ARTCI
AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE
CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2024-1129

DE L'AUTORITE DE PROTECTION DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 29 AOÛT 2024

PORTANT AVERTISSEMENT ET MISE EN DEMEURE DE LA SOCIETE CORIS BANK INTERNATIONAL COTE D'IVOIRE (CBI-CI) EN MATIERE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Conseil de Régulation : 31 Av Noguès, Imble Broadway 2ème étage 17 BP 110 Abj 17 Tél: +225 27 20 34 43 04 - Fax: +225 27 20 34 43 02
Siège Direction Générale : Marcory Anoumabo, 18 BP 2203 Abj 18 Tél: +225 27 20 34 43 73 / 74 - Fax: + 225 27 20 34 43 75
www.artci.ci

L'AUTORITE DE PROTECTION,

Vu le Règlement n°15/2002/CM/UEMOA du 23 mai 2002 relatif aux systèmes de paiement dans les états membres de l'Union Economique et Monétaire Ouest Africaine (UEMOA) ;

Vu la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Vu la Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité ;

Vu la Loi n°2013-546 du 30 juillet 2013 relative aux Transactions électroniques ;

Vu la Loi n°2014-136 du 24 mars 2014 portant règlementation des bureaux d'information sur le crédit ;

Vu la Loi n°2016-992 du 14 novembre 2016 relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme ;

Vu la Loi n°2019-869 du 14 Octobre 2019 modifiant l'Ordonnance 2009-385 du 1er décembre 2009 portant règlementation bancaire ;

Vu la Loi n°2024-352 du 06 juin 2024 relative aux communications électroniques ;

Vu l'Ordonnance n°2011-367 du 03 novembre 2011 portant règlementation des systèmes financiers décentralisés ;

Vu le Décret n°2012-934 du 19 septembre 2012 portant organisation et fonctionnement de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) ;

Vu le Décret n°2014-105 du 12 mars 2014 portant définition des conditions de fourniture des prestations de cryptologie ;

Vu le Décret n°2014-106 du 12 mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique ;

Vu le Décret n°2015-79 du 04 février 2015 fixant les modalités de dépôt des déclarations, de présentation des demandes, d'octroi et de retrait des autorisations pour le traitement des données à caractère personnel ;

Vu le Décret n°2019-947 du 13 novembre 2019 portant nomination du Président de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le Décret n°2019-985 du 27 Novembre 2019 portant nomination des Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire (ARTCI) ;

Vu le Décret n°2022-265 du 13 Avril 2022 portant nomination du Directeur Général de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire (ARTCI) ;

Vu le Décret n°2022- 783 du 12 Octobre 2022 portant renouvellement partiel du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/ TIC Côte d'Ivoire, en abrégé ARTCI ;

Vu l'Arrêté n°511/MPTIC/CAB du 11 novembre 2014 portant définition du profil et fixant les conditions d'emploi du correspondant à la protection des données à caractère personnel ;

Vu la Décision n°2013-0003 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 20 septembre 2013 portant règlement intérieur ;

Vu la Décision n°2014-0020 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 03 septembre 2014 portant adoption des règles de conduites relatives au traitement et à la protection des données à caractères personnel ;

Vu la Décision n°2014-0021 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 03 septembre 2014 portant conditions et critères applicables à la limitation du traitement des données à caractère personnel ;

Vu la Décision n°2014-0022 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 03 septembre 2014 portant conditions de la suppression des liens vers les données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communication électronique accessibles au public ;

Vu la Décision n°2017-353 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 octobre 2017 portant vérification préalable ;

Vu la Décision n°2017-354 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Vu la Décision n°2020-0581 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 30 juillet 2020 fixant les critères et les conditions d'exercice des activités de Correspondant à la protection des données, personne morale, audit de conformité, formation ;

Vu la Décision n°2021-0676 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 04 Août 2021 portant procédure de contrôle en matière de protection des données à caractère personnel ;

Vu la Décision n°2023-0920 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 20 Juillet 2023 portant approbation de la liste des contrôles en matière de protection des données à caractère personnel pour l'année 2023 ;

Vu le courrier n°23-01272/DG/DCNS/DCPD/SPDS/JLC du 19 septembre 2023 portant information de la mission de contrôle ;

Vu les Procès-verbaux de contrôle n° 008/02/2024 du 13, 14, 15, 16 février 2024 ;

Par les motifs suivants :

I. Faits et procédure

Considérant que l'article 46 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, dispose que l'Autorité de Protection veille à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de ladite loi et de ses décrets d'application ;

Considérant qu'aux termes des articles 47 et suivants de la Loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, l'Autorité de Protection est chargée de procéder par le biais d'agents assermentés, à des vérifications portant sur tout traitement de données à caractère personnel et de prononcer des sanctions administratives et pécuniaires à l'égard des responsables du traitement qui ne se conforment pas aux dispositions de la présente Loi ;

Considérant la Décision n°2021-0676 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 04 Août 2021 portant procédure de contrôle en matière de protection des données à caractère personnel ;

Considérant que la société Coris Bank International (CBI-CI) a été identifiée par la Décision n°2023-0920 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 20 Juillet 2023 portant approbation de la liste des contrôles en matière de protection des données à caractère personnel pour l'année 2023 comme un responsable du traitement à contrôler ;

Considérant que par lettre n°23-01272/ DG/DCNS/DCPD/SPDS/JLC du 19 septembre 2023, la société Coris Bank International (CBI-CI) a été informée que la mission de contrôle en matière de protection des données à caractère personnel, se tiendra les 12,13, 14, 15, 16 février 2024 dans son agence de Yamoussoukro ;

Cette mission avait pour objet de vérifier le respect par la société Coris Bank International (CBI-CI) de l'ensemble des dispositions de la Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ainsi que celles de ses sous-traitants ;

Ainsi, les agents assermentés ont effectué des contrôles sur les traitements de données à caractère personnel des clients, du personnel, des visiteurs et sur les traitements mis en œuvre par la société Coris Bank International (CBI-CI) et ses sous-traitants ;

Considérant que l'Autorité de Protection a effectué les contrôles suivants :

- Contrôle des activités du Chef d'Agence ;
- Contrôle des activités de la chargée de clientèle (Conseiller clientèle par intérim) ;
- Contrôle des activités de la caissière ;
- Contrôle des activités de la Direction Juridique ;
- Contrôle des activités de la Direction Informatique ;
- Contrôle des activités du responsable conformité ;
- Contrôle des activités du Correspondant à la Protection ;
- Contrôle des procédures et de la documentation ;
- Contrôle du site internet ;
- Autres constats.

Considérant qu'à l'issue du contrôle, une copie des Procès-verbaux de contrôle n° 008/02/2024 du 13, 14, 15, 16 février 2024, contradictoirement dressés et signés, a été remise à la société Coris Bank International (CBI-CI).

II. Motifs de la Décision :

A) Sur les manquements à l'obligation de conformité et d'autorisation de traitement avec la Loi n°2013-450 du 19 juin 2013 relative à la protection des données personnelles

Considérant qu'aux termes de l'article 7 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le traitement portant sur un numéro national d'identification ou tout autre identifiant de la même nature, notamment les numéros de téléphone est soumis à autorisation préalable de l'Autorité de Protection, avant toute mise en œuvre ;

Considérant que l'article 53 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données personnelles dispose que : « *les responsables de traitement de données à caractère personnel disposent d'un délai de six (06) mois, à compter de la date de l'entrée en vigueur de la présente loi, pour se mettre en conformité avec ses dispositions* » ;

Considérant que l'article 2 de la Décision n°2017-354 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel dispose que : « *la mise en conformité implique que les mesures techniques, organisationnelles et juridiques, nécessaires pour la protection des données à caractère personnel ont été prises par le Responsables du traitement* » ;

Considérant que l'article 4 de la Décision n°2017-354 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel dispose que : « (...) *la demande de mise en conformité est adressée à l'Autorité de Protection* » ;

Considérant qu'au moment du contrôle, l'Autorité de Protection a constaté :

- ***L'absence d'autorisations spécifiques de traitement au sens de l'article 7 de Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel et de ses textes d'application ;***

- ***L'absence d'autorisation de mise en conformité au sens de la Décision n°2017-354 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.***

Par conséquent, l'Autorité de Protection considère que la société Coris Bank International (CBI-CI) n'a pas respecté les dispositions des articles 7 et 53 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

B) Sur le non-respect du principe de la légitimité et licéité des traitements

Considérant que conformément aux dispositions de l'article 14 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le traitement de données à caractère personnel est considéré comme légitime si la personne concernée donne expressément son consentement préalable ;

Considérant toutefois que le consentement doit être exprès, non équivoque, libre spécifique et éclairé ;

Considérant que la personne concernée doit avoir été suffisamment informée par le responsable du traitement, avant de donner librement son consentement, afin d'être en mesure de comprendre d'une part, la portée et les conséquences de son consentement, et d'autre part, les avantages et les inconvénients du traitement ;

Considérant que lors du contrôle et après analyse des documents, l'Autorité de Protection a constaté sans que la liste ne soit exhaustive :

- L'existence d'un accord des salariés pour l'installation du dispositif de vidéosurveillance ;

- L'existence d'une clause de protection des données personnelles dans le KYC (personne morale ou personne physique) ;

- L'existence d'un formulaire de recueil du consentement contenant des cases à cocher pour l'embauche, le recrutement, la gestion de la paie, le suivi de la carrière et le respect des obligations règlementaires ;

- ***L'absence de clauses relatives à la protection des données personnelles dans les conditions générales d'utilisation du produit « contrat porteur-carte de retrait/ paiement de compte et de produits électroniques ;***

- ***L'absence de recueil de consentement spécifique dans les conditions générales de compte (compte chèque et compte épargne) ;***

- ***L'absence de clauses de données personnelles dans le contrat de travail ;***

Dès lors, l'Autorité de Protection considère que tous les traitements opérés satisfont partiellement au principe de la légitimité prévus à l'article 14 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

C) Sur les finalités

Considérant l'article 16 de la Loi relative à la protection des données à caractère personnel qui dispose que les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités ;

Considérant que lors du contrôle et l'analyse des documents, l'Autorité de Protection a constaté, sans que la liste ne soit exhaustive :

- L'Existence de finalités de traitement de données à caractère personnel dans les formulaires de souscriptions (ouverture de comptes, etc…) ;

- L'Existence de finalités de traitement de données à caractère personnel pour les salariés ;

- Les finalités liées à l'utilisation des dispositifs de vidéosurveillance sont identifiées et clairement définies ;

- L'Existence de finalités dans la charte de protection des données personnelles affichées dans les locaux de la CBI-CI ;

Considérant que pour que la finalité d'un traitement de données soit légitime, il est nécessaire qu'à tous les stades et à tout moment, celui-ci repose soit sur le consentement de la personne concernée soit sur l'un des cas prévus par dérogation à l'exigence de consentement ;

Dès lors, l'Autorité de Protection considère que les finalités sont déterminées, explicites mais illégitimes.

D) Sur la période de conservation des données traitées

Considérant que l'article 16 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel dispose que, les données traitées doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ;

Considérant que lors du contrôle et après analyse des documents, l'Autorité de Protection a constaté :

- L'Existence d'une politique de gestion des archives ;
- L'Existence d'une durée d'utilité administrative pendant laquelle les archives courantes et intermédiaires doivent être conservées ;
- **La conservation définitive des documents lorsque ceux-ci ont une valeur historique ;**
- **Les durées de conservation ne sont pas clairement définies dans la politique d'archives ;**
- L'Existence d'un correspondant archive par direction pour la consultation des documents ;
- L'Existence de délai de conservation des données dans la charte de protection des données personnelles ;
- La conservation des données des salariés dans des armoires ignifuges fermées à clé ;
- **La conservation des arrêts maladies annuellement et transmis aux archives après l'expiration du délai d'un an ;**
- **Un délai de conservation imprécis pour les curriculums vitae reçus numériquement ;**
- **La conservation annuelle des arrêts maladies. A l'expiration de ce délai, les arrêts sont transmis aux archives sans précision des délais ;**
- **Les contrats arrivés à expiration sont conservés sans précision de délai ;**
- Les cartons d'archives sont conservés en tenant compte de la « conservation trentenaire (prescription) » ;
- Les données collectées dans le cadre des activités de la conformité sont conservées pendant dix (10) ans suivant la règlementation bancaire ;
- Les données collectées dans le cadre des activités de la conformité sont conservées dans les armoires ignifuges et sur un cloud stocké en local ;
- « Les données issues d'un signalement n'ayant pas abouti à une procédure disciplinaire ou judiciaire seront détruites ou archivées, après anonymisation dans un délai de deux (02) mois suivant la fin des investigations » ;
- **« Les données issues d'un signalement suivi d'une procédure disciplinaire ou judiciaire sont conservées pour l'intégralité de la durée de la procédure puis archivées jusqu'à la fin du délai légal prescrit en vigueur » ;**

- **La politique de contrôle d'accès ne précise pas le délai de suppression des comptes après qu'ils ont été bloqués du système d'information ;**

Considérant que la société Coris Bank International (CBI-CI) ne dispose pas de délai de conservation clairement définis pour certaines données ;

Considérant que la société Coris Bank International (CBI-CI) n'a pu fournir à l'Autorité de Protection, les durées de conservation pour tous les différents points de contrôles ;

Dès lors, l'Autorité de Protection, au regard de la nature des données traitées considère que le principe de la conservation limité des données est partiellement respecté.

E) Sur la proportionnalité des données collectées

Considérant que selon les dispositions de l'article 16 de la Loi n°2013-450 du 19 juin 2013, relative à la protection des données à caractère personnel, les données traitées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ;

Considérant que lors du contrôle et après analyse des documents, l'Autorité de Protection a constaté sans que la liste ne soit exhaustive :

- ***La collecte du nom, prénoms, adresse, la date et lieu de naissance, le domicile, la filiation de la partie adverse dans le cadre des contentieux aux fins d'éviter les homonymies ;***

- ***La collecte du noms, prénoms, date et lieu de naissance, la filiation, les informations sur le patrimoine du débiteur dans le cadre du recouvrement ;***

- ***La collecte des informations sur la progéniture peut être faite dans certains cas ;***

- ***L'absence de politique de gestion des données sensibles ;***

Considérant que la société Coris Bank International (CBI-CI) n'a pu fournir à l'Autorité de Protection, les textes qui autorisent la collecte des informations sur la progéniture ;

Considérant l'absence de politique de gestion des données sensibles ;

Par conséquent, l'Autorité de Protection considère que le principe de la proportionnalité n'est pas respecté.

F) Sur les destinataires ou catégories de destinataires habilités à recevoir communication des données

Considérant les dispositions de l'article 9 de la Loi n°2013-450 relative à la protection des données à caractère personnel, le responsable du traitement est tenu d'indiquer les destinataires habilités à recevoir communication des données traitées ;

Considérant que les destinataires internes et externes doivent être clairement identifiés ;

Considérant qu'à l'issue du contrôle et après analyse des documents, la société Coris Bank International (CBI CI) indique que les destinataires des données traitées sont les suivants :

- La cellule nationale de traitement de l'Information financière (CENTIF) ;
- La société SANLAM dans le cadre de la convention d'assurance « coris éducation ;
- La société ALLIANZ dans le cadre des conventions d'assurance ALLIANZ ;
- Les partenaires pour les transferts d'argent (Western Union, money gram, RIA, orange money, rapidex, jubaexpress, MTN MOMO) ;
- Les cabinets d'assistance juridique que sont la SCPA Konan-Loan Associés et le Cabinet KS associés ;
- La holding au Burkina Faso pour les données collectées sur le site.

Considérant que les destinataires des données internes et externes mentionnés communiqués à l'Autorité de Protection sont incomplets, insuffisants, non clairement identifiés ;

Considérant que les ***transferts de données à caractère personnel opérés par la société Coris Bank International (CBI-CI) à destination du Burkina Faso ne sont pas déclarés à l'Autorité de Protection ;***

L'Autorité de Protection considère que :

- ***les destinataires des données sont incomplets et ne disposent pas d'autorisation de traitement ;***
- ***les destinataires des données ne sont pas clairement identifiés ;***
- ***les transferts de données à caractère personnel opérés par la société Coris Bank International (CBI-CI) ne sont pas en conformité avec la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.***

G) Sur la transparence des traitements

Considérant qu'aux termes des articles 18 et 28 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la transparence implique l'information obligatoire et claire des personnes concernées par le responsable du traitement ;

Qu'il s'agit en l'espèce pour le responsable du traitement de faire preuve de transparence vis-à-vis des personnes concernées qui devront notamment être informées. Les affiches ou des pictogrammes doivent indiquer, d'une façon claire et visible, les informations suivantes :

- de l'identité du Responsable du traitement et le cas échéant, celle de son représentant dûment mandaté ;
- de la finalité du traitement ;
- du fait que la société Coris Bank International (CBI-CI) soit placée sous vidéosurveillance ;
- des catégories de données concernées ;
- des destinataires auxquels les données sont susceptibles d'être communiquées ;
- de l'existence et des modalités d'exercice de leur droit d'accès et de rectification ;
- de la durée de conservation des données ;
- de l'éventualité de tout transfert de données à destination de pays tiers.
- le numéro de l'Autorisation délivrée par l'Autorité de Protection

Considérant que lors du contrôle et après analyse des documents, l'Autorité de Protection a constaté entre autres :

- L'existence d'une clause relative à la protection des données personnelles qui contient les finalités, la durée de conservation, les droits des personnes concernées et l'adresse du correspondant (formulaires KYC) ;

- Les conventions d'assurance ALLIANZ (groupe décès emprunteurs coris, coris assistance obsèques, coris bourses études) contiennent une clause relative à la protection des données personnelles ;

- **L'absence de mentions d'informations sur la protection des données personnelles sur les formulaires d'ouverture de compte ;**
- L'existence de la politique de confidentialité sur le site internet ;
- **L'existence d'un dispositif de vidéosurveillance contenant que les finalités, la durée de conservation, les contacts téléphoniques et l'adresse mail du Correspondant à la protection pour l'exercice des droits ;**
- **Le formulaire de signalement (exercice du droit d'alerte) ne contient pas de dispositions sur la protection des données personnelles ;**

- **La convention d'assurance SANLAM « coris éducation » ne prévoit pas de clauses relatives à la protection des données personnelles ;**

Considérant que l'affiche de la vidéosurveillance ne contient pas le numéro de la décision d'autorisation de traitement ;

Par conséquent, **l'Autorité de Protection considère que les traitements effectués au moyen de la vidéosurveillance et des formulaires ci-dessus énumérés ne sont pas conformes au principe de la transparence.**

H) Sur les droits des personnes concernées

Considérant que les articles 9 et 29 à 34 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel prescrivent que le responsable du traitement doit indiquer dans sa demande, la fonction de la personne ou le service auprès duquel s'exercent les droits reconnus aux personnes concernées, notamment les droits d'accès, de rectification, de suppression ;

Considérant que lors du contrôle et après analyse des documents, l'Autorité de Protection a constaté entre autres :

- L'existence d'un correspondant à la protection des données ;
- L'accès à toutes les ressources de la banque ;
- Il est associé à toutes les prises de décisions dans le cadre de la protection des données personnelles ;
- Il est assisté par des relais (chef d'agence et chef de service) pour l'accompagner dans ses fonctions de correspondant ;
- L'existence du contact du correspondant à la protection dans la procédure client ;
- **L'absence de procédure de réclamation des droits des personnes concernées ;**
- L'existence d'une fiche de poste pour le correspondant ;
- L'existence d'une charte de protection des données personnelles ;
- Le correspondant dépend administrativement du Directeur Général et fonctionnellement du comité du risque (comité spécialisé du conseil d'administration) ;
- **Le correspondant n'a pas déposé de rapport annuel auprès de l'Autorité de Protection.**

L'Autorité de Protection considère que les droits des personnes concernées sont partiellement respectés.

I) Sur les mesures de sécurité

Considérant que l'article 40 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel dispose que le responsable du traitement est tenu de prendre toute précaution au regard de la nature des données et, notamment, pour

empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Considérant que lors du contrôle et après analyse des documents, l'Autorité de Protection a constaté entre autres :

- L'existence d'un contrôle d'accès par badge pour l'entrée à la salle serveur ;
- L'existence d'un dispositif de vidéosurveillance pour la sécurité des biens et des personnes ;
- L'accès à la salle de visualisation des écrans s'effectue par badge ;
- L'Utilisation d'un mot de passe minimum de dix (10) caractères alphanumériques pour une durée de validité de trois (03) mois ;
- L'existence d'une double authentification et une surveillance sur les différents accès aux applications et infrastructures générés par Wallix ;
- L'existence d'un login et mot de passe et d'un token pour l'accès aux applications métiers ;
- L'existence d'un antivirus sur les postes de travail ;
- L'existence d'un serveur dédié pour les archives électroniques ;
- L'existence d'un plan de continuité ;
- L'existence d'une politique de sauvegarde des données centralisée au niveau du groupe ;
- L'existence d'un certificat SSL (TLS.1.3) sur le site internet de CBI-CI ;
- L'existence d'une politique de sécurité du système d'information ;
- L'existence d'une politique de mot de passe ;
- L'existence d'une politique de contrôle d'accès basée sur les normes (iso 27001, 27002, 27005, PCI DSS) ;
- L'existence d'une veille périodique sur la sécurité du système d'information pour d'éventuelles vulnérabilités et mise à jour des applications et anti-virus ;

L'Autorité de Protection considère que les mesures de sécurité sont suffisantes.

J) Sur les procédures internes de la société Coris Bank International (CBI CI)

Considérant que la société Coris Bank International (CBI CI) a communiqué plusieurs procédures à l'Autorité de Protection.

Considérant que l'analyse de ces procédures, sans que la liste ne soit exhaustive, fait ressortir les points suivants :

- **L'existence d'une procédure de traitement des réclamations clients. Toutefois, les réclamations contenues dans cette procédure portent sur les opérations et les cas de fraude en matière bancaire. Les aspects liés à la protection des données personnelles ne sont pas pris en compte ;**

- L'existence d'une charte utilisateur des ressources informatiques. Cette charte adoptée en avril 2015 prévoit des mentions relatives à la date, la signature des utilisateurs, une disposition sur la protection des données personnelles et de la propriété intellectuelle ;

- L'existence d'une procédure d'exercice du droit d'alerte ou de signalement qui contient quelques dispositions sur la protection des données à caractère personnel ;

- L'Existence d'une charte de protection des données à caractère personnel qui contient les finalités, les destinataires habilités, les durées de conservation, les droits des personnes concernées, l'adresse mail du correspondant et la procédure de règlement amiable des réclamations ;

- L'Existence d'une cartographie des risques IT ***qui ne prend pas en compte les risques liés à la protection des données personnelles ;***

Dès lors, l'Autorité de Protection considère que les procédures internes sont partiellement conformes à la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

K) Sur les sous-traitants et prestataires de services

Considérant que l'article 40 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel dispose que le responsable du traitement est tenu de choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements à effectuer.

Qu'il incombe au responsable du traitement ainsi qu'aux sous-traitants de veiller au respect de ces mesures ;

Considérant que le responsable du traitement a communiqué une liste de sous-traitants et partenaires ;

Considérant qu'à l'issue du contrôle et après analyse des documents, l'Autorité de Protection a constaté en autres que la quasi-totalité des sous-traitants et partenaires du Responsable du traitement ne disposent pas d'autorisation de traitement de données ou de mise en conformité ;

Qu'il s'agît sans que la liste ne soit exhaustive :

- **La Soprabanking pour la maintenance de l'application « Amplitude RH » ;**

- **La société Coditrans pour la livraison des colis ;**

- **Le recours à la société SANLAM dans le cadre de la convention d'assurance « coris éducation » ;**

- **Les sociétés Intel Security, securicom, 911 security, securimax, etc…pour la sécurité électronique ;**

- **Les partenaires pour les transferts d'argent (Western Union, money gram, RIA, orange money, rapidex, jubaexpress,) ;**

- **Les cabinets d'assistance juridique que sont la SCPA Konan-Loan Associés et le Cabinet KS associés ;**

- **La société de gardiennage EGIB pour la sécurité des biens et des services.**

Considérant **qu'aucun des sous-traitants cités ne disposent d'autorisation de traitement de données à caractère personnel ou d'autorisation de mise en conformité ;**

Considérant par **ailleurs que la liste complète des sous-traitants n'a pas été communiqué à l'Autorité de Protection ;**

L'Autorité de Protection considère que **les dispositions de l'articles 40 et 41 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données personnelles n'ont pas été respectées.**

L) Sur les logiciels et applications

Considérant qu'au moment du contrôle, le responsable du traitement a indiqué avoir recours à des applications métiers dont « amplitude » ;

Considérant qu'au moment du contrôle, ladite application n'avait pas fait l'objet d'autorisation de traitement ;

Considérant que toutes les applications métiers utilisées par le responsable du traitement n'ont pas été autorisées ;

Dès lors, l'Autorité de Protection considère les applications ne sont pas conformes aux dispositions ***de l'article 7 de Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel et de ses textes d'application ;***

M) Contrôle du site Internet du Responsable du traitement

L'Autorité de Protection constate sans que la liste ne soit exhaustive :

- L'existence d'un certificat SSL ;

- **L'absence de politique de protection des données personnelles ;**
- **L'absence de mentions légales ;**
- **L'absence de politique de cookies ;**
- **L'absence de contact du correspondant à la protection des données ;**
- **Le site est développé par 3W basé à Dakar ;**
- **L'existence d'un formulaire d'ouverture de compte collectant des données personnelles (nom, prénom, adresse mail, numéro de téléphone).**

L'Autorité de Protection considère que le site internet ne prend pas en compte les exigences liées aux principes de la protection des données à caractère personnel.

N) Autres constats

L'Autorité de Protection constate également :

- **Les contrats avec les sociétés SMO et EGIB ne contiennent pas de clauses sur la protection des données personnelles ;**

- **Le contrat avec la société de maintenance du système de sécurité électronique des agences CBC-CI ne contient pas de clause sur la protection des données personnelles ;**

L'Autorité de Protection considère que les contrats ne prennent pas en compte les exigences liées aux principes de la protection des données à caractère personnel.

Considérant enfin, les dispositions des articles 49 à 53 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel et l'article 17 de la Décision n°2021-0676 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 04 Août 2021 portant procédure de contrôle en matière de protection des données à caractère personnel ;

Après avoir délibéré,

DECIDE :

Article 1 :

Conformément aux dispositions de l'article 49 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel et l'article 17 de la Décision n°2021-0676 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 04 Août 2021 portant procédure de contrôle en matière de protection des données à

caractère personnel, l'Autorité de Protection prononce à l'égard de la société Coris Bank International (CBI-CI) :

- **un avertissement** pour non-respect des obligations découlant de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

- **une mise en demeure de faire cesser les manquements observés dans les soixante (60) jours à compter de la réception de la présente décision ;**

- **une mise en demeure de débuter son processus de mise en conformité dans un délai de trente (30) jours à compter de la réception de la présente.**

Article 2 :

L'Autorité de Protection prononcera l'une des mesures prévues par l'article 51 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel en cas de non-respect de la présente mise en demeure par la société Coris Bank International (CBI-CI).

Article 3 :

Les agents assermentés de l'Autorité de Protection effectueront des contrôles afin de s'assurer du respect de la présente décision conformément à la décision n°2021-0676 de l'Autorité de Protection en date du 04 août 2021 portant procédure de contrôle en matière de protection des données à caractère personnel.

Article 4 :

La présente décision prend effet à compter de la date de sa notification.

Article 5 :

Le Directeur Général est chargé de l'exécution de la présente décision, qui sera publiée sur le site internet de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire et celui de l'Autorité de Protection.

Fait à Abidjan, le 29 Août 2024
En deux (2) exemplaires originaux

Le Président

Autorité de régulation des Télécommunications / TIC de Côte d'Ivoire
Le Président
ARTCI

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL