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

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2024-1128

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 IVOIRIENNE DE BANQUE (SIB) EN MATIERE DE PROTECTION DES DONNEES PERSONNELLES

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°23-01269 DG/DCNS/DCPD/SPDS/JLC du 19 Septembre 2023 portant information de la mission de contrôle ;

Vu les Procès-verbaux de contrôle n° 005/01/2024 des 22,23,24,25,26 janvier 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 de l'article 47 de la Loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, l'Autorité de Protection s'assure que l'usage des technologies de l'information et de la communication ne porte pas atteinte ou ne comporte pas de menace pour la liberté et la vie privée des utilisateurs situés sur l'ensemble du territoire national ;

Qu'à ce titre, elle 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 l'article 9 de la même décision dispose que l'Autorité de Protection procède à la publication sur son site internet, du programme annuel de contrôle, et cette publication vaut information du responsable du traitement ;

Considérant que la SIB 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 ;

Considérant que par lettre référencée 23-01269/DG/DCNS/DCPD/SPDS/JLC, la SIB a été informée de la mission de contrôle en matière de protection des données personnelles dans son agence de Daloa ;

Considérant que la SIB, Société Anonyme de droit ivoirien avec Conseil d'Administration, au capital de 10.000.000.000 FCFA, est un établissement bancaire dont le siège social est situé Abidjan Plateau, Boulevard de la République, Immeuble Alpha 2000 ;

Les 22,23,24,25,26, en application de 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, des agents assermentés de l'Autorité de Protection ont mené une opération de contrôle sur place au sein de l'agence SIB de la ville de Daloa ;

Cette mission avait pour objet de vérifier le respect par la SIB 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 SIB et ses sous-traitants ;

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

- Contrôle sur la sécurité ;
- Contrôle du dispositif de vidéosurveillance ;
- Contrôle sur l'alerte professionnelle ;
- Contrôle sur la formation ;
- Contrôle de la géolocalisation ;
- Contrôle sur les procédures ;
- Contrôle sur les droits des personnes concernées ;
- Contrôle sur les activités du correspondant à la protection des données ;
- Contrôle des activités du chargé des relations clients ;
- Contrôle des activités du Chef d'agence ;
- Contrôle de la responsable de sécurité des systèmes d'information ;
- Contrôle des activités du conseiller clientèle ;
- Contrôle des activités du Responsable administratif (Chef de caisse) ;
- Contrôle des activités du correspondant à la protection des données personnelles ;
- Contrôle du site internet ;

Considérant qu'à l'issue du contrôle, une copie des Procès-verbaux de contrôle n° 005/01/2024 des 22,23,24,25,26 janvier 2024 contradictoirement dressés et signés, a été remise à la SIB.

II. Motifs de la Décision :

A) Sur les manquements aux obligations de conformité et d'autorisations de traitements 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 effectué par l'Autorité de Protection, la société SIB ne disposait pas :

- **d'autorisations de traitement de données 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 ;**
- **d'autorisation unique de traitement au sens de la Décision n°2017-0354 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 SIB 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 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, l'Autorité de Protection a constaté :

- l'existence de recueil de consentement dans le livret d'entrée en relation ;
- l'existence de clauses de protection des données personnelles dans les conventions de compte particulier ;
- l'existence de mentions légales contenant un recueil de consentement dans les formulaires SIBNET et SIBSMS ;
- l'existence d'un recueil de consentement dans le cadre du système BIC (Bureau Information et Crédit) ;
- le recueil du consentement dans le cadre de la géolocalisation n'est pas spécifique ;
- **le recours à l'intérêt légitime comme fondement légal ;**
- l'existence d'une fiche de recueil de consentement lors du processus de recrutement ;
- l'existence d'une étape de recueil de consentement du candidat dans le projet de procédure de recrutement communiqué pour les candidats admis à l'entretien ;
- **l'absence de formulaire de recueil du consentement dans le cadre des prospections ;**
- **l'absence de clauses relatives à la protection des données personnelles dans les contrats à durée déterminée, indéterminée et contrats de stage ;**
- **l'absence de fiche de recueil de consentement dans le cadre de la gestion des ressources humaines ;**
- l'existence d'une fiche de recueil de consentement dans le cadre de la vidéosurveillance ;
- l'existence d'une fiche de recueil de consentement dans le cadre de la gestion des Ressources Humaines. **Toutefois, le consentement n'est pas spécifique à la géolocalisation ;**
- **l'absence de recueil de consentement pour la collecte d'informations via les cookies à travers le site internet ;**
- l'existence d'un formulaire de recueil de consentement dans le livret d'entrée en relation. **Toutefois, ce consentement est général et absolu ;**

Considérant que le consentement doit être une manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte le traitement de ses données ;

Considérant également que lors du contrôle et après analyse des documents communiqués, le responsable du traitement n'a pu fournir à l'Autorité de Protection, toutes les preuves du

consentement ou les dérogations à l'exigence du consentement préalable des clients, des salariés et des fournisseurs.

Dès lors, l'Autorité de Protection considère que tous les traitements opérés satisfont partiellement au principe de la légitimité ;

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, l'Autorité de Protection a constaté que les finalités pour lesquelles les données étaient collectées étaient déterminées et explicites ;

Considérant que le Responsable du traitement ne dispose pas d'autorisation de traitement ou de mise en conformité ;

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, l'Autorité de Protection a constaté :

- La conservation des dossiers clients pendant la durée de la relation contractuelle et pendant une durée de deux (02) ans après la fermeture du compte ;
- **Les données (enregistrement) de la vidéosurveillance sont conservées pendant une durée de trois (03) mois dans le respect de la règlementation locale (certification PCI DSS)** ;
- La sauvegarde des données du système de contrôle d'accès est effectuée automatiquement pendant une durée de trois (03) mois. A l'expiration des trois (03) mois, les données sont supprimées automatiquement ;
- **La durée de conservation illimitées pour certaines données (dossiers juridiques, dossiers financiers)** ;
- l'existence d'un cadre de classement des documents de la SIB contenant les durées de conservation des documents et données par direction ;
- l'existence d'une procédure d'archivage;
- l'existence d'une procédure groupe de conservation des données personnelles ;

Considérant que la SIB 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 limitée 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 :

- L'existence d'une politique de gestion des données sensibles ;
- **La collecte du nom du père, nom de la mère, nombre d'enfants à charge dans le contrat de travail** ;
- L'existence d'une fiche de recueil de consentement pour le traitement des données personnelles dans le cadre de la gestion de la relation clients. Elle contient les informations suivantes : date et lieu de naissance, l'adresse postale, l'adresse mail, le numéro de téléphone ;
- **La collecte des données de santé pour les dossiers de prêts (poids, âge, taille et tension artérielle)** ;
- **La collecte de la date et le lieu de naissance dans le formulaire d'exercice des droits ;**

Considérant que la SIB n'a pu fournir à l'Autorité de Protection, les textes qui autorisent la collecte du nom du père, nom de la mère, nombre d'enfants à charge dans le contrat de travail.

Par conséquent, l'Autorité de Protection considère que le principe de la proportionnalité est partiellement 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 ;

Qu'à l'issue du contrôle, la SIB indique que les destinataires des données traitées sont les suivants, sans que la liste ne soit exhaustive :

- la société WAFA ASSURANCE dans le cadre de la souscription aux produits d'assurance ;
- le siège de la SIB au Maroc ;
- la SOPRA dans le cadre de la maintenance de DELTA-BANK ;
- la société ATOS en France, dans le cadre des compensations ;
- l'externalisation des données à destination du Maroc, la Belgique, Monaco, etc... ;

Considérant que la liste des sous-traitants a été communiquée à l'Autorité de Protection pour analyse

Considérant que la communication des données traitées au siège au Maroc, en Belgique et tous les autres pays hors de l'espace CEDEAO constitue des transferts des données à destination d'un pays tiers ;

Considérant que la **SIB ne dispose pas d'autorisations de transferts de données ;**

L'Autorité de Protection considère que les transferts de données à caractère personnel opérés par la SIB 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 ;
- 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.

En cas d'utilisation d'un dispositif de vidéosurveillance, des 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 SIB 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 communiqués, l'Autorité de Protection a constaté sans que la liste ne soit exhaustive :

- **l'existence de pictogrammes installés dans le hall, à l'entrée de l'agence et dans le guichet automatique contenant la finalité, la durée de conservation, les contacts du correspondant** ;
- l'Existence de mentions légales sur les formulaires et dans les contrats ;
- l'Existence de mentions d'informations dans les formulaires de recueil du consentement (RH, vidéosurveillance, gestion de la relation client, recrutement, formulaire de mise à jour) ;
- **l'Absence de mentions d'informations sur la fiche KYC ;**
- **l'Absence d'information sur les droits des personnes concernées sur le site internet ;**
- **l'Absence d'informations sur le Correspondant à la protection des données personnelles sur le site internet ;**
- **L'existence de plusieurs affiches d'information de l'existence d'un dispositif de vidéosurveillance contenant la finalité, la durée de conservation de trois (03) mois, les contacts du correspondant pour l'exercice des droits ;**
- **l'absence d'information des personnes concernées de la possibilité de désactiver le système de géolocalisation dans leurs sphères privées ;**
- l'existence d'une circulaire d'information sur la mise en ligne de procédure sur les données personnelles ;
- l'Existence d'une politique de protection des données personnelles affichée dans la banque ;

Considérant les non-conformités constatées ci-dessus ;

Par conséquent, l'Autorité de Protection considère que le principe de la transparence est partiellement respecté.

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 qu'à l'issue du contrôle et après analyse de la documentation, l'Autorité de Protection constate :

- L'existence d'un Correspondant à la Protection des données personnelles ;
- L'existence d'une procédure d'exercice de droits ;
- L'existence d'un formulaire d'exercice des droits sur les données personnelles contenant une mention d'information relative à la protection des données personnelles ;
- **Le recours à l'intérêt légitime dans certains cas comme motif de refus de demande pour l'exercice des droits ;**
- **la collaboration entre le Correspondant du groupe *attijariwafa bank* et le Correspondant de la SIB sur les questions liées au RGPD** ;
- l'existence d'une fiche de poste dénommée « DATA PROTECTION OFFICER » ;
- l'existence de référents dans chaque direction ;
- **L'existence d'une procédure de gestion des remontées des violations des données personnelles fondée sur le RGPD** ;
- l'existence d'un registre de traitements de données ;
- Le Correspondant a reçu des formations en matière de protection des données personnelles ;
- Le Correspondant a suivi une formation en matière de protection des données personnelles ;
- **Le correspondant ne dispose pas de codes et mots de passe pour l'accès aux fichiers et données ;**
- **la procédure de gestion des droits des personnes concernées communiqué ne prend pas en compte le droit au retrait du consentement ;**

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 qu'à l'issue du contrôle et après analyse de la documentation, l'Autorité de Protection constate :

- **la sécurité physique des locaux est assurée par les sociétés de gardiennage suivantes : SECURICOM, PUISSANCE 6 et G4S ;**
- l'existence de caméras de vidéosurveillance ;
- L'existence d'un système de contrôle d'accès avec option digicode et lecteur de badge ;
- L'existence d'un système d'alarme anti-intrusion ;
- L'existence d'une politique et d'une fiche de gestion des habilitations ;
- L'existence d'une charte des administrateurs du système d'information. **Toutefois, la charte ne précise pas la procédure détaillée en cas d'infraction, la gestion des violations, des mesures urgentes, la notification, l'enquête et les actions collectives** ;
- L'existence d'une politique antivirale ;
- **l'Absence de définition de la fréquence de mise à jour de la politique virale en fonction des évaluations et des changements de la réglementation ;**
- l'Existence d'une politique de gestion des accès distants. **Toutefois, cette politique ne prévoit pas de sensibilisation ni la formation des utilisateurs distants ;**
- l'Existence d'une politique de gestions des clés cryptographiques. **Toutefois, cette politique n'identifie pas les types de données personnelles traitées dans leur contexte des clés cryptographiques. Elle ne spécifie pas également le type de support utilisé pour les sauvegardes à distance et en local ;**
- **l'absence de plan de réponse aux incidents spécifiques aux accès distants ;**
- **l'absence de procédure claire en cas de violation des accès distants ;**
- L'Existence d'une politique de gestion des identités des accès logiques ;
- l'existence d'une politique de gestion des incidences de sécurité. **Toutefois, cette politique ne précise pas le délai et les moyens de notification aux personnes concernées ;**

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

J) Sur les procédures internes de SIB

Considérant que la SIB a communiqué plusieurs procédures à l'Autorité de Protection dont la liste est mentionnée aux annexes des procès-verbaux.

Considérant qu'à l'issue du contrôle et après analyse de la documentation, l'Autorité de Protection constate notamment :

- l'existence d'un dispositif d'alerte professionnelle qui contient la procédure de conformité et de déclaration de soupçon, la procédure de remontée interne d'opération suspecte, la procédure de gestion des incidents relatifs aux risques opérationnels, le dispositif de gestion des disfonctionnements. **Cependant, toutes les procédures précitées ne prennent pas en compte les aspects liés à la protection des données personnelles** ;

- la politique de conformité est conçue pour répondre aux exigences de la bonne gouvernance prévue par la circulaire n°05/2017/CB/C relative à la gestion de la conformité aux normes en vigueur pour les établissements de crédit et les compagnies financières. **Toutefois, cette procédure ne prend pas en compte les principes liés à la protection des données personnelles** ;

- la procédure globale de gestion des risques s'inscrit dans le cadre du respect de la circulaire n°01 et 04-2017 de la Commission Bancaire de UEMOA. **Toutefois, cette procédure ne prend pas en compte les aspects liés à la protection des données personnelles, notamment les risques liés à la protection des données personnelles** ;

- l'existence d'une procédure de gestion des données sensibles qui s'applique aux employés, clients, partenaires commerciaux. Elle définit les données sensibles et l'inventaire des données sensibles. Elle contient également les contacts du correspondant pour l'exercice des droits des personnes concernées. **Cependant, elle ne comporte pas l'analyse de la proportionnalité des données sensibles** ;

- l'existence d'une procédure d'entrée en relation avec les sous-traitants. Elle prévoit entre autres les obligations aux sous-traitants sur la protection des données personnelles, la clause de suppression des données par les sous-traitants, l'information immédiate du responsable du traitement des violations de données personnelles, etc.…

- l'existence d'une procédure de conservation des données personnelles ;

- l'existence d'une procédure de privacy by design et by défaut **axée sur le RGPD. Cette procédure prévoit que la cnil peut être consultée en cas de doute pour évaluer la conformité du traitement après la réalisation d'une AIPD ;**

- l'existence d'une charte de protection des données personnelles (Groupe). Elle prend en compte la loi n°2013-450 du 19 juin 2013 relative à la protection des données personnelles, les grandes lignes émises par la Commission Européenne sur la protection des données personnelles, les conventions comme référentiels et textes règlementaires ;

- l'existence d'une politique des cookies groupe. **Toutefois, elle ne précise pas clairement la durée de conservation et les données exactes partagées sur les réseaux sociaux ;**

- l'existence d'une politique de protection des données personnelles. **Cependant, elle utilise comme base juridique, l'intérêt légitime dans le respect de la vie privée, des intérêts, droits et libertés fondamentales, dans la lutte contre la fraude, la prospection commerciale par voie postale, l'évaluation de la satisfaction, clients**. Les notifications des violations des données personnelles sont faites dans les meilleurs délais et la mesure du possible dans un délai de 72 heures après avoir pris connaissance de toutes violations ;

- L'existence d'une procédure d'archives. **Cependant, elle permet la conservation illimitée des noms et prénoms (page 21), des données du relevé bancaire (page 44), ouverture et clôture de compte, ouverture de compte entreprise**, des bulletins de paie (page 22), des frais médicaux conservés pendant cinq (05) ans, etc… ;

- l'existence d'une cartographie des risques globale. Elle prend en compte les mesures de sécurité pour les accès non autorisés aux données, les fuites et divulgation des données, modification non autorisée des données, l'inaccessibilité des données, les sanctions liées en cas de non-respect des dispositions ;

- l'existence d'une procédure de gestion des incidents aux risques opérationnels. **Cependant, les délais de conservation ne sont pas précisés et les aspects liés à la protection des données personnel ne sont pas pris en compte** ;

- l'existence d'une procédure de remontée interne des opérations suspectes. **Toutefois, les durées de conservations ne sont pas définies et les aspects liés à la protection des données personnelles ne sont pas pris en compte** ;

- l'existence de conformité (déclaration de soupçon). **Toutefois, les durées de conservations ne sont pas définies et les aspects liés à la protection des données personnelles ne sont pas pris en compte** ;

- l'existence d'une procédure de recrutement. **Toutefois, les durées de conservations ne sont pas définies et les aspects liés à la protection des données personnelles ne sont pas pris en compte** ;

- l'existence d'une circulaire d'information sur la mise en ligne de procédure sur les données à caractère personnel. Elle précise entre autres l'existence d'une procédure d'exercice des droits, de gestion des remontées des violations des données personnelles, d'analyse de conformité d'un traitement ;

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 la SIB

Considérant que l'article 40 alinéa 1 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 l'article 40 alinéa 2 de la même Loi dispose que, lorsque le traitement est mis en œuvre pour le compte du responsable du traitement, celui-ci choisit un sous-traitant qui apporte des garanties au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect de ces mesures ;

Considérant qu'au moment du contrôle et après analyse des documents, l'Autorité de Protection constate :

- l'existence d'un courrier à l'attention des prestataires et sous-traitants en vue de leur mise en conformité avec la loi relative à la protection des données personnelles ;
- l'existence de clauses à la protection des données personnelles dans les contrats de sous-traitance ;
- l'Existence d'une politique de sous-traitant qui prend en compte la protection des données personnelles ;
- l'Existence d'un questionnaire d'évaluation des sous-traitants qui prends en compte les aspects liés à la protection des données à caractère personnel ;
- **Les sociétés VEONE DIGITAL, SECURICOM, PUISSANCE 6, G4S SECURE SOLUTIONS ne disposent pas d'autorisation de traitement de données ou d'Autorisation de mise en conformité** ;
- Le modèle de contrat de sous-traitance communiqué contient une clause relative à la protection des données personnelles. **Toutefois, les contrats en cours de validité ne comportent de clauses relatives à la protection des données personnelles ;**

Par conséquent, l'Autorité de Protection considère que les mesures prises pour les sous-traitants sont partiellement respectées.

Considérant 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 en 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 SIB :

- **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 soixante (60) jours pour débuter leur processus de mise en conformité**

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 SIB.

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

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL