**Délibération n° 2019-020/AT/APDP du 30 décembre 2019**

**Portant autorisation de collecte, traitement et transfert des données alphanumériques, biométriques et de santé des assurés de Atlantique Assurances Bénin IARDT.**

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 :

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

**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 de madame Ismath MAMADOU BIO -TCHANE et de monsieur Onésime Gérard MADODE, en qualité de membres de l'APDP précédemment, Commission Nationale de l'Informatique et des Libertés (CNIL);

**Vu** le règlement intérieur de l'Autorité de Protection des Données à caractère Personnel (APDP) ex Commission Nationale de l'Informatique et des Libertés (CNIL), en date du 25 janvier 2019;

**Vu** la lettre n° 074-2019/AAB-IARDT/DG/SP du 26 mars 2019 par laquelle le Directeur Général de Atlantique Assurances Bénin IARDT a sollicité l'autorisation pour la collecte, le traitement et le transfert des données alphanumériques, biométriques et de santé de ses assurés vers le Maroc;

**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 EXPOSE CE QUI SUIT:**

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

### 1-1 . Objet

Par lettre n° 074-2019/AAB-IARDT/DG/SP du 26 mars 2019, le Directeur Général de Atlantique Assurances Bénin IARDT a sollicité l'autorisation pour la collecte, le traitement et le transfert des données alphanumériques, biométriques et de santé de ses assurés vers la société Pactilis Sarl dont le siège est à Casablanca (Maroc).

### 1-2 . Responsable du traitement

Est considéré comme responsable du traitement, aux termes des dispositions de l'article 1er du livre préliminaire du code du numérique, ***« 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 Général de Atlantique Assurances Bénin IARDT.

## II- Examen de la demande d'autorisation du traitement

### 2-1. Recevabilité

Au regard des dispositions des articles 380, 381 et 407 du code du numérique, la demande du requérant est recevable.

### 2-2 . Finalités

Aux termes des dispositions de l'article 383.3 du 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 Directeur Général de Atlantique Assurances Bénin IARDT indique que le traitement envisagé a pour finalités de faciliter la gestion des contrats d'assurances et de contrôler l'identité des bénéficiaires lors des soins en Tiers Payant à travers une carte contenant leurs empreintes digitales.

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

**2-3 . Droits des personnes concernées**

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

- **Droit à l'information préalable**

Aux termes des dispositions de l'article 415 du code du numérique, 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 des courriers électroniques, lors des réponses écrites au questionnaire qui leur est soumis, par les informations sur intranet ou par affichage.

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

Conformément aux dispositions des articles 389 alinéa 1er, 390 et 415.8 et 10 du code du numérique, le consentement des personnes concernées est requis.

Le Directeur Général de Atlantique Assurances Bénin IARDT précise qu'il requiert à partir d'un formulaire dûment rempli par les assurés leur consentement.

**2.3.2- Droit d'accès**

L'article 437. 1, 2 et 3 du code du numérique dispose : ***« 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 note que le droit d'accès des assurés à leurs données personnelles est garanti par le requérant. Ce droit s'exerce par courrier électronique ou par courrier postal adressé au responsable du traitement ou déposé directement dans ses locaux.

L'APDP note que le délai de communication des informations demandées en cas d'exercice du droit d'accès fixé à 24 heures par le requérant est raisonnable, conformément aux dispositions de l'article 437 du code du numérique.

### 2.3.3- Droit d'opposition

Conformément aux dispositions de l'article 440 alinéa 1er du code du numérique, « ***Toute personne physique a le droit de s'opposer, à tout moment, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement*** ».

Le droit d'opposition est garanti par le requérant. Toutefois, les modalités d'exercice de ce droit n'ont pas été précisées.

Le requérant doit indiquer aux personnes concernées les modalités d'exercice du droit d'opposition, conformément aux dispositions de l'article 440 du code du numérique qui prévoient entre autres 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.

L'Autorité rappelle au requérant que la réponse à la demande d'opposition doit être donnée dans un délai maximum de trente (30) jours suivant la date de réception de la demande, conformément aux dispositions de l'article 440 précité.

### 2.3.4- Droit de rectification et de suppression

Conformément aux dispositions de l'article 441 du code du numérique, les droits de rectification et de suppression par les personnes concernées doivent être assurés par le requérant.

Le requérant déclare que ce droit est garanti à ses clients conformément aux clauses contractuelles. Cependant, les modalités d'exercice de ce droit n'ont pas été précisées.

Le requérant doit indiquer aux personnes , les modalités d'exercice du droit de rectification et de suppression, en application des dispositions de l'article 441 du code du numérique qui prévoient entre autres, 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.

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 441 précité.

**2.3.5-Droit à la portabilité**

Aux termes des 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 de 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 ce responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle*** ».

Le requérant déclare que ce droit est garanti à ses clients.

L'Autorité en prend acte.

**2-4. Proportionnalité**

Conformément aux dispositions de l'article 383.4 du code du numérique, « ***Les données collectées doivent être 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 de Atlantique Assurances Bénin IARDT.

Les catégories de données collectées sont de trois ordres. Il s'agit de :

- **données sur l'identité des assurés *et des bénéficiaires*** : Nom et prénoms, date et lieu de naissance ;
- ***données de santé des assurés et des bénéficiaires*** : affections, soins reçus ;
- **empreintes digitales *des assurés et des bénéficiaires*** **:** les deux index.

Ces informations sont recueillies aussi bien auprès des assurés et des bénéficiaires (empreintes digitales), de l'employeur (données sur l'identité) que des médecins traitants (données de santé).

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 Directeur Général de Atlantique Assurances Bénin IARDT déclare que les données seront conservées pour la durée nécessaire à l'exécution du contrat. Il affirme que ces données seront ensuite archivées pendant dix (10) ans, conformément à l'article 404 du code des assurances appelé Code CIMA qui dispose : « ***Les entreprises doivent conserver pendant dix ans au***

***moins leurs livres de comptabilité, les lettres qu'elles reçoivent, les copies des lettres qu'elles adressent, ainsi que toutes pièces justificatives de leurs opérations ».***
L'autorité rappelle au requérant qu'il doit se conformer aux dispositions des articles 338.22, 383.6 et 433 du code du numérique relatives à la conservation et à l'archivage des données collectées.

### 2-6. Interconnexion de bases de données

Le requérant indique qu'il ne procède pas à l'interconnexion de bases de données.

L'Autorité en prend acte.

### 2-7. Sous-traitance :

Le requérant indique qu'il utilise les services de trois sous-traitants à savoir Pactilis SARL, Digital Ocean et Microsoft Ireland Operations Limited qui interviennent dans la chaîne de traitement des données à caractère personnel respectivement pour la gestion des contrats d'assurances, la vérification des droits et l'édition des certificats de prise en charge, la gestion des assurés et de leurs dossiers.

Le réquérant déclare qu'un contrat de confidentialité a été signé avec chacun de ses sous-traitants.

L'Autorité en prend acte.

### 2-8. Traitement des données de santé et des données biométriques

Aux termes des dispositions de l'article 394 du code du numérique, le traitement des données sensibles telles que les données de santé et les données biométriques est en principe interdit.

Toutefois, l'interdiction est levée et les conditions et modalités de traitement des données sensibles sont prévues aux points 1 à 15 dudit article.

En ce qui concerne les données de santé, le requérant indique que le traitement est effectué sous la supervision d'un professionnel de santé et que les informations communiquées par les clients à Atlantique Assurances Bénin IARDT sont conservées sur un disque dur interne protégé dans un coffre-fort. Ces données sont consultées sur la base d'un profil d'habilitation et de contrôle d'accès logique (mot de passe, pin, etc.).

S'agissant des données biométriques, le requérant affirme que les empreintes des deux index (main gauche et main droite) seront collectées sur un lecteur d'empreintes digitales du modèle "Gilles Leroux Industries" lequel procèdera à leur enregistrement sur une carte ; la finalité étant de permettre l'identification et l'authentification des bénéficiaires des garanties souscrites.

L'APDP estime qu'en raison de l'activité du requérant qui consiste dans la conclusion et la gestion en ligne de contrats d'assurances santé, le traitement de données de santé et de données biométriques est justifié au regard des dispositions de l'article 394 du code du numérique.

### 2-9. Sécurité

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

Les locaux abritant les équipements de traitement des données personnelles sont protégés par des agents de sécurité. Des mesures de sécurité contre les incendies, les surtensions et les phénomènes électromagnétiques sont prises en compte pour assurer la résilience constante desdits équipements.

- **Sécurité logique des données**

Les obligations de confidentialité sont garanties par la mise en place des habilitations aux personnes qui, en raison de leur fonction ou pour les besoins du service, ont directement accès aux données traitées grâce à un système d'identification par mot de passe.

Des dispositions sont également prises pour assurer l'intégrité des données à travers le système de gestion des autorisations d'accès, des logs et le cryptage des données mis en place.

La sauvegarde des données est effectuée trois (03) fois dans la journée en local et sur un site distant. Des dispositions sont prises pour assurer la disponibilité permanente des données grâce à l'architecture n-tiers avec plusieurs bases de données en cas de panne du système.

Un plan de reprise et de continuité d'activités est prévu en cas de sinistres ou de pannes.

L'Autorité estime que les mesures de sécurité physique des locaux et logique des données sont acceptables.

## III- Examen de la demande de transfert de données

Le Directeur Général de Atlantique Assurances Bénin IARDT sollicite l'autorisation de transfert des données personnelles collectées vers son partenaire Pactilis Sarl dont le siège est à Casablanca au Maroc.

Il convient, pour l'examen de cette demande, de se référer à l'analyse précédente sur les points ci-après : consentement et principe de légitimité, droits des personnes concernées, durée de conservation et mesures de sécurité.

Seront cependant examinées, la finalité, la proportionnalité et les garanties dans le pays destinataires.

### 3.1- Finalité

Le requérant déclare que les données collectées sont transférées au Maroc sur la plateforme de la société Pactilis Sarl.

La finalité du transfert est le traitement des données à caractère personnel en vue de la gestion des contrats d'assurances. Cela implique la gestion du backoffice, l'établissement des états de remboursement et les statistiques.

Le transfert des données envisagé est donc justifié au regard de sa finalité.

### 3.2- Proportionnalité

Les catégories de données transférées sont : nom et prénoms, date et lieu de naissance et données de santé.

L'APDP considère que les données faisant l'objet du transfert sont adéquates, pertinentes et non excessives au regard de la finalité.

### 3.3- Garanties dans le pays destinataire

Aux termes des dispositions de l'article 391 alinéa 1er du code du numérique, le transfert de données à caractère personnel vers un Etat tiers ou une organisation internationale ne peut avoir lieu que lorsque l'Autorité constate que l'Etat ou l'organisation internationale en question assure un niveau de protection équivalent à celui mis en place par les dispositions du code du numérique en République du Bénin.

Le Directeur Général de Atlantique Assurances Bénin IARDT indique que les données à caractère personnel seront transférées à la société Pactilis Sarl au Maroc. Il existe dans ce pays la Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP). De même, la société Pactilis est dotée de plusieurs accréditations et elle a introduit une demande d'autorisation de traitement auprès de la CNDP.

Par ailleurs, à l'instar du Bénin, le Maroc est membre du Réseau Africain des Autorités de Protection des Données Personnelles (RAPDP).

Eu égard à ce qui précède, l'Autorité estime équivalent le niveau de garanties qu'offre le pays destinataire des données des clients de Atlantique Assurances Bénin IARDT.

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

**Enjoint au requérant de veiller à ce que la société Pactilis accomplisse effectivement auprès de l'Autorité en charge de la protection des données personnelles du Maroc, les formalités d'autorisation requises et en rendre compte à l'APDP.**

**Recommande au requérant de :**

- **Informer les personnes concernées par le traitement, des modalités d'exercice de leurs droits d'opposition, de rectification et de suppression des données à caractère personnel;**

- **se conformer aux dispositions des articles 338.22, 383.6 et 433 du code du numérique relatives à la conservation et à l'archivage des données à caractère personnel.**

**Rappelle au requérant que :**

- **le traitement déclaré ne saurait être détourné de ses finalités ;**
- **le responsable du traitement, son représentant et ses sous-traitants doivent veiller à la mise en œuvre effective des mesures de sécurité, conformément aux dispositions de l'article 426 du code du numérique ;**
- **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, conformément aux dispositions de l'article 387 du code du numérique;**
- **sa responsabilité est engagée en cas de manquement aux prescriptions du code du numérique, conformément aux dispositions de l'article 451 dudit code.**

**Sous réserve de ce qui précède,**

**Autorise la mise en œuvre du traitement automatisé des données à caractère personnel des clients de Atlantique Assurances Bénin IARDT et le transfert desdites données vers la société Pactilis SARL au Maroc.**

**Conformément aux dispositions des articles 462 et 489 du code du numérique, l'APDP se réserve le droit de procéder à des contrôles aux fins de s'assurer du respect par le réquérant des termes et conditions de la présente délibération.**

**Cette autorisation est valable pour une durée de deux (02) ans à compter de sa notification.**

Le Président,

**Etienne Marie FIFATIN**