Délibération n° 2020-022/AT/APDP du 29 mai 2020
portant autorisation de traitement des données alphanumériques, biométriques et de santé des salariés de Coris Bank International Benin.

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 :

- Amouda ABOU SEYDOU ;
- Nicolas BENON ;
- Guy-Lambert YEKPE;
- Soumanou OKE ;
- Imourane LEKOYO.

Vu la loi n° 90-32 du 11 décembre 1990 portant Constitution de la République du Bénin, modifiée par la loi n° 2019-40 du 07 novembre 2019 ;

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", deuxième mandature ;

Vu le règlement intérieur de l'Autorité de Protection des Données Personnelles (APDP) du 25 janvier 2019 ;

Vu la lettre n° 2127/09/19/DG/DS/DSI/AS du 17 septembre 2019, par laquelle le Directeur Général de Coris Bank International Bénin a transmis des formulaires de demande d'autorisation et de déclaration à l'APDP ;

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 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° 2127/09/19/DG/DS/DSI/AS du 17 septembre 2019, le Directeur Général de Coris Bank International Bénin sollicite de l'APDP l'autorisation de traitement des données alphanumériques, biométriques et de santé des salariés de son entreprise.

1-2 . Responsable du traitement

Est considéré comme responsable de traitement, aux termes des dispositions de l'article 1er 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 Coris Bank International Bénin.

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

CORIS BANK INTERNATIONAL Bénin déclare que le traitement des données personnelles de ses salariés a pour finalités la gestion du personnel et le contrôle d'accès à la banque.

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, qu'il garantit le droit à l'information préalable par courrier électronique.

L'APDP en prend acte.

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

Conformément aux dispositions des articles 389 alinéa 1er, 390 et 415 points 8 et 10 du code du numérique, le consentement des personnes concernées est requis.

Le requérant précise qu'il recueille le consentement des personnes dont les données sont collectées par écrit.

L'APDP en prend acte.

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 des salariés à leurs données personnelles est garanti et s'exerce auprès du responsable du traitement par courrier électronique ou postal.

Il précise qu'en cas d'exercice du droit d'accès, la réponse est donnée à la personne concernée dans un délai maximal de 60 jours.

L'APDP en prend acte.

2.3.3- Droit d'opposition

Conformément aux dispositions de l'article 440 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 requérant déclare que le droit d'opposition est garanti aux personnes dont les données sont traitées.

L'APDP en prend acte.

Elle recommande toutefois au requérant, d'indiquer aux salariés, les modalités d'exercice du droit d'opposition, conformément aux dispositions de l'article 440 du code du numérique.

2.3.4- Droit de rectification et de suppression

Conformément aux dispositions de l'article 441 du code du numérique, le droit de rectification et de suppression par les personnes concernées par un traitement de données à caractère personnel doit être assuré par le requérant.

Ce droit est garanti par le requérant aux personnes concernées par le traitement et s'exerce auprès du responsable du traitement.

L'Autorité en prend acte.

Elle rappelle toutefois, 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.

2.3.5- Droit à la portabilité

Suivant les 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... ».*

Le requérant déclare qu'il garantit ce droit aux salariés dont les données personnelles sont traitées.

L'Autorité en prend acte.

Elle recommande toutefois au requérant, d'indiquer aux personnes concernées les modalités d'exercice dudit droit dans le respect des dispositions de l'article 438 sus cité.

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 salariés de Coris Bank International Bénin.

Les catégories de données collectées sont :

- données nominatives : **Nom et prénoms, date et lieu de naissance, nationalité, situation matrimoniale, date d'embauche, Identifiant Fiscal Unique (IFU), numéro d'immatriculation à la Caisse Nationale de Sécurité Sociale (CNSS), numéro à la Caisse de Retraite par Répartition Avec Epargne (CRRAE).**
- données sensibles : **empreintes digitales (un doigt), données de santé.**

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 ne donne aucune précision sur la durée de conservation des données personnelles collectées.

Le requérant doit limiter la durée de conservation des données personnelles des salariés à celle nécessaire à l'atteinte des finalités, conformément aux dispositions de l'article 383.6 du code du numérique.

2-6 Communication des données à d'autres organismes au Bénin

Le requérant déclare qu'il communique les données personnelles de ses salariés à la BCEAO, à la Cellule Nationale de Traitement des Informations Financières (CENTIF), à la Caisse de Retraite par Répartition Avec Epargne (CRRAE) et à la Caisse Nationale de Sécurité Sociale (CNSS).

Ces communications ont pour finalités le respect des clauses d'adhésion à la CNSS et au CRRAE ainsi que le respect des obligations réglementaires de la BCEAO.

L'Autorité en prend acte.

2-7 Sous-traitance

Le requérant indique qu'il utilise les services d'un médecin de travail qui exerce son activité sous le sceau du secret professionnel.

L'Autorité en prend acte.

2-8 Traitement des données de santé

L'article 394 du code du numérique dispose entre autres 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 prévus aux points 1 à 15 de l'article précité.

Le requérant indique 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.

Les informations de santé fournies par les salariés sont conservées uniquement par le responsable de santé et les résultats sont communiqués directement à chaque salarié par le médecin du travail.

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

2-9 Traitement des données biométriques

Il ressort des dispositions de l'article 394 du code du numérique que le traitement des données biométriques est interdit. Toutefois, l'interdiction ne s'applique pas dans certains cas particuliers prévus aux points 1 à 15 de l'article précité.

Coris Bank International Bénin indique qu'il collecte les empreintes digitales d'un (01) doigt en vue du contrôle des accès aux bâtiments.
Les empreintes sont prises par un lecteur d'empreintes digitales.

L'Autorité en prend acte.

Elle recommande toutefois au requérant, de chiffrer ou d'anonymiser les données biométriques lors de leur sauvegarde.

2-10 Mesures de sécurité

- **Sécurité physique**

Les salles abritant les équipements de traitement des données sont protégées par un système d'accès électronique. Des équipements de sécurité contre les incendies, les surtensions et les phénomènes électromagnétiques sont installés pour assurer la protection et la résilience constante des systèmes de traitement.

- **Sécurité logique**

La confidentialité et l'intégrité des données personnelles 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.

Un logiciel de gestion des logs est installé aux fins d'audit.

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

La sauvegarde des données est effectuée mensuellement.

Des mesures de sécurité spécifiques pour la protection du réseau informatique et de la base de données personnelles contre les intrusions sont également prises dans le cadre de ce traitement.

Les personnes impliquées dans le traitement sont informées de la législation en vigueur en matière de protection des données personnelles.

L'Autorité estime que les mesures de sécurité prises par le requérant sont satisfaisantes. Elle recommande néanmoins le chiffrement des données biométriques, la sauvegarde régulière ainsi que la mise en place d'une procédure visant à tester et évaluer les mesures techniques prises.

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

Enjoint à Coris Bank International Bénin d'avoir à limiter la durée de conservation des données personnelles des salariés à celle nécessaire à l'atteinte des finalités, conformément aux dispositions de l'article 383.6 du code du numérique.

Recommande au requérant de :

- **indiquer aux personnes concernées, les modalités d'exercice des droits d'opposition, de rectification, et de suppression ainsi que du droit à la portabilité, conformément aux dispositions des articles 440, 441 et 438 du code du numérique ;**

- **chiffrer ou anonymiser les données biométriques lors de leur sauvegarde et prévoir des sauvegardes rapprochées planifiées de manière automatique ;**

- **mettre en place une procédure visant à tester, analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.**

Rappelle au requérant que :

- **le traitement déclaré ne saurait être détourné de ses finalités ;**
- **en cas d'exercice du droit de rectification et 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 441 du code du numérique.**
- **un registre des activités du traitement menées doit être tenu, conformément aux dispositions de l'article 435 du code du numérique ;**

- **un rapport annuel d'activités de traitement menées doit être adressé à l'Autorité , en application des dispositions de l'article 387 dernier alinéa 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 le traitement des données alphanumériques, biométriques et de santé des salariés de Coris Bank International Bénin.

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 requérant des termes et conditions de la présente autorisation.

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

Le Président,

Etienne Marie FIFATIN

APDP
AUTORITE DE PROTECTION DES DONNEES PERSONNELLES