l'installation des systèmes de vidéosurveillance.

I. Les différents types de vidéosurveillance et les conditions d'utilisation

A. Les différents types de vidéosurveillance

Il existe trois (03) types de vidéosurveillance :

1. La vidéosurveillance dissuasive

Elle a pour but de prévenir la mise en danger et les perturbations de la paix par des actes répréhensibles imputables à l'homme. Elle se fait normalement de manière permanente et sert à filmer les images des personnes à partir des caméras qui sont ensuite enregistrées sur une plateforme.

Les données collectées par un système de vidéosurveillance, dans la mesure où elles ont été enregistrées, peuvent être évaluées ultérieurement et utilisées à des fins répressives. Les autorités compétentes peuvent ainsi, par exemple, clarifier un comportement nuisible, analyser des atteintes graves aux biens et aux personnes et rechercher l'auteur d'une infraction.

2. La vidéosurveillance à titre d'observation

Son but est de prévenir les dérangements techniques qui pourraient affecter le bon fonctionnement et l'état des installations, par exemple la régulation du trafic et du flux des personnes.

3. La vidéosurveillance invasive

Elle est utilisée dans le domaine public pour surveiller tout acte ou évènement se déroulant dans les lieux publics qui peuvent être utilisés par des particuliers, sans l'intervention d'agent public, d'une manière libre et gratuite (rues, parcs, lieux de promenades, etc). Elle peut dans certains cas porter atteinte aux libertés et à la vie privée des personnes.

B. Les conditions d'utilisation de la vidéosurveillance

L'installation de caméras dans les locaux professionnels ou domiciles doit poursuivre un objectif clairement défini, légal et légitime.

Dans le cas particulier de la vidéosurveillance au travail, l'employeur a l'obligation d'informer et de consulter les instances représentatives du personnel avant toute décision d'installation de caméra.

Le dispositif installé ne doit pas entraîner un contrôle généralisé et permanent du personnel. Ainsi ces caméras peuvent avoir pour but d'aider à la sécurisation des biens et des personnes par dissuasion ou identification des auteurs de vols et ou de tentatives d'effraction et de dégradations du matériel ou d'agressions.

Elles peuvent :

- Etre installées au niveau des entrées et sorties des bâtiments, des issues de secours et des voies de circulation ;
- Filmer les zones d'entrepôt de marchandises ou de biens de valeur ;
- Filmer les façades extérieures des locaux de l'entreprise et ses installations.

En revanche, il est interdit de filmer :

- Une voie publique ou une rue s'il s'agit d'une caméra privée ;
- Les salariés sur leur poste de travail, sauf circonstances particulières (par exemples : salarié manipulant de l'argent, à condition que la caméra filme la caisse et non le caissier ; entrepôt stockant des biens de valeurs au sein duquel travaillent des manutentionnaires) ;
- Les zones de pause ou de repos des salariés ;
- Les toilettes ;
- Les locaux des syndicats, des représentants du personnel ou leur accès lorsqu'il ne mène qu'à ces seuls lieux.

II. Les obligations du responsable de traitement

A. Les obligations de déclaration / Formalités

Le traitement de données personnelles opéré via un système de vidéosurveillance doit faire l'objet d'une déclaration préalable auprès de l'Autorité de Protection des Données Personnelles conformément aux

dispositions de l'article 405 du code du numérique. Pour ce faire les formulaires de déclaration ou d'autorisation de collecte de données sont téléchargeables sur le site web de l'APDP :
https://www.apdp.bj

B. Les droits des personnes filmées

Les personnes concernées que sont les employés ou les visiteurs doivent être informés des activités des caméras de vidéosurveillance.

Ainsi, l'information individuelle des employés peut se faire au moyen de note de service, de courriel personnalisé ou formalisé par voie d'avenant au contrat de travail. Cependant, cette information n'est pas exigible si les locaux concernés ne sont pas accessibles auxdits salariés.

Quant aux usagers ou visiteurs, l'information devra leur être portée par des affiches de signalisation de l'activité des caméras de vidéosurveillance de façon visible. Lesdites affiches devront comporter les informations suivantes :

- La photo de la caméra ;
- Les références du récépissé de déclaration du traitement auprès de l'APDP ;
- Le nom du responsable de traitement ;
- Les finalités poursuivies à travers la mesure ou l'intérêt légitime de sécuriser les locaux en option;
- La possibilité d'introduire une réclamation auprès de l'APDP (article 448 du code du numérique) ;
- La procédure à suivre pour demander l'accès aux enregistrements visuels les concernant.

Les demandes de suppression des images enregistrées doivent obéir aux conditions bien définies à l'article 441 du code du numérique.

La suppression des images doit être effectuée dans les quarante-cinq (45) jours qui suivent la réception de la demande.

C. L'accès aux données personnelles (images et / ou sons)

Seules les personnes habilitées par le responsable de traitement, dans le cadre de leurs fonctions, peuvent visionner les images.

Ces personnes doivent être particulièrement formées et sensibilisées aux règles de mise en œuvre d'un

système de vidéosurveillance et sur le respect de la vie privée des personnes.

L'accès aux images doit être sécurisé pour éviter que des personnes non autorisées ne puissent les visionner conformément aux dispositions de l'article 425 du code du numérique.

D. La durée de conservation des données personnelles

La délibération n° 2016-008/RE/CNIL du 09 novembre 2016 portant conditions de mise en place et d'utilisation d'un système de vidéosurveillance, en son article 6 dispose que les données collectées doivent être conservées pour une durée maximum d'un (01) mois. Au terme de ce délai, elles doivent être effacées, sauf en cas d'enquêtes judiciaires justifiées.

« Toutefois, suite à la promulgation de la loi 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, qui précise qu'en cas d'exercice du droit de suppression, un délai de quarante-cinq (45) jours est imparti au responsable de traitement, il convient de réajuster la durée de conservation préalablement limitée à (01 mois).

De ce fait, la durée de conservation des images et/ou sons enregistrés est désormais appréciée au regard de la finalité du traitement envisagé et non plus en fonction de la seule capacité technique de stockage de l'enregistreur. »

Le responsable de traitement peut donc étendre la durée de conservation des images collectées à condition d'obtenir l'accord préalable de l'Autorité de Protection des Données Personnelles dont la décision sera fondée sur les raisons qui motivent cette extension.

Il convient de signaler que dans le cadre de sa mission de protection des données personnelles et de la vie privée, l'APDP, au cours de l'année 2019, a renforcé la sensibilisation par des appels à déclaration adressés aussi bien aux responsables de structures publiques ou privées qui font recours à la vidéosurveillance sur les lieux de travail qu'aux autorités qui en font usage dans le but d'assurer la sécurité publique. Plus d'une cinquantaine d'institutions ont alors favorablement répondu en déclarant leurs systèmes de collecte de données personnelles par vidéosurveillance.

PARTIE -IV

ANNEXE

QUELQUES DÉLIBÉRATIONS

Délibération n° 2019-016/AT/APDP du 05 septembre 2019

Portant autorisation de collecte et de traitement des données alphanumériques et biométriques des usagers de la Direction Générale de la Police Républicaine (DGPR) aux fins d'établissement des passeports et cartes de séjour sécurisés par la Direction de l'Emigration et de l'Immigration (DEI)

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 :

- ABOU SEYDOU Amouda ;
- BENON Nicolas ;
- YEKPE Guy-Lambert ;
- 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 la Commission Nationale de l'Informatique et des Libertés (CNIL) en date du 25 janvier 2019 ;

Vu la lettre n° 355/DGPR/SG/DSIC/SLPSI/SA du 26 février 2019, par laquelle le Directeur Général de la Police Républicaine (DGPR) a déclaré auprès de l'APDP, plusieurs traitements de données à caractère personnel ;

Vu le rapport du Conseiller Guy-Lambert YEKPE 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 ;

EMET LA DECISION SUIVANTE :

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

1-1. Objet

Par lettre n° 355/DGPR/SG/DSIC/SLPSI/SA du 26 février 2019, le Directeur Général de la Police Républicaine (DGPR) sollicite de l'Autorité de Protection des Données Personnelles (APDP), une autorisation pour la collecte et le traitement par la Direction de l'Emigration et de l'Immigration (DEI), des données à caractère personnel aux fins d'établissement des titres de voyages et des cartes de séjour.

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 nº 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 du traitement est le Directeur de l'Émigration et de l'Immigration.

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.

2-1. Finalité

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 ses finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables ».

La finalité du traitement envisagé par la DGPR est la production des passeports et des cartes de séjour sécurisés.

L'Autorité estime que la finalité existe, qu'elle est légitime, explicite et non frauduleuse.

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.

Il ressort du formulaire renseigné qu'aucune disposition n'a été prévue par le requérant pour assurer le droit à l'information préalable.

- **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 portant code du numérique, le consentement des personnes concernées est requis.
Toutefois, l'article 389 du code du numérique dispose qu'il « **peut être dérogé à cette exigence du consentement lorsque le traitement est nécessaire :**

1- au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

2- à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées...»

Le type de traitement mis en œuvre par le requérant révèle que le consentement donné par les personnes concernées est tacite. Par ailleurs, le responsable du traitement agit dans le cadre de l'exécution d'une mission d'intérêt public et dans le cadre de la convention de Vienne du 18 août 1967.

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 ;**

… ».

Le requérant indique que le droit d'accès est garanti et peut être exercé par tout moyen auprès de lui-même.

Cependant les modalités d'exercice de ce droit ne sont pas précisées par le requérant. De même, aucun délai de réponse aux personnes concernées n'est indiqué par le requérant, en cas d'exercice du droit d'accès.

2-3-2. 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 droit de rectification est garanti par le requérant à ses usagers-clients et se fait par une demande adressée à la Direction de l'Emigration et de l'Immigration.

L'Autorité rappelle qu'en cas d'exercice de ce droit, 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.

2-4. Proportionnalité

Conformément aux dispositions de l'article 383-4 :

« **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 clients et usagers de la Direction de l'Emigration et de l'Immigration.

Les catégories de données collectées sont : nom et prénoms, date et lieu de naissance, sexe, teint, taille, photo, empreintes digitales, couleur des cheveux, adresse au Bénin, filiation, profession, contact, email.

Lesdites informations sont recueillies directement auprès des personnes concernées.

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

2-5. Durée de conservation des données collectées

Le requérant envisage conserver les données collectées pendant une durée illimitée pour des raisons sécuritaires.

Au vu des éléments du dossier, il parait plus convenable d'indiquer au requérant de limiter la durée de conservation des données à dix (10) ans. Cette durée pourra se renouveler sur demande du responsable du traitement et après apurement du fichier.

2-6. Délégué à la protection des données personnelles

Aux termes des dispositions de l'article 430 de la loi portant code du numérique, « **Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque :**

1- **le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;**

2- **les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou**

3- **les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 394 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 395…** »

L'APDP note que le requérant n'a pas de Délégué à la protection des données personnelles.

2-7. Traitement des données biométriques

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

La DGPR indique que la finalité poursuivie par le traitement est de produire des passeports et cartes de séjour sécurisés.

Les catégories de données collectées sont les empreintes digitales et les éléments du dispositif technique utilisé sont des écrans, des PC, des caméras, un système de lecture de documents.

Par ailleurs, elle précise que la collecte porte sur les empreintes des dix (10) doigts de la main.

L'APDP estime que le traitement des données biométriques est justifié au regard de la loi.

2-8. Sous-Traitance :

Le requérant indique qu'il utilise les services d'un sous-traitant dénommé «GEB Afrique» qui intervient pour la production des passeports et cartes de séjour sécurisés à partir des données personnelles reçues du Service Emigration et Immigration.

2-8. Sécurité

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

Le requérant indique qu'un système de contrôle d'accès biométrique est utilisé pour sécuriser les accès à la salle hébergeant les équipements de traitement des données personnelles.

- **Sécurité logique des données**

L'étude du système révèle qu'un système d'authentification est mis en place pour contrôler l'identité des personnes qui accèdent au serveur de données.

Le requérant indique qu'il a déployé des moyens pour garantir la confidentialité, l'intégrité (données cryptées) des données personnelles collectées.

La sauvegarde des données est effectuée deux (02) fois par jour. Des dispositions sont prises pour rendre disponibles les données grâce à l'architecture n-tiers avec plusieurs bases de données.

Un système de collecte et sauvegarde des logs est disponible pour assurer la traçabilité des actions effectuées sur le système pour des raisons d'audit ou de contrôle et pour identifier tout intervenant dans le système.

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

En cas d'indisponibilité du serveur, les données de la base pourront être immédiatement restaurées à travers l'architecture n-tiers.

L'APDP considère que les mesures de sécurité prises par la DGPR sont satisfaisantes.

PAR CES MOTIFS ET APRÈS EN AVOIR DÉLIBÉRÉ CONFORMÉMENT À LA LOI,

➢ **Enjoint à la DGPR d'avoir à :**

- **garantir le droit à l'information préalable conformément aux dispositions de l'article 415 du code du numérique ;**
- **désigner un Délégué à la protection des données personnelles, conformément aux dispositions de l'article 430 du code du numérique ;**
- **limiter la durée de conservation des données personnelles collectées à dix (10) ans et procéder à leur archivage dans le respect des dispositions de l'article 383.6 du code du numérique.**

Recommande au requérant d'indiquer aux personnes concernées, les modalités d'exercice des droits d'accès, de rectification et de suppression.

➢ **Rappelle au requérant que :**

- **le traitement déclaré ne saurait être détourné de ses finalités ;**
- **en cas d'exercice des droits d'accès, de rectification et de suppression, des délais de réponse sont prescrits par les dispositions des articles 437 et 441 du code du numérique ;**
- **il doit veiller au respect des dispositions de l'article 386 du code du numérique relatives à la sous-traitance ;**

- **un registre des activités de traitement doit être tenu, conformément aux dispositions de l'article 435 du code du numérique ;**
- **un rapport annuel d'activités, en application des dispositions de l'article 387 dernier alinéa du code du numérique, doit être adressé à l'Autorité ;**
- **conformément aux dispositions de l'article 451 du code du numérique, la responsabilité de la DGPR et de son sous-traitant est engagée en cas de manquement aux prescriptions du livre V^{ième} dudit code.**

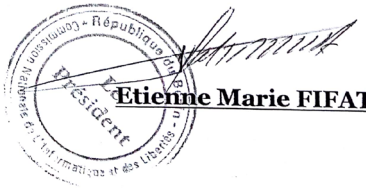
Sous réserve de ce qui précède,

autorise, la mise en œuvre du traitement des données à caractère personnel objet de la présente délibération, par la Direction Générale de la Police Républicaine.

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 ultérieurs aux fins de s'assurer du respect par le requérant des termes et conditions de la présente délibération.

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

Le Président,



Etienne Marie FIFATIN

Délibération n° 2019-018/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 données

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

Délibération n° 2019-015/AT/APDP du 14 août 2019

Portant autorisation de traitement de données alphanumériques, et de santé sur l'application GOMEDICAL

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 :

- ABOU SEYDOU Amouda ;
- BENON Nicolas ;
- YEKPE Guy-Lambert ;
- 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 23 mai 2019 par laquelle monsieur KOUNOU Gilles, représentant la société GOMEDICAL, a sollicité une autorisation de l'Autorité de Protection des Données Personnelles (APDP), aux fins de traitement de données alphanumériques et de santé sur l'application GOMEDICAL ;

Vu le rapport du Conseiller Guy-Lambert YEKPE 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

Le Président de la société GOMEDICAL, sollicite une autorisation auprès de l'Autorité de Protection des Données Personnelles, aux fins de procéder au traitement de données alphanumériques et de santé à partir de l'application GOMEDICAL.

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 no 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 le Président de la société GOMEDICAL.

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 requérant indique que le traitement envisagé a pour finalités d'offrir d'une part, un meilleur mécanisme de prise de rendez-vous entre les patients et les médecins et d'autre part, de permettre la gestion efficace

des données médicales du patient de même que la maîtrise de l'emploi du temps du médecin traitant.

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 à travers les conditions générales d'utilisation.

- **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 envisagé. Les implications liées à leur consentement sont indiquées dans les mentions sur formulaires.

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 adhérents ou utilisateurs à leurs données personnelles est assuré par la société GOMEDICAL. Ce droit s'exerce directement sur l'application via un compte disposant d'un mot de passe OTP (One Time Password).

Les informations demandées sont communiquées immédiatement aux personnes concernées par le traitement en cas d'exercice du droit d'accès.

L'Autorité note que ce droit est garanti aux usagers de l'application GOMEDICAL.

Elle rappelle toutefois que le délai de réponse ne saurait dépasser les soixante (60) jours qui suivent la réception de la demande.

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 utilisateurs de l'application GOMEDICAL.

- **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.

La société GOMEDICAL indique que ce droit est assuré aux utilisateurs de son application.

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, l'Autorité constate que les modalités d'exercice de ce droit par les utilisateurs de l'application n'ont pas été précisées.

Le requérant doit indiquer aux personnes concernées, les modalités d'exercice du droit d'opposition.

L'Autorité rappelle que s'agissant du droit d'opposition, 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.

Cet article précise en substance que l'exercice du droit de rectification et de suppression se fait sur demande écrite, datée, signée et adressée au responsable du traitement ou à son représentant par voie postale ou

électronique.

Le requérant indique que le droit de rectification et de suppression est garanti aux utilisateurs de l'application.

Les modalités d'exercice de ce droit n'ont toutefois pas été précisées.

Le requérant doit indiquer aux personnes concernées, les modalités d'exercice du droit de rectification et de suppression.

L'Autorité rappelle qu'en cas d'exercice de ce droit, 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.

2-4. 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 professionnels de la santé et toute personne susceptible de recevoir des soins.

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

a- données nominatives : Nom et prénoms, date et lieu de naissance, numéro de téléphone, emploi du temps, position géographique, spécialité, numéro d'inscription à l'ordre ;

b- données sensibles : Données de santé (mensurations, dossier hématologique, données de consultation (date, heure, âge, profession, spécialité, unité sanitaire), données de vaccination, antécédent sanitaire (maladie plus hospitalisation, allergies…) et photo faciale.

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 indique que les données collectées sont conservées pour une durée minimale de 15 ans.

Il est cependant à noter qu'en application des dispositions de l'article 383.6 du code du numérique, la durée de conservation des données collectées doit être limitée à celle nécessaire à l'atteinte des finalités du traitement.

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 relatives à la santé est interdit. Cependant, l'interdiction ne s'applique pas dans certains cas particuliers prévus aux points 1 à 15 de l'article précité.

Le requérant indique que l'application met en contact des médecins et des patients utilisateurs de ladite application.

GOMEDICAL précise également que le traitement est effectué sous la surveillance d'un professionnel des soins de santé conformément aux dispositions de l'article 394.7 du code du numérique.

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. Sécurité

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

Le serveur est hébergé dans un Cloud et aussi dans le Datacenter de MTN Bénin.

- **Sécurité logique des données**

Le requérant déclare garantir les obligations de confidentialité par la mise en place des habilitations nécessaires aux personnes qui en raison de leur fonction ou pour les besoins du service ont directement accès aux données personnelles traitées. Un engagement est signé pour garantir la confidentialité des données personnelles.

La technique de chiffrement prévue permet d'assurer l'intégrité des données.

Des dispositions sont également prises pour assurer la disponibilité des données à travers des serveurs répartis en cas de sinistres ou de pannes.

Des scannes et audits trimestriels sont prévus pour tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité des données.

L'Autorité note que ces mesures sont satisfaisantes.

PAR CES MOTIFS ET APRES EN AVOIR DELIBERE CONFORMEMENT A LA LOI,

Recommande au requérant de :

- **limiter la durée de conservation des données collectées et des cookies à celle nécessaire à l'atteinte des finalités ;**
- **veiller à ce que la confidentialité des données soient préservée conformément aux dispositions de l'article 425 du code du numérique.**

Rappelle au requérant que :

- **le traitement déclaré ne saurait être détourné de ses finalités ;**
- **le responsable du traitement ou son représentant doit veiller au respect des mesures de sécurité conformément à toutes les dispositions de l' article 426 ;**
- **conformément aux dispositions de l'article 451 du code du numérique, sa responsabilité est engagée, en cas de manquement aux prescriptions du livre V^{ème} dudit code.**
- **un registre des activités du traitement doit être tenu, conformément aux dispositions de l'article 435 du code du numérique ;**

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

Sous réserve de ce qui précède,

La société GOMEDICAL est autorisée à mettre en œuvre le traitement des données visé dans la présente délibération.

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 ultérieurs aux fins de s'assurer du respect par le requérant des termes et conditions de la présente autorisation.

La présente autorisation est valable pour une durée de deux (2) ans à compter de sa notification.

Le Président,

Etienne Marie FIFATIN

AUTORITE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Rue 6.076 « Immeuble El MARZOUK Joël »

Tel : (+229) 21 32 57 88 / 69 55 00 00
01 BP : 04837 Cotonou
Email: contact@apdp.bj
https://www.apdp.bj

Prévu par l'article 481 de la loi n°2017-20 du 20 avril 2018 portant code du numérique en République du Bénin.

2019

Rue 6.076 « Aïdjèdo, Immeuble El MARZOUK Joël »
COTONOU

Tél. 21 32 57 88 / 69 55 00 00
01 BP : 04837
Site web : www.apdp.bj
Email : contact@apdp.bj