SHC

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

CONSEIL DE REGULATION

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0714

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

EN DATE DU 1er FEVRIER 2022

PORTANT AUTORISATION DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL PAR

LE GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES (CGAP)

ENQUETES LIEES AUX PLAINTES DES CLIENTS DES SERVICES FINANCIERS NUMERIQUES

(COTE D'IVOIRE)

L'AUTORITE DE PROTECTION,

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 l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication ;

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° 2016-483 du 07 juillet 2016 portant nomination des Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le Décret n°2016-851 du 19 Octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

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 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 conduite relatives au traitement et à la protection des données à caractère personnel (DCP) ;

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 (DCP) ;

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°2016-0201 de l'Autorité de protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et agrément en matière de Protection des données à caractère personnel ;

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°2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

Vu la Décision n°2020-0581 de l'Autorité de protection 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 Résolution n°2021-161 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 30 juin 2021 portant nomination du Directeur Général par Intérim de l'ARTCI;

Par les motifs suivants :

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES (CGAP), un centre de recherche pour la Promotion de l'Inclusion Financière des personnes à faible revenu ;

Considérant que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est administré et hébergé en Côte d'Ivoire par la Banque Mondiale ;

Que dans le cadre de son action au sein de la zone UEMOA, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a initié un projet régional de laboratoire pour la protection des utilisateurs des Services Financiers Numériques (SFN).

Considérant que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES envisage organiser des enquêtes téléphoniques auprès des utilisateurs des SFN, en vue d'appréhender les risques liés à l'usage desdits services ;

Considérant que les plaintes des usagers de ses services permettront également d'appréhender ces risques ;

Considérant que l'article 47 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 est chargée de recevoir les déclarations et d'octroyer les autorisations, pour la mise en œuvre de traitements de données à caractère personnel ;

L'Autorité de protection est compétente pour examiner la demande d'autorisation de traitements initiée par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES :

- **Sur la recevabilité de la demande d'autorisation**

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 qu'en l'espèce, le demandeur voudrait collecter les données à caractère personnel des utilisateurs des Services Financiers Numériques en Côte d'Ivoire, dont le numéro de téléphone ;

Ledit traitement doit être autorisé par l'Autorité de protection, pour être mis en œuvre ;

Considérant qu'aux termes de l'article 7 précité, la demande d'autorisation est présentée par le responsable du traitement ou son représentant légal ;

Que l'article 1 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, définit le responsable du traitement comme étant la personne physique ou morale, publique ou privée, 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 ;

Considérant que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES envisage organiser des enquêtes téléphoniques auprès des utilisateurs des SFN, en vue d'appréhender les traitements des plaintes liés à l'usage desdits services ;

Qu'à cet effet, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES va collecter, traiter, stocker, et communiquer des données à caractère personnel relatives aux utilisateurs des SFN qui se sont plaints desdits services ;

L'Autorité de protection en conclut que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a la qualité de Responsable du traitement.

Considérant qu'aux termes de l'article 9 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la demande d'autorisation doit contenir les mentions minimums relatives à la dénomination sociale de la personne morale, au Responsable du traitement, à son siège social, à l'identité de son représentant légal, à son numéro d'immatriculation au registre du commerce et du crédit mobilier, à son numéro de déclaration fiscale, aux finalités du traitement, à la durée de conservation des données traitées, aux dispositions prises pour assurer la sécurité des traitements, à la protection et à la confidentialité des données traitées ;

Considérant que lesdites mentions figurent dans la demande d'autorisation formulée par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES ;

Qu'ainsi, il satisfait aux conditions de forme exigées par les articles 7 et 9 de la Loi n°2013-450 relative à la protection des données à caractère personnel ;

En conséquence, l'Autorité de protection déclare, la demande du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES, recevable en la forme.

- **Sur la légitimité et la licéité du traitement**

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 ;

Que toutefois, il peut être dérogé à cette exigence du consentement préalable lorsque le responsable du traitement est dûment autorisé et que le traitement est nécessaire à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée ;

Considérant que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES indique qu'il procèdera à la collecte des données des plaignants des Services Financiers Numériques à travers les prestataires de SFN ;

Considérant que cette initiative vise à analyser les risques auxquels font face les consommateurs de services financiers numériques afin d'y apporter des solutions ;

Que dès lors, le traitement a pour objectif la protection des consommateurs de services financiers numériques en vue de promouvoir le développement de l'inclusion financière en Côte d'Ivoire ;

Qu'il convient de noter que le traitement est nécessaire à la sauvegarde des intérêts des consommateurs de services financiers numériques ;

Par conséquent, il peut donc être déroger au principe du consentement préalable, lors de la communication des données par les partenaires SFN au GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES ;

Considérant en outre que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES indique qu'il procédera au recueil du consentement préalable au début de l'enquête ou de l'entretien téléphonique et avant toute autre collecte de données ;

Des lors, l'Autorité de protection considère que le consentement recueilli au début de l'enquête est suffisant pour assurer le respect du principe de la légitimité ;

- **Sur la finalité**

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 qu'en l'espèce, le demandeur procède au traitement de données à caractère personnel afin de :

- comprendre et identifier les risques encourus par les utilisateurs des SFN par une analyse des plaintes ;
- trouver et proposer des solutions aux prestataires des SFN, aux institutions financières, aux régulateurs/ superviseurs...

L'Autorité de protection considère que ces finalités sont déterminées, explicites et légitimes.

- **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 qu'en l'espèce, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a indiqué qu'il conservera les données traitées pendant six (06) mois maximum ;

L'autorité de protection, au regard de la nature des données traitées et de la finalité du traitement, considère que ce délai n'est pas excessif.

L'Autorité de protection prescrit donc au GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES de :

- conserver les données collectées 6mois à compter de la fin des enquêtes ;
- supprimer les données collectées après l'expiration du délais ci-dessus mentionné.

- **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 qu'en l'espèce, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES indique que le traitement concerne les données suivantes :

- **les données d'identification :** Nom, prénom ;
- **les données d'identification national :** numéro de téléphone ;
- les raisons des plaintes et l'appréciation des utilisateurs des SFN sur le traitement de la plainte ;
- **les données de localisation** : lieu de résidence (zone rurale ou urbaine).

Il y a lieu de constater que les données collectées, telles qu'elles sont décrites dans la demande d'autorisation, sont pertinentes, adéquates, et non excessives au regard de la finalité.

- **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, selon lesquelles la demande d'autorisation adressée à l'Autorité de protection doit contenir les destinataires habilités à recevoir communication des données traitées ;

Considérant qu'en l'espèce, le demandeur communique les données aux prestataires de services que sont :

- KANTAR, entreprise de call center basée au Sénégal, chargée des entretiens téléphoniques avec la cible ;
- HORUS, chargée des analyses des résultats des enquêtes réalisées, basée en France.

L'Autorité de protection considère ces partenaires susvisés comme destinataires de données et prescrit également, que les données traitées soient communiquées aussi :

- aux agents habilités du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES ;
- au Procureur de la République ;
- aux Officiers de Police Judiciaire munis d'une réquisition;
- aux agents assermentés de l'Autorité de protection habilités, dans le cadre de l'exécution de leurs missions ;
- aux autorités et Administrations publiques Ivoiriennes habilitées dans le cadre de leurs missions.

Considérant qu'en l'espèce, le demandeur affirme qu'il effectuera un transfert de données vers ses sous-traitants HORUS et KANTAR respectivement situés en France au Sénégal.

L'Autorité de protection prescrit que lesdites données ne fassent l'objet d'aucun transfert vers des pays tiers hors CEDEAO, sans son autorisation préalable.

- **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 demandeur de faire preuve de transparence vis à vis des personnes concernées qui devront notamment être informées :

- 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.

Qu'à cette fin, le demandeur indique que ces informations seront lues aux personnes concernées au début de l'entretien, préalablement à toute collecte ;

L'Autorité de protection prescrit, avant le démarrage effectif de ce projet que :

- Les mentions minimums ci-dessus énumérées soient inscrites sur les sites du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES et celui de ses prestataires HORUS et KANTAR ;

- Une note d'information sur les données recueillies et l'usage qui en sera fait, soient mis à la disposition des usagers sur les sites des partenaires prestataires des SFN ;
- Que les prestataires de service mobile numériques, partenaires du projet informent les personnes concernées par tous moyens : messages (sms ou en langues locales), mails, ou appels enregistrés ou affichages dans leurs locaux.

- **Sur les droits d'accès direct, d'opposition, de rectification 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 le demandeur indique que les droits d'accès direct, d'opposition, de rectification, d'effacement, de portabilité, de retrait du consentement donné, et de suppression, pourront être exercés auprès du prestataire chargé des enquêtes téléphoniques ;

Elle le fait au début des entretiens avec les usagers ;

Considérant toutefois que le demandeur n'a pas désigné de correspondant à la protection ;

L'Autorité de protection prescrit au GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES de désigner un correspondant à la protection, auprès duquel les personnes concernées pourront exercer leurs droits.

- **Sur les mesures de sécurité**

Considérant qu'en application de l'article 41 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le responsable du traitement et le sous-traitant prennent toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient détruites, déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance ;

En vue de respecter cette exigence de la loi, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a mis en place des mesures spécifiques, afin de garantir la confidentialité, l'intégrité et la disponibilité des données collectées.

Considérant qu'au vu des éléments techniques fournis par le demandeur, le niveau de sécurité du système d'information du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES lui permet de mettre en œuvre son projet d'enquête téléphonique pour les finalités déclarées ;

Qu'il en résulte que le demandeur a pris toutes les mesures nécessaires en vue d'assurer la sécurité des données ;

L'Autorité de protection considère que les mesures de sécurité logique et physique nécessaires sont garanties.

Après en avoir délibéré,

DECIDE :

Article 1 :

Les prestataires de Services Financiers Numériques sont autorisés à communiquer au GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES :

- **les données d'identification :** Nom, prénom,
- **les données d'identification national :** numéro de téléphone ;
- **l'objet des plaintes et l'avis des utilisateurs des SFN sur le traitement de la plainte ;**
- **les données de localisation** : lieu de résidence (zone rurale ou urbaine).

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est autorisé à effectuer la collecte, l'enregistrement, le traitement, l'analyse, le stockage et la communication des données à caractère personnel ci-dessus énumérées.

Il est dérogé à l'exigence du consentement préalable des consommateurs des SFN qui se sont plaint desdits services car le traitement sollicité relève de la sauvegarde de l'intérêt ou des droits et libertés fondamentaux des personnes concernées.

Les données non mentionnées ne devront aucunement faire l'objet d'un quelconque traitement de la part du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES.

Article 2 :

Les données traitées par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES ne peuvent être utilisées à des fins autres que celles précisées dans la demande d'autorisation.

Toute réutilisation de ces données à d'autres fins doit faire l'objet d'une autorisation préalable de l'Autorité de protection.

Article 3 :

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a l'obligation de procéder au recueil du consentement préalable des personnes concernées, par l'enregistrement des consentements préalables en début d'entretien.

Les mentions d'informations devront figurer sur son site et sur ceux de ses prestataires, indépendamment des conditions générales d'informations.

Article 4 :

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est autorisé à communiquer les données traitées :

- **pour la réalisation de ses enquêtes :**

- à ses agents habilités ;
- à KANTAR, au sénégal ;
- à HORUS, en France

- **pour l'exécution des missions de service public:**

- au Procureur de la République ;
- aux Officiers de Police Judiciaire munis d'une réquisition ;
- aux Agents assermentés de l'Autorité de protection habilités, dans le cadre de l'exécution de leurs missions ;
- aux Agents habilités de l'administration publique habilités dans le cadre de leurs missions.

Il est interdit au GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES de transférer, sans autorisation préalable de l'Autorité de protection, les données collectées vers des pays tiers, hors de la CEDEAO.

Article 5 :

Les données sont conservées par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES, pendant un délai de six (06) mois, à compter de la fin de l'enquête.

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est tenu de supprimer lesdites données après l'expiration de ce délai.

En cas de litige, les données sont conservées jusqu'à la fin de la procédure judiciaire, lorsque la décision de justice rendue est devenue définitive.

Smc

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

CONSEIL DE REGULATION

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0715

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

EN DATE DU 1er FEVRIER 2022

PORTANT AUTORISATION DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL PAR

LE GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES (CGAP)

ENQUETES SUR LES RISQUES ET IMPACTS LIES A L'USAGE DU CREDIT DIGITAL ET DES SERVICES FINANCIERS NUMERIQUES

(COTE D'IVOIRE)

L'AUTORITE DE PROTECTION,

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 l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication ;

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 ;

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° 2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le Décret n°2016-851 du 19 Octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

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 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 conduite relatives au traitement et à la protection des données à caractère personnel (DCP) ;

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 (DCP) ;

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°2016-0201 de l'Autorité de protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et agrément en matière de Protection des données à caractère personnel ;

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°2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

Vu la Décision n°2020-0581 de l'Autorité de protection 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 Résolution n°2021-161 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 30 juin 2021 portant nomination du Directeur Général par Intérim de l'ARTCI;

Par les motifs suivants :

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES (CGAP), un centre de recherche pour la Promotion de l'Inclusion financière des personnes à faible revenu ;

Considérant que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est administré et hébergé en Côte d'Ivoire par la Banque Mondiale ;

Que dans le cadre de son action au sein de la zone UEMOA, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a initié un projet régional de laboratoire pour la protection des utilisateurs des Services Financiers Numériques (SFN).

Considérant que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES envisage de faire une enquête visant à appréhender les risques et les impacts liés à l'usage du crédit digital et des Services Financiers Numériques par l'analyse des informations et avis des usagers ;

Qu'à cet effet, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES voudrait auditionner des clients du crédit digital et des utilisateurs des SFN ;

Considérant que l'article 47 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 est chargée de recevoir les déclarations et d'octroyer les autorisations, pour la mise en œuvre de traitements de données à caractère personnel ;

L'Autorité de protection est compétente, pour examiner la demande d'autorisation de traitements initiée par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES :

- **Sur la recevabilité de la demande d'autorisation**

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 qu'en l'espèce, le demandeur voudrait collecter les données à caractère personnel des utilisateurs des Services Financiers Numériques et du crédit digital, dont leur numéro de téléphone ;

Ledit traitement doit être autorisé par l'Autorité de protection, pour être mis en œuvre ;

Considérant qu'aux termes de l'article 7 précité, la demande d'autorisation est présentée par le responsable du traitement ou son représentant légal ;

Que l'article 1 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, définit le responsable du traitement comme étant la personne physique ou morale, publique ou privée, 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 ;

Considérant que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a initié un projet régional de laboratoire pour la protection des utilisateurs des Services Financiers Numériques.

Que pour la mise en œuvre de ce projet, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES envisage de mener une enquête par téléphone visant à évaluer les usages et impacts du crédit numérique sur la vie des utilisateurs.

Qu'à cet effet, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES collectera, traitera, stockera et communiquera les données à caractère personnel desdits utilisateurs.

L'Autorité de protection en conclut que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a la qualité de Responsable du traitement.

Considérant qu'aux termes de l'article 9 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la demande d'autorisation doit contenir les mentions minimums relatives à la dénomination sociale de la personne morale, au Responsable du traitement, à son siège social, à l'identité de son représentant légal, à son numéro d'immatriculation au registre du commerce et du crédit mobilier, à son numéro de déclaration fiscale, aux finalités du traitement, à la durée de conservation des données traitées, aux dispositions prises pour assurer la sécurité des traitements, à la protection et à la confidentialité des données traitées ;

Considérant que lesdites mentions figurent dans la demande d'autorisation formulée par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES ;

Qu'elle satisfait aux conditions de forme exigées par les articles 7 et 9 de la Loi n°2013-450 relative à la protection des données à caractère personnel ;

En conséquence, l'Autorité de protection déclare, la demande du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES, recevable en la forme.

- **Sur la légitimité et la licéité du traitement**

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 ;

Que toutefois, il peut être dérogé à cette exigence du consentement préalable lorsque le responsable du traitement est dûment autorisé et que le traitement est nécessaire à

la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée ;

Considérant que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES indique qu'il procèdera à la collecte des données des plaignants des Services Financiers Numériques à travers les prestataires de SFN ;

Considérant que cette initiative vise à analyser les risques auxquels font face les consommateurs de services financiers numériques afin d'y apporter des solutions ;

Que dès lors, le traitement a pour objectif la protection des consommateurs de services financiers numériques en vue de promouvoir le développement de l'inclusion financière en Côte d'Ivoire ;

Qu'il convient de noter que le traitement est nécessaire à la sauvegarde des intérêts des consommateurs de services financiers numériques ;

Par conséquent, il peut donc être déroger au principe du consentement préalable, lors de la communication des données par les partenaires SFN au GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES ;

Considérant en outre que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES indique qu'il procédera au recueil du consentement préalable au début de l'enquête ou de l'entretien téléphonique et avant toute autre collecte de données ;

Des lors, l'Autorité de protection considère que le consentement recueilli au début de l'enquête est suffisant pour assurer le respect du principe de la légitimité ;

- **Sur la finalité**

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 ;

Qu'en l'espèce, les traitements envisagés par le CGAP ont pour finalités de :

- Comprendre et identifier les risques encourus par les utilisateurs des SFN ;
- L'évaluation des usages et impacts du crédit numérique sur la vie des utilisateurs et sur le marché du crédit numérique

L'Autorité de protection considère que ces finalités sont déterminées, explicites et légitimes.

- **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 qu'en l'espèce, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a indiqué qu'il conservera les données traitées pendant six (06) mois maximum ;

L'autorité de protection, au regard de la nature des données traitées et de la finalité du traitement, considère que ce délai n'est pas excessif.

L'Autorité de protection prescrit donc au GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES de :

- conserver les données collectées 6mois à compter de la fin des enquêtes ;
- supprimer les données collectées après l'expiration du délais ci-dessus mentionné.

- **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 qu'en l'espèce, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES indique que le traitement concerne les données suivantes :

- **les données d'identification :** Nom, prénom, tranche d'âge, sexe ;
- **les données d'identification national :** numéro de téléphone ;
- **les informations d'ordre économique et financier** : les types de SFN et des crédits numériques utilisés, les fréquences et difficultés rencontrées dans l'utilisation de ces services, revenus, montants opération, montant des prêts contractés ;
- **les données d'ordre professionnel ;** profession
- **les données de localisation** : adresse géographique
- **les données relatives à l'appréciation sur les difficultés sociales des personnes :** conditions de vie, niveau d'éducation

Il y a lieu de constater que les données collectées, telles qu'elles sont décrites dans la demande d'autorisation, sont pertinentes, adéquates, et non excessives au regard de la finalité.

- **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, selon lesquelles la demande d'autorisation adressée à l'Autorité de protection doit contenir les destinataires habilités à recevoir communication des données traitées ;

Considérant qu'en l'espèce, le demandeur interagit avec les prestataires de services que sont :

- KANTAR au Sénégal ;
- HORUS, en France ;

L'Autorité de protection considère ces partenaires susvisés comme destinataires de données et prescrit également, que les données traitées soient communiquées, aussi :

- aux agents habilités du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES;
- au Procureur de la République ;
- aux Officiers de Police Judiciaire munis d'une réquisition;
- aux agents assermentés de l'Autorité de protection habilités, dans le cadre de l'exécution de leurs missions ;
- aux autorités et Administrations publiques Ivoiriennes dans le cadre de leurs missions.

Considérant qu'en l'espèce, le demandeur affirme qu'il effectuera un transfert de données vers ses sous-traitants HORUS et KANTAR situés respectivement en France au Sénégal .

L'Autorité de protection prescrit que lesdites données ne fassent l'objet d'aucun transfert vers des pays tiers hors CEDEAO, sans son autorisation préalable.

- **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 demandeur de faire preuve de transparence vis à vis des personnes concernées qui devront notamment être informées :

- 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.

Qu'à cette fin, le demandeur indique que ces informations seront lues aux personnes concernées au début de l'entretien, préalablement à toute collecte ;

L'Autorité de protection prescrit, avant le démarrage effectif de ce projet que :

- Les mentions minimums ci-dessus énumérées soient inscrites sur les sites du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES et celui de ses prestataires HORUS et KANTAR ;
- Une note d'information sur les données recueillies et l'usage qui en sera fait, soient mis à la disposition des usagers sur les sites des partenaires prestataires des SFN ;
- Que les prestataires de service mobile money, partenaires du projet informent les personnes concernées par tous moyens : messages (sms ou en langues locales), mails, ou appels enregistrés ou affichages dans leurs locaux.

L'Autorité de protection considère que le principe de transparence n'est pas respecté.

- **Sur les droits d'accès direct, d'opposition, de rectification 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 le demandeur indique que les droits d'accès direct, d'opposition, de rectification, d'effacement, de portabilité, de retrait du consentement donné, et de suppression, pourront être exercés auprès du prestataire chargé des enquêtes téléphoniques ;

Elle le fait au début des entretiens avec les usagers ;

Considérant toutefois que le demandeur n'a pas désigné de correspondant à la protection ;

L'Autorité de protection prescrit au GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES de désigner un correspondant à la protection, auprès duquel les personnes concernées pourront exercer leurs droits.

- **Sur les mesures de sécurité**

Considérant qu'en application de l'article 41 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le responsable du traitement et le sous-traitant prennent toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient détruites, déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance ;

En vue de respecter cette exigence de la loi, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a mis en place des mesures spécifiques afin de garantir la confidentialité, l'intégrité et la disponibilité des données collectées.

Considérant qu'au vu des éléments techniques fournis par le demandeur, et après vérification préalable de l'Autorité de protection, le niveau de sécurité du système d'information du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES lui permet de mettre en œuvre son projet d'enquête téléphonique pour les finalités déclarées ;

Qu'il en résulte que le demandeur a pris toutes les mesures nécessaires en vue d'assurer la sécurité des données ;

L'Autorité de protection considère que les mesures de sécurité logique et physique nécessaires sont garanties.

Après en avoir délibéré,

DECIDE :

Article 1 :

Les prestataires de Services Financiers Numériques sont autorisés à communiquer au GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES :

- **les données d'identification :** Nom, prénom, tranche d'âge, sexe ;
- **les données d'identification national :** numéro de téléphone ;
- **les informations d'ordres économique et financier** : les types de Services Financiers Numériques (SFN) et de crédits numériques utilisés, les fréquences et les difficultés rencontrées dans l'utilisation de ces services, les revenus, le montant des opérations, le montant des prêts contractés ;
- **les données d'ordre professionnel ;** profession ;
- **les données de localisation** : adresse géographique ;
- **les données relatives à l'appréciation sur les difficultés sociales des personnes :** conditions de vie, niveau d'éducation.

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est autorisé à effectuer la collecte, et l'enregistrement, le traitement, le stockage et la communication des données à caractère personnel ci-dessus énumérées.

Il est dérogé à l'exigence du consentement préalable des bénéficiaires des prêts liés aux services financiers numériques (SFN) car le traitement sollicité relève de la sauvegarde de l'intérêt ou des droits et libertés fondamentaux des personnes concernées.

Les données visées au présent article concernent un échantillon de trois milles (3000) utilisateurs des Services Financiers Numériques.

Les données non mentionnées ne devront aucunement faire l'objet d'un quelconque traitement de la part du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES.

Article 2 :

Les données traitées par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES ne peuvent être utilisées à des fins autres que celles précisées dans la demande d'autorisation.

Toute réutilisation de ces données à d'autres fins doit faire l'objet d'une autorisation préalable de l'Autorité de protection.

Article 3 :

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a l'obligation de procéder au recueil du consentement préalable des personnes concernées, par l'enregistrement des consentements préalables en début d'entretien.

Les mentions d'informations devront figurer sur son site et sur ceux de ses prestataires, indépendamment des conditions générales d'informations.

Article 4 :

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est autorisé à communiquer les données traitées :

- **pour le besoin de ses enquêtes :**

- à ses agents habilités ;
- à KANTAR, au Sénégal ;
- à HORUS, en France.

- **pour l'exécution des missions de service public:**

- au Procureur de la République ;
- aux Officiers de Police Judiciaire munis d'une réquisition ;
- aux Agents assermentés de l'Autorité de protection habilités, dans le cadre de l'exécution de leurs missions ;
- aux Agents habilités de l'Administration publique habilités dans le cadre de leurs missions.

Il est interdit au GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES de transférer, sans autorisation préalable de l'Autorité de protection, les données collectées vers des pays tiers, hors de la CEDEAO.

Article 5 :

Les données sont conservées par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES, pendant un délai de six (06) mois, à compter de la fin de l'enquête.

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est tenu de supprimer lesdites données après l'expiration de ce délai.

En cas de litige, les données sont conservées jusqu'à la fin de la procédure judiciaire, lorsque la décision de justice rendue est devenue définitive.

Article 6 :

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES informe les personnes concernées de leurs droits d'accès direct, d'opposition, d'effacement, de portabilité, de retrait du consentement donné, de rectification et de suppression.

Elle le fait au début des entretiens téléphoniques, et par le biais de mention sur son site internet.

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est tenu de définir une procédure de gestion des droits des personnes concernées.

Article 7 :

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES désigne un correspondant à la protection auprès de l'Autorité de protection.

Il notifie la désignation dudit correspondant à l'Autorité de protection par un courrier officiel.

Le correspondant à la protection tient une liste des traitements effectués, immédiatement accessible à toute personne concernée en faisant la demande.

Article 8 :

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES veille au respect des dispositions de la Loi relative à la protection des données à caractère personnel par ses sous-traitants.

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est tenu de mettre en place un dispositif de :

- formation pour son correspondant à la protection et ses agents habilités;
- sensibilisation pour son personnel.

Article 9 :

Conformément à l'article 42 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est tenu d'établir pour le compte de l'Autorité de protection un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES communique ce rapport à l'Autorité de protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 10 :

L'Autorité de protection procède à des contrôles auprès du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 11 :

La présente décision entre en vigueur à compter de la date de sa notification au GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES.

Article 12 :

Le Directeur Général par Intérim est chargé de l'exécution de la présente décision, qui sera publiée au Journal Officiel de la République de Côte d'Ivoire et 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 1er février 2022
En deux (2) exemplaires originaux

Le Président

Autorité de Régulation des Télécommunications / ARTCI

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

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

CONSEIL DE REGULATION

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0716

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

EN DATE DU 1er FEVRIER 2022

PORTANT AUTORISATION DE TRANSFERT DE DONNEES A CARACTERE PERSONNEL PAR GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES (CGAP) VERS LA FRANCE

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

L'AUTORITE DE PROTECTION,

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 l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'information et de la Communication ;

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 ;

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° 2016-483 du 07 juillet 2016 portant nomination des Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le Décret n°2016-851 du 19 Octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

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 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 des Télécommunications/tic de Côte d'Ivoire en date du 03 septembre 2014 portant adoption des règles de conduite relatives au traitement et à la protection des données à caractère personnel (DCP) ;

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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et agrément en matière de Protection des données à caractère personnel ;

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 relativeà la protection des données à caractère personnel ;

Vu la Décision n°2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

Vu la Décision n°2020-0581 de l'Autorité de protection 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 Les Décisions n°2022-0714 et n°2022-0715 de l'Autorité de protection de la République de Côte d'Ivoire en date du 1er Février 2022 portant Autorisation de traitement de données à caractère personnel par le Groupe Consultatif d'Assistance aux Pauvres (GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES) ;

Vu la Résolution n°2021-161 du Conseil de Régulation en date du 30 juin 2021 portant nomination du Directeur Général par Intérim ;

Par les motifs suivants :

Considérant que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est administré et hébergé en Côte d'Ivoire par la Banque Mondiale, et que dans le cadre de son action au sein de la zone UEMOA, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a initié un projet régional de laboratoire pour la protection des consommateurs des Services Financiers Numériques (SFN).

Considérant que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES envisage réaliser des analyses résultantes d'enquêtes téléphoniques visant à appréhender les risques et les impacts liés à l'usage du crédit digital et des Services Financiers Numériques, par appel téléphonique auprès des clients du crédit digital et des consommateurs des SFN ;

Que le résultat de ces enquêtes téléphoniques devra être transmis à son sous-traitant HORUS basé en France, pour les besoins d'analyse ;

Considérant que l'article 47 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 est chargée d'autoriser les transferts transfrontaliers de données à caractère personnel dans les conditions fixées par 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, le traitement des données à caractère personnel ;

L'Autorité de protection est compétente, pour examiner la demande d'autorisation de transfert initiée par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES :

- **Sur la recevabilité de la demande d'autorisation de transfert**

Considérant que l'article 7 du 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, dispose que la demande d'autorisation pour le transfert de données à caractère personnel vers les pays tiers doit être présentée par une personne morale de droit ivoirien ;

Que cette demande contient, outre les informations requises à l'article 9 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, un mémoire comportant les extraits de casiers judiciaires des principaux dirigeants sociaux de la personne morale qui fait la demande, datant de moins de trois mois ;

Considérant que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est une personne morale de droit ivoirien, qui a fourni dans le cadre de sa demande de transfert, les informations requises à l'article 9 ci-dessus et l'extrait du casier judiciaire de son représentant légal en Côte d'Ivoire daté de moins de trois (03) mois ;

Il convient de noter que la demande de transfert présentée par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est accompagnée de tous les éléments exigés par

l'article 7 du 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 ;

En conséquence, l'Autorité de protection considère la demande de transfert le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES, recevable en la forme ;

- **Sur la nature des données, objets du transfert**

L'Autorité de protection constate que le transfert envisagé par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES concerne les données dont le traitement a été autorisé par les décisions n°2022-0714 en date du 1er Février 2022 et n°2022-0715 en date du 1er Février 2022 :

- **les données d'identification :** Nom, prénom, tranche d'âge, sexe ;
- **les données d'identification national :** numéro de téléphone ;
- **les informations d'ordre économique et financier** : les types de SFN et des crédits numériques utilisés, les fréquences et difficultés rencontrées dans l'utilisation de ces services, revenus, montants opération, montant des prêts contractés ;
- **les données d'ordre professionnel :** profession ;
- **les données de localisation** : lieu de résidence (zone rurale ou urbaine) ;
- **les données relatives à l'appréciation sur les difficultés sociales des personnes :** conditions de vie, niveau d'éducation ;
- **les raisons des plaintes et l'appréciation des utilisateurs des SFN sur le traitement des plaintes** ;

Considérant que les données suscitées sont traitées dans le cadre analyses et enquêtes téléphonique visant à identifier et évaluer les risques liés à l'usage des SFN et leurs impacts et ceux du crédit numérique sur la vie des utilisateurs ; traitement autorisé par les décisions n°2022-0714 et n°2022-0715 en date du 1er Février 2022 ;

L'Autorité de protection considère que les données que la demanderesse envisage de transférer sont adéquates, pertinentes et non excessives, au regard du transfert.

- **Sur le motif et les finalités du transfert**

Considérant qu'en l'espèce, la demande de transfert soumise par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES à l'Autorité de protection, a pour finalité de communiquer les données traitées à la société HORUS, en France ;

Qu'en effet, la société HORUS est son sous-traitant chargé des analyses relatives aux enquêtes réalisées dans le cadre du projet ;

L'Autorité de protection en déduit que la finalité existe et qu'elle est explicite et légitime.

- **Sur le pays d'hébergement et le cadre juridique relatif aux données à caractère personnel appliqué dans le pays destinataire**

Considérant qu'aux termes de l'article 26 de la Loi n°450-2013 relative à la protection des données â caractère personnel, le responsable d'un traitement ne peut être autorisé à transférer des données à caractère personnel vers un pays tiers, que si cet Etat assure un niveau de protection supérieur ou équivalent de la vie privée, des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet ;

Qu'il en résulte que le transfert de données ä caractère personnel vers *un* pays tiers ne peut être autorisé que si le pays destinataire a une Autorité de protection et un niveau de protection adéquat ;

Considérant qu'en l'espèce, le pays destinataire des données transférées est la France, pays de l'Union Européenne soumis au Règlement Général sur la Protection des données (RGPD) ;

Considérant que la France a une Autorité de protection, dénommée Commission Nationale de l'Informatique et des Libertés (CNIL) ;

Qu'ainsi, les données sont transférées vers un pays qui a une Autorité de Protection et un niveau de protection adéquat ;

L'Autorité de protection considère que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a apporté des garanties appropriées à la protection des données transférées à la société HORUS, en France ;
En conséquence, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES peut être autorisé à transférer vers la France, les données telles que mentionnées dans le dossier de demande de transfert ;

Toutefois, l'Autorité de protection prescrit à la demanderesse de lui fournir les outils de la conformité au Règlement Général de la Protection des Données (RGPD) de la société HORUS, constituant la preuve que cette dernière est en conformité avec la Loi en vigueur dans le pays destinataire des données.

- **Sur la garantie d'accès sans obstacle aux données transférées par la personne concernée pour l'exercice de ses droits et par les pouvoirs publics ivoirien pour l'exercice de leurs prérogatives respectives.**

Considérant que le demandeur indique que les personnes concernées pourront faire valoir leurs droits d'accès direct, d'opposition, de rectification et de suppression auprès du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES ;

Considérant par ailleurs que la CNIL de la France et l'Autorité de protection de la Côte d'ivoire sont toutes les deux membres de la Conférence Internationale des Autorités de protection des données personnelles au sein de laquelle elles coopèrent pour la protection des droits de leurs citoyens respectifs ;

L'Autorité de protection en déduit que le transfert envisagé présente des garanties suffisantes d'accès sans obstacle aux données transférées par la personne concernée, pour l'exercice de ses droits et par les pouvoirs publics ivoiriens pour l'exercice de leurs prérogatives respectives.

Toutefois, l'Autorité de protection prescrit au GROUPE CONSULTATIF d'ASSISTANCE AUX PAUVRES de désigner un correspondant à la protection.

- **Sur les mesures de sécurité**

Considérant que les mesures de sécurité concernent les garanties de protection, de conservation, de confidentialité des données à caractère personnel, les modalités de transmission de données, et la garantie d'exploitation des fichiers contenant les données â caractère personnel quel que soit le support technique utilisé ;

Qu'au vu des éléments techniques fournis dans le formulaire, le niveau de sécurité du système d'information que le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES a mis en œuvre pour effectuer le transfert de données à caractère personnel est suffisant pour garantir la confidentialité des données ;

Considérant par ailleurs que la Commission Nationale de l'informatique et des Libertés (CNIL) veille au respect des obligations légales des responsables de traitement établis sur son territoire ;

L'Autorité de protection considère que les mesures de sécurité nécessaires sont garanties.

Après en avoir délibéré,

DECIDE :

Article 1 :

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est autorisé à transférer les données collectées vers la société HORUS, conformément aux décisions n°2022-0714 et n°2022-0715 en date du 1er Février 2022.

Le transfert des données traitées devra respecter les conditions de communication des données prévues à l'article 4 des décisions n°2022-0714 et n°2022-0715 en date du 1er Février 2022.

Les données non mentionnées ne devront faire l'objet d'aucun autre traitement de la part du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES.
Il est interdit, au destinataire de transférer à nouveau, les données dans un autre pays, sans l'accord préalable du responsable du traitement d'origine et information de l'Autorité de protection de la République de Côte d'Ivoire.

Les données transférées ne devront pas être utilisées pour des finalités incompatibles avec les finalités initiales.

Article 2 :

Tout autre transfert est soumis à l'autorisation préalable de l'Autorité de protection.

Avant tout transfert des données hors de la Côte d'Ivoire, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est tenu de les stocker sur le territoire de la République de Côte d'Ivoire.

Article 3 :

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est tenu de recueillir le consentement préalable des personnes concernées, avant tout transfert des données.
Il devra apporter la preuve du recueil du consentement à l'Autorité de protection.

Conformément aux dispositions de l'article 1 de la décision n°2014-0021 du 3 septembre 2014 portant conditions et critères applicables à la limitation du traitement des données à caractère personnel, les personnes concernées doivent avoir été suffisamment informées par le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES, avant de donner librement leur consentement, afin d'être en mesure de comprendre d'une part, la portée et les conséquences de leur consentement, et d'autre part, les avantages et les inconvénients du traitement.

Article 4 :

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est tenu d'informer les personnes concernées, des finalités du traitement et de leurs droits d'accès direct, d'opposition, de rectification, d'effacement, de portabilité, de retrait du consentement donné, de suppression.

Il le fait par le biais de :

- mentions sur son site internet ;
- d'informations véhiculés par ses partenaires de service financiers numériques (mails, messages sms).

- au début des entretiens téléphoniques.

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES est tenu de définir une procédure de gestion des droits des personnes concernées.

Elle veille également à la mise en œuvre de la politique de sécurisation des données, telles que mentionnées dans le dossier de demande d'autorisation de transfert.

Article 5 :

En application de l'article 8 du 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, le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES établit un rapport annuel sur le transfert de données à caractèrepersonnel vers les pays tiers.

Le GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 6 :

L'Autorité de protection procède â des contrôles auprès du GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES, afin de vérifier le respect de la présente disposition, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 7 :

La présente décision entre en vigueur â compter de la date de sa notification au GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES.

Article 8 :

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

Fait à Abidjan, le 01 Février 2022
En deux (2) exemplaires originaux

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

SMC

ARTCI
AUTORITÉ DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

CONSEIL DE REGULATION

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0717

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

EN DATE DU 1er FEVRIER 2022

PORTANT AUTORISATION DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL PAR MAISOIN SARL

L'AUTORITE DE PROTECTION,

Vu l' Acte uniforme OHADA du 15 décembre 2010 portant sur le droit commercial Général ;

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 l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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° 2016-483 du 07 juillet 2016 portant nomination de membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le Décret n°2019-372 du 24 avril 2019 portant nomination du Directeur Général de l'Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI) ;

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°2018-361 du 23 mars 2018 portant réglementation de la télémédecine en Côte D'Ivoire ;

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°2014-0021 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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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°2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

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 de l'activité :

- du correspondant à la protection des données, personne morale ;
- de formation en matière de protection des données à caractère personnel ;
- d'audit en matière de protection des données à caractère personnel ;

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 données à caractère personnel ;

Vu la Résolution n°2021-161 du 30 juin 2021 portant désignation du Directeur Général par Intérim de l'Autorité de Régulation des Télécoms/TIC de Côte d'Ivoire (ARTCI) .

Par les motifs suivants :

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par la société **MAISOIN**, Société à Responsabilité Limitée, au capital d'un million (1 000 000) de francs CFA, sise à Abidjan, Cocody. Riviera Bonoumin, 09 BP 2852 Abidjan 09, immatriculée au Registre du Commerce et du Crédit mobilier sous le numéro CI-ABJ-2019-B-211991 ;

Considérant que **MAISOIN SARL** est une entreprise qui a pour objet social l'amélioration de l'accès aux soins de santé pour les habitants de la Côte d'Ivoire ;

Considérant que l'article 47 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 est chargée de recevoir les déclarations et d'octroyer les autorisations, pour la mise en œuvre de traitements de données à caractère personnel ;

L'Autorité de protection est compétente, pour examiner la demande d'autorisation de traitements initiée par **MAISOIN SARL** :

- **Sur la recevabilité de la demande d'autorisation**

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 les données médicales, 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 qu'en l'espèce, la demanderesse collecte et stocke par le biais de son application web et mobile dénommé « MaiSoin », les données de santé des patients qui ont recours à ladite application ;

Qu'en outre, l'application collecte également les données à caractère personnel des utilisateurs dont le numéro de téléphone des patients et le numéro de la Carte Nationale d'Identité (CNI) des professionnels de la santé ;

Qu'en application des dispositions précitées, lesdits traitements doivent être autorisés par l'Autorité de protection, pour être mis en œuvre ;

Considérant que selon l'article 7 précité de la même loi, la demande d'autorisation est présentée par le responsable du traitement ou son représentant légal ;

Que l'article 1 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, définit le responsable du traitement comme étant la personne physique ou morale, publique ou privée, 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 ;

Considérant qu'aux termes de l'article 9 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la demande d'autorisation doit contenir les mentions minimums relatives à la dénomination sociale de la personne morale, au Responsable du traitement, à son siège social, à l'identité de son représentant légal, à son numéro d'immatriculation au registre du commerce et du crédit mobilier, à son numéro de déclaration fiscale, aux finalités du traitement, à la durée de conservation des données traitées, aux dispositions prises pour assurer la sécurité des traitements, à la protection et à la confidentialité des données traitées ;

Considérant que lesdites mentions figurent dans la demande d'autorisation formulée par **MAISOIN SARL** ;

Que ladite demande satisfait les conditions de forme exigées par les articles 7 et 9 de la Loi n°2013-450 relative à la protection des données à caractère personnel ;

En conséquence, l'Autorité de protection considère que la demande de **MAISOIN SARL** est recevable en la forme.

- **Sur la légitimité et la licéité du traitement**

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 la demanderesse procède à la collecte des données auprès, des professionnels de la santé et des patients de son application ; qu'il s'agit d'une collecte directe de données à caractère personnel ;

Considérant cependant que la demanderesse indique qu'elle procédera au recueil du consentement préalable par le biais de : formulaire de recueil du consentement, conditions générales d'utilisation de l'application, sms et e-mail.

L'Autorité de protection considère que le principe de la légitimité n'est pas pleinement respecté :

Aussi, l'Autorité de protection prescrit à **MAISOIN SARL** de :

- prévoir des cases à cocher pour le consentement spécifique relatif à la géolocalisation, aux données de connexion , aux données de navigation et aux données de santé ;
- segmenter le consentement par catégorie des données collectées ;
- prévoir un formulaire numérique pour le recueil de consentement exprès avant le partage des données avec les tiers ;
- prévoir un dispositif pour le recueil de consentement des parents pour les mineurs ;
- mettre en place des conditions générales permettant d'éclairer le consentement de l'usager.

- **Sur la finalité**

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 qu'en l'espèce, la demanderesse procède au traitement de données à caractère personnel afin, de mettre en relation des professionnels de la santé avec les patients pour la réalisation des soins à domicile, la télémédecine et les analyses épidémiologiques ;

L'Autorité de protection considère que cette finalité est déterminée, explicite et légitime.

- **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 qu'en l'espèce, **MAISOIN SARL** a indiqué qu'elle conservera les données traitées durant trente (30) ans et sur une période de deux (02) semaines après la réception de l'e-mail de suppression du compte de l'utilisateurs.

L'Autorité de protection au regard de la finalité du traitement considère que le délai de 30 ans est excessif.

Par conséquent, l'Autorité prescrit à la demanderesse de conserver :

- les données traitées durant cinq (05) ans en base active et quinze (15) ans en archivage ;

- la demanderesse doit également mettre en œuvre une politique d'archivage électronique des données avec une durée de conservation spécifique pour chaque catégorie de données.

En cas de contentieux, il est prescrit à **MAISOIN SARL** de conserver les données traitées jusqu'au règlement définitif du contentieux.

- **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 qu'en l'espèce, **MAISOIN SARL** indique que le traitement concerne les données suivantes :

✓ **Pour les professionnels de la santé :**

- **les données d'identification :** Nom, prénom, date, lieu de naissance, signature;
- **les données de situation professionnelle :**profession, numéro d'ordre des médecins, spécialité professionnelle ;
- **les données de localisation :** Adresse géographique, coordonnées Global Positioning System (GPS) du centre de santé;
- **les données de connexions :** cookies, e-mail, adresse IP ;
- **les numéros d'identification nationale** : numéro de téléphone, carte nationale d'identité (CNI),passeport.
- **Les données d'infraction :** extrait du casier du judiciaire.

✓ **Pour les patients :**

- **les données d'identification :** Nom, prénom, date, lieu de naissance ;
- **les données de localisation :** Adresse géographique, lieu d'habitation, coordonnées Global Positioning System (GPS) ;
- **les données médicales :** pathologie, affection, antécédents familiaux, données relatives aux soins, situations ou comportements à risques, résultats d'examens.

Il y a lieu de constater que les données collectées, telles qu'elles sont décrites dans la demande d'autorisation sont pertinentes, adéquates, et non excessives au regard de la finalité.

- **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, selon lesquelles la demande d'autorisation adressée à l'Autorité de protection doit contenir les destinataires habilités à recevoir communication des données traitées ;

Considérant qu'en l'espèce, la demanderesse précise que les destinataires desdites données sont :

- Les services internes de **MAISOIN SARL** ;
- Les professionnels de santé ;
- Google cloud platform ;
- Hôpitaux et clinique.

L'Autorité de protection prescrit que les données traitées soient communiquées, aussi :

- au Procureur de la République ;
- aux Officiers de Police Judiciaire de Côte d'Ivoire munis d'une réquisition;
- aux agents assermentés de l'Autorité de protection (ARTCI) habilités, dans le cadre de leurs missions ;
- aux agents habilités de l'administration publique dans le cadre de leurs missions.

MAISOIN SARL ne doit avoir accès au dossier médical des patients, qu'à des fins de maintenance.
Le dossier médical des patients doit-être chiffré et la clé de déchiffrage est exclusivement détenu par **le patient, les professionnels de la santé, les hôpitaux et les cliniques.**
Les données destinées à la réalisation d'analyses épidémiologiques doivent être anonymisées avant toute communication à des tiers autorisés.

L'Autorité de protection prescrit que lesdites données ne fassent l'objet d'aucun transfert vers des pays tiers, sans autorisation préalable ;

- **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 la demanderesse de faire preuve de transparence vis à vis des personnes concernées qui devront notamment être informées :

- 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.

Qu'à cette fin, la demanderesse indique qu'un formulaire de recueil du consentement, des conditions générales d'utilisation de son application, une mention dans le contrat et dans les e-mails permettront aux personnes concernées d'être informées de leurs droits, préalablement à toute collecte ;

Considérant que ces formalités ne suffisent pas à satisfaire le principe de transparence ;

L'Autorité de protection prescrit à **MAISOIN SARL** de compléter les informations portées à la connaissance des personnes concernées par les mentions relatives à la finalité des traitements, et la description exhaustive des données personnelles traitées par catégorie :

- Catégorie 1 : patients
- Catégorie 2 : professionnels de santé.

- **Sur les droits d'accès direct, d'opposition, de rectification 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, d'opposition, d'effacement.

Considérant que la demanderesse n'indique pas le service ou la direction auprès de laquelle les clients pourront exercer les droits d'accès direct, d'opposition, de rectification, d'effacement, de portabilité, de retrait du consentement donné, et de suppression, pourront être exercés. Qu'en outre, la demanderesse n'a pas désigné de correspondant à la protection.

L'Autorité de protection prescrit à **MAISOIN SARL** de :

- désigner un correspondant à la protection, auprès duquel les personnes concernées pourront exercer leurs droits ;
- élaborer une procédure de gestion des droits des personnes concernées ;
- élaborer une charte de protection des données personnelles.

- **Sur les mesures de sécurité**

Considérant qu'en application de l'article 41 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le responsable du traitement et le sous-traitant prennent toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher

qu'elles soient détruites, déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance ;

Considérant que les mesures de sécurité doivent couvrir l'aspect physique (les données stockées sur des supports papiers) et logique (supports informatiques) ;

Considérant que **MAISOIN SARL** a réalisé une analyse d'impact relative à la vie privée qui a conclu que de bonnes pratiques de protection de données à caractère personnel ont été mises en place par la demanderesse ;

Considérant qu'au vu des éléments techniques fournis par la demanderesse, du site internet et de l'application « MAISOIN », il y a lieu de relever que **MAISOIN SARL** a un niveau de sécurité satisfaisant pour la mise en œuvre du traitement envisagé ;

Cependant, l'Autorité de protection prescrit à la demanderesse de :

- renforcer la sécurité physique en y ajoutant un contrôle d'accès, au regard des données de santé traitées ;
- opter pour un certificat SSL offrant un niveau de confiance plus élevé ;
- l'application « MAISOIN » fait intervenir différents acteurs (patients, professionnels de la santé, gestionnaires de la plateforme...). Les données traitées étant particulièrement sensibles, il serait opportun que l'entreprise entame un processus de mise en conformité en vue de couvrir efficacement tous les aspects liés à la protection des données personnelles
- élaborer une politique de gestion des cookies et autres traceurs.

Après en avoir délibéré,

DECIDE :

Article 1 :

MAISOIN SARL est autorisée à effectuer la collecte, et l'enregistrement des données à caractère personnel ci-après :

✓ **Pour les professionnels de la santé :**

- **les données d'identification :** Nom, prénom, date, lieu de naissance, signature;
- **les données de situation professionnelle :**profession, numéro d'ordre des médecins, spécialité professionnelle ;

- **les données de localisation :** Adresse géographique, coordonnées Global Positioning System (GPS) du centre de santé;
- **les données de connexions :** cookies, e-mail, adresse IP ;
- **les numéros d'identification nationale** : numéro de téléphone, carte nationale d'identité (CNI),passeport.
- **Les données d'infraction :** extrait du casier du judiciaire.

✓ **Pour les patients :**

- **les données d'identification :** Nom, prénom, date, lieu de naissance ;
- **les données de localisation :** Adresse géographique, lieu d'habitation, coordonnées Global Positioning System (GPS) ;
- **les données médicales :** pathologie, affection, antécédents familiaux, données relatives aux soins, situations ou comportements à risques, résultats d'examens ;

Les données visées au présent article concernent les usagers de l'application **MAISOIN SARL** dans le cadre.de la mise en relation des professionnels de la santé avec les patients pour la réalisation des soins à domicile, la télémédecine et les analyses épidémiologiques

Les données non mentionnées ne devront aucunement faire l'objet d'un quelconque traitement de la part de **MAISOIN SARL**.

Article 2 :

Les données traitées par **MAISOIN SARL** ne peuvent être utilisées à des fins autres que celles précisées dans la demande d'autorisation.

Toute réutilisation de ces données à d'autres fins doit faire l'objet d'une autorisation préalable de l'Autorité de protection

Article 3 :

MAISOIN SARL a l'obligation de procéder au recueil du consentement préalable des personnes concernées, par l'insertion de :

- mécanisme de recueil du consentement exprès sur son application pour chaque finalité.
- prévoir des cases à cocher pour le consentement spécifique relatif à la géolocalisation, aux données de connexion ,aux données de navigation et aux données de santé;

- segmenter le consentement par catégorie des données collectées ;
- prévoir un formulaire numérique pour le recueil de consentement exprès avant le partage des données avec les tiers ;
- prévoir un dispositif pour le recueil de consentement des parents pour les mineurs ;
- mettre en place des conditions générales permettant d'éclairer le consentement des utilisateurs de l'application.

Conformément aux dispositions de l'article 1 de la décision n°2014-0021 du 03 septembre 2014 portant conditions et critères applicables à la limitation du traitement des données à caractère personnel, la personne concernée doit avoir été suffisamment informée par **MAISOIN SARL** 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.

Article 4 :

MAISOIN SARL est autorisée à communiquer les données traitées :

- au service interne de **MAISOIN SARL**;
- aux professionnels de santé dans le respect des termes de leur contrat ;
- à google cloud platform ;
- au Procureur de la République ;
- aux Officiers de Police Judiciaire de Côte d'Ivoire munis d'une réquisition ;
- aux agents assermentés de l'Autorité de protection (ARTCI) habilités, dans le cadre de l'exécution de leurs missions ;
- aux agents de l'administration publique dans le cadre de leurs missions.

Il est interdit à **MAISOIN SARL** de transférer, **sans autorisation préalable de l'Autorité de protection**, les données collectées vers des pays tiers.

Article 5 :

MAISOIN SARL ne doit avoir accès au dossier médical des patients, qu'à des fins de maintenance.
Le dossier médical des patients doit-être chiffré et la clé de déchiffrage est exclusivement détenu par **le patient, les professionnels de la santé, les hôpitaux et les cliniques.**
MAISOIN SARL est tenue d'anonymiser les données traitées à des fins d'analyses épidémiologiques avant toute communication à des tiers autorisés.

Article 6 :

MAISOIN SARL conserve l'ensemble des données traitées :

- pendant cinq (05) ans en base active et quinze (15) ans en archivage ;
- la demanderesse doit également mettre en œuvre une politique d'archivage électronique des données avec une durée de conservation spécifique pour chaque catégorie de données.

En cas de contentieux, il est prescrit à **MAISOIN SARL** de conserver les données traitées jusqu'au règlement définitif du contentieux.

Article 7 :

MAISOIN SARL informe les personnes concernées de leurs droits d'accès direct, d'opposition, d'effacement, de portabilité, de retrait du consentement donné, de rectification et de suppression. Elle le fait par le biais de mentions dans les conditions générales d'utilisation de son application mobile « MAISOIN » ;

MAISOIN SARL doit également définir une politique gestion des droits des personnes concernées

Article 8 :

MAISOIN SARL désigne un correspondant à la protection auprès de l'Autorité de protection.

Elle notifie la désignation dudit correspondant à l'Autorité de protection par un courrier officiel.

Le correspondant à la protection tient une liste des traitements effectués, immédiatement accessible à toute personne concernée en faisant la demande.

Article 9 :

MAISOIN SARL veille au respect des dispositions de la Loi relative à la protection des données à caractère personnel par ses sous-traitants.

MAISOIN SARL est tenue de mettre en place un dispositif de :

- formation pour son correspondant à la protection et ses agents habilités
- sensibilisation sur la protection des données à caractère personnel pour son personnel ;
- gestion des habilitations des utilisateurs de l'application pour limiter les accès aux seules données qui sont strictement nécessaires aux utilisateurs en fonction de leurs besoins.

Article 10 :

Conformément à l'article 42 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, **MAISOIN SARL** est tenue d'établir pour le compte de l'Autorité de protection un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

MAISOIN SARL communique ce rapport à l'Autorité de protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 11 :

L'Autorité de protection procède à des contrôles auprès de **MAISOIN SARL** afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 12 :

MAISOIN SARL est tenue de procéder au paiement des frais de dossiers auprès du greffe de l'ARTCI, conformément à la décision n°2016-021 de l'Autorité de protection de la République de Côte d'Ivoire fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel.

Article 13 :

La présente décision entre en vigueur à compter de la date de sa notification à **MAISOIN SARL**.

Article 14 :

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

Fait à Abidjan, le 01 Février 2022
En deux (2) exemplaires originaux

Le Président

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

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

SMC

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

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

CONSEIL DE REGULATION

DECISION N°2022-0718

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

EN DATE DU 1er FEVRIER 2022

PORTANT AUTORISATION DE TRANSFERT DE DONNEES A CARACTERE PERSONNEL

VERS LA FRANCE PAR MAISOIN SARL

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

SMC

L'AUTORITE DE PROTECTION,

Vu l'Acte uniforme OHADA du 15 décembre 2010 portant sur le droit commercial général ;

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 l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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° 2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le Décret N°2018-361 du 23 mars 2018 portant réglementation de la télémédecine en Côte D'Ivoire ;

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 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°2014-0021 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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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°2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

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 de l'activité :

- du correspondant à la protection des données, personne morale ;
- de formation en matière de protection des données à caractère personnel ;
- d'audit en matière de protection des données à caractère personnel ;

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 données à caractère personnel ;

Vu la Résolution n°2021-161 du 30 juin 2021 portant désignation du Directeur Général par Intérim de l'Autorité de Régulation des Télécoms/TIC de Côte d'Ivoire (ARTCI).

Par les motifs suivants :

Considérant que **MAISOIN**, est une Société à Responsabilité Limitée au capital d'un million (1 000 000) de francs CFA, sise à Abidjan, Cocody. Riviera Bonoumin, 09 BP 2852 Abidjan 09, immatriculée au Registre du Commerce et du Crédit mobilier sous le numéro CI-ABJ-2019-B-211991 ; a introduit auprès de l'Autorité de Protection une demande d'autorisation de transfert de données à caractère personnel ;

Considérant que **MAISOIN SARL** est une entreprise qui a pour objet social l'amélioration de l'accès aux soins de santé pour les habitants de la Côte d'Ivoire ;

Considérant que l'article 47 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 est chargée d'autoriser le transfert transfrontalier de données à caractère personnel, dans les conditions fixées par 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.

L'Autorité de protection est compétente, pour examiner la demande d'autorisation de transfert des données personnelles initiée par **MAISOIN SARL**.

- **Sur la recevabilité de la demande d'autorisation de transfert**

Considérant que l'article 7 du décret 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, dispose que la demande d'autorisation pour le transfert de données à caractère personnel vers les pays tiers doit être présentée par une personne morale de droit ivoirien.

Que cette demande contient, outre les informations requises à l'article 9 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, un mémoire comportant les extraits de casiers judiciaires des principaux dirigeants sociaux de la personne morale qui fait la demande, datant de moins de trois mois ;

Considérant que **MAISOIN SARL** est une société à responsabilité limitée de droit ivoirien immatriculée au Registre du Commerce et du Crédit Mobilier, qui a fourni dans le cadre de sa demande de transfert l'extrait du casier judiciaire de son Gérant daté de moins de 03 mois ;

Il convient de noter que la demande d'autorisation de transfert de données personnelles introduite par la société **MAISOIN SARL** contient tous les éléments exigés par l'article 7 précité ;

Ainsi, l'Autorité de protection considère que la demande d'autorisation de transfert initiée par la société **MAISOIN SARL** est recevable ;

- **Sur la nature des données objet du transfert**

L'autorité de protection constate que le transfert envisagé par la demanderesse concerne les données suivantes dont le traitement a été autorisé par la décision n°2022-0717 en date du 1er Février 2022 :

✓ **Les données des professionnels de la santé :**

- **les données d'identification :** Nom, prénom, date, lieu de naissance, signature;
- **les données de situation professionnelle :**profession, numéro d'ordre des médecins, spécialité professionnelle ;
- **les données de localisation :** Adresse géographique, coordonnées Global Positioning System (GPS) du centre de santé;
- **les données de connexions :** cookies, e-mail, adresse IP ;
- **les numéros d'identification nationale** : numéro de téléphone, carte nationale d'identité (CNI),passeport.
- **Les données d'infraction :** extrait du casier du judiciaire.

✓ **Les données des patients :**

- **les données d'identification :** Nom, prénom, date, lieu de naissance ;

- **les données de localisation :** Adresse géographique, lieu d'habitation, coordonnées Global Positioning System (GPS) ;
- **les données médicales :** pathologie, affection, antécédents familiaux, données relatives aux soins, situations ou comportements à risques, résultats d'examens.

Considérant que les données suscitées sont traitées dans par la demanderesse par le biais de son application afin de mettre en relation des professionnels de la santé avec les patients pour la réalisation des soins à domicile, la télémédecine et les analyses épidémiologiques ; traitement autorisé par la décision n°2022-0717 en date du 1er Février 2022 ;

L'Autorité de protection considère que les données que la demanderesse envisage de transférer sont adéquates, pertinentes et non excessives, au regard du transfert.

- **Sur le motif et les finalités du transfert**

Considérant qu'en l'espèce, la demande de transfert soumise par **MAISOIN SARL** à l'Autorité de protection a pour finalité le stockage des données des professionnels de la santé et des patients sur le serveur de **GOOGLE PLATFORM** en FRANCE.

Qu'en effet, **MAISOIN SARL** et **GOOGLE PLATFORM** ont respectivement la qualité de responsable du traitement et de sous- traitant ;

L'Autorité de protection en déduit que la finalité de la demanderesse est explicite et légitime.

- **Sur le nom du pays d'hébergement et le cadre juridique relatif aux données à caractère personnel appliqué dans le pays destinataire**

Considérant qu'aux termes de l'article 26 de la loi n°2013-450 du 19 Juin 2013 relatif à la protection des données à caractère personnel, le responsable d'un traitement ne peut être autorisé à transférer les données à caractère personnel vers les pays destinataires que si cet Etat assure un niveau de protection supérieur ou équivalent de la vie privée, des libertés et droit fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet.

Qu'il en résulte que le transfert de données à caractère personnel vers un pays tiers ne peut être autorisé que si ce pays destinataire dispose d'une autorité de protection et un niveau de protection adéquat.

Considérant qu'en l'espèce, le pays destinataire des données transférées est la France, pays de l'Union Européenne soumis au Règlement Général sur la Protection des données (RGPD) ;

Considérant que la FRANCE a une Autorité de protection, dénommée la Commission Nationale de l'Informatique et des Libertés (CNIL) ;

Qu'ainsi, les données sont transférées vers un pays qui a une Autorité de Protection et un niveau de protection adéquat ;

L'Autorité de protection considère que **MAISOIN SARL** a apporté des garanties appropriées à la protection des données transférées à **GOOGLE PLATFORM,** en FRANCE ;

En conséquence, **MAISOIN SARL** peut être autorisé à transférer vers la FRANCE, les données telles que mentionnées dans le dossier de demande de transfert.

Toutefois, l'Autorité de protection prescrit à la demanderesse de lui fournir les outils de la conformité au Règlement Général de la Protection des Données (RGPD) de **GOOGLE PLATFORM**, constituant la preuve que cette dernière est en conformité avec la Loi en vigueur dans le pays destinataire des données.

- **Sur la garantie d'accès sans obstacle aux données transférées par la personne concernée pour l'exercice de ses droits et par les pouvoirs publics ivoiriens pour l'exercice de leurs prérogatives respectives**

Considérant que la demanderesse indique que les personnes concernées pourront faire valoir leur droit d'accès direct, d'opposition, de rectification, de suppression auprès **de MAISOIN SARL ;**

L'Autorité de protection en déduit que le transfert envisagé présente des garanties suffisantes d'accès sans obstacles aux données transférées par la personne concernée pour l'exercice de ses droits et par les pouvoirs publics ivoiriens pour l'exercice de leurs prérogatives respectives ;

Toutefois, l'Autorité de protection prescrit que **MAISOIN SARL** désigne un correspondant à la protection des données à caractère personnel ;

- **Sur les mesures de sécurité**

Considérant qu'en application de l'article 41 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le responsable

du traitement et le sous-traitant prennent toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient détruites, déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance ;

Considérant que les mesures de sécurité doivent couvrir l'aspect physique (les données stockées sur des supports papiers) et logique (supports informatiques) ;

Considérant qu'au vu des éléments techniques fournis par la demanderesse, du site internet et de l'application « MAISOIN », il y a lieu de relever que **MAISOIN SARL** a un niveau de sécurité satisfaisant pour la mise en œuvre du traitement envisagé. Cependant, l'Autorité de protection prescrit à la demanderesse de :

- Renforcer la sécurité physique en y ajoutant un contrôle d'accès, au regard des données de santé traitées ;
- Opter pour un certificat SSL offrant un niveau de confiance plus élevé ;
- **MAISOIN SARL,** doit entamer son processus de mise en conformité en vue de couvrir efficacement tous les aspects liés à la protection des données personnelles élaborer une politique de gestion des cookies et autres traceurs.

L'Autorité de Protection considère que les mesures de sécurité logique et physique nécessaires sont garanties.

Après en avoir délibéré,

DECIDE :

Article 1 :

MAISOIN SARL est autorisée à transférer les données à caractère personnel vers la FRANCE, conformément à la décision n°2022-0717 en date du 1er Février 2022 :

✓ **Les données des professionnels de la santé :**

- **les données d'identification :** Nom, prénom, date, lieu de naissance, signature;
- **les données de situation professionnelle :**profession, numéro d'ordre des médecins, spécialité professionnelle ;
- **les données de localisation :** Adresse géographique, coordonnées Global Positioning System (GPS) du centre de santé;
- **les données de connexions :** cookies, e-mail, adresse IP ;
- **les numéros d'identification nationale** : numéro de téléphone, carte nationale d'identité (CNI),passeport.
- **Les données d'infraction :** extrait du casier du judiciaire.

✓ **Les données des patients**

- **les données d'identification :** Nom, prénom, date, lieu de naissance ;
- **les données de localisation :** Adresse géographique, lieu d'habitation, coordonnées Global Positioning System (GPS) ;
- **les données médicales :** pathologie, affection, antécédents familiaux, données relatives aux soins, situations ou comportements à risques, résultats d'examens.

Les données visées au présent article concernent les utilisateurs de l'application « MAISOIN ».

Les données non mentionnées ne devront aucunement faire l'objet d'un quelconque traitement de la part de **MAISOIN SARL**.

Il est interdit, au destinataire de transférer à nouveau, les données dans un autre pays, sans l'accord préalable du responsable du traitement d'origine.

Les données transférées ne devront pas être utilisées pour des finalités incompatibles avec les finalités initiales.

A.R.T.C.I
COURRIER ARRIVÉE DCNS
LE 20 MAI 2022
N°

FAX

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

CONSEIL DE REGULATION

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0735

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE COTE D'IVOIRE

PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL PAR LA SOCIETE SADEV AFRIC

L'AUTORITE DE PROTECTION,

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° 2015-532 du 20 juillet 2015 portant Code du travail ;

Vu l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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° 2016-483 du 07 juillet 2016 portant nomination de membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le Décret n°2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

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 de Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (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 l'Arrêté n°2017-016 MEPS/CAB du 02 juin 2017 déterminant la liste des travaux légers autorisés aux enfants dont l'âge est compris entre 13 et 16 ans ;

Vu l'Arrêté n°2017-017 MEPS/CAB du 02 juin 2017 déterminant la liste des travaux dangereux et interdits aux enfants ;

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°2014-0021 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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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°2019-0494 du Conseil de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

Vu la Décision n°2021-0676 du Conseil de Régulation des Télécommunications/TIC 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 Résolution n°2021-161 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 30 juin 2021 portant désignation d'un Directeur Général par Intérim de l'ARTCI ;

Vu le Rapport d'audit de protection des données personnelles de SADEV-AFRIC ;

Par les motifs suivants :

Considérant que conformément à l'article 53 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, les responsables du traitement doivent procéder à la mise en conformité des traitements qu'ils opèrent avec ladite loi ;

Considérant que pour faciliter cette mise en conformité l'Autorité de protection a, par décision n°2017-0354 du 26 octobre 2017, défini la 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 ;

Considérant que SADEV-AFRIC est une société à responsabilité limitée (SARL) de droit ivoirien, ayant son siège social à Daloa Lot 108 Ilot 13 Quartier des OLIVIERS ;

Considérant que SADEV-AFRIC a saisi l'Autorité de protection d'une demande de mise en conformité ;

Que par ailleurs, SADEV-AFRIC a effectué son audit de protection des données personnelles ;

Considérant les recommandations contenues dans le rapport d'audit de protection des données personnelles ;

Après en avoir délibéré,

DECIDE :

Article 1 :

SADEV-AFRIC est autorisé à effectuer les traitements des données mentionnées dans l'annexe 1 de la présente décision.

Les données non mentionnées dans l'annexe 1 ne devront aucunement faire l'objet d'un quelconque traitement de la part de SADEV-AFRIC.

Article 2 :

SADEV-AFRIC est autorisé à effectuer les traitements énumérés dans l'annexe 2 de la présente décision.

Article 3 :

SADEV-AFRIC est autorisé à communiquer les données traitées uniquement aux destinataires habilités notamment :

- les agents de la société, suivant leurs habilitations ;
- les énumérateurs et autres contractuels ;
- les clients ayant sollicité les prestations de la société ;
- les partenaires techniques et commerciaux ;
- les autorités publiques ivoiriennes habilitées, dans le cadre de l'exercice de leurs missions ;
- le Procureur de la république ;
- les officiers de police judiciaire munis d'une réquisition ;
- les agents assermentés de l'Autorité de protection, dans le cadre de leurs missions de contrôle.

Article 4 :

SADEV-AFRIC est tenu fournir à l'Autorité de Protection, des Règles d'Entreprise Contraignantes (BCR), pour approbation, avant tout transfert de données vers les Etats Unis pour la sauvegarde des données auprès de COMMERCAR.

Avant tout transfert de données hors de la Côte d'Ivoire, SADEV-AFRIC est tenu de les stocker sur le territoire de la République de Côte d'Ivoire.

Tout autre transfert est soumis à l'autorisation préalable de l'Autorité de protection.

Article 5 :

Conformément à l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, SADEV-AFRIC doit s'assurer que, ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle relatives aux traitements de données qu'ils opèrent.

Il incombe à SADEV-AFRIC, ainsi qu'à ses clients et sous-traitants, de veiller au respect de ces mesures.

Article 6 :

Les traitements de données autorisés dans la présente décision correspondent aux dix (10) finalités suivantes :

- Gestion de la bonne tenue des études terrains ;
- Gestion administrative et financière ;
- Gestion des Ressources Humaines et Administrative du Personnel ;
- Gestion des accès, du réseau informatique et de la sécurité informatique/Administration du réseau et du système d'information ;
- Suivi des missions et rendements des agents ;
- Gestion de la formation du personnel et des énumérateurs ;
- Gestion de la Supervision des équipes ;
- Gestion du matériel d'enquête ;
- Gestion de la prospection commerciale/Recherche de nouveaux marchés ;
- Gestion des transferts de données hors CEDEAO.

Les traitements afférents aux finalités ci-dessus sont listés dans l'annexe 3 de la présente décision.

Article 7 :

SADEV-AFRIC est tenu de mettre en œuvre les prescriptions énoncées dans l'annexe 4 de la présente décision. Elle le fait dans les délais prévus dans ladite annexe.

La mise en œuvre desdites prescriptions fera l'objet d'un contrôle par l'Autorité de Protection.

L'Autorité de protection délivrera une attestation de conformité à SADEV-AFRIC, lorsque toutes les prescriptions auront été mises en œuvre.

Article 8 :

En application de l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, SADEV-AFRIC est tenu d'établir, pour le compte de l'Autorité de protection, un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

SADEV-AFRIC communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 9 :

L'Autorité de Protection procède à des contrôles auprès de SADEV-AFRIC, afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 10 :

SADEV-AFRIC est tenu de procéder au paiement des frais de dépôts de demande d'autorisation auprès du Greffe de l'ARTCI, conformément à la Décision n°2016-0201 de l'Autorité de protection de la République de Côte d'Ivoire fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel.

L'Autorité de Protection lui délivrera une facture à cet effet.

Article 11 :

La présente Décision entre en vigueur à compter de la date de sa notification à SADEV-AFRIC.

Article 12 :

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

Fait à Abidjan, le 05 Mai 2022
En deux (2) exemplaires originaux

Le Président

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

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

A.R.T.C.I
COURRIER ARRIVÉE DCNS
LE 20 MAI 2022
N°

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

CONSEIL DE REGULATION

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0736

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

EN DATE DU 05 MAI 2022

PORTANT AUTORISATION DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL PAR SANIA CIE (DINOR APP)

L'AUTORITE DE PROTECTION,

Vu l'Acte uniforme OHADA du 15 décembre 2010 portant sur le droit commercial Général ;

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°2017-540 du 03 août 2017 fixant les règles relatives à la régulation, au contrôle et au suivi des activités des filières Hévéa et Palmier à huile ;

Vu l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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° 2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

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 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°2014-0021 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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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°2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

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 de l'activité :

- du correspondant à la protection des données, personnes morales ;
- de formation en matière de protection des données à caractère personnel ;
- d'audit en matière de protection des données à caractère personnel ;

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 données à caractère personnel ;

Vu la Résolution n°2021-161 du 30 juin 2021 portant désignation du Directeur Général par Intérim de l'Autorité de Régulation des Télécoms/TIC de Côte d'Ivoire (ARTCI) ;

Par les motifs suivants :

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par la société **SANIA CIE**, Société Anonyme, au capital de quarante-quatre milliards cent dix millions (44 110 000 000) de francs CFA, sise à Abidjan, Zone industrielle de Vridi – Rue du Textile, 01 BP 2949 Abidjan 01, immatriculée au Registre du Commerce et du Crédit mobilier sous le numéro CI-ABJ-2008-M2-13989 ;

Considérant que **SANIA CIE** est une entreprise qui a pour objet social l'achat, l'importation, la transformation et la commercialisation de tous produits alimentaires, chimiques, cosmétiques naturels ou artificiels et d'alcools ;

Considérant que l'article 47 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 est chargée de recevoir les déclarations et d'octroyer les autorisations, pour la mise en œuvre de traitement des données à caractère personnel ;

L'Autorité de protection est compétente, pour examiner la demande d'autorisation de traitements initiée par **SANIA CIE** :

- **Sur la recevabilité de la demande d'autorisation**

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 qu'en l'espèce, la demanderesse collecte et stocke par le biais de son application web et mobile dénommée « Dinor App », les données à caractère personnel des utilisateurs dont le numéro de téléphone des clients ;

Qu'en application des dispositions précitées, lesdits traitements doivent être autorisés par l'Autorité de protection, pour être mis en œuvre ;

Considérant que selon l'article 7 précité de la même loi, la demande d'autorisation est présentée par le responsable du traitement ou son représentant légal ;

Que l'article 1 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, définit le responsable du traitement comme étant la personne physique ou morale, publique ou privée, 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 ;

Considérant que **SANIA CIE** prévoit par le biais de son application d'offrir une expérience personnalisée aux utilisateurs, notamment en leur permettant d'avoir des lieux favoris pour l'achat de produits de la marque DINOR, mais également d'avoir des recettes favorites et bénéficier des promotions ;

Considérant qu'au regard du caractère sensible des données qui feront l'objet de traitements, l'Autorité de protection a demandé à **SANIA CIE** de réaliser une analyse d'impact relative à la protection des données ;

Que les résultats de cette analyse ont été communiqués à l'Autorité de protection, et ont permis à la demanderesse de définir un plan d'action afin de réduire les risques d'atteintes à la vie privée.
L'Autorité de protection en conclut que **SANIA CIE** a la qualité de responsable du traitement.

Considérant qu'aux termes de l'article 9 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la demande d'autorisation doit contenir les mentions minimums relatives à la dénomination sociale de la personne morale, au Responsable du traitement, à son siège social, à l'identité de son représentant légal, à son numéro d'immatriculation au registre du commerce et du crédit mobilier, à son numéro de déclaration fiscale, aux finalités du traitement, à la durée de conservation des données traitées, aux dispositions prises pour assurer la sécurité des traitements, à la protection et à la confidentialité des données traitées ;

Considérant que lesdites mentions figurent dans la demande d'autorisation formulée par **SANIA CIE ;**

Que ladite demande satisfait les conditions de forme exigées par les articles 7 et 9 de la Loi n°2013-450 relative à la protection des données à caractère personnel ;

En conséquence, l'Autorité de protection considère que la demande de **SANIA CIE** est recevable en la forme ;

- **Sur la légitimité et la licéité du traitement**

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 la demanderesse procède à la collecte des données auprès des clients utilisateurs de son application ; qu'il s'agit d'une collecte directe de données à caractère personnel ;

Considérant cependant que la demanderesse indique qu'elle procédera au recueil du consentement préalable par le biais de conditions générales d'utilisation de l'application ;

L'Autorité de protection considère que le principe de la légitimité n'est pas pleinement respecté :

Aussi, l'Autorité de protection prescrit à **SANIA CIE** de :

- prévoir des cases à cocher pour le consentement spécifique relatif à la géolocalisation, la prospection, aux données de connexion et aux données de navigation ;
- segmenter le consentement par catégorie des données collectées ;
- prévoir un formulaire numérique pour le recueil de consentement exprès avant le partage des données avec les tiers.

- **Sur la finalité**

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 qu'en l'espèce, la demanderesse procède au traitement de données à caractère personnel afin de :

- offrir une expérience personnalisée aux utilisateurs ;
- avoir des lieux favoris pour l'achat de produits de la marque DINOR ;
- avoir des recettes favorites ;
- et bénéficier des promotions.

L'Autorité de protection considère que cette finalité est déterminée, explicite et légitime.

- **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 qu'en l'espèce, **SANIA CIE** a indiqué qu'elle conservera les données traitées pendant tout le temps d'utilisation de l'application par les utilisateurs et procèdera à la suppression desdites données dès la suppression du compte par l'utilisateur.

En outre, les données de connexion, et de navigation sont conservées pendant un (01) an à compter de leur enregistrement.

L'Autorité de protection au regard de la finalité du traitement considère que ces délais sont insuffisants.

L'Autorité prescrit à la demanderesse de conserver :

- les données traitées durant cinq (05) ans en base active et dix (10) ans en archivage ;
- la demanderesse doit également mettre en œuvre une politique d'archivage électronique des données avec une durée de conservation spécifique pour chaque catégorie de données.

En cas de contentieux, il est prescrit à **SANIA CIE** de conserver les données traitées jusqu'au règlement définitif du contentieux.

- **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 qu'en l'espèce, **SANIA CIE** indique que le traitement concerne les données suivantes :

- **les données d'identification :** nom, prénom, date et lieu de naissance ;
- **les données de localisation :** GSM, lieu de résidence, GPS ;
- **les données de connexions :** e-mail, identifiant, mot de passe, adresse IP, pages consultées ;
- **les données d'identification nationale :** numéro de téléphone.

Il y a lieu de constater que les données collectées, telles qu'elles sont décrites dans la demande d'autorisation sont pertinentes, adéquates, et non excessives au regard de la finalité.

- **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, selon lesquelles la demande d'autorisation adressée à l'Autorité de protection doit contenir les destinataires habilités à recevoir communication des données traitées ;

Considérant qu'en l'espèce, la demanderesse précise que les destinataires desdites données sont :

- Les services internes habilités de SANIA CIE ;
- Big five Abidjan ;
- Digital Ocean aux USA.

L'Autorité de protection prescrit que les données traitées soient communiquées, aussi :

- au Procureur de la République ;
- aux Officiers de Police Judiciaire de Côte d'Ivoire munis d'une réquisition;
- aux agents assermentés de l'Autorité de protection (ARTCI) habilités, dans le cadre de leurs missions ;
- aux agents habilités de l'administration publique dans le cadre de leurs missions.

L'Autorité de protection prescrit que lesdites données ne fassent l'objet d'aucun transfert vers des pays tiers, sans autorisation préalable.

- **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 la demanderesse de faire preuve de transparence vis-à-vis des personnes concernées qui devront notamment être informées :

- 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.

Qu'à cette fin, la demanderesse indique qu'un formulaire de recueil du consentement, des conditions générales d'utilisation de son application, permettront aux personnes concernées d'être informées de leurs droits, préalablement à toute collecte ;

Considérant que ces formalités ne suffisent pas à satisfaire le principe de transparence ;

L'Autorité de protection prescrit à **SANIA CIE** de compléter les informations portées à la connaissance des personnes concernées par les mentions relatives à la finalité des traitements, la description exhaustive des données personnelles traitées, les destinataires auxquels les données sont susceptibles d'être communiqués, l'éventualité de tout transfert de données à destination de pays tiers.

- **Sur les droits d'accès direct, d'opposition, de rectification 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, d'opposition, d'effacement.

Considérant que la demanderesse indique que la direction support est l'entité auprès de laquelle les clients pourront exercer les droits d'accès direct, d'opposition, de rectification, d'effacement, de portabilité, de retrait du consentement donné, et de suppression, pourront être exercés.

Qu'en outre, la demanderesse n'a pas désigné de correspondant à la protection.

L'Autorité de protection prescrit à **SANIA CIE** :

- de désigner un correspondant à la protection, auprès duquel les personnes concernées pourront exercer leurs droits ;
- d'élaborer une procédure de gestion des droits des personnes concernées ;
- d'élaborer une charte de protection des données personnelles.

- **Sur les mesures de sécurité**

Considérant qu'en application de l'article 41 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le responsable du traitement et le sous-traitant prennent toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient détruites, déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance ;

Considérant que les mesures de sécurité doivent couvrir l'aspect physique (les données stockées sur des supports papiers) et logique (supports informatiques) ;

Considérant qu'au vu des éléments techniques fournis par la demanderesse, et après étude de l'analyse d'impact, l'Autorité de protection conclu que le système d'information de la société **SANIA CIE**, présente un niveau de sécurité suffisant pour le traitement de données personnelles ;

Cependant, l'Autorité de protection prescrit à la demanderesse de maintenir à jour le système d'exploitation, et aussi les applications utilisées afin d'être moins vulnérable aux différentes attaques.

Après en avoir délibéré,

DECIDE :

Article 1 :

SANIA CIE est autorisée à effectuer la collecte, et l'enregistrement des données à caractère personnel ci-après :

- **les données d'identification :** nom, prénom, date, lieu de naissance ;
- **les données de localisation :** GSM, lieu de résidence, GPS ;
- **les données de connexions :** e-mail, identifiant, mot de passe, adresse IP, pages consultées ;
- **les données d'identification nationale :** numéro de téléphone.

Les données visées au présent article concernent les usagers de l'application **« DINOR APP »**

Les données non mentionnées ne devront aucunement faire l'objet d'un quelconque traitement de la part de **SANIA CIE**.

Article 2 :

Les données traitées par **SANIA CIE** ne peuvent être utilisées à des fins autres que celles précisées dans la demande d'autorisation.

Toute réutilisation de ces données à d'autres fins doit faire l'objet d'une autorisation préalable de l'Autorité de protection

Article 3 :

SANIA CIE a l'obligation de procéder au recueil du consentement préalable des personnes concernées, par l'insertion de :

- cases à cocher pour le consentement spécifique relatif à la géolocalisation, la prospection, aux données de connexion et aux données de navigation ;
- une segmentation du consentement par catégorie des données collectées ;
- un formulaire numérique pour le recueil de consentement exprès avant le partage des données avec les tiers.

Conformément aux dispositions de l'article 1 de la décision n°2014-0021 du 03 septembre 2014 portant conditions et critères applicables à la limitation du traitement des données à caractère personnel, la personne concernée doit avoir été suffisamment informée par **SANIA CIE** 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.

Article 4 :

SANIA CIE est autorisée à communiquer les données traitées :

- aux services internes de **SANIA CIE** ;
- à BIG FIVE ;
- au Procureur de la République ;
- aux Officiers de Police Judiciaire de Côte d'Ivoire munis d'une réquisition ;
- aux agents assermentés de l'Autorité de protection (ARTCI) habilités, dans le cadre de l'exécution de leurs missions ;
- aux agents de l'administration publique dans le cadre de leurs missions.

Il est interdit à **SANIA CIE** de transférer, **sans autorisation préalable de l'Autorité de protection**, les données collectées vers des pays tiers.

Article 5 :

SANIA CIE conserve l'ensemble des données traitées :

- pendant cinq (05) ans en base active et dix (10) ans en archivage ;
- la demanderesse doit également mettre en œuvre une politique d'archivage électronique des données avec une durée de conservation spécifique pour chaque catégorie de données.

En cas de contentieux, il est prescrit à **SANIA CIE** de conserver les données traitées jusqu'au règlement définitif du contentieux.

Article 6 :

SANIA CIE informe les personnes concernées de leurs droits d'accès direct, d'opposition, d'effacement, de portabilité, de retrait du consentement donné, de rectification et de suppression. Elle le fait par le biais de mentions dans les conditions générales d'utilisation de son application « DINOR APP » ;

SANIA CIE doit également définir une politique de gestion des droits des personnes concernées.

Article 7 :

SANIA CIE désigne un correspondant à la protection auprès de l'Autorité de protection.

Elle notifie la désignation dudit correspondant à l'Autorité de protection par un courrier officiel.

Le correspondant à la protection tient une liste des traitements effectués, immédiatement accessible à toute personne concernée en faisant la demande.

Article 8 :

SANIA CIE veille au respect des dispositions de la Loi relative à la protection des données à caractère personnel par ses sous-traitants.

SANIA CIE est tenue de mettre en place un dispositif de :

- formation pour son correspondant à la protection et ses agents habilités ;
- sensibilisation sur la protection des données à caractère personnel pour son personnel ;
- gestion des habilitations des utilisateurs de l'application pour limiter les accès aux seules données qui sont strictement nécessaires aux utilisateurs en fonction de leurs besoins.

Article 9 :

Conformément à l'article 42 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, **SANIA CIE** est tenue d'établir pour le compte de l'Autorité de protection un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

SANIA CIE communique ce rapport à l'Autorité de protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 10 :

L'Autorité de protection procède à des contrôles auprès de **SANIA CIE** afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 11 :

SANIA CIE est tenue de procéder au paiement des frais de dossiers auprès du greffe de l'ARTCI, conformément à la décision n°2016-021 de l'Autorité de protection de la République de Côte d'Ivoire fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel.

Article 12 :

La présente décision entre en vigueur à compter de la date de sa notification à **SANIA CIE**.

Article 13 :

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

Fait à Abidjan, le 05 Mai 2022
En deux (2) exemplaires originaux

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL ident

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

A.R.T.C.I
COURRIER ARRIVÉE DCNS
LE 20 MAI 2022
N°

DECISION N°2022-0737

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

EN DATE DU 05 MAI 2022

PORTANT AUTORISATION DE TRANSFERT DE DONNEES A CARACTERE PERSONNEL VERS LES USA PAR SANIA CIE

L'AUTORITE DE PROTECTION,

Vu l'Acte uniforme OHADA du 15 décembre 2010 portant sur le droit commercial général ;

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°2017-540 du 03 août 2017 fixant les règles relatives à la régulation, au contrôle et au suivi des activités des filières Hévéa et Palmier à huile ;

Vu l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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° 2016-483 du 07 juillet 2016 portant nomination de membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

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 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°2014-0021 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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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°2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

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 de l'activité :

- du correspondant à la protection des données, personnes morales ;
- de formation en matière de protection des données à caractère personnel ;
- d'audit en matière de protection des données à caractère personnel ;

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 données à caractère personnel ;

Vu la Résolution n°2021-161 du 30 juin 2021 portant désignation du Directeur Général par Intérim de l'Autorité de Régulation des Télécoms/TIC de Côte d'Ivoire (ARTCI) ;

Par les motifs suivants :

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par la société **SANIA Cie**, Société Anonyme, au capital de quarante-quatre milliards cent dix millions (44 110 000 000) de francs CFA, sise à Abidjan, Zone industrielle de Vridi – Rue du Textile, 01 BP 2949 Abidjan 01, immatriculée au Registre du Commerce et du Crédit mobilier sous le numéro CI-ABJ-2008-M2-13989 ;

Considérant que **SANIA CIE** est une entreprise qui a pour objet social l'achat, l'importation, la transformation et la commercialisation de tous produits alimentaires, chimiques, cosmétiques naturels ou artificiels et d'alcools ;

Considérant que l'article 47 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 est chargée d'autoriser le transfert transfrontalier de données à caractère personnel, dans les conditions fixées par 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.

L'Autorité de protection est compétente, pour examiner la demande d'autorisation de transfert des données personnelles initiée par **SANIA CIE**.

- **Sur la recevabilité de la demande d'autorisation de transfert**

Considérant que l'article 7 du décret 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, dispose que la demande d'autorisation pour le transfert de

données à caractère personnel vers les pays tiers doit être présentée par une personne morale de droit ivoirien.

Que cette demande contient, outre les informations requises à l'article 9 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, un mémoire comportant les extraits de casiers judiciaires des principaux dirigeants sociaux de la personne morale qui fait la demande, datant de moins de trois mois ;

Considérant que **SANIA CIE** est une société anonyme avec Conseil d'Administration, immatriculée au Registre du Commerce et du Crédit Mobilier ;

Considérant que SANIA CIE n'a pas fourni dans le cadre de sa demande de transfert l'extrait du casier judiciaire de son Directeur Général ;

Il convient de noter que la demande d'autorisation de transfert de données personnelles introduite par la société **SANIA CIE** ne contient pas tous les éléments exigés par l'article 7 précité ;

Toutefois, l'Autorité de protection considère que la demande d'autorisation de transfert initiée par la société **SANIA CIE** est recevable sous réserve de la communication par celle-ci de l'extrait de casier judiciaire de ses principaux dirigeants sociaux ;

- **Sur la nature des données objet du transfert**

L'autorité de protection constate que le transfert envisagé par la demanderesse concerne les données suivantes dont le traitement a été autorisé par la décision n°2022-0736 en date du 05 Mai 2022 :

- **les données d'identification :** nom, prénom, date et lieu de naissance ;
- **les données de localisation :** GSM ; lieu de résidence ;
- **les données de connexions :** e-mail, identifiant, mot de passe, adresse IP, pages consultées ;
- **les données d'identification nationale :** numéro de téléphone.

Considérant que les données suscitées sont traitées par la demanderesse par le biais de son application « DINOR APP » afin de :

- offrir une expérience personnalisée aux utilisateurs ;
- avoir des lieux favoris pour l'achat de produits de la marque DINOR.
- avoir des recettes favorites.
- et bénéficier des promotions.

L'Autorité de protection considère que les données que la demanderesse envisage de transférer sont adéquates, pertinentes et non excessives, au regard du transfert.

- **Sur le motif et les finalités du transfert**

Considérant qu'en l'espèce, la demande de transfert soumise par **SANIA CIE** à l'Autorité de protection a pour finalité l'hébergement de l'application « DINOR APP » sur le serveur de **DIGITAL OCEAN** aux Etats Unis.

Qu'en effet, **SANIA CIE** et **DIGITAL OCEAN** ont respectivement la qualité de responsable du traitement et de sous- traitant ;

L'Autorité de protection en déduit que la finalité de la demanderesse est explicite et légitime.

- **Sur le nom du pays d'hébergement et le cadre juridique relatif aux données à caractère personnel appliqué dans le pays destinataire**

Considérant qu'aux termes de l'article 26 de la loi n°2013-450 du 19 Juin 2013 relatif à la protection des données à caractère personnel, le responsable d'un traitement ne peut être autorisé à transférer les données à caractère personnel vers les pays destinataires que si cet Etat assure un niveau de protection supérieur ou équivalent de la vie privée, des libertés et droit fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet.

Qu'il en résulte que le transfert de données à caractère personnel vers un pays tiers ne peut être autorisé que si ce pays destinataire dispose d'une autorité de protection et un niveau de protection adéquat.

Considérant qu'en l'espèce, les USA sont le pays destinataire des données transférées ;

Considérant que les USA sont un pays qui ne garantit pas un niveau de protection adéquat ;

Considérant que peuvent être autorisés sous réserve de certaines garanties, un transfert, ou un ensemble de transferts, de données à caractère personnel vers des pays tiers n'assurant pas un niveau de protection adéquat. Ces garanties peuvent notamment résulter de clauses contractuelles appropriées ou de règles contraignantes d'entreprise.

L'Autorité de protection considère que **SANIA CIE** n'a pas apporté des garanties suffisantes à la protection des données transférées à **DIGITAL OCEAN,** aux USA ;

En conséquence, **SANIA CIE** ne peut être autorisée à transférer les données telles que mentionnées dans le dossier de demande de transfert, vers les USA, que si elle fournit des clauses contractuelles appropriées relatives au transfert de données qui la lient à son sous-traitant DIGITAL OCEAN ou des règles contraignantes d'entreprise.

- **Sur la garantie d'accès sans obstacle aux données transférées par la personne concernée pour l'exercice de ses droits et par les pouvoirs publics ivoiriens pour l'exercice de leurs prérogatives respectives**

Considérant que la demanderesse indique que les personnes concernées pourront faire valoir leur droit d'accès direct, d'opposition, de rectification, de suppression auprès de **SANIA CIE ;**

L'Autorité de protection en déduit que le transfert envisagé présente des garanties suffisantes d'accès sans obstacles aux données transférées par la personne concernée pour l'exercice de ses droits et par les pouvoirs publics ivoiriens pour l'exercice de leurs prérogatives respectives ;

Toutefois, l'Autorité de protection prescrit que **SANIA CIE** désigne un correspondant à la protection des données à caractère personnel.

- **Sur les mesures de sécurité**

Considérant qu'en application de l'article 41 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le responsable du traitement et le sous-traitant prennent toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient détruites, déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance ;

Considérant que les mesures de sécurité doivent couvrir l'aspect physique (les données stockées sur des supports papiers) et logique (supports informatiques) ;

Considérant qu'au vu des éléments techniques fournis par la demanderesse, et après étude de l'analyse d'impact, l'Autorité de protection conclu que le système d'information de la société **SANIA CIE**, présente un niveau de sécurité suffisant pour le traitement de données personnelles ;

Cependant, l'Autorité de protection prescrit à la demanderesse de maintenir à jour le système d'exploitation, et aussi les applications utilisées afin d'être moins vulnérable aux différentes attaques.

L'Autorité de Protection considère que les mesures de sécurité logique et physique nécessaires sont garanties.

Après en avoir délibéré,

DECIDE :

Article 1 :

SANIA CIE est autorisée à transférer les données à caractère personnel vers les Etats Unis, conformément à la décision n°2022-0736 en date du 05 Mai 2022 :

- **les données d'identification :** nom, prénom, date et lieu de naissance ;
- **les données de localisation :** GSM ; lieu de résidence ;
- **les données de connexions :** e-mail, identifiant, mot de passe, adresse IP, pages consultées ;
- **les données d'identification nationale :** numéro de téléphone.

Les données visées au présent article concernent les utilisateurs de l'application « DINOR APP ».

Les données non mentionnées ne devront aucunement faire l'objet d'un quelconque traitement de la part de **SANIA CIE**.

Il est interdit, au destinataire de transférer à nouveau, les données dans un autre pays, sans l'accord préalable du responsable du traitement d'origine et l'Autorité de protection.

Les données transférées ne devront pas être utilisées pour des finalités incompatibles avec les finalités initiales.

Article 2 :

SANIA CIE est tenue d'apporter toutes les garanties nécessaires pour préserver la sécurité des données faisant l'objet de transfert.

Tout autre transfert est soumis à l'autorisation préalable de l'Autorité de protection.

Avant tout transfert des données hors de la Côte d'Ivoire, **SANIA CIE** est tenue de les stocker sur le territoire de la République de Côte d'Ivoire.

Article 3 :

SANIA CIE doit communiquer des clauses contractuelles relatives au transfert de données qui la lient à son sous-traitant **DIGITAL OCEAN** ou des règles contraignantes d'entreprise à l'Autorité de protection dans les trente (30) jours suivant la notification de la présente décision.

SANIA CIE doit également fournir l'extrait du casier judiciaire de son Directeur Général, datant de moins de trois (03) mois, quinze (15) jours après la date de notification de la présente décision.

Article 4 :

SANIA CIE est tenue de recueillir le consentement préalable des personnes concernées, avant tout transfert des données.

Elle devra apporter la preuve du recueil du consentement à l'Autorité de protection.

Conformément aux dispositions de l'article 1 de la décision n°2014-0021 du 3 septembre 2014 portant conditions et critères applicables à la limitation du traitement des données à caractère personnel, les personnes concernées doivent avoir été suffisamment informées par **SANIA CIE**, avant de donner librement leur consentement, afin d'être en mesure de comprendre d'une part, la portée et les conséquences de leur consentement, et d'autre part, les avantages et les inconvénients du traitement.

Article 5 :

SANIA CIE est tenue d'informer les personnes concernées des finalités du traitement et de leur droit d'accès, de rectification et de suppression par le biais des mentions légales sur son application.

La demanderesse doit également définir une procédure de gestion des droits des personnes concernées.

Article 6 :

En application de l'article 8 du Décret 2015-79 du 4 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 personnelles,

SANIA CIE établit un rapport annuel sur le transfert de donnée à caractère personnel vers les pays tiers au plus tard le 31 janvier de l'année suivante.

Article 7 :

SANIA CIE est tenue de désigner un correspondant à la protection des données chargé de tenir la liste des traitements effectués, immédiatement accessible à toutes personnes concernées faisant la demande ;

Elle notifie la désignation dudit Correspondant à l'Autorité de protection par un courrier officiel.

Article 8 :

L'Autorité de protection procède à des contrôles auprès de **SANIA CIE**, afin de vérifier le respect de la présente décision dont, la violation donnera lieu à des sanctions selon la règlementation en vigueur.

Article 9 :

Les données objet du transfert doivent être chiffrées lors de leur transmission.

Article 10 :

La présente décision entre en vigueur à compter de sa notification à **SANIA CIE**.

Article 11 :

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

Fait à Abidjan, le 05 Mai 2022
En deux (2) exemplaires originaux

Le Président

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

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0738

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE CÔTE D'IVOIRE

EN DATE DU 05 MAI

PORTANT APPROBATION DE LA LISTE DES CONTROLES EN MATIERE DE PROTECTION DES

DONNEES A CARACTERE PERSONNEL

POUR L'ANNEE 2022

L'AUTORITE DE PROTECTION,

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 l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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° 2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

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 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 conduite relatives au traitement et à la protection des données à caractère personnel (DCP) ;

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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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 de l'activité :

- de correspondant à la protection des données, personnes morales ;
- de formation en matière de protection des données à caractère personnel ;
- d'audit en matière de protection des données à caractère personnel

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 Résolution n°2021-161 du Conseil de Régulation de l'Autorité de Régulation Télécommunications /TIC de Côte d'Ivoire en date du 30 juin 2021 portant nomination du Directeur Général par Intérim de l'ARTCI;

Par les motifs suivants :

Considérant que l'article 47 de la Loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel énonce que 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 ;

- 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 qu'aux termes de l'article 3 de la décision N° 2021- 0676 en date du 04 Août 2021 portant Procédure de Contrôle en matière de Protection Des Données à Caractère Personnel, l'Autorité de protection établit la liste des entreprises devant faire l'objet de contrôle en vue de s'assurer du respect des prescriptions ou leurs obligations 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.

Après en avoir délibéré,

DECIDE :

Article 1 :

Le Conseil de Régulation approuve la liste des contrôles joint en annexe.

Article 2 :

La publication de cette décision vaut information des Responsables de traitements concernées conformément aux dispositions de l'article 9 de la décision n° 2021- 0676 en date du 04 Août 2021 portant Procédure de Contrôle en matière de Protection Des Données à Caractère Personnel.

Article 3 :

La présente décision n'exclut pas les autres types de contrôles de l'Autorité de protection prévus par les dispositions de la Décision n°2021- 0676 en date du 04 Août 2021 portant Procédure de Contrôle en matière de Protection des Données à Caractère Personnel et la réglementation en vigueur.

Article 4 :

Le Directeur Général par Intérim de l'Autorité de protection est chargé de l'exécution de la présente décision qui sera publiée au journal officiel de la République de Côte d'Ivoire, sur le site internet de l'ARTCI et celui de l'Autorité de protection.

Article 5 :

La présente décision rentre en vigueur à compter de la publication sur les sites de l'ARTCI.

Fait à Abidjan, le 05 Mai 2022
En deux (2) exemplaires originaux

Le Président

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

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

LISTE DES ENTREPRISES A CONTRÔLER EN MATIERE DE PROTECTION DES DONNEES PERSONNELLES 2022

Secteur d'Activités	Raison sociale
AGRO INDUSTRIE	NESTLE
BANQUES ET ASSURANCES	BICICI
	SANLAM COTE D'IVOIRE
SANTE	CLINIQUE FARAH
HOTELERIE	HOTEL TIAMA
CABINETS DE RECRUTEMENT ET DE FORMATION	CIFIP
SECURITE ELECTRONIQUE / SECURITE INFORMATIQUE	CRYPTONEO
ETABLISSMENT CONCESSIONNAIRE DE SERVICE PUBLIC	QUIPUX

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0742
DE L'AUTORITE DE PROTECTION
DE LA REPUBLIQUE DE COTE D'IVOIRE
EN DATE DU 5 JUILLET 2022
PORTANT AUTORISATION DE TRAITEMENT
DE DONNEES A CARACTERE PERSONNEL
PAR VERSUS BANK
(VIDEOSURVEILLANCE)

Conseil de Régulation : 31 Av Nogués, 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 l'ordonnance n°2009-385 du 1er décembre 2009 portant règlementation bancaire ;

Vu l'ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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 ;

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°2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

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 de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

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 ;

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 caractère personnel (DCP);

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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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°2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

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°2021-0629 de l'Autorité de protection de la République de Côte d'Ivoire en date du 23 Février 2021 portant autorisation de traitement de données à caractère personnel par VERSUS BANK ;

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 ;

Par les motifs suivants :

- **Sur la compétence de l'Autorité de Protection**

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par **VERSUS BANK** sise à Abidjan, Plateau, Boulevard Botreau Roussel, Avenue Joseph Anoma, Immeuble Crrae-Uemoa01 BP 2056 Abidjan 01, téléphone 27 20 25 60 99, immatriculée au numéro 096/MEMI/DGAT/DAG/SDVA du 16 Février 2012.

Considérant que **VERSUS BANK est une entreprise exerçant dans le domaine bancaire.**

Considérant que l'article 47 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 est chargée de recevoir les déclarations et d'octroyer les autorisations, pour la mise en œuvre de traitement des données à caractère personnel ;

Dès lors l'Autorité de Protection est compétente, pour examiner la demande d'autorisation de traitement initiée par **VERSUS BANK ;**

- **Sur la recevabilité de la demande d'autorisation**

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, le traitement des données à caractère personnel comportant des données biométriques sont soumis à autorisation préalable de l'Autorité de Protection, avant toute mise en œuvre ;

Considérant qu'en l'espèce, **VERSUS BANK** envisage de collecter, et de stocker les données à caractère personnel, tels que, les numéros de plaques d'immatriculations, et les données biométriques, notamment les images et, les mouvements de toutes personnes à l'intérieur et aux alentours de son siège social ;

Qu'en application des dispositions précitées, lesdits traitements doivent être autorisés par l'Autorité de protection, pour être mis en œuvre ;

Considérant que selon l'article 7 précité, la demande d'autorisation est présentée par le responsable du traitement ou son représentant légal ;

Que l'article 1 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, définit le responsable du traitement comme étant la personne physique ou morale, publique ou privée, 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 ;

Considérant qu'en l'espèce, **VERSUS BANK** a décidé de mettre en place un système de vidéosurveillance en vue d'assurer la sécurité des biens et des personnes au sein de sa structure ;

Que pour ce faire, elle a décidé de collecter et de traiter les données à caractère personnel des visiteurs et des membres de son personnel ;
L'Autorité de Protection en conclut que **VERSUS BANK** a qualité de Responsable du traitement ;

Considérant qu'aux termes de l'article 9 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la demande d'autorisation doit contenir les mentions minimums relatives à la dénomination sociale de la personne morale, au Responsable du traitement, à son siège social, à l'identité de son représentant légal, à son numéro d'immatriculation au registre du commerce et du crédit mobilier, à son numéro de déclaration fiscale, aux finalités du traitement, à la durée de conservation des données traitées, aux dispositions prises pour assurer la sécurité des traitements, à la protection, à la confidentialité des données traitées et à la fonction de la personne ou le service auprès duquel s'exercent les droits des personnes concernées ;

Qu'en l'espèce, la demande d'autorisation de **VERSUS BANK** contient les mentions minimums prescrites par l'article 9 précité ;

Considérant qu'au regard de tout ce qui précède, ladite demande satisfait les conditions de formes exigées par les articles 7 et 9 de la loi n°2013-450 relative à la protection des données à caractère personnel ;

L'Autorité de Protection déclare que la demande de **VERSUS BANK** est recevable en la forme.

- **Sur la légitimité et la licéité du traitement**

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 que **VERSUS BANK** envisage de collecter et de stocker les données à caractère personnel des personnes présentes dans ses locaux et aux alentours, par le biais d'un système de vidéosurveillance ;

Considérant toutefois que **VERSUS BANK** n'apporte pas la preuve que les personnes concernées ont exprimé leur consentement préalable au traitement de leurs données ;

Considérant par ailleurs, que l'existence d'un système de vidéosurveillance doit être portée à la connaissance de toute personne filmée ou susceptible de l'être, de façon claire et permanente, par un pictogramme placé à hauteur de vue, dans les zones filmées par les caméras ;

Considérant en outre, que l'utilisation d'un système de vidéosurveillance au sein d'une entreprise est subordonnée à l'accord du personnel, qui doit exprimer clairement son consentement à son installation ;

L'Autorité de Protection prescrit à **VERSUS BANK** de mettre en place un processus de recueil individuel du consentement de son personnel ;

L'Autorité de Protection prescrit également à **VERSUS BANK**, d'informer les personnes concernées de l'existence du dispositif de vidéosurveillance, au moyen de pictogrammes placés de façon visible dans les zones sous surveillance.

- **Sur la finalité**

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 qu'en l'espèce, **VERSUS BANK** envisage la mise en place d'un système de vidéosurveillance, aux fins :

- d'assurer la sécurité des biens et des personnes ;

- d'anticiper et de réagir en cas d'incendies et accidents ;

- d'identifier les auteurs de vols, de dégradations ou d'agressions ;

L'Autorité de Protection considère que lesdites finalités sont déterminées, explicites et légitimes.

- **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 qu'en l'espèce, **VERSUS BANK** a indiqué que les données traitées sont conservées pendant trente (30) jours avec recyclage automatique.

L'Autorité de protection considère que cette durée de conservation n'est pas excessive.

Toutefois, l'Autorité de Protection prescrit que les données traitées soient conservées pendant une durée de trente (30) jours, et en cas d'incidents, pendant une période d'un (01) an à compter de la dernière sauvegarde mensuelle des données traitées.

- **Sur la proportionnalité des données traitées**

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 qu'en l'espèce, **VERSUS BANK** indique que le traitement concerne les données suivantes :

- **Données d'identification :** les images des visiteurs et des membres de son personnel ;
  les numéros de plaque d'immatriculation, modèle et couleur des véhicules ;
- **Données de localisation :** les différents mouvements détectés par les caméras dans les lieux placés sous surveillance.

En conséquence, l'Autorité de Protection conclut que les données collectées sont pertinentes, adéquates et non excessives au regard des finalités.

- **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, selon lesquelles la demande d'autorisation adressée à l'Autorité de protection doit contenir les destinataires habilités à recevoir communication des données traitées ;

Considérant que la visualisation des images doit être restreinte aux seuls destinataires habilités, en charge de la sécurité des locaux ou installations sous surveillance ;

Considérant en l'espèce que **VERSUS BANK** indique que les destinataires des données traitées sont les personnes en charge de la sécurité de la vidéosurveillance, à savoir :

- Le chef de service sécurité des systèmes d'information ;
- Le contrôleur informatique sénior, chargé de la sécurité des systèmes électroniques et données à caractère personnel ;
- Le contrôleur informatique.

Considérant que les destinataires susmentionnés sont les agents des services internes de **VERSUS BANK** ;

Qu'en l'espèce, **VERSUS BANK** n'a pas mentionné dans son formulaire de demande d'autorisation qu'elle effectuera un transfert de données ;

L'Autorité de Protection prescrit que lesdites données ne fassent l'objet d'aucun transfert, ni d'aucune communication aux services non habilités de **VERSUS BANK** :

L'Autorité de Protection autorise également que les données traitées soient communiquées, le cas échéant :

- aux agents assermentés et habilités de l'Autorité de Protection dans le cadre de leurs missions ;

- aux Autorités publiques ivoiriennes compétentes, par le biais de leurs agents habilités, agissant dans le cadre de leurs missions ;

- au Procureur de la République de Côte d'Ivoire ;

- aux Officiers de Police Judiciaire de Côte d'Ivoire, munis d'une réquisition.

- **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 **VERSUS BANK** de faire preuve de transparence vis à vis des personnes concernées qui devront notamment être informées :

- de l'identité du responsable du traitement et le cas échéant, celle de son représentant dûment mandaté ;
- des finalités 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 leurs droits d'accès et de rectifications,
- de la durée de conservation des données,
- de l'éventualité de tout transfert de données à destination de pays tiers ;

Considérant que les personnes concernées (salariés, clients, visiteurs etc.) doivent être clairement informées de l'existence d'un système de vidéosurveillance et des destinataires des informations traitées ;

Considérant que, **VERSUS BANK** indique que les personnes concernées sont informées de l'existence d'un système de vidéosurveillance par voie d'affichage ;

Considérant que le formulaire de demande d'autorisation indique qu'il existe des pictogrammes aux différents endroits où sont installées les caméras ;

Que les mentions devant figurer sur les pictogrammes n'ont pas été mentionnées dans le formulaire de demande d'autorisation.

L'Autorité de Protection prescrit à **VERSUS BANK de mentionner de façon claire et visible**.

les informations suivantes sur les différents pictogrammes:

- le nom du responsable de traitement ;
- le fait que l'établissement est placé sous vidéosurveillance ;
- la finalité de ce dispositif (la sécurité des biens et des personnes) ;
- les coordonnées du contact pour l'exercice, par les personnes concernées, des droits d'accès, de rectification et d'opposition ;
- le numéro de l'autorisation octroyée par l'Autorité de protection.

- **Sur les droits d'accès direct, d'opposition, de rectification 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, d'effacement ;

Considérant que **VERSUS BANK** indique que les droits d'accès, d'opposition, de rectification, de suppression et retrait du consentement, pourront être exercés auprès de son correspondant à la protection ;

L'Autorité de Protection considère que les dispositions relatives, à la désignation d'un correspondant à la protection pour l'exercice des droits d'accès direct, d'opposition, de rectification, des personnes concernées sont respectées.

- **Sur les mesures de sécurité**

Considérant qu'en application de l'article 41 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le responsable du traitement et le sous-traitant prennent toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient détruites, déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance ;

Considérant que les mesures de sécurité doivent couvrir l'aspect physique et logique ;

Considérant qu'au vu des éléments techniques fournis dans le formulaire de demande d'autorisation, le niveau de sécurité du système d'information de VERSUS BANK lui permet de mettre en œuvre la vidéosurveillance dans ses locaux et leurs alentours pour les finalités déclarées ;

Qu'il ressort des documents communiqués par VERSUS BANK, qu'elle a pris toutes les mesures nécessaires en vue d'assurer la sécurité des données, conformément aux dispositions de l'article 41 de la Loi susmentionnée ;

L'Autorité de Protection considère que les mesures de sécurité logique et physique nécessaires sont garanties.

Après en avoir délibéré,

DECIDE :

Article 1 :

VERSUS BANK est autorisée à effectuer la collecte, l'enregistrement et le stockage des données à caractère personnel ci-après :

- les données d'identification : numéro de plaque d'immatriculation, modèle et couleur des véhicules;
- les données de localisation : les différents mouvements détectés par les caméras dans les lieux placés sous surveillance ;
- les données biométriques : images des personnes.

Les données visées au présent article concernent les employés et visiteurs de **VERSUS BANK**

Article 2 :

Les données traitées par **VERSUS BANK** ne peuvent être utilisées à des fins autres que celles précisées dans la demande d'autorisation.

Toute réutilisation de ces données à d'autres fins doit faire l'objet d'une autorisation préalable de l'Autorité de Protection.

Article 3 :

VERSUS BANK l'obligation de procéder au recueil du consentement préalable, formel des personnes concernées. Elle devra en fournir les preuves à l'Autorité de Protection.

Les pictogrammes installés par VERSUS BANK
doivent indiquer, d'une façon claire et visible, les informations suivantes :

- le nom du responsable de traitement,
- le fait que l'établissement est placé sous vidéosurveillance ;
- la finalité de ce dispositif (la sécurité des personnes et des biens) ;
- les coordonnées du contact pour l'exercice, par les personnes concernées, des droits d'accès de rectification et d'opposition
- le numéro de l'autorisation octroyée par l'Autorité de Protection.

Article 8 :

Le correspondant à la protection désigné par **VERSUS BANK** tient une liste des traitements effectués, immédiatement accessible à toute personne concernée en faisant la demande.

Article 9 :

VERSUS BANK veille au respect des dispositions de la Loi relative à la protection des données à caractère personnel.

VERSUS BANK est tenue de mettre en place:

- un dispositif de formation de son correspondant à la protection et de ses agents habilités.

- un dispositif de sensibilisation de son personnel.

La formation devra être sanctionnée par un certificat ou une attestation de formation.

Article 10 :

VERSUS BANK veille au respect des dispositions de la Loi relative à la protection des données à caractère personnel par ses sous-traitants.

Conformément à l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, **VERSUS BANK** doit s'assurer que, ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle relatives aux traitements de données qu'ils opèrent.

Il incombe à **VERSUS BANK** ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

VERSUS BANK est tenu de :

- s'assurer de la viabilité et de la sécurité du réseau de transmission en vue de garantir la sécurité de la vie privée des personnes prises en images ;
- veiller à la sécurité du disque dur chargé de stocker les images et du système d'exploitation ;
- veiller à la mise à jour du système d'exploitation et les applications qui y sont installées afin de conserver et de garantir la sécurité.

Article 11 :

Conformément à l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, **VERSUS BANK** est tenue d'établir pour le compte de l'Autorité de Protection un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

VERSUS BANK communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 12 :

L'Autorité de Protection procède à des contrôles auprès de VERSUS BANK, afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 13 :

La présente décision entre en vigueur à compter de la date de sa notification à VERSUS BANK

Article 14 :

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

Fait à Abidjan, le 05 Juillet 2022
En deux (2) exemplaires originaux

Le Président

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

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

ARTCI

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0743

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 05 JUILLET 2022

PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL PAR LA STANBIC BANK

L'AUTORITE DE PROTECTION,

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°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°2018-573 du 13 juin 2018 portant régime juridique du gel des avoirs illicites ;

Vu l'ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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 ;

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°2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le décret n°2018-439 relatif à la mise en œuvre des sanctions ciblées liées au financement du terrorisme et à la prolifération des armes de destruction massive ;

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 de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

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 ;

Vu l'arrêté n° 511/MPTIC/CAB du 11 novembre 2014 portant définition ou 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°2014-0021 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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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°2018-0431 du 20 septembre 2018 portant autorisation de traitements de données à caractère personnel par la STANBIC BANK ;

Vu la décision n°2019-0494 du Conseil de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

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 ;

Par les motifs suivants :

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par la STANBIC BANK, Société Anonyme avec Conseil d'Administration au capital de 22.900.000.000 CFA sise à Abidjan-Marcory, 26 BP 701 Abidjan 26, immatriculée au Registre du Commerce et du Crédit Mobilier sous le numéro CI-ABJ-2015-B-26822.

Considérant que la STANBIC BANK est une Banque, filiale de Standard Bank Group d'Afrique du Sud ;

Considérant que l'article 47 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 est chargée de recevoir les déclarations et d'octroyer les autorisations, pour la mise en œuvre de traitements des données à caractère personnel ;

L'Autorité de Protection est compétente, pour examiner la demande d'autorisation de traitements initiée par la STANBIC BANK ;

- **Sur la recevabilité de la demande d'autorisation**

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 des données à caractère personnel comportant des données biométrique est soumis à autorisation préalable de l'Autorité de protection, avant toute mise en œuvre ;

Considérant qu'en l'espèce, la STANBIC BANK voudrait procéder à l'enregistrement des instructions ou engagements donnés au téléphone par ses clients ;

Considérant que la voix est une donnée biométrique, et qu'en application des dispositions précitées, ledit traitement doit être autorisé par l'Autorité de protection, pour être mis en œuvre ;

Considérant qu'aux termes de l'article 7 précité, la demande d'autorisation est présentée par le responsable du traitement ou son représentant légal ;

Que l'article 1 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, définit le responsable du traitement comme étant la personne physique ou morale, publique ou privée, 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 ;

Considérant que la STANBIC BANK voudrait enregistrer les communications faites au téléphone avec leurs clients ;

Que ladite opération nécessite la collecte des données à caractère personnel des différents clients ;

L'Autorité de protection en conclut que la STANBIC BANK a la qualité de responsable du traitement.

Considérant qu'aux termes de l'article 9 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la demande d'autorisation doit contenir les mentions minimums relatives à la dénomination sociale de la personne morale, au Responsable du traitement, à son siège social, à l'identité de son représentant légal, à son numéro d'immatriculation au registre du commerce et du crédit mobilier, à son numéro de déclaration fiscale, aux finalités du traitement, à la durée de conservation des données traitées, aux dispositions prises pour assurer la sécurité des traitements, à la protection et à la confidentialité des données traitées ;

Considérant que lesdites mentions figurent dans la demande d'autorisation formulée par la STANBIC BANK ;

Que ladite demande satisfait les conditions de forme exigées par les articles 7 et 9 de la loi n°2013-450 relative à la protection des données à caractère personnel ;

En conséquence, l'Autorité de protection déclare la demande de la STANBIC BANK recevable en la forme ;

- **Sur la légitimité et la licéité du traitement**

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 que STANBIC BANK procède à la collecte des données directement auprès des personnes concernées;

Considérant que STANBIC BANK indique qu'elle recueille le consentement préalable des clients par le biais de formulaire et par message vocal d'information avant le début de la conversation téléphonique ;

L'Autorité de protection considère le traitement projeté par STANBIC BANK comme légitime et licite sous réserve de la transmission par cette dernière de la preuve du recueil du consentement des personnes concernés ;

Aussi, l'Autorité de protection prescrit-elle à STANBIC BANK, de lui transmettre copie de la preuve du recueil du consentement.

- **Sur la finalité**

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 le traitement envisagé par la demanderesse a pour finalité l'enregistrement des instructions ou engagements donnés au téléphone par les clients;

Considérant que pour se faire, elle a décidé de collecter, d'organiser et de conserver les données à caractère personnel ;

L'Autorité de protection considère que cette finalité est déterminée, explicite et légitime.

- **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 qu'en l'espèce, la demanderesse a indiqué qu'elle souhaiterait conserver les dites données pendant dix (10) ans ;

L'Autorité de Protection, au regard de la nature des données traitées et de la finalité du traitement, considère que ce délai est excessif.

L'Autorité de Protection, prescrit de conserver les données pendant six (6) mois à compter du dernier contact et pendant un (1) an en ce qui concerne les documents d'analyse.

- **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 qu'en l'espèce, la STANBIC BANK indique que le traitement concerne les données suivantes :

- **les données d'état civil :** nom et prénom ;
- **les données d'informations d'ordre économique et financier :** revenus, situation financière, instructions de paiement ;
- **les données de connexion :** identifiants des terminaux.

Il y'a lieu de constater que les données traitées, telles que décrites dans la demande d'autorisation sont adéquates, pertinentes et non excessives, au regard de la finalité du traitement.

Toutefois, l'Autorité de protection considère que la voix est également une donnée collectée dans le cadre de l'enregistrement donc devrait être également mentionnée les données collectées.

- **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, selon lesquelles la demande d'autorisation adressée à l'Autorité de protection doit contenir les destinataires habilités à recevoir communication des données traitées ;

Considérant qu'en l'espèce, la demanderesse a précisé qu'elle communiquera ses données à la STANBIC BANK.

L'Autorité de protection autorise la communication des données traitées uniquement :

- aux agents habilités de STANBIC BANK ;
- au Procureur de la République ;
- aux Officiers de Police Judiciaire ;
- aux Autorités publiques ivoiriennes agissant dans le cadre de leurs missions ;
- aux Agents assermentés de l'ARTCI.

Considérant qu'en dehors des destinataires précités, STANBIC BANK n'entend ni communiquer, ni transférer à aucune autre structure, les données traitées;

L'Autorité de protection prescrit que les données traitées soient uniquement communiquées aux destinataires précités ;

- **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 demandeur de faire preuve de transparence vis à vis des personnes concernées qui devront notamment être informées :

- 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.

Qu'à cette fin, la demanderesse indique que des mentions légales sur formulaires ainsi qu'un message vocal permettront aux personnes concernées d'être informées de leurs droits, préalablement à toute collecte ;

L'autorité de protection considère que le principe de la transparence est respecté.

- **Sur les droits d'accès direct, d'opposition, de rectification 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 la demanderesse indique que les droits d'accès direct, d'opposition, de rectification, d'effacement, de portabilité, de retrait du consentement donné, et de suppression, pourront être exercés auprès d'elle-même ;

Considérant que la demanderesse à désigner un correspondant à la protection des données à caractère personnel ;

L'Autorité de protection prescrit à la STANBIC BANK, que les différents droits reconnus à la personne concernée soient exercés auprès de son correspondant.

- **Sur les mesures de sécurité**

Considérant qu'en application de l'article 41 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le responsable du traitement et le sous-traitant prennent toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient détruites, déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance ;

Considérant que les mesures de sécurité doivent couvrir l'aspect physique (les données stockées sur des supports papiers) et logique (supports informatiques) ;

Considérant qu'au vu des éléments techniques fournis dans le formulaire, le niveau de sécurité de la STANBIC BANK lui permet de mettre en œuvre le traitement de données à caractère personnel pour la finalité déclarée ;

Qu'il en résulte que le demandeur a pris toutes les mesures nécessaires en vue d'assurer la sécurité des données ;

L'Autorité de protection considère que les mesures de sécurité logique et physique nécessaires sont garanties.

Toutefois, l'Autorité de protection prescrit à la STANBIC BANK de :

- Maintenir à jour les systèmes d'exploitation et les applications utilisées afin d'être moins vulnérable aux différentes attaques ;
- Définir une fréquence de renouvellement des mots de passe afin de réduire le risque et l'impact des piratages de compte.

Après en avoir délibéré,

DECIDE :

Article 1 :

STANBIC BANK est autorisée à effectuer la collecte et l'enregistrement des données à caractère personnel ci-après :

- **les données d'état civil** : nom et prénom ;
- **les données d'informations d'ordre économique et financier** : revenus, situation financière, instructions de paiement ;
- **les données biométriques** : voix ;
- **les données de connexion :** identifiants des terminaux ;

Les données visées au présent article concernent les salariés et les clients de la STANBIC BANK.

Les données non mentionnées ne devront aucunement faire l'objet d'un quelconque traitement de la part de la STANBIC BANK.

Article 2 :

Les données traitées par la STANBIC BANK ne peuvent pas être utilisées à des fins autres que celles précisées dans la demande d'autorisation.

Toute réutilisation de ces données à d'autres fins, doit faire l'objet d'une autorisation préalable de l'Autorité de protection.

Article 3 :

La STANBIC BANK est autorisé à communiquer les données traitées à l'article 1 de la présente décision :

- aux agents habilités de STANBIC BANK ;
- au Procureur de la République ;
- aux Officiers de Police Judiciaire ;
- aux Autorités publiques ivoiriennes agissant dans le cadre de leurs missions ;
- aux Agents assermentés de l'ARTCI.

Il est interdit à la STANBIC BANK de transférer, sans autorisation préalable de l'Autorité de protection, les données collectées vers des pays tiers.

Article 4 :

Les données sont conservées pendant six (06) mois à compter du dernier contact et pendant un (01) an en ce qui concerne les documents d'analyse.

Les données doivent être supprimées après expiration du délai de conservation.

En cas de litige, les données doivent être conservées jusqu'à la fin de la procédure.

Article 5 :

STANBIC BANK informe les personnes concernées de leurs droits d'accès direct, d'opposition, d'effacement, de portabilité, de retrait du consentement donné, de rectification et de suppression.

Elle le fait par le biais de mentions légales sur ses formulaires.

STANBIC BANK est tenu de définir une procédure de gestion des droits des personnes concernées.

Article 6 :

Le Correspondant à la protection désigné par la STANBIC BANK, tient une liste des traitements effectués, immédiatement accessible à toute personne concernée faisant la demande.

La société STANBIC BANK est tenue de mettre en place un dispositif de :

- formation pour son correspondant et ses agents habilités ;
- sensibilisation de son personnel.

Article 7 :

Conformément à l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, STANBIC BANK doit s'assurer que ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements de données qu'elles opèrent.

Article 8 :

Conformément à l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, STANBIC BANK est tenu d'établir pour le compte de l'Autorité de Protection un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

STANBIC BANK communique ce rapport à l'Autorité de protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 9 :

L'Autorité de protection procède à des contrôles auprès de la STANBIC BANK, afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 10 :

La présente décision entre en vigueur à compter de la date de sa notification à la STANBIC BANK

Article 11 :

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

Fait à Abidjan, le 05 Juillet 2022
En deux (2) exemplaires originaux

Le Président

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

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0744
DE L'AUTORITE DE PROTECTION
DE LA REPUBLIQUE DE COTE D'IVOIRE
EN DATE DU 5 JUILLET 2022
PORTANT AUTORISATION DE TRAITEMENT
DE DONNEES A CARACTERE PERSONNEL
PAR LA SOCIETE DE LIMONADERIES ET BRASSERIES
D'AFRIQUE (SOLIBRA TREICHVILLE)
(VIDEOSURVEILLANCE)

Conseil de Régulation : 31 Av Nogués, 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 l'acte uniforme OHADA du 15 décembre 2010 portant sur le droit commercial général ;

Vu la loi n°99-437 du 6 juillet 1999 portant modification de la loi n° 64-293 du 1er août 1964 portant code des débits de boissons et des mesures contre l'alcoolisme telle que modifiée par l'annexe à la loi n° 70-726 du 31 décembre 1970 portant loi de finances pour la gestion 1971 ;

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 l'ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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 ;

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°2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

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 de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

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 ;

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 caractère personnel (DCP) ;

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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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°2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

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 ;

Par les motifs suivants :

- **Sur la compétence de l'Autorité de Protection**

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par SOLIBRA, sise à Abidjan, 35 rue des brasseurs, Treichville, 01 BP 1304 Abidjan 01 téléphone 27 21 21 12 00.

Considérant que SOLIBRA est une société spécialisée dans l'exploitation de malteries, brasseries et limonaderies ;

Considérant que l'article 47 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 est chargée de recevoir les déclarations et d'octroyer les autorisations, pour la mise en œuvre de traitement des données à caractère personnel ;

L'Autorité de Protection est compétente, pour examiner la demande d'autorisation de traitement initiée par SOLIBRA.

- **Sur la recevabilité de la demande d'autorisation**

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, le traitement des données à caractère personnel comportant des données biométriques sont soumis à autorisation préalable de l'Autorité de Protection, avant toute mise en œuvre ;

Considérant qu'en l'espèce, SOLIBRA envisage de collecter, et de stocker les données à caractère personnel, tels que, les numéros de plaques d'immatriculations, et les données biométriques, notamment les images et, les mouvements de toutes personnes à l'intérieur et aux alentours de son siège social ;

En application des dispositions précitées, lesdits traitements doivent être autorisés par l'Autorité de protection, pour être mis en œuvre ;

Considérant que selon l'article 7 précité, la demande d'autorisation est présentée par le responsable du traitement ou son représentant légal ;

Que l'article 1 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, définit le responsable du traitement comme étant la personne physique ou morale, publique ou privée, 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 ;

Considérant qu'en l'espèce, SOLIBRA a décidé de mettre en place un système de vidéosurveillance en vue d'assurer la sécurité des biens et des personnes au sein de sa structure ;

Que pour ce faire, elle a décidé de collecter et de traiter les données à caractère personnel des visiteurs et des membres de son personnel ;
L'Autorité de Protection en conclut que SOLIBRA a la qualité de Responsable du traitement ;

Considérant qu'aux termes de l'article 9 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la demande d'autorisation doit contenir les mentions minimums relatives à la dénomination sociale de la personne morale, au Responsable du traitement, à son siège social, à l'identité de son représentant légal, à son numéro d'immatriculation au registre du commerce et du crédit mobilier, à son numéro de déclaration fiscale, aux finalités du traitement, à la durée de conservation des données traitées, aux dispositions prises pour assurer la sécurité des traitements, à la protection, à la confidentialité des données traitées et à la fonction de la personne ou le service auprès duquel s'exercent les droits des personnes concernées ;

Qu'en l'espèce, la demande d'autorisation de SOLIBRA contient les mentions minimums prescrites par l'article 9 précité ;

Considérant qu'au regard de tout ce qui précède, ladite demande satisfait les conditions de formes exigées par les articles 7 et 9 de la loi n°2013-450 relative à la protection des données à caractère personnel ;

L'Autorité de Protection déclare que la demande de SOLIBRA est recevable en la forme.

- **Sur la légitimité et la licéité du traitement**

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 que SOLIBRA envisage de collecter et de stocker les données à caractère personnel des personnes présentes dans ses locaux et aux alentours, par le biais d'un système de vidéosurveillance ;

Considérant toutefois que SOLIBRA n'apporte pas la preuve que les personnes concernées ont exprimé leur consentement préalable au traitement de leurs données ;

Considérant par ailleurs, que l'existence d'un système de vidéosurveillance doit être portée à la connaissance de toute personne filmée ou susceptible de l'être, de façon claire et permanente, par un pictogramme placé à hauteur de vue, dans les zones filmées par les caméras ;

Cependant, SOLIBRA indique dans son formulaire de demande d'autorisation que des affiches et des panneaux sont installés à l'intérieur et à l'extérieur du site ;

Toutefois, les informations qui y figurent n'ont pas été mentionnées ;

Considérant en outre, que l'utilisation d'un système de vidéosurveillance au sein d'une entreprise est subordonnée à l'accord du personnel, qui doit exprimer clairement son consentement à son installation ;

L'Autorité de protection prescrit à SOLIBRA de mettre en place un processus de recueil individuel du consentement de son personnel ;

L'Autorité de Protection prescrit également à SOLIBRA, de lui faire parvenir les images des pictogrammes et affiches afin de vérifier si les informations qui y figurent sont conformes à l'article 28 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

- **Sur la finalité**

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 qu'en l'espèce, SOLIBRA envisage la mise en place d'un système de vidéosurveillance, aux fins de :

- assurer la sécurité des biens et des personnes ;

- anticiper et de réagir en cas d'incendies et accidents ;

- prévention des atteintes aux biens ;

- prévention d'actes terroristes ;

- régulation du trafic routier au sein du site ;

L'Autorité de Protection considère que lesdites finalités sont déterminées, explicites et légitimes.

- **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 qu'en l'espèce, SOLIBRA a indiqué que les données traitées sont conservées pendant trente (30) jours mais ne mentionne pas le sort desdites données au-delà de la période de conservation ;

L'Autorité de Protection prescrit que les informations enregistrées soient conservées pendant une durée de trente (30) jours, et en cas d'incidents, pendant une période d'un (01) an à compter de la dernière sauvegarde mensuelle des données traitées.

L'Autorité de Protection prescrit également à SOLIBRA de communiquer les informations relatives au sort des données au-delà de la période de conservation.

- **Sur la proportionnalité des données traitées**

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 qu'en l'espèce, SOLIBRA indique que le traitement concerne les données suivantes :

- les images des visiteurs et des membres de son personnel ;
- les numéros de plaque d'immatriculation, modèle et couleur des véhicules au sein du site;
- les différents mouvements détectés par les caméras dans les lieux placés sous surveillance.
- L'intérieur de l'usine ;

En conséquence, l'Autorité de Protection conclut que les données collectées sont pertinentes, adéquates et non excessives au regard des finalités.

- **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, selon lesquelles la demande d'autorisation adressée à l'Autorité de protection doit contenir les destinataires habilités à recevoir communication des données traitées ;

Considérant que la visualisation des images doit être restreinte aux seuls destinataires habilités, en charge de la sécurité des locaux ou installations sous surveillance ;

Considérant qu'il est mentionné dans le procès-verbal de vérification préalable de la SOLIBRA que les destinataires des données traitées sont les personnes en charge de la sécurité de la vidéosurveillance, à savoir :

- le correspondant à la protection
- le responsable sureté ;
- l'assistant sureté
- le responsable sécurité et système d'information et délégué à la protection ;

- le prestataire (accompagné d'une personne habilité dans le cadre de la maintenance)

Considérant que les destinataires susmentionnés sont les agents des services internes de SOLIBRA hormis le prestataire NT PROTECT ;

Considérant par ailleurs que, SOLIBRA ne mentionne pas dans son formulaire qu'elle effectuera un transfert de données ;

L'Autorité de Protection prescrit que lesdites données ne fassent l'objet d'aucun transfert, ni d'aucune communication aux services non habilités de SOLIBRA ;

L'Autorité de Protection autorise également que les données traitées soient communiquées, le cas échéant :

- aux agents assermentés et habilités de l'Autorité de Protection dans le cadre de leurs missions ;

- aux Autorités publiques ivoiriennes compétentes, par le biais de leurs agents habilités, agissant dans le cadre de leurs missions ;

- au Procureur de la République de Côte d'Ivoire ;

- aux Officiers de Police Judiciaire de Côte d'Ivoire, munis d'une réquisition.

- **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 SOLIBRA de faire preuve de transparence vis à vis des personnes concernées qui devront notamment être informées :

- de l'identité du responsable du traitement et le cas échéant, celle de son représentant dûment mandaté ;
- des finalités 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 leurs droits d'accès et de rectifications,
- de la durée de conservation des données,
- de l'éventualité de tout transfert de données à destination de pays tiers ;

Considérant que les personnes concernées (salariés, clients, visiteurs etc.) doivent être clairement informées de l'existence d'un système de vidéosurveillance et des destinataires des informations traitées ;

Considérant que, SOLIBRA indique que lesdites informations sont communiquées aux personnes concernées, par le biais de plusieurs pictogrammes et affiches ;

Que cependant SOLIBRA n'a pas rapporté la preuve de l'existence des pictogrammes et des informations devant y figurer.

L'Autorité de Protection prescrit à SOLIBRA d'informer les personnes concernées de l'existence d'un dispositif de vidéosurveillance, au moyen de pictogrammes et affiches placés de façon visible, dans les zones sous surveillance.

Les pictogrammes et affiches doivent indiquer, d'une façon claire et visible, les informations suivantes :

- le nom du responsable de traitement,
- le fait que l'établissement est placé sous vidéosurveillance,
- la finalité de ce dispositif (la sécurité des biens et des personnes),
- les coordonnées du contact pour l'exercice, par les personnes concernées, des droits d'accès, de rectification et d'opposition ;
- le numéro de l'autorisation octroyée par l'Autorité de protection.

- **Sur les droits d'accès direct, d'opposition, de rectification 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, d'effacement ;

Considérant que SOLIBRA indique dans son formulaire de demande d'autorisation que les droits d'accès direct, d'opposition, de rectification et de suppression, pourront être exercés auprès du responsable sureté ;

Considérant toutefois que SOLIBRA a désigné un correspondant à la protection ;

L'Autorité de Protection prescrit à SOLIBRA que les droits d'accès, de rectification et d'effacement des personnes concernées s'exercent auprès de son correspondant à la protection.

- **Sur les mesures de sécurité**

Considérant qu'en application de l'article 41 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le responsable du traitement et le sous-traitant prennent toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient détruites, déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance ;

Considérant que les mesures de sécurité doivent couvrir l'aspect physique et logique;

Considérant qu'au vu des éléments techniques fournis dans le formulaire de demande d'autorisation, et du procès-verbal de contrôle préalable, le niveau de sécurité du système d'information de SOLIBRA lui permet de mettre en œuvre la vidéosurveillance dans ses locaux et leurs alentours pour les finalités déclarées ;

Qu'il ressort des documents communiqués par SOLIBRA, qu'elle a pris toutes les mesures nécessaires en vue d'assurer la sécurité des données, conformément aux dispositions de l'article 41 de la Loi susmentionnée ;

L'Autorité de Protection considère que les mesures de sécurité logique et physique nécessaires sont garanties.

Après en avoir délibéré,

DECIDE :

Article 1 :

SOLIBRA est autorisée à effectuer la collecte, l'enregistrement et le stockage des données à caractère personnel ci-après :

- les données d'identification : numéro de plaque d'immatriculation, modèle et couleur des véhicules;
- les données de localisation : les différents mouvements détectés par les caméras dans les lieux placés sous surveillance ;
- les données biométriques : images des personnes.

Les données visées au présent article concernent les employés et visiteurs de SOLIBRA.

Article 2 :

Les données traitées par SOLIBRA ne peuvent être utilisées à des fins autres que celles précisées dans la demande d'autorisation.

Toute réutilisation de ces données à d'autres fins doit faire l'objet d'une autorisation préalable de l'Autorité de Protection.

Article 3 :

SOLIBRA a l'obligation de procéder au recueil du consentement préalable, formel des personnes concernées. Elle devra en fournir les preuves à l'Autorité de Protection.
SOLIBRA doit informer ses salariés et ses visiteurs, de l'existence d'un dispositif de vidéosurveillance, au moyen de pictogrammes et affiches placés de façon visible à hauteur de vue dans les zones filmées par les caméras.
Les pictogrammes doivent indiquer, d'une façon claire et visible, les informations suivantes :

- le nom du responsable de traitement,
- le fait que l'établissement est placé sous vidéosurveillance ;
- la finalité de ce dispositif (la sécurité des personnes et des biens) ;
- les coordonnées du contact pour l'exercice, par les personnes concernées, des droits d'accès de rectification et d'opposition
- le numéro de l'autorisation octroyée par l'Autorité de Protection.

Article 4 :

SOLIBRA est tenue d'informer les personnes concernées sur leurs droits d'accès direct à l'information, d'opposition, de rectification et de suppression par voie d'affichage dans les zones filmées par les caméras.

Ces droits pourront être exercés auprès du correspondant à la protection désigné par SOLIBRA.

Article 5 :

SOLIBRA est autorisée à installer les caméras de vidéosurveillance à son siège de Treichville dans les zones telles qu'indiquer dans le formulaire de demande d'autorisation.

Les caméras pouvant filmer les zones de circulation ne doivent pas porter atteinte à la vie privée des personnes concernées en ne filmant pas l'intérieur des véhicules ou des habitations aux alentours du site.

SOLIBRA ne doit pas positionner les caméras de vidéosurveillance sur les postes de travail de ses employés.

SOLIBRA ne doit pas poser des caméras de vidéosurveillance dans les toilettes, et lieux de pause ou de repos de ses employés.

Article 6

SOLIBRA est autorisée à communiquer les données traitées :

- à ses agents habilités,
- aux agents des Administrations publiques compétentes dûment habilités, dans le cadre de leurs missions,
- au Procureur de la République
- aux Officiers de Police Judiciaire munis d'une réquisition.

Il est interdit à SOLIBRA de communiquer les données traitées aux personnes non habilitées.

Article 7 :

SOLIBRA conserve les données collectées pendant une durée de trente (30) jours et en cas d'incidents, pendant une période d'un (01) an, à compter de la dernière sauvegarde mensuelle des données traitées.

Article 8 :

Le correspondant à la protection désigné par SOLIBRA tient une liste des traitements effectués, immédiatement accessible à toute personne concernée en faisant la demande.

Article 9 :

SOLIBRA veille au respect des dispositions de la Loi relative à la protection des données à caractère personnel par ses sous-traitants.

Conformément à l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, SOLIBRA doit s'assurer que, ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle relatives aux traitements de données qu'ils opèrent.

Il incombe à SOLIBRA ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

SOLIBRA est tenue de :

- s'assurer de la viabilité et de la sécurité du réseau de transmission en vue de garantir la sécurité de la vie privée des personnes prises en images ;
- veiller à la sécurité du disque dur chargé de stocker les images et du système d'exploitation ;
- veiller à la mise à jour du système d'exploitation et les applications qui y sont installées afin de conserver et de garantir la sécurité.

Article 10 :

Conformément à l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, SOLIBRA est tenue d'établir pour le compte de l'Autorité de Protection un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

SOLIBRA communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 11 :

L'Autorité de Protection procède à des contrôles auprès de SOLIBRA, afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 12 :

La présente décision entre en vigueur à compter de la date de sa notification à SOLIBRA.

Article 13 :

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

Fait à Abidjan, le 05 Juillet 2022
En deux (2) exemplaires originaux

Le Président

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

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0745

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

EN DATE DU 5 JUILLET

PORTANT AUTORISATION DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL PAR LE CABINET DU PREMIER MINISTRE DANS LE CADRE DU PROGRAMME ECONOMIQUE POUR L'INNOVATION ET LA TRANSFORMATION DES ENTREPRISES (PEPITE)

L'AUTORITE DE PROTECTION,

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 l'ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication ;

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 ;

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°2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

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 de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

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 ;

Vu le décret n°2022-269 du 19 avril 2022 portant nomination du Premier Ministre, Chef du Gouvernement ;

Vu le décret n°2022-270 du 20 avril 2022 portant nomination des Membres du Gouvernement ;

Vu le décret n°2022-301 du 04 mai 2022 portant attributions des Membres du Gouvernement ;

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°2014-0021 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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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°2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

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 de l'activité :

- du correspondant à la protection des données, personne morale ;
- de formation en matière de protection des données à caractère personnel ;
- d'audit en matière de protection des données à caractère personnel ;

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 données à caractère personnel ;

Par les motifs suivants :

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par le Cabinet du Premier Ministre, Organisme étatique, sis à Abidjan, Plateau Boulevard Angoulvant, 01 BP 1533 Abidjan 01 ;

Considérant que le **Cabinet du Premier Ministre** a pour mission de mener à bien les différents projets du Gouvernement ;

Considérant que l'article 47 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 est chargée de recevoir les déclarations et d'octroyer les autorisations, pour la mise en œuvre de traitements de données à caractère personnel ;

L'Autorité de protection est compétente, pour examiner la demande d'autorisation de traitements initiée par le **Cabinet du Premier Ministre** :

- **Sur la recevabilité de la demande d'autorisation**

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 les données médicales, 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 qu'en l'espèce, la demanderesse collecte et stocke par le biais de sa plateforme, le numéro de téléphone des dirigeants sociaux et gérants d'entreprise.

Qu'en application des dispositions précitées, lesdits traitements doivent être autorisés par l'Autorité de protection, pour être mis en œuvre ;

Considérant que selon l'article 7 précité de la même loi, la demande d'autorisation est présentée par le responsable du traitement ou son représentant légal ;

Que l'article 1 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, définit le responsable du traitement comme étant la personne physique ou morale, publique ou privée, 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.

Considérant qu'aux termes de l'article 9 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la demande d'autorisation doit contenir les mentions minimums relatives à la dénomination sociale de la personne morale, au Responsable du traitement, à son siège social, à l'identité de son représentant légal, à son numéro d'immatriculation au registre du commerce et du crédit mobilier, à son numéro de déclaration fiscale, aux finalités du traitement, à la durée de conservation des données traitées, aux dispositions prises pour assurer la sécurité des traitements, à la protection et à la confidentialité des données traitées ;

Considérant que lesdites mentions figurent dans la demande d'autorisation formulée par le **Cabinet du Premier Ministre ;**

Que ladite demande satisfait les conditions de forme exigées par les articles 7 et 9 de la loi n°2013-450 relative à la protection des données à caractère personnel ;

En conséquence, l'Autorité de protection considère que la demande du **Cabinet du Premier Ministre** est recevable en la forme ;

- **Sur la légitimité et la licéité du traitement**

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 la demanderesse procède à la collecte des données auprès, des dirigeants sociaux et gérants d'entreprises de 14 secteurs ;

Qu'il s'agit d'une collecte directe de données à caractère personnel ;

Considérant cependant que la demanderesse indique qu'elle procédera au recueil du consentement préalable par le biais de courriel.

L'Autorité de protection considère que le principe de la légitimité n'est pas pleinement respecté ;

Aussi, l'Autorité de protection prescrit au **Cabinet du Premier Ministre** de :

- prévoir un formulaire numérique pour le recueil de consentement exprès des personnes concernées ;
- prévoir une bannière de configuration et de consentement pour les cookies utilisés sur le site internet ;
- mettre en place des conditions générales d'utilisation permettant d'éclairer le consentement de l'utilisateur.

- **Sur la finalité**

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 qu'en l'espèce, la demanderesse procède au traitement de données à caractère personnel afin de sélectionner les entreprises à fort potentiel, sur la base de critères d'éligibilité et d'évaluation clairement définis.

L'Autorité de protection considère que cette finalité n'est pas déterminée et explicite.

L'Autorité de protection, après analyse des documents fournis par le **Cabinet du Premier Ministre**, considère que les traitements opérés par le **Cabinet du Premier Ministre** ont pour finalités :

- Renforcer les écosystèmes d'affaires ;
- Soutenir l'entrepreneuriat ;
- Contribuer à faire émerger des entreprises fortes et résilientes.

- **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 qu'en l'espèce, le **Cabinet du Premier Ministre** a indiqué qu'il conservera les données traitées durant dix (10) ans.

L'Autorité de protection au regard de la finalité du traitement considère que le délai de 10 ans n'est pas excessif.

Toutefois, l'Autorité prescrit à la demanderesse qu'au-delà du délai de 10 ans, les données conservées fassent l'objet d'anonymisation à des fins statistiques.

En cas de contentieux, il est prescrit au **Cabinet du Premier Ministre** de conserver les données traitées jusqu'au règlement définitif du contentieux.

- **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 qu'en l'espèce, le **Cabinet du Premier Ministre** indique que le traitement concerne les données suivantes :

- **les données d'identification :** nom, prénom;
- **les données de vie professionnelle :** curriculum vitae, fonction, lettre de motivation ;
- **les données d'ordre économique et financier :** revenus, situation financière ;
- **les données de localisation :** Adresse géographique;
- **les données de connexions :** e-mail, adresse IP ;
- **les numéros d'identification nationale** : numéro de téléphone, numéro de sécurité sociale.

Il y a lieu de constater que les données collectées, telles qu'elles sont décrites dans la demande d'autorisation sont pertinentes, adéquates, et non excessives au regard de la finalité.

- **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, selon lesquelles la demande d'autorisation adressée à l'Autorité de protection doit contenir les destinataires habilités à recevoir communication des données traitées ;

Considérant qu'en l'espèce, la demanderesse précise que les destinataires desdites données sont :

- Les services internes du **Cabinet du Premier Ministre** ;
- Les services gouvernementaux.

Considérant que la notion de services gouvernementaux est imprécise.

L'Autorité de protection prescrit que les données traitées soient communiquées aux destinataires ci-dessous :

- aux services internes du Cabinet du Premier Ministre ;
- aux agents habilités de l'administration publique dans le cadre de leurs missions ;
- au Procureur de la République ;
- aux Officiers de Police Judiciaire de Côte d'Ivoire munis d'une réquisition;
- aux agents assermentés de l'Autorité de protection (ARTCI) habilités, dans le cadre de leurs missions.

L'Autorité de protection prescrit que lesdites données ne fassent l'objet d'aucun transfert vers des pays tiers, sans autorisation préalable ;

- **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 la demanderesse de faire preuve de transparence vis à vis des personnes concernées qui devront notamment être informées :

- 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.

Qu'à cette fin, la demanderesse indique que des courriels permettront aux personnes concernées d'être informées de leurs droits, préalablement à toute collecte ;

Considérant que ces formalités ne suffisent pas à satisfaire le principe de transparence ;

L'Autorité de protection prescrit au **Cabinet du Premier Ministre** de compléter les informations portées à la connaissance des personnes concernées par des mentions sur les formulaires d'inscription, par des mentions légales et conditions générales d'utilisation sur le site internet.

L'Autorité de protection prescrit également au **Cabinet du Premier Ministre** de compléter les informations portées à la connaissance des personnes concernées par les mentions relatives à la finalité des traitements, la description exhaustive des données personnelles traitées, les destinataires auxquels les données sont susceptibles d'être communiqués, l'éventualité de tout transfert de données à destination de pays tiers.

- **Sur les droits d'accès direct, d'opposition, de rectification 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, d'opposition, d'effacement.

Considérant que la demanderesse n'indique pas le service ou la direction auprès de laquelle les personnes concernées pourront exercer leurs droits d'accès direct, d'opposition, de rectification, d'effacement, de portabilité, de retrait du consentement donné, et de suppression, pourront être exercés ;

Qu'en outre, la demanderesse n'a pas désigné de correspondant à la protection ;

L'Autorité de protection prescrit au Cabinet du Premier Ministre de :

- désigner un correspondant à la protection, auprès duquel les personnes concernées pourront exercer leurs droits ;
- élaborer une procédure de gestion des droits des personnes concernées ;
- élaborer une charte de protection des données personnelles.

- **Sur les mesures de sécurité**

Considérant qu'en application de l'article 41 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le responsable du traitement et le sous-traitant prennent toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient détruites, déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance ;

Considérant que les mesures de sécurité doivent couvrir l'aspect physique (les données stockées sur des supports papiers) et logique (supports informatiques) ;

Considérant qu'au vu des éléments techniques fournis dans les différents formulaires, les traitements de données à caractère personnel mis en œuvre offrent un bon niveau de confidentialité. Les recommandations formulées devront être appliquées afin d'optimiser la sécurité des données.

Cependant, l'Autorité de protection prescrit à la demanderesse de :

- **Sur les serveurs et les postes de travail** : Maintenir à jour les systèmes d'exploitation, et aussi les applications utilisées afin d'être moins vulnérable aux différentes attaques ;

- **Sur la plateforme web** :

    - Mettre en place des mentions d'informations sur la plateforme web afin d'informer les visiteurs sur les données collectées, la finalité, la durée de conservation etc.

    - Ajouter les pages relatives aux mentions légales, Conditions Générales d'Utilisation (CGU) et politique de confidentialité ;

    - Implémenter une bannière de recueil du consentement et de configuration des cookies ;

- Modifier les adresses de connexion par défaut et limiter le nombre de tentatives de connexion infructueuses.

- **Sur la sécurité du système en général** :

  solliciter un audit de sécurité auprès de la Direction de la Confiance Numérique et des Systèmes d'informations de l'ARTCI, pour une analyse approfondie en vue de ressortir et corriger les failles de sécurité.

Après en avoir délibéré,

DECIDE :

Article 1 :

Le **Cabinet du Premier Ministre** est autorisé à effectuer la collecte, et l'enregistrement des données à caractère personnel ci-après :

- **les données d'identification :** Nom, prénom;
- **les données de vie professionnelle :** curriculum vitae, fonction, lettre de motivation ;
- **les données d'ordre économique et financier :** revenus, situation financière ;
- **les données de localisation :** Adresse géographique;
- **les données de connexions :** e-mail, adresse IP ;
- **les numéros d'identification nationale** : numéro de téléphone, numéro de sécurité sociale.

Les données visées au présent article concernent les dirigeants et gérants d'entreprises.

Les données non mentionnées ne devront aucunement faire l'objet d'un quelconque traitement de la part du **Cabinet du Premier Ministre**.

Article 2 :

Les données traitées par le **Cabinet du Premier Ministre** ne peuvent être utilisées à des fins autres que celles précisées dans la demande d'autorisation.

Toute réutilisation de ces données à d'autres fins doit faire l'objet d'une autorisation préalable de l'Autorité de protection.

Article 3 :

Le **Cabinet du Premier Ministre** a l'obligation de procéder au recueil du consentement préalable des personnes concernées, par l'insertion de :

- prévoir un formulaire numérique pour le recueil de consentement exprès des personnes concernées ;
- prévoir une bannière de configuration et de consentement pour les cookies utilisés sur le site internet ;
- mettre en place des conditions générales d'utilisation permettant d'éclairer le consentement de l'utilisateur.

Conformément aux dispositions de l'article 1 de la décision n°2014-0021 du 03 septembre 2014 portant conditions et critères applicables à la limitation du traitement des données à caractère personnel, la personne concernée doit avoir été suffisamment informée par le **Cabinet du Premier Ministre** 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.

Article 4 :

Le **Cabinet du Premier Ministre** est autorisé à communiquer les données traitées :

- aux services internes du **Cabinet du Premier Ministre** ;
- aux agents habilités de l'administration publique dans le cadre de leurs missions ;
- au Procureur de la République ;
- aux Officiers de Police Judiciaire de Côte d'Ivoire munis d'une réquisition;
- aux agents assermentés de l'Autorité de protection (ARTCI) habilités, dans le cadre de leurs missions.

Il est interdit au **Cabinet du Premier Ministre** de transférer, sans autorisation préalable de l'Autorité de protection, les données collectées vers des pays tiers.

Article 5 :

Le **Cabinet du Premier Ministre** conserve l'ensemble des données traitées pendant dix (10) ans et au-delà du délai les anonymise pour des fins statistiques.

En cas de contentieux, le **Cabinet du Premier Ministre** conserve les données traitées jusqu'au règlement définitif du contentieux.

Article 6 :

Le **Cabinet du Premier Ministre** informe les personnes concernées de leurs droits d'accès direct, d'opposition, d'effacement, de portabilité, de retrait du consentement

donné, de rectification et de suppression. Elle le fait par le biais de mentions légales et de conditions générales d'utilisation sur le site internet de la plateforme.

L'Autorité de protection prescrit également au **Cabinet du Premier Ministre** de compléter les informations portées à la connaissance des personnes concernées par les mentions relatives à la finalité des traitements, la description exhaustive des données personnelles traitées, les destinataires auxquels les données sont susceptibles d'être communiqués, l'éventualité de tout transfert de données à destination de pays tiers.

Le **Cabinet du Premier Ministre** doit également définir une politique gestion des droits des personnes concernées

Article 7 :

Le **Cabinet du Premier Ministre** désigne un correspondant à la protection auprès de l'Autorité de protection.

Il notifie la désignation dudit correspondant à l'Autorité de protection par un courrier officiel.

Le correspondant à la protection tient une liste des traitements effectués, immédiatement accessible à toute personne concernée en faisant la demande.

Article 8 :

Le **Cabinet du Premier Ministre** veille au respect des dispositions de la Loi relative à la protection des données à caractère personnel par ses sous-traitants.

Le **Cabinet du Premier Ministre** est tenu de mettre en place un dispositif de :

- formation pour son correspondant à la protection et ses agents habilités
- sensibilisation sur la protection des données à caractère personnel pour son personnel ;

Article 9 :

Conformément à l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le **Cabinet du Premier Ministre** est tenu d'établir pour le compte de l'Autorité de protection un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

Le **Cabinet du Premier Ministre** communique ce rapport à l'Autorité de protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 10 :

L'Autorité de protection procède à des contrôles auprès du **Cabinet du Premier Ministre** afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 11 :

Le **Cabinet du Premier Ministre** est tenu de procéder au paiement des frais de dossiers auprès du greffe de l'ARTCI, conformément à la décision n°2016-021 de l'Autorité de protection de la République de Côte d'Ivoire fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel.

Article 12 :

La présente décision entre en vigueur à compter de la date de sa notification au **Cabinet du Premier Ministre**.

Article 13 :

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

Fait à Abidjan, le 05 Juillet 2022
En deux (2) exemplaires originaux

Le Président

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

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0746

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 5 JUILLET 2022

PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL PAR

ORANGE CÔTE D'IVOIRE

L'AUTORITE DE PROTECTION,

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°2015-532 du 20 juillet 2015 portant Code du travail ;

Vu la loi n°2016-412 du 15 Juin 2016 relative à la consommation ;

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°2017-803 du 07 décembre 2017 d'orientation de la société de l'information de Côte d'Ivoire ;

Vu l'ordonnance n°2019-495 du 12 juin 2019 portant institution d'un dispositif de contrôle des flux de communications électroniques des entreprises de télécommunications/TIC ;

Vu l'ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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 ;

Vu le décret n°2013-301 du 02 mai 2013 relatif à l'homologation des équipements terminaux et radioélectriques et à l'agrément d'installateur ;

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 de traitement des données à caractère personnel ;

Vu le décret n°2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le décret n°2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

Vu le décret n°2017-193 du 22 mars 2017 portant identification des abonnés des services de Télécommunications/TIC ouverts au public et des utilisateurs des cybercafés ;

Vu le décret n°2017-829 du 14 décembre 2017 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel pour l'intégration des grands facturiers à la plateforme électronique de partage des informations sur le crédit ;

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 de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

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 ;

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 conditions au traitement des données à caractère personnel (DCP) ;

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°2014-0029 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 27 novembre 2014 relative aux fixations des délais de communication des informations par les opérateurs et fournisseurs de services à l'ARTCI ;

Vu la décision n°2016-0112 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 11 février 2016 portant autorisation de traitement de données à caractère personnel par la société Orange Côte d'Ivoire S.A (Offre Personnal Cloud) ;

Vu la décision n°2016-0113 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 11 février 2016 portant autorisation de transfert de données à caractère personnel vers la France (Orange Group) par la société Orange Côte d'Ivoire SA ;

Vu la décision n°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

Vu la décision n°2017-0347 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 11 Octobre 2016 portant autorisation de traitement en matière de protection des données à caractère personnel « Right Q » par la société Orange Côte d'Ivoire S.A ;

Vu la décision n°2017-0348 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 11 Octobre 2016 portant autorisation de traitement de données à caractère personnel par la société Orange Côte d'Ivoire S.A (funspace) ;

Vu la décision n°2017-0349 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 11 octobre 2016 portant autorisation de transfert de données à caractère personnel vers la Belgique par la société Orange Côte d'Ivoire (funspace) ;

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°2019-0494 du Conseil de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

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 de l'activité ;

- du correspondant à la protection des données, personnes morales ;
- de formation en matière de protection des données à caractère personnel ;
- d'audit en matière de protection des données à caractère personnel ;

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 données à caractère personnel ;

Vu le cahier des charges de l'opérateur ORANGE CÔTE D'IVOIRE annexé à sa licence individuelle pour l'établissement et l'exploitation d'un réseau de communications électroniques ouvert au public ;

Vu le rapport d'audit de protection des données personnelles de ORANGE CÔTE D'IVOIRE;

Par les motifs suivants :

Considérant que conformément à l'article 53 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, les responsables du traitement doivent procéder à la mise en conformité des traitements qu'ils opèrent avec ladite loi ;

Considérant que pour faciliter cette mise en conformité l'Autorité de protection a, par décision n°2017-0354 du 26 octobre 2017 définit la 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 ;

La société ORANGE COTE D'IVOIRE S.A est une société anonyme de droit ivoirien, avec conseil d'administration et un capital de 6 026 000 000 FCFA, qui exerce dans les télécommunications/ TIC, dont le siège social est sis à Marcory, Boulevard Giscard d'Estaing, Immeuble le Quartz, 11 BP 202 Abidjan 11, Tél : (225) 27 21 23 90 00;

Considérant que ORANGE COTE D'IVOIRE a saisi l'Autorité de protection d'une demande de mise en conformité ;

Considérant que ORANGE COTE D'IVOIRE a désigné un correspondant à la protection et a procédé à la formation de son personnel ;

Que par ailleurs, ORANGE COTE D'IVOIRE a effectué son audit de protection des données personnelles ;

Considérant les recommandations contenues dans le rapport d'audit de protection des données personnelles ;

Après en avoir délibéré,

DECIDE :

Article 1 :

ORANGE COTE D'IVOIRE est autorisée à effectuer les traitements des données mentionnées dans l'annexe 1 de la présente décision.

Les données non mentionnées dans l'annexe 1 ne devront aucunement faire l'objet d'un quelconque traitement, de la part de ORANGE COTE D'IVOIRE.

Article 2 :

ORANGE COTE D'IVOIRE est autorisée à effectuer les traitements énumérés dans l'annexe 3 de la présente décision.

Article 3 :

ORANGE COTE D'IVOIRE est autorisée à transférer vers la France, les données énumérées dans l'annexe 2 de la présente décision.

Article 4 :

ORANGE COTE D'IVOIRE est autorisée à communiquer les données traitées uniquement aux destinataires habilités, notamment :

- les services internes de la société, suivant leurs habilitations ;
- les autorités publiques ivoiriennes habilitées dans le cadre de l'exercice de leurs missions ;
- le Procureur de la république et les officiers de police judiciaire munis d'une réquisition ;
- le siège du groupe ORANGE en France ;
- la société Next Gen Innovation en Belgique ;
- la société RIGHTCOM SARL, au Bénin ;
- les sous-traitants ;
- les avocats et intermédiaires de justice ;

Article 5 :

L'Autorité de protection interdit à ORANGE COTE D'IVOIRE de transférer sans autorisation préalable de l'Autorité de protection, les données traitées vers des pays tiers, autres que la France, la Belgique et le Bénin.

ORANGE COTE D'IVOIRE est tenue avant tout transfert de données hors de la Côte d'Ivoire, de les stocker sur le territoire de la République de Côte d'Ivoire.

Article 6 :

Conformément à l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, ORANGE COTE D'IVOIRE doit s'assurer que ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle relatives aux traitements de données qu'ils opèrent.

Il incombe à ORANGE COTE D'IVOIRE ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

Article 7 :

Les traitements de données autorisés dans la présente décision correspondent aux cent quinze (115) finalités énumérées à l'annexe 3 de la présente décision.

Les traitements afférents aux finalités ci-dessus sont listés dans l'annexe 4 de la présente décision.

Article 8 :

ORANGE COTE D'IVOIRE est tenue de mettre en œuvre les prescriptions énoncées dans l'annexe 5 de la présente décision. Elle le fait dans les délais prévus dans ladite annexe.

La mise en œuvre desdites prescriptions fera l'objet d'un contrôle par l'Autorité de Protection.

L'Autorité de protection délivrera une attestation de conformité à ORANGE COTE D'IVOIRE, lorsque toutes les prescriptions auront été mises en œuvre.

Article 9 :

En application de l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, ORANGE COTE D'IVOIRE est tenue d'établir, pour le compte de l'Autorité de protection, un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

ORANGE COTE D'IVOIRE communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 10 :

L'Autorité de Protection procède à des contrôles auprès de ORANGE COTE D'IVOIRE, afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 11 :

ORANGE COTE D'IVOIRE est tenue de procéder au paiement des frais de dépôts de demande d'autorisation auprès du Greffe de l'ARTCI, conformément à la Décision n°2016-0201 de l'Autorité de protection de la République de Côte d'Ivoire fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel.

L'Autorité de Protection lui délivrera une facture à cet effet.

Article 12 :

La présente Décision entre en vigueur à compter de la date de sa notification à ORANGE COTE D'IVOIRE.

Article 13 :

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

Fait à Abidjan, le 05 Juillet 2022
En deux (2) exemplaires originaux

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0747

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 5 JUILLET 2022

PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL PAR LA CAISSE NATIONALE DE PREVOYANCE SOCIALE (IPS-CNPS)

L'AUTORITE DE PROTECTION,

Vu la loi n°99-476 du 02 août 1999 portant définition et organisation des Institutions de Prévoyance Sociale ;

Vu la loi n°99-477 du 02 août 1999 portant modification du Code de Prévoyance Sociale ;

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°2015-532 du 20 juillet 2015 portant Code du travail ;

Vu l'ordonnance n°2019-636 du 17 juillet 2019 portant Institution des régimes de prévoyance sociale des travailleurs indépendants ;

Vu l'ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

Vu le décret n°2000-487 du 12 juillet 2000 portant création de l'Institution de Prévoyance Sociale dénommée « Caisse Nationale de Prévoyance Sociale » l'IPS-CNPS ;

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 ;

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 de traitement des données à caractère personnel ;

Vu le décret n°2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le décret n°2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

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 de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le décret n°2020-308 du 04 mars 2020 fixant les modalités de fonctionnement des régimes de prévoyance sociale des travailleurs indépendants ;

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 ;

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 l'arrêté n°2020-065 du 16 juillet 2020 fixant le revenu plancher par catégorie socioprofessionnelles et le revenu plafond du régime social des travailleurs indépendants ;

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 conditions au traitement des données à caractère personnel (DCP) ;

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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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°2019-0494 du Conseil de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

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 de l'activité :

- du correspondant à la protection des données, personnes morales ;
- de formation en matière de protection des données à caractère personnel ;
- d'audit en matière de protection des données à caractère personnel ;

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 données à caractère personnel ;

Vu le rapport d'audit de protection des données personnelles de l'IPS-CNPS ;

Par les motifs suivants :

Considérant que conformément à l'article 53 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, les responsables du traitement doivent procéder à la mise en conformité des traitements qu'ils opèrent avec ladite loi ;

Considérant que pour faciliter cette mise en conformité l'Autorité de protection a, par décision n°2017-0354 du 26 octobre 2017 définit la 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 ;

Considérant que l'IPS-CNPS (Institution de Prévoyance Sociale, Caisse Nationale de Prévoyance Sociale) est une société privée autonome de type particulier, qui demeure sous la tutelle de l'Etat de Côte d'Ivoire, avec pour mission principale : la gestion du régime général obligatoire de prévoyance sociale du secteur privé et assimilé, qui couvre quatre (04) branches de la sécurité sociale que sont les prestations familiales, les accidents du travail et les maladies professionnelles, l'assurance maternité et l'assurance vieillesse. Son siège social est sis à l'Avenue Lamblin au Plateau 01 BP 317 Abidjan 01 ; (+225) 27 20 25 21 00 ;

Considérant que l'IPS-CNPS a saisi l'Autorité de protection d'une demande de mise en conformité ;

Considérant que l'IPS-CNPS a désigné un correspondant à la protection et a procédé à la formation de son personnel ;

Que par ailleurs, l'IPS-CNPS a effectué son audit de protection des données personnelles ;

Considérant les recommandations contenues dans le rapport d'audit de protection des données personnelles ;

Après en avoir délibéré,

DECIDE :

Article 1 :

L'IPS-CNPS est autorisée à effectuer les traitements des données mentionnées dans l'annexe 1 de la présente décision.

Les données non mentionnées dans l'annexe 1 ne devront aucunement faire l'objet d'un quelconque traitement, de la part de l'IPS-CNPS.

Article 2 :

L'IPS-CNPS est autorisée à effectuer les traitements pour les finalités énumérées dans l'annexe 3 de la présente décision.

Article 3 :

L'IPS-CNPS est autorisée à transférer les données autorisées vers les destinations visées dans l'annexe 2 de la présente décision.

Article 4 :

L'IPS-CNPS est autorisée à communiquer les données traitées uniquement aux destinataires habilités, notamment :

- aux agents suivant leurs habilitations ;
- aux notaires, huissiers, avocats,
- aux banques partenaires (Bridge Bank, UBA, SGCI, Banque Atlantique, la BNI, Ecobank),
- aux impôts, hôpitaux partenaires,
- à la Caisse Générale de Retraite des Agents de l'Etat (CGRAE) ;
- au Fonds de Développement de la Formation Professionnelle (FDFP) ;
- à l'IPS-CNAM ;

- aux autorités publiques ivoiriennes habilitées agissant dans le cadre de l'exercice de leurs missions ;
- au Procureur de la république ;
- aux officiers de police judiciaire munis d'une réquisition;
- aux sous-traitants suivant leur domaine d'activités ;
- aux neuf (09) caisses partenaires de la CEDEAO ;
- aux dix-sept (17) caisses partenaires hors CEDEAO, dans les conditions prévues à l'article 5.

Article 5 :

L'Autorité de protection interdit à l'IPS-CNPS de transférer sans autorisation préalable de l'Autorité de protection, les données traitées vers des pays tiers, autres que ceux autorisés.

L'IPS-CNPS est tenue avant tout transfert de données hors de la Côte d'Ivoire, de les stocker sur le territoire de la République de Côte d'Ivoire.

Article 6 :

Conformément à l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, L'IPS-CNPS doit s'assurer que ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle relatives aux traitements de données qu'ils opèrent.

Il incombe à l'IPS-CNPS, ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

Article 7 :

Les traitements de données autorisés dans la présente décision correspondent aux finalités visées dans l'annexe 3 de la présente décision.

Article 8 :

L'IPS-CNPS est tenue de mettre en œuvre les prescriptions énoncées dans l'annexe 4 de la présente décision. Elle le fait dans les délais prévus dans ladite annexe.

La mise en œuvre desdites prescriptions fera l'objet d'un contrôle par l'Autorité de Protection.

L'Autorité de protection délivrera une attestation de conformité à l'IPS-CNPS, lorsque toutes les prescriptions auront été mises en œuvre.

Article 9 :

En application de l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, l'IPS-CNPS est tenue d'établir, pour le compte de l'Autorité de protection, un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

L'IPS-CNPS communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 10 :

L'Autorité de Protection procède à des contrôles auprès de l'IPS-CNPS, afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 11 :

L'IPS-CNPS est tenue de procéder au paiement des frais de dépôts de demande d'autorisation auprès du Greffe de l'ARTCI, conformément à la Décision n°2016-0201 de l'Autorité de protection de la République de Côte d'Ivoire fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel.

L'Autorité de Protection lui délivrera une facture à cet effet.

Article 12 :

La présente Décision entre en vigueur à compter de la date de sa notification à l'IPS-CNPS.

Article 13 :

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

Fait à Abidjan, le 05 Juillet 2022
En deux (2) exemplaires originaux

Le Président

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

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0748

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 5 JUILLET 2022

PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL PAR FARMSTRONG COMMODITIES

L'AUTORITE DE PROTECTION,

Vu la loi n°2010-72 du 30 septembre 2010 portant interdiction de la traite et les pires formes de travail des enfants en Côte d'Ivoire ;

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°2014-390 du 20 juin 2014 d'orientation sur le développement durable ;

Vu la loi n°2015-532 du 20 juillet 2015 portant Code du travail ;

Vu la loi n°2015-537 du 20 juillet 2015 d'orientation agricole de Côte d'Ivoire ;

Vu l'ordonnance n°2000-583 du 17 août 2000 fixant les objectifs de l'action économique de l'Etat en matière de commercialisation de café et du cacao modifiée par l'ordonnance n°2001-46 du 31 janvier 2001 ;

Vu l'ordonnance n°2001-46 du 31 janvier 2001 modifiant l'article 11 de l'ordonnance n°2000-583 du 17 août 2000 fixant les objectifs économiques de l'action de l'Etat en matière de commercialisation du café et du cacao ;

Vu l'ordonnance n°2001-47 du 31 janvier 2001 relative à la redevance professionnelle en matière de café et de cacao ;

Vu l'ordonnance n°2001-666 du 24 octobre 2001 modifiant l'ordonnance n°2000-583 du 17 août 2000 fixant les objectifs économiques de l'action de l'Etat en matière de commercialisation du café et du cacao ;

Vu l'ordonnance n°2008-225 du 05 août 2008 portant aménagement du taux du Droit proportionnel d'enregistrement sur les actes de confirmation de vente de café et cacao ;

Vu l'ordonnance n°2008-259 du 19 septembre 2008 modifiant et complétant l'ordonnance n°2000-583 du 17 août 2000 fixant les objectifs de l'action économique de l'Etat en matière de commercialisation du café et du cacao, telle que modifiée par les ordonnances n ° 2001-46 du 31 janvier 2001 et n ° 2001-666 du 24 octobre 2001 ;

Vu l'ordonnance n°2011-481 du 28 décembre 2011 fixant les règles relatives à la commercialisation du café et du cacao ;

Vu l'ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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 ;

Vu le décret n°2012-1008 du 17 octobre 2012 fixant les modalités de commercialisations du cacao et du café ;

Vu le décret n°2012-1009 du 17 octobre 2012 fixant les conditions d'exercice de la profession d'acheteur de produits café et cacao ;

Vu le décret n°2012-1010 du 17 octobre 2012 règlementant la profession d'exportateur de café et de cacao ;

Vu le décret n°2012-1011 du 17 octobre 2012 fixant les modalités de conditionnement du cacao à l'exportation ;

Vu le décret n°2012-1012 du 17 octobre 2012 fixant les modalités de conditionnement des cafés verts à l'exportation ;

Vu le décret n°2012-1013 du 17 octobre 2012 relatif à la tierce détention en matière de café-cacao ;

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°2014- 290 du 21 mai 2014 portant application de la loi n°2010-272 du 30 septembre 2010 portant interdiction de la traite et les pires formes de travail des enfants en côte d'Ivoire ;

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°2017-321 du 24 mai 2015 relatif à la mise en œuvre des projets de certification et de programmes de durabilité dans la filière café-cacao ;

Vu le décret n°2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le décret n°2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

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 de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

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 ;

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 l'arrêté n°2017-016 MPS/CAB du 02 juin 2017 déterminant la liste des travaux légers autorisés aux enfants dont l'âge est compris entre treize (13) et seize (16) ans ;

Vu l'arrêté n°444/MINADER/CAB du 25 juillet 2018 déterminant la liste de manquements donnant lieu au retrait de l'agrément pour la mise en œuvre des projets de certification et de programmes de durabilité dans la filière Café-Cacao, ainsi que pour l'achat du café ou du cacao certifié ou durable ;

Vu l'arrêté n°445/MINADER/CAB du 25 juillet 2018 déterminant les mentions devant figurer dans les contrats relatifs à la mise en œuvre des projets de certification et de programmes de durabilité dans la filière Café-Cacao ;

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 conditions au traitement des données à caractère personnel (DCP) ;

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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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°2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

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 de l'activité :

- du correspondant à la protection des données, personnes morales ;
- de formation en matière de protection des données à caractère personnel ;
- d'audit en matière de protection des données à caractère personnel ;

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 données à caractère personnel ;

Vu le rapport d'audit de protection des données personnelles de FARMSTRONG COMMODITIES ;

Par les motifs suivants :

Considérant que conformément à l'article 53 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, les responsables du traitement doivent procéder à la mise en conformité des traitements qu'ils opèrent avec ladite loi ;

Considérant que pour faciliter cette mise en conformité l'Autorité de protection a, par décision n°2017-0354 du 26 octobre 2017 définit la 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 ;

Considérant que Farmstrong Commodities est une société à responsabilité limitée unipersonnelle exerçant dans le développement durable.

Considérant que Farmstrong Commodities a pour objectif de déployer des solutions pour l'amélioration des conditions de vie des planteurs et de leur famille, ainsi que le développement des matières agricoles.

Considérant que Farmstrong Commodities dont le siège social est sis à la Riviera Palmeraie Boulevard Triangle, 25 BP 981 Abidjan 25, téléphone (+225) 27 31 62 19 18/ 07 79 95 72 11, a saisi l'Autorité de protection d'une demande de mise en conformité ;

Considérant que Farmstrong Commodities a désigné un correspondant à la protection et a procédé à la formation de son personnel ;

Que par ailleurs, Farmstrong Commodities a effectué son audit de protection des données personnelles ;

Considérant les recommandations contenues dans le rapport d'audit de protection des données personnelles ;

Après en avoir délibéré,

DECIDE :

Article 1 :

Farmstrong Commodities est autorisée à effectuer les traitements des données mentionnées dans l'annexe 1 de la présente décision.

Les données non mentionnées dans l'annexe 1 ne devront aucunement faire l'objet d'un quelconque traitement, de la part de Farmstrong Commodities.

Article 2 :

Farmstrong Commodities est autorisée à effectuer les traitements énumérés dans l'annexe 3 de la présente décision.

Article 3 :

Farmstrong Commodities est autorisée à transférer vers la Suisse, les données énumérées dans l'annexe 2 de la présente décision.

Article 4 :

Farmstrong Commodities est autorisée à communiquer les données traitées uniquement aux destinataires habilités, notamment :

- les services internes de Farmstrong Commodities suivant leur niveau d'habilitation et partenaires des projets ;
- le siège de Farmstrong Commodities en Suisse ;
- au Conseil du Café Cacao ;

- les autorités publiques ivoiriennes habilitées agissant dans le cadre de l'exercice de leurs missions ;
- le Procureur de la république ;
- les officiers de police judiciaire munis d'une réquisition;
- ASCOMA et AMSA assurances ;
- les sous-traitants suivant leur domaine d'activités.

Article 5 :

L'Autorité de protection interdit à Farmstrong Commodities de transférer sans autorisation préalable de l'Autorité de protection, les données traitées vers des pays tiers, autre que la Suisse.

Farmstrong Commodities est tenue avant tout transfert de données hors de la Côte d'Ivoire, de les stocker sur le territoire de la République de Côte d'Ivoire.

Article 6 :

Conformément à l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, Farmstrong Commodities doit s'assurer que ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle relatives aux traitements de données qu'ils opèrent.

Il incombe à Farmstrong Commodities ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

Article 7 :

Les traitements de données autorisés dans la présente décision correspondent aux finalités listées dans l'annexe 3 de la présente décision.

Article 8 :

Farmstrong Commodities est tenue de mettre en œuvre les prescriptions énoncées dans l'annexe 4 de la présente décision. Elle le fait dans les délais prévus dans ladite annexe.
La mise en œuvre desdites prescriptions fera l'objet d'un contrôle par l'Autorité de Protection.

L'Autorité de protection délivrera une attestation de conformité à Farmstrong Commodities lorsque toutes les prescriptions auront été mises en œuvre.

Article 9 :

En application de l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, Farmstrong Commodities est tenue d'établir, pour

le compte de l'Autorité de protection, un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

Farmstrong Commodities communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 10 :

L'Autorité de Protection procède à des contrôles auprès Farmstrong Commodities, afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 11 :

Farmstrong Commodities est tenue de procéder au paiement des frais de dépôts de demande d'autorisation auprès du Greffe de l'ARTCI, conformément à la décision n°2016-0201 de l'Autorité de protection de la République de Côte d'Ivoire fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel.

L'Autorité de Protection lui délivrera une facture à cet effet.

Article 12 :

La présente Décision entre en vigueur à compter de la date de sa notification à Farmstrong Commodities.

Article 13 :

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

Fait à Abidjan, le 05 Juillet 2022
En deux (2) exemplaires originaux

Le Président

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

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0800

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

EN DATE DU 17 NOVEMBRE 2022

PORTANT AVERTISSEMENT ET MISE EN DEUMEURE DE L'HÔTEL TIAMA EN MATIERE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Conseil de Régulation : 31 Av Nogués, 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 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 l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication ;

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°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°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°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 de 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 l'Arrêté n° 003 du 24 mars 2022 portant nomination des Membres de la Commission Nationale de Classement des Etablissements de Tourisme ;

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°2017-354 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°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°2022-0738 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 05 mai 2022 portant approbation de la liste des contrôles en matière de Protection des données à caractère personnel pour l'année 2022

Vu le Procès-verbal de contrôle n° 001/07/2022 du mardi 12 juillet 2022 ;

I. Faits et procédure

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 ;

Qu'en application de l'article 9 de la décision précité, l'Autorité de Protection a par décision n°2022-0738 en date du 05 mai 2022 portant approbation de la liste des contrôles en matière de Protection des données à caractère personnel pour l'année

2022 identifié l'Hôtel TIAMA comme entreprise à contrôler au titre de l'exercice 2021-2022

Considérant que l'Hôtel TIAMA est un établissement hôtelier de cent trente-sept (137) chambres situées à Abidjan, dans la commune du Plateau, en face du Commissariat du 1er arrondissement du Plateau ;

Que le 12 juillet 2022, les agents assermentés de l'Autorité de Protection ont mené une opération de contrôle sur place au sein des locaux de l'Hôtel TIAMA.

Que cette mission avait pour objet de vérifier le respect par l'Hôtel TIAMA de l'ensemble des dispositions de la Loi n°2013-450 du 19 juin 2013 relative à la Protection des données à caractère personnel.

Qu'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 les sous-traitants de l'Hôtel TIAMA.

Considérant qu'à l'issue du contrôle, la copie du procès-verbal n° 001-07/2022 contradictoirement dressé a été remise à l'Hôtel TIAMA.

II. Motifs de la Décision :

A) Sur le manquement à l'obligation de conformité avec la Loi n°2013-450 du 19 juin 2013 relative à la Protection des données personnelles

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 personnelles 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 Responsable 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 personnelles dispose que : « (...) la demande de mise en conformité est adressée à l'Autorité de Protection » ;

Considérant qu'au moment du contrôle sur place, l'Hôtel TIAMA n'avait introduit aucune demande de mise en conformité et ne disposait pas d'autorisation de traitement 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 personnelles ;

L'Autorité de Protection considère que l'Hôtel TIAMA n'a pas respecté les dispositions des articles 53 de la Loi n°2013-450 du 19 juin 2013 relative à la Protection des données à caractère personnel et les dispositions des articles 2 et 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.

B) Sur le manquement à l'obligation d'obtenir une autorisation de traitement

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 qu'en l'espèce, l'Hôtel TIAMA collecte et stocke entre autres données à caractère personnel, le numéro de téléphone, les numéros de plaque d'immatriculation, les images des visiteurs et des membres de son personnel ;

Qu'en application des dispositions précitées, lesdits traitements doivent être autorisés par l'Autorité de Protection, pour être mis en œuvre ;

Considérant que lors du contrôle, le Responsable du traitement n'a pu fournir les autorisations pour les traitements de données à caractère personnel effectués dans le cadre de ces activités ;

L'Autorité de Protection considère que l'Hôtel TIAMA n'a pas respecté les dispositions de l'article 7 précité.

C) 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, l'Hôtel TIAMA n'a pu fournir la preuve du recueil du consentement des clients, des salariés et des fournisseurs ;

Considérant par ailleurs que lors du contrôle, l'Hôtel TIAMA n'a pu fournir un motif de dérogation 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 ne satisfont pas au principe de la légitimité.

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'Hôtel TIAMA a indiqué que:

- les données de la vidéosurveillance sont conservées pendant une durée de trois (03) mois ;
- les données biométriques sont conservées indéfiniment ;
- les données des agents et salariés de l'Hôtel TIAMA sont conservées indéfiniment ;
- les registres d'accès des visiteurs sont conservés pendant une durée dix (10) ans.

Considérant que l'Hôtel TIAMA n'a pu fournir à l'Autorité de Protection, les durées de conservation pour tous les autres traitements de données personnelles effectués ;

Dès lors, l'Autorité de Protection, au regard de la nature des données traitées considère que les durées de conservation évoquées sont excessives.

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, l'Hôtel TIAMA a indiqué collecter les données biométriques pour la gestion des absences et des présences, la paie du personnel interne et externe, la gestion des incendies ;

Considérant que l'article 3 du décret n°2018-454 du 09 mai 2018 relatif au Registre National des Personnes Physiques, dispose que l'authentification des données biographiques et biométriques des personnes physiques relève de la compétence exclusive de l'Office National de l'Etat Civil et de l'Identification (ONECI) ;

Conformément à l'article 3 du décret n°2018-454 du 09 mai 2018 relatif au Registre National des Personnes Physiques, l'authentification et le stockage des données biométriques relèvent exclusivement de la compétence de l'Office National de l'Etat Civil et de l'Identification (ONECI) ;

Considérant que le recours à un dispositif de biométrie doit avant tout répondre à un véritable impératif de sécurité et cela lorsqu'il n'y a plus d'autre alternative ;

Que la biométrie ne doit, par conséquent, être utilisée qu'en dernier recours, lorsqu'il n'existe aucun autre moyen pour atteindre les finalités du traitement envisagé ;

Considérant que lors du contrôle, l'Hôtel TIAMA a indiqué l'existence d'une dérogation (utilisation de codes) pour les personnes à empreintes réduites ;

Considérant que l'utilisation de la biométrie pour le contrôle de présence des travailleurs et la paie n'est pas nécessaire parce qu'elle présente des risques majeurs d'atteinte à la vie privée ;

Considérant que l'utilisation de la biométrie n'est ni nécessaire ni proportionnée pour atteindre la finalité envisagée ;

En conséquence, l'Autorité de Protection considère comme disproportionné le traitement des données biométriques pour le pointage des travailleurs et la paie et prescrit à l'Hôtel TIAMA d'utiliser d'autres moyens moins intrusifs notamment le pointage par badge ou par code.

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 identifiés ;

Considérant qu'à l'issue du contrôle, l'Hôtel TIAMA indique que les destinataires des données traitées sont les suivants :

- Le superviseur, les pompiers, le responsable technique pour la vidéosurveillance ;
- Le service des Ressources Humaines et Comptabilité pour les données biométriques et les données des ressources humaines ;

- Les services de police auxquels sont communiquées les données des clients de l'hôtel ;

Considérant que les destinataires internes et externes mentionnés dans le procès-verbal de contrôle sont insuffisants ;

Considérant que les destinataires externes des données des Ressources humaines et des clients de l'Hôtel TIAMA ne sont pas clairement identifiés ;

Considérant qu'en cas d'incident sur le logiciel AMADEUS, la société AMADEUS SENEGAL est sollicitée pour une prise en main ;

Considérant que le logiciel QUALIPRO est détenu par la société SAPHIR CONSULT qui en assure la maintenance et est basée en Tunisie ;

Considérant que les interventions à distance de AMADEUS SENEGAL et SAPHIR CONSULT constituent des transferts de données ;

Considérant que l'Hôtel TIAMA ne dispose pas d'autorisations de transferts de données ;

L'Autorité de Protection considère que les destinataires ou catégories de destinataires habilités à recevoir communication des données ne sont pas clairement identifiés.

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 :

- 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 :

- l'identité du Responsable du traitement et le cas échéant, celle de son représentant dûment mandaté ;
- le fait que l'Hôtel TIAMA soit placé sous vidéosurveillance ;
- la finalité du traitement;
- les catégories de données concernées ;
- les destinataires auxquels les données sont susceptibles d'être communiquées;
- l'existence et des modalités d'exercice des droits de la personne concernée;
- la durée de conservation des données ;
- le numéro de l'Autorisation délivrée par l'Autorité de Protection.

Considérant que nulle part dans l'Hôtel, il n'a été observé l'existence d'une affiche informant les clients, salariés et visiteurs sur les traitements effectués par l'Hôtel TIAMA ;

Que les fiches d'hébergement, de réservation et de collecte d'informations ne comportent aucune mention relative à la Protection des données personnelles ;

Qu'en outre les mentions légales et politique de confidentialité figurant sur le site internet de l'Hôtel TIAMA sont celles de Google ;

Que par ailleurs, ces mentions légales sont difficilement accessibles aux personnes concernées ;

Considérant que l'Hôtel TIAMA a installé un dispositif de vidéosurveillance ;

Considérant que l'Hôtel TIAMA ne dispose pas d'affiches ou de pictogrammes contenant les mentions ci-dessus évoquées ;

Considérant que l'Hôtel TIAMA ne dispose pas d'autorisation de traitement de données à caractère personnel pour la vidéosurveillance ;

Par conséquent, l'Autorité de Protection considère que l'Hôtel TIAMA ne respecte pas l'obligation de transparence imposée par la Loi n°2013-450 du 19 juin 2013 relative à la Protection des données à caractère personnel.

H) Sur le dispositif biométrique

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 des données à caractère personnel comportant des données biométriques est soumis à autorisation préalable de l'Autorité de Protection, avant toute mise en œuvre ;

Considérant que l'Hôtel TIAMA ne dispose pas d'autorisation de traitement pour le dispositif de biométrie ;

Considérant qu'au moment du contrôle, aucune formalité préalable n'a été effectuée par l'Hôtel TIAMA ;

Par conséquent, l'Autorité de Protection considère que le traitement effectué au moyen de la biométrie n'est pas conforme à la loi n°2013-450 du 19 juin 2013 relative à la Protection des données à caractère personnel.

I) Sur la gestion des ressources humaines

Considérant que les ressources humaines de l'Hôtel TIAMA utilisent le logiciel de paie « PROGEPA » et que la maintenance est assurée par le cabinet CAP SARL ;

Considérant que l'application utilisée pour le pointage est KELYO et développée par la société BODET ;

Considérant que l'Hôtel TIAMA ne dispose pas d'autorisation de traitement de données pour les ressources humaines ;

Considérant que les applications utilisées ne sont pas conformes aux dispositions de la loi n°2013-450 du 19 juin 2013 relative à la Protection des données à caractère personnel ;

L'Autorité de Protection considère que les traitements effectués pour gestion des ressources humaines ne sont pas conformes à la loi n° n°2013-450 du 19 juin 2013 relative à la Protection des données à caractère personnel.

J) 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 l'Hôtel TIAMA dispose d'un registre de plaintes des clients, d'une fiche de réservation, annulation et modification, d'un cahier de réservation pour les navettes ;

Que toutefois, l'Hôtel TIAMA ne dispose pas d'une procédure de gestion des droits des personnes concernées ;

Considérant les articles 9 et 12 de la loi n°2013-450 du 19 juin 2013 relative à la Protection des données à caractère personnel ;

Considérant que les clients et les salariés n'ont pas connaissance des droits des personnes concernées ;

Considérant que l'Hôtel TIAMA ne dispose pas de Correspondant à la Protection ;

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

K) 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 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 l'Hôtel TIAMA a recours aux applications et sous-traitants suivants :

- la maintenance de la vidéosurveillance par la société IT HOSPITALITY ;
- la maintenance du dispositif biométrique par la société GSS (Gestion des Systèmes de Sécurité) ;
- l'application KELYO utilisée pour le pointage biométrique et développée par la société BODET ;
- le logiciel de paie PROGEPA dont la maintenance assurée par le cabinet CAP SARL ;
- le logiciel AMADEUS pour les réservations des clients dont la maintenance est assurée par AMADEUS SENEGAL ;
- le logiciel QUALIPRO utilisé pour la gestion des plaintes et détenu par la société SAPHIR CONSULT basée en Tunisie ;
- l'application MAILCHIMP pour la newsletter ;
- la société GSIA qui assure la sécurité physique et détient un registre d'accès des visiteurs ;

Considérant qu'aucun des sous-traitants ci-dessus cités ne disposent d'autorisation de traitement de données et ne sont pas conformes à la loi n°2013-450 du 19 juin 2013 relative à la Protection des données à caractère personnel ;

Considérant qu'aucun des responsables du traitement ci-dessus cités n'a débuté son processus de mise en conformité avec la loi n°2013-450 du 19 juin 2013 relative à la Protection des données à caractère personnel.

Considérant que le contrôle a révélé des insuffisances en termes de sécurité du système d'information, notamment :

- L'inexistence de politiques de sécurité du système d'information, de gestion des mots de passe, de gestion des accès et des habilitations ;

- L'utilisation sur les postes de travail et les applications de mots de passe faibles, sans durée de validité limitée ;
- Le partage de mots de passe entre plusieurs administrateurs ;
- L'absence de système automatisé de détection et de suppression des données au-delà des durées de conservation ;
- La faiblesse des mesures de Protection physique de la salle serveur.

L'Autorité de Protection considère que les mesures de sécurité mises en œuvre sont insuffisantes.

Considérant enfin que l'Autorité de Protection, à travers le contrôle effectué constate :

- **L'absence d'autorisation de traitement de données pour l'Hôtel TIAMA ;**
- **L'absence de mise en conformité à la loi relative à la Protection des données à caractère personnel pour l'Hôtel TIAMA ;**
- **L'absence de garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements à effectuer par les sous-traitants ;**
- **Le non-respect des principes liés à la Protection des données à caractère personnel par l'Hôtel TIAMA et ses sous-traitants ;**
- **Le non-respect des principes de la légitimité, de la proportionnalité, de la durée limitée de la conservation des données, droits des personnes concernées, de la transparence ;**
- **Le non-respect de l'information des personnes concernées et de la transparence ;**
- **La méconnaissance du personnel de l'Hôtel TIAMA en matière de Protection des données personnelles ;**
- **L'absence d'autorisation pour le dispositif de vidéosurveillance ;**
- **L'absence d'autorisation pour le dispositif de biométrique ;**
- **L'inexistence d'affiche ou de pictogramme pour la vidéosurveillance ;**
- **L'absence de procédure relative aux droits des personnes concernées ;**
- **L'absence de preuve garantissant le respect de la Protection des données personnel traitées par les logiciels utilisés au sein de l'Hôtel TIAMA ;**
- **Les transferts de données à caractère personnel non autorisés vers le SENEGAL et la TUNISIE ;**
- **La non-désignation du correspondant à la Protection des données à caractère personnel.**

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 l'Hôtel TIAMA :

- 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 se mettre en conformité** avec la loi n°2013-450 du 19 juin 2013 relative à la Protection des données à caractère personnel **dans les soixante (60) jours à compter de la réception de la présente décision.**

Article 2 :

L'Hôtel TIAMA est tenu de désigner un correspondant à la Protection des données conformément aux dispositions de la loi n°2013-450 du 19 juin 2013 relative à la Protection des données à caractère personnel et de 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 dans **les trente (30) jours** à compter de la réception de la présente.

Article 3 :

Si l'Hôtel TIAMA ne s'est pas conformé à la présente mise en demeure, 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.

Article 4 :

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 5 :

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

Article 6 :

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 dans le journal officiel de la République.

Fait à Abidjan, le 17 Novembre 2022
En deux (2) exemplaires originaux

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

DECISION N°2022-0801

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

EN DATE DU 17 NOVEMBRE 2022

PORTANT AVERTISSEMENT ET MISE EN DEMEURE DU CABINET CIFIP EN MATIERE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Conseil de Régulation : 31 Av Nogués, 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 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 l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication ;

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°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°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°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 de 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°2017-354 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°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°2022-0738 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 05 mai 2022 portant approbation de la liste des contrôles en matière de protection des données à caractère personnel pour l'année 2022

Vu le Procès-verbal de contrôle n° 002/07/2022 du Jeudi 14 juillet 2022 ;

I. Faits et procédure

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 ;

Qu'en application de l'article 9 de la décision précité, l'Autorité de Protection a par décision n°2022-0738 en date du 05 mai 2022 portant approbation de la liste des contrôles en matière de protection des données à caractère personnel pour l'année 2022 identifié le Cabinet CIFIP comme entreprise à contrôler au titre de l'exercice 2021-2022

Considérant que le cabinet CIFIP est un cabinet spécialisé dans la formation, le recrutement, le bilan professionnel et le conseil en gestion stratégique en ressources humaines, situé dans la commune de Cocody Vallon ;

Que le 12 juillet 2022, les agents assermentés de l'Autorité de Protection ont mené une opération de contrôle sur place au sein des locaux du Cabinet CIFIP.

Que cette mission avait pour objet de vérifier le respect par le Cabinet CIFIP de l'ensemble des dispositions de la Loi n° 2013-450 du 19 juin 2013 relative à la Protection des données à caractère personnel.

Qu'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 les sous-traitants du Cabinet CIFIP.

Considérant qu'à l'issue du contrôle, la copie du procès-verbal n° 002-07/2022 contradictoirement dressé et signé a été remise au Cabinet CIFIP.

II. Motifs de la Décision :

A. Sur le manquement à l'obligation de conformité avec la Loi n°2013-450 du 19 juin 2013 relative à la protection des données personnelles

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 personnelles 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 personnelles 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, le cabinet CIFIP n'avait introduit aucune demande de mise en conformité et ne disposait pas d'autorisation de traitement 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 personnelles ;

Considérant qu'au moment du contrôle effectué par l'Autorité de Protection, le cabinet CIFIP a communiqué une liste de formation et d'audit datée du 10 juin 2022, réalisée par un cabinet d'accompagnement ;

L'Autorité de Protection considère que le cabinet CIFIP n'a pas respecté les dispositions des articles 53 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données personnelles et les dispositions des articles 2 et 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 personnelles.

B. Sur le manquement à l'obligation d'obtenir une autorisation de traitement

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 qu'en l'espèce, le cabinet CIFIP collecte et stocke entre autres données à caractère personnel, le numéro de téléphone, les Curriculum Vitae des postulants et des membres de son personnel ;

Qu'en application des dispositions précitées, lesdits traitements doivent être autorisés par l'Autorité de Protection, pour être mis en œuvre ;

Considérant que lors du contrôle, le Responsable du traitement n'a pu fournir les autorisations de traitement pour les points de contrôles effectués ;

L'Autorité de Protection considère que le cabinet CIFIP n'a pas respecté les dispositions de l'article 7 précité.

C. 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, le cabinet CIFIP n'a pu fournir la preuve du recueil du consentement des clients, des salariés et des fournisseurs ;

Considérant par ailleurs que lors du contrôle, le cabinet CIFIP n'a pu fournir un motif de dérogation 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 dans les points de contrôle ne satisfont pas au principe de la légitimité ;

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, le cabinet CIFIP a indiqué que :

- les dossiers physiques des candidats retenus et non retenus sont conservés pendant deux (02) à trois (03) ans dans des cartons d'archives dans les armoires des salles d'entretien ;

- les documents sont confiés à la société « LASSIRE DECHETS SERVICE (LDS) pour les opérations d'enlèvement et de destruction par incinération sous la supervision du CIAPOL, à l'expiration du délai de conservation ;

- les fiches de présence pour les formations sont conservées indéfiniment ;

- les données des agents et salariés du cabinet CIFIP sont conservés selon une durée indéfinie ;

- les données numériques des candidats sont conservées indéfiniment ;

- les boites de messagerie sont supprimées immédiatement au départ du salarié de l'entreprise.

Considérant que les durées de conservation des dossiers physiques des candidats retenus et non retenus et des agents et salariés du cabinet CIFIP sus mentionnées sont excessives au regard des finalités pour lesquelles elles sont collectées ;

Considérant que la suppression immédiate des boites de messagerie des salariés au départ du salarié de l'entreprise ne constitue pas une bonne pratique au regard de la pratique décisionnelle de l'ARTCI ;

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

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

Considérant que selon 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 identifiés ;

Considérant qu'à l'issue du contrôle, le cabinet CIFIP indique que les destinataires des données traitées sont les suivants :

- le Directeur Général de CIFIP qui occupe également les fonctions de Responsable du Département formation et de Responsable des Ressources Humaines ;
- le partenaire Central Test basé en France pour les tests psychotechniques ;
- les clients auxquels sont communiqués les dossiers des candidats retenus ;
- les directeurs des Ressources Humaines des entreprises clientes en Côte d'Ivoire et (hors période COVID) en Afrique du Nord, Afrique Centrale et en Europe ;
- la société « LASSIRE DECHETS SERVICE (LDS) pour les opérations d'enlèvement et de destruction par incinération sous la supervision du CIAPOL ;
- la société SIGEXCI, Cabinet d'expertise comptable chargée de la paie des salariés ;
- la société ASCOMA pour l'assurance maladie du personnel de CIFIP ;
- la BICICI pour les virements des salaires des agents de CIFIP ;

Considérant que les destinataires internes mentionnés dans le procès-verbal de contrôle sont insuffisants ;

Considérant que les destinataires externes des données des Ressources humaines du cabinet CIFIP ne sont pas clairement identifiés ;

Considérant que le cabinet CIFIP ne dispose pas d'autorisations de transferts de données pour les données communiquées au partenaire Central Test pour les tests psychotechniques en France ;
L'Autorité de Protection considère que les destinataires ou catégories de destinataires habilités à recevoir communication des données ne sont pas clairement identifiés.

F) 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 :

- 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.

Considérant que le cabinet CIFIP ne dispose pas d'affiches ou de pictogrammes contenant les mentions ci-dessus évoquées ;

Considérant que nulle part dans le cabinet CIFIP, il n'a été observé l'existence d'une affiche informant les clients, salariés et visiteurs sur les traitements effectués par le cabinet CIFIP ;

Considérant que lors du contrôle, le Cabinet CIFIP n'a pu fournir la preuve du respect des dispositions précitées à l'endroit des personnes concernées ;

Considérant que le cabinet CIFIP ne dispose pas d'affiches ou de mentions sur les formulaires de candidatures mise à disposition des candidats ;

Par conséquent, l'Autorité de Protection considère que le Cabinet CIFIP ne respecte pas l'obligation de transparence imposée par la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

G) 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 le Cabinet CIFIP ne dispose pas d'une procédure de gestion des droits des personnes concernées ;

Considérant les articles 9 et 12 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Considérant que les clients et les salariés n'ont pas connaissance des droits des personnes concernées ;

Considérant que le Cabinet CIFIP ne dispose pas de Correspondant à la protection ;

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

H) 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 choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique 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 cabinet CIFIP a recours aux sous-traitants suivants :

- la société « LASSIRE DECHETS SERVICE (LDS) pour les opérations d'enlèvement et de destruction par incinération sous la supervision du CIAPOL ;
- la société SIGEXCI, Cabinet d'expertise comptable chargée de la paie des salariés ;
- la société ASCOMA pour l'assurance maladie du personnel de CIFIP ;
- le Central Test basé en France pour les tests psychotechniques ;

Considérant qu'aucun des sous-traitants ci-dessus cités ne dispose d'autorisation de traitement de données et n'est pas conforme à la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Considérant que le contrôle a révélé des insuffisances en termes de sécurité du système d'information, notamment :

- l'inexistence de politiques de sécurité du système d'information, de gestion des mots de passe, de gestion des accès et des habilitations ;
- l'utilisation sur les postes de travail et les applications de mots de passe faibles, sans durée de validité appropriée ;
- l'utilisation d'un système de login sans double authentification pour l'accès à la messagerie servant de banque de Curriculum Vitae ;
- l'absence de mentions d'information et de recueil du consentement sur le site internet de CIFIP ;

L'Autorité de Protection considère que les mesures de sécurité mises en œuvre sont insuffisantes.

Considérant enfin que l'Autorité de Protection, à travers le contrôle effectué constate :

- **L'absence d'autorisation de traitement de données pour le cabinet CIFIP ;**
- **L'absence de mise en conformité à la loi relative à la protection des données à caractère personnel pour le cabinet CIFIP ;**
- **L'absence de garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements à effectuer par les sous-traitants ;**
- **Le non-respect des principes liés à légitimité, de la durée limitée de la conservation des données, droits des personnes concernées, de la transparence ;**
- **Le non-respect de l'information des personnes concernées et de la transparence ;**
- **L'absence de procédure relative aux droits des personnes concernées ;**
- **Les transferts de données non autorisés vers la France ;**
- **La non-désignation du correspondant à la protection des données à caractère personnel ;**
- **L'insuffisance des mesures de sécurité et de confidentialité des données.**

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 du cabinet CIFIP :

- **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 se mettre en conformité** avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel **dans les soixante (60) jours à compter de la réception de la présente décision.**

Article 2 :

Le cabinet CIFIP est tenu de désigner un correspondant à la protection des données conformément aux dispositions de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel et de 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 dans **les trente (30) jours** à compter de la réception de la présente.

Article 3 :

Si le cabinet CIFIP ne s'est pas conformé à la présente mise en demeure, 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.

Article 4 :

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 5 :

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

Article 6 :

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 17 Novembre 2022
En deux (2) exemplaires originaux

Le Président

ARTCI

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

SMC

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0802

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 17 NOVEMBRE 2022

PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL PAR LA SOCIETE MANSA BANK COTE D'IVOIRE

Conseil de Régulation : 31 Av Nogués, 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 Économique et Monétaire Ouest Africaine (UEMOA) ;

Vu l'Acte Uniforme révisé de 2014 relatif au Droit des sociétés commerciales et du groupement d'intérêt économique ;

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°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 l'Ordonnance 2009-385 du 1er Décembre 2009 portant réglementation bancaire ;

Vu l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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°2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

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°2021-911 du 22 décembre 2021 portant adoption d'un cadre commun d'architecture référentiel de données ;

Vu le Décret n°2021-915 du 22 décembre 2021 portant adoption politique de sécurité et système d'information administrative publique ;

Vu le Décret n°2021-916 du 22 décembre 2021 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) & PPIC ;

Vu le Décret n°2022-265 du 13 avril 2022 portant nomination du Directeur Général de l'Autorité de Régulation des Télécommunications 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 de 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°2014-0021 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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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 de l'activité :

- du correspondant à la protection des données, personnes morales ;
- de formation en matière de protection des données à caractère personnel ;
- d'audit en matière de protection des données à caractère personnel ;

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 de données à caractère personnel ;

Par les motifs suivants :

Considérant que conformément à l'article 53 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, les responsables du traitement doivent procéder à la mise en conformité des traitements qu'ils opèrent avec ladite loi ;

Considérant que pour faciliter cette mise en conformité, l'Autorité de protection a, par décision n°2017-0354 du 26 octobre 2017, définit la 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 ;

Considérant que la société MANSA BANK COTE D'IVOIRE, Société Anonyme de droit ivoirien avec Conseil d'Administration, au capital de 15 707 650 000 FCFA ayant son siège social à Abidjan-Cocody - Riviera Golf 4, 01 BP 6160 Abidjan 01, immatriculée au registre du commerce et du crédit mobilier d'Abidjan sous le numéro CI-ABJ-2017-B-19569 ;

Considérant que la société MANSA BANK COTE D'IVOIRE a désigné un Correspondant, personne physique à la protection, après avoir procédé à la formation de son personnel ;

Que par ailleurs, la société MANSA BANK COTE D'IVOIRE a effectué son audit de situation ;

Considérant les recommandations et les prescriptions faites par l'Autorité de protection ;

Après en avoir délibéré,

DECIDE :

Article 1 :

La société MANSA BANK COTE D'IVOIRE est autorisée à effectuer le traitement de données mentionnées dans l'annexe 1 de la présente décision.

Les données non mentionnées dans l'annexe 1 ne devront aucunement faire l'objet d'un quelconque traitement, de la part de la société MANSA BANK COTE D'IVOIRE.

Article 2 :

La société MANSA BANK COTE D'IVOIRE est autorisée à effectuer les traitements énumérés dans l'annexe 3 de la présente décision.

Article 3 :

La société MANSA BANK COTE D'IVOIRE est autorisée à communiquer les données traitées, uniquement aux destinataires habilités, notamment :

- les services internes de MANSA BANK COTE D'IVOIRE, suivant leurs habilitations;
- les administrations publiques habilitées, dans le cadre de l'exercice de leurs missions ;
- le Procureur de la république ;
- les officiers de police judiciaire munis d'une réquisition ;
- la Banque Centrale des Etats de l'Afrique de l'Ouest ;
- les Bureaux d'Informations Crédit de l'espace UEMOA établis en Côte d'Ivoire ;
- les banques et établissements financiers partenaires ;
- les sous-traitants du fait de leurs contrats de prestations ;
- les Avocats et intermédiaires de justice ;
- le Fonds pour le Développement de la Formation Professionnelle (FDFP) ;
- la Cellule Nationale du Traitement de l'Information Financière (CENTIF) ;
- la Caisse nationale de prévoyance sociale (CNPS) ;
- la Direction Générale des Impôts (DGI) ;
- la Direction Générale de la Douane ;
- l'Inspection du travail ;
- les Cabinets de formation en relation contractuelles avec MANSA BANK COTE D'IVOIRE ;
- l'Inspection générale d'Etat ;
- la Commission bancaire ;
- les Commissaires aux comptes ;

- les commissaires de justice ;
- les assurances et courtier en assurance ;
- le Bureau d'Information sur le Crédit (BIC) ;
- le cabinet pour le recouvrement ;
- le Ministère en charge des finances ;
- la Police Economique ;
- le Trésor public (FINEX) ;

Article 4 :

MANSA BANK COTE D'IVOIRE est autorisée à transférer vers le Maroc, la sauvegarde des données énumérées dans l'annexe 2 de la présente décision.

MANSA BANK COTE D'IVOIRE est tenue de rédiger des clauses contractuelles type ou tout autre garantie appropriée pour les transferts de données effectués vers ce pays, et les communiquer à l'Autorité de protection, dès réception de la présente.

Avant tout transfert de données hors de la Côte d'ivoire, la société MANSA BANK COTE D'IVOIRE est tenue de stocker les données visées à l'annexe 2 sur le territoire de la République de Côte d'ivoire.

Article 5 :

Conforment à l'article 40 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la société MANSA BANK COTE D'IVOIRE doit s'assurer que ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle relatives aux traitements de données qu'ils opèrent.

Article 6 :

Les traitements de données autorisés dans la présente décision correspondent aux finalités visées dans l'annexe 3 de la présente décision.

Article 7 :

MANSA BANK COTE D'IVOIRE est tenue de mettre en œuvre les prescriptions énoncées dans l'annexe 4 de la présente décision. Elle le fait dans les délais prévus dans ladite annexe.

La mise en œuvre desdites prescriptions fera l'objet d'un contrôle par l'Autorité de protection.

L'Autorité de protection délivrera une attestation de conformité à MANSA BANK COTE D'IVOIRE, lorsque toutes les prescriptions auront été mises en œuvre.

Article 8 :

En application de l'article 42 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la société MANSA BANK COTE D'IVOIRE est tenue d'établir, pour le compte de l'Autorité de protection, un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

La société MANSA BANK COTE D'IVOIRE communique ce rapport à l'Autorité de protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 9 :

L'Autorité de protection procède à des contrôles auprès de la société MANSA BANK COTE D'IVOIRE, afin de vérifier le respect des dispositions de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 10 :

La société MANSA BANK COTE D'IVOIRE est tenue de procéder au paiement des frais de dépôts de demande d'autorisation auprès du Greffe de l'ARTCI, conformément à la Décision n°2016-0201 de l'Autorité de protection de la République de Côte d'Ivoire fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel.

L'Autorité de protection lui délivrera une facture à cet effet.

Article 11 :

La présente décision entre en vigueur à compter de la date de sa notification à la société MANSA BANK COTE D'IVOIRE.

Article 12 :

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

Fait à Abidjan, le 17 Novembre 2022
En deux (2) exemplaires originaux

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

ARTCI

ARTCI

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0803

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 17 NOVEMBRE 2022

PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL PAR

ADVANS CÔTE D'IVOIRE

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

Vu l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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 ;

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 de 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°2014-0021 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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

Vu la Décision n°2017-0353 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°2017-0354 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 ;

Vu la Décision n°2019-0494 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

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 le Rapport d'audit de protection des données personnelles de ADVANS COTE D'IVOIRE.

Par les motifs suivants :

Considérant que conformément à l'article 53 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, les responsables du traitement doivent procéder à la mise en conformité des traitements qu'ils opèrent avec ladite loi ;

Considérant que pour faciliter cette mise en conformité, l'Autorité de protection a, par décision n°2017-0354 du 26 octobre 2017, définit la 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 ;

Considérant que **ADVANS Côte d'Ivoire,** Société Anonyme au capital social de 6 650 000 000 F CFA, immatriculée au registre du commerce et du crédit mobilier sous le numéro CI-ABJ-2009-B-4691 sise à Abidjan-Marcory, boulevard Brazzaville,01 BP 11825 Abidjan 01, Téléphone : +225 27 21 26 05 68 ; a saisi l'Autorité de protection d'une demande de mise en conformité ;

Considérant qu'ADVANS Côte d'Ivoire est une institution de microfinance qui fournit des produits de crédit et d'épargne ainsi qu'une gamme complète de services financiers.

Considérant que ADVANS Côte d'Ivoire a désigné un Correspondant à la protection et procédé à la formation de son personnel ;

Que par ailleurs, que ADVANS Côte d'Ivoire a effectué son audit de protection des données personnelles ;

Considérant enfin les recommandations contenues dans le rapport d'audit de protection ;

Après en avoir délibéré,

DECIDE :

Article 1 :

ADVANS Côte d'Ivoire est autorisée à effectuer le traitement de données mentionnées dans l'annexe 1 de la présente décision.

Les données non mentionnées dans l'annexe 1 ne devront aucunement faire l'objet d'un quelconque traitement, de la part de ADVANS Côte d'Ivoire.

Article 2 :

ADVANS Côte d'Ivoire est autorisée à communiquer les données traitées, uniquement aux destinataires habilités, notamment :

- les services internes de la société, suivant leurs habilitations ;
- les administrations publiques habilitées, dans le cadre de l'exercice de leurs missions;
- le Procureur de la république ;
- les officiers de police judiciaire munis d'une réquisition ;
- la Banque Centrale des Etats de l'Afrique de l'Ouest ;
- les Bureaux d'Information sur le Crédit établis sur le territoire de la Côte d'Ivoire;
- la Direction de la Microfinance ;
- L'Association Professionnelle des Systèmes Financiers Décentralisés ;
- les Avocats et intermédiaires de justice

Article 3 :

ADVANS Côte d'Ivoire est autorisée à transférer, les données énumérées dans l'annexe 2 de la présente décision, vers **ADVANS INTERNATIONAL PARIS** en France.

Tout autre transfert est soumis à l'autorisation préalable de l'Autorité de Protection.

ADVANS Côte d'Ivoire est tenue de rédiger des clauses contractuelles type ou toute autre garantie appropriée pour les transferts de données effectués vers la France, et les communiquer à l'Autorité de protection.

Avant tout autre transfert de données hors de la Côte d'Ivoire, ADVANS Côte d'Ivoire est tenue de les stocker sur le territoire de la République de Côte d'ivoire.

Article 5 :

Conforment à l'article 40 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, ADVANS Côte d'Ivoire doit s'assurer que ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle relatives aux traitements de données qu'ils opèrent.

Article 6 :

Les traitements de données autorisés dans la présente décision correspondent aux finalités énumérées dans l'annexe 3 de la présente décision.

Article 7 :

ADVANS Côte d'Ivoire est tenue de mettre en œuvre les prescriptions énoncées dans l'annexe 4 de la présente décision. Elle le fait dans les délais prévus dans ladite annexe.

La mise en œuvre desdites prescriptions fera l'objet d'un contrôle par l'Autorité de protection.

L'Autorité de protection délivrera une attestation de conformité à ADVANS Côte d'Ivoire, lorsque toutes les prescriptions auront été mises en œuvre.

Article 8 :

En application de l'article 42 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, ADVANS Côte d'Ivoire est tenue d'établir, pour le compte de l'Autorité de protection, un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

ADVANS Côte d'Ivoire communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 9 :

L'Autorité de protection procède à des contrôles auprès de ADVANS Côte d'Ivoire, afin de vérifier le respect des dispositions de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 10 :

ADVANS Côte d'Ivoire est tenue de procéder au paiement des frais de dépôts de demande d'autorisation auprès du Greffe de l'ARTCI, conformément à la Décision n°2016-0201 de l'Autorité de protection de la République de Côte d'Ivoire fixant les

frais de dossiers et d'agrément en matière de protection des données à caractère personnel.

L'Autorité de protection lui délivrera une facture à cet effet.

Article 11 :

La présente décision entre en vigueur à compter de la date de sa notification à ADVANS Côte d'Ivoire.

Article 12 :

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

Fait à Abidjan, le 17 Novembre 2022
En deux (2) exemplaires originaux

Le Président

ARTCI

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0821

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 22 DECEMBRE 2022

PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE

PERSONNEL PAR LE GROUPE OLAM

Conseil de Régulation : 31 Av Nogués, 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 la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Vu la Loi n° 2010-272 du 20 juillet 2015 portant Code du travail ;

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 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° 2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

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°2021-916 du 22 décembre 2021 portant adoption du référentiel général de sécurité des systèmes d'information et du plan de protection des infrastructures critiques ;

Vu le Décret n°2022-265 du 13 avril 2022 portant nomination du Directeur Général de l'Autorité 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 de 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°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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

Vu 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 ;

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 données à caractère personnel ;

Vu le Rapport d'audit de protection des données personnelles du GROUPE OLAM;

Par les motifs suivants :

Considérant que conformément à l'article 53 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, les responsables du traitement doivent procéder à la mise en conformité des traitements qu'ils opèrent avec ladite loi ;

Considérant que pour faciliter cette mise en conformité l'Autorité de Protection a, par décision n°2017-0354 du 26 octobre 2017, défini la 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 ;

Considérant que le GROUPE OLAM est un ensemble de sociétés de droit ivoirien, filiales ivoiriennes de la multinationale OLAM International Limited, qui est une entreprise alimentaire et agroalimentaire ;

Que le Groupe OLAM ayant son siège social à Treichville, Boulevard de Vridi, Rue des Conteneurs, Face SOCOPAO, Zone portuaire, 01 BP V 215 Abidjan 01, est constitué de deux entités que sont OLAM Food Ingredients (OFI) et OLAM Agri (OGA).

Considérant que le GROUPE OLAM a saisi l'Autorité de Protection d'une demande de mise en conformité ;

Que par ailleurs, le GROUPE OLAM a effectué son audit de protection des données personnelles ;

Considérant les recommandations contenues dans le rapport d'audit de protection des données personnelles ;

Après en avoir délibéré,

DECIDE :

Article 1 :

Le GROUPE OLAM est autorisé à effectuer les traitements des données mentionnées dans l'annexe 1 de la présente décision.

Les données non mentionnées dans l'annexe 1 ne devront aucunement faire l'objet d'un quelconque traitement de la part du GROUPE OLAM.

Article 2 :

Le GROUPE OLAM est autorisé à effectuer les traitements énumérés dans l'annexe 2 de la présente décision.

Article 3 :

Le GROUPE OLAM est autorisé à communiquer les données traitées uniquement aux destinataires habilités notamment :

1. les services internes de la société, suivant leurs habilitations
2. les autorités publiques ivoiriennes habilitées, dans le cadre de l'exercice de leurs missions
3. la maison mère à Singapour, le siège et les filiales du Groupe
4. les Banques
5. les assurances
6. les clients
7. les fournisseurs
8. les partenaires
9. la BCEAO
10. les ambassades
11. la CIE/SODECI
12. les cabinets de traduction et de formation
13. le comité national de surveillance des actions de lutte contre la traite l'exploitation et le travail des enfants (CNS)
14. les sous-traitants
15. le Procureur de la République

16. les officiers de police judiciaire munis d'une réquisition
17. les agents assermentés de l'Autorité de Protection, dans le cadre de leurs missions de contrôle

Article 4 :

Le GROUPE OLAM est autorisé à effectuer des transferts de données à caractère personnel vers Singapour, le Royaume-Uni, l'Inde et les Pays Bas.

Le Groupe OLAM est tenu de soumettre à l'ARTCI, des Règles d'Entreprise Contraignantes (BCR) pour approbation.

Avant tout transfert de données hors de la Côte d'Ivoire, le GROUPE OLAM est tenu de les stocker sur le territoire de la République de Côte d'Ivoire.

Tout autre transfert est soumis à l'autorisation préalable de l'Autorité de Protection.

Article 5 :

Conformément à l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le GROUPE OLAM doit s'assurer que, ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle relatives aux traitements de données qu'ils opèrent.

Il incombe au GROUPE OLAM ainsi qu'à ses clients et sous-traitants, de veiller au respect de ces mesures.

Article 6 :

Les traitements de données autorisés dans la présente décision correspondent aux trente-quatre (34) finalités suivantes :

1. la gestion des programmes de durabilité
2. la gestion du suivi et évaluation
3. la gestion du shipping
4. la localisation des parcelles
5. la gestion juridique
6. la gestion des ressources humaines
7. la gestion administrative
8. la gestion de la logistique
9. la gestion financière
10. la gestion informatique
11. la gestion de la communication
12. la sécurité des biens et des personnes
13. l'installation de système de biométrie OUTSPAN IVOIRE S.A
14. l'installation de système de biométrie OLAM COCOA PROCESSING CI S.A. (site San Pedro)

15. l'installation de système de biométrie OLAM COCOA PROCESSING CI S.A. (site Abidjan)
16. l'installation de système de biométrie MANTRA IVOIRE S.A
17. l'installation de système de biométrie OLAM IVOIRE S.A.(Site Anyama)
18. l'installation de caméras OUTSPAN IVOIRE S.A
19. l'installation de caméras OLAM COCOA PROCESSING CI S.A. (site San-Pedro)
20. l'installation de caméras OLAM COCOA PROCESSING CI S.A. (site Abidjan)
21. l'installation de caméras MANTRA IVOIRE S.A
22. l'installation de caméras OLAM IVOIRE S.A (Site Anyama)
23. la paie du personnel
24. le Recrutement
25. la Gestion des contrats
26. la formation des agents et des producteurs
27. l'identification des producteurs
28. la gestion des fournisseurs
29. la gestion des paiements
30. l'Amélioration des conditions de vie des producteurs et leurs familles
31. le transfert vers Singapour
32. le transfert vers le Royaume-Uni
33. le transfert vers l'Inde
34. le transfert vers les Pays Bas

Les traitements afférents aux finalités ci-dessus sont listés dans l'annexe 3 de la présente décision.

Article 7 :

Le Groupe OLAM est tenu de mettre en œuvre les prescriptions énoncées dans l'annexe 4 de la présente décision. Elle le fait dans les délais prévus dans ladite annexe.

La mise en œuvre desdites prescriptions fera l'objet d'un contrôle par l'Autorité de Protection.

L'Autorité de Protection délivrera une attestation de conformité au Groupe OLAM, lorsque toutes les prescriptions auront été mises en œuvre.

Article 8 :

En application de l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le Groupe OLAM est tenu d'établir, pour le compte de l'Autorité de Protection, un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

Le Groupe OLAM communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 9 :

L'Autorité de Protection procède à des contrôles auprès du Groupe OLAM, afin de vérifier le respect de la présente décision dont la violation donnera lieu à des sanctions conformément à la règlementation en vigueur.

Article 10 :

Le Groupe OLAM est tenu de procéder au paiement des frais de dépôts de demande d'autorisation auprès du Greffe de l'ARTCI, conformément à la Décision n°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel.

L'Autorité de Protection lui délivrera une facture à cet effet.

Article 11 :

La présente Décision entre en vigueur à compter de la date de sa notification au Groupe OLAM.

Article 12 :

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

Fait à Abidjan, le 22 Décembre 2022
En deux (2) exemplaires originaux

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

- **Etat-civil, Identité, Données d'identification :** Noms et prénoms, date et lieu de naissance, âge, sexe, taille, photos, signature, extrait de naissance

- **Vie personnelle :** Situation matrimoniale, acte de mariage, nombre d'enfants et leurs âges, nombre d'enfants à charge, sexe et niveau scolaire des enfants, les données sur les enfants et les conjoints, certificat de naissance des enfants, informations sur le conjoint, contrat de bail légalisé.

- **Vie professionnelle :** Date d'embauche, poste, produit pour lequel l'employé travail, manager, liste des applications auxquelles accéder, date d'arrivée du courrier, login, données sur la machine, service et département, matricule, date d'entrée dans l'entreprise, fonction, situation professionnelle, respect des droits fondamentaux des employés, conditions de vie et de sécurité des employés et fournisseurs, l'actionnariat, fonction du signataire, formations, qualifications, appréciation de bonne exécution, curriculum vitae et diplôme, niveau scolaire, niveau social, niveau d'étude, registre de commerce, déclaration fiscale d'entreprise et d'existence, certificat de mise à jour au niveau de la CNPS, actionnaire, nombre de parcelle, superficie de la plantation, volume récolté, nombre d'hectares des cacaoyers, document demandé, ancienneté dans l'entreprise, Numéro compte contribuable, catégorie professionnelle, cachet de la coopérative, ordre de mission, lettre d'invitation, code office (code pays, code section et code producteur), rendement, âge de la plantation, nombre de travailleurs de la plantation, nombre de part, données corporate.

- **Informations d'ordre économique et financier :** Capital social, préfinancement, capacité de financement, compte bancaire, relevé d'identité bancaire, demande de prêt, solde, niveau de revenu, montant de la prime du producteur, salaire (brut, net), avantages en nature, salaire et autre avantage.

- **Données de connexion :** Adresse mail

- **Données de localisation :** Lieu d'habitation (ville ou village), situation géographique, adresse, boite postale, lieu de résidence, géolocalisation de la parcelle et du lieu où le producteur a été enquêté, site de réalisation de l'activité, localité de résidence, zone, certificat de résidence, lieu d'habitation, GPS, données GPS de la plantation, localité de la coopérative, localisation des plantations.

- **Numéro d'identification national :** Numéro CNPS, numéro de téléphone, numéro Carte Nationale d'Identité et période de validité, numéro passeport ou carte consulaire, copie du permis, copie de la pièce d'identité du propriétaire ; certificat de nationalité.

- **Données sensibles**

- **Données médicales** Maladies professionnelles, accidents de travail, données statistiques (maladies dans l'entreprise), arrêt maladie, information d'ordre médical, hauteur de la prise en charge, attestation de la prise en charge, carnet de vaccination.

- **Autres données sensibles** Empreinte digitale, filiation, lien de filiation

Fait à Abidjan, le 22 Décembre 2022

Le Président

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

Dr COTY Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

ANNEXE 2

DONNEES AUTORISEES AU TRANSFERT

Données d'identification	Noms et prénoms, âge, sexe, taille, nationalité ou pays de naissance, photos.
Données de la vie personnelle	Acte de mariage, nombre d'enfants à charge, sexe, certificat, identité du conjoint et des enfants, informations d'ordre familiale, contrat de bail légalisé.
Données de la vie professionnelle	Poste, produit pour lequel l'employé travail, service et département, l'actionnariat, fonction du signataire, formations, qualifications, appréciation de bonne exécution, nombre de parcelle, superficie de la plantation, volume récolté, nombre d'hectares des cacaoyers, rendement, âge de la plantation, nombre de travailleurs de la plantation, nombre de part, données corporate.
Données d'informations d'ordre économique et financier	Capital social, compte bancaire, relevé d'identité bancaire, demande de prêt, solde, niveau de revenu.
Données de localisation	Lieu d'habitation (ville ou village), situation géographique, adresse, boite postale, lieu de résidence, géolocalisation de la parcelle et du lieu où le producteur a été enquêté, site de réalisation de l'activité, localité de résidence, zone, données GPS de la plantation, localité de la coopérative, localisation des plantations.
Données de connexion	Adresse mail
Numéro d'identification national	Numéro CNPS, numéro de téléphone, numéro Carte Nationale d'Identité et période de validité, copie de la pièce d'identité du propriétaire, numéro de téléphone.
Autres données sensibles	Filiation

Fait à Abidjan, le 22 Décembre 2022

Le Président

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

Dr COTY Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

ANNEXE 3 : LISTE DES TRAITEMENTS PAR FINALITE

FINALITES	TRAITEMENTS
La gestion administrative	- Collecte; - Consultation ; - Communication ; - Stockage ; - Transfert ; - Transmission ; - Archivage ; - Analyse ; - Conservation ; - Enregistrement ; - Extraction .
La gestion informatique	- Sondage ; - Collecte ; - Transmission ; - Transfert.
L'installation de système de biométrie OUTSPAN IVOIRE S.A	- Collecte ; - Enregistrement ; - Communication ; - Transmission.
L'installation de système de biométrie OLAM COCOA PROCESSING CI S.A. (site San-Pedro)	- Collecte ; - Enregistrement ; - Communication ; - Transmission.
L'installation de système de biométrie OLAM COCOA PROCESSING CI S.A. (site Abidjan)	- Collecte ; - Enregistrement ; - Communication ; - Transmission.
L'installation de système de biométrie MANTRA IVOIRE S.A	- Collecte ; - Enregistrement ; - Communication ; - Transmission.

L'installation de système de biométrie OLAM IVOIRE S.A. (Site Anyama)	- Collecte ; - Enregistrement ; - Communication ; - Transmission.
La gestion juridique	- Extraction ; - Transmission ; - Stockage ; - Communication ; - Consultation ; - Collecte ; - Analyse ; - Réception.
L'amélioration des conditions de vie des producteurs et leurs familles	- Collecte ; - Consultation ; - Enregistrement ; - Communication ; - Stockage ; - Analyse ; - Transmission ; - Archivage.
La gestion des fournisseurs	- Collecte ; - Enregistrement ; - Communication ; - Stockage ; - Analyse ; - Transmission ; - Transfert ; - Modification ; - Conservation ; - Organisation ; - Adaptation ; - Consultation ; - Utilisation.
La gestion des programmes de durabilité	- Consultation ; - Collecte ; - Communication ; - Transmission ; - Stockage ; - Vérification des données ; - Archivage ; - Actualisation.

La formation des agents et producteurs	- Collecte ; - Communication ; - Transmission ; - Stockage ; - Actualisation.
La gestion des contrats	- Collecte ; - Enregistrement ; - Communication ; - Analyse ; - Stockage ; - Exploitation.
La gestion financière	- Analyse ; - Communication ; - Enregistrement ; - Stockage ; - Collecte ; - Transmission ; - Transfert ; - Consultation ; - Extraction ; - Exploitation.
Le recrutement	- Collecte ; - Enregistrement ; - Communication ; - Stockage ; - Transfert ; - Conservation ; - Exploitation ; - Transmission.
La gestion des paiements	- Extraction ; - Vérification ; - Enregistrement ; - Communication ; - Stockage ; - Collecte ; - Transmission ; - Transfert ; - Consultation ; - Exploitation.

La paie du personnel	- Extraction ; - Vérification ; - Enregistrement ; - Communication ; - Stockage ; - Collecte ; - Transmission ; - Transfert ; - Consultation ; - Exploitation.
La gestion des ressources humaines	- Diffusion des informations ; - Consultation ; - Collecte ; - Communication ; - Analyse ; - Stockage ; - Vérification des données ; - Actualisation ; - Archivage.
L'identification des producteurs	- Collecte ; - Enregistrement ; - Communication ; - Stockage ; - Transmission.
La localisation des parcelles	- Collecte ; - Enregistrement ; - Analyse ; - Communication ; - Transmission ; - Conservation - Communication
La gestion du shipping	- Collecte ; - Enregistrement ; - Stockage ; - Consultation ; - Transmission ; - Transfert.
La gestion de la logistique	- Collecte ; - Enregistrement ; - Stockage ; - Consultation ; - Transmission ;

	- Transfert .
La sécurité des biens et des personnes	- Inspection ; - Collecte ; - Vidéosurveillance ; - Enregistrement ; - Stockage.
La gestion de suivi et évaluation	- Enregistrement ; - Collecte ; - Exploitation ; - Transmission ; - Transfert.
Le transfert de données vers la Singapour	- la collecte ; - la communication ; - le stockage ; - l'archivage.
Le transfert de données vers le Royaume-Uni	- la collecte ; - la communication ; - le stockage ; - l'archivage.
Le transfert de données vers l'Inde	- la collecte ; - la communication ; - le stockage ; - l'archivage.
Le transfert de données les Pays bas	- la collecte ; - la communication ; - le stockage ; - l'archivage.
La gestion de la communication	- Extraction ; - Collecte ; - Enregistrement ; - Stockage ; - Transmission.
L'installation de caméras OUTSPAN IVOIRE S.A	- Collecte ; - Stockage ; - Enregistrement ; - Consultation ; - Transmission.

L'installation de caméras OLAM COCOA PROCESSING CI S.A. (site San-Pedro)	- Collecte ; - Stockage ; - Enregistrement ; - Consultation ; - Transmission.
L'installation de caméras OLAM COCOA PROCESSING CI S.A. (site Abidjan)	- Collecte ; - Stockage ; - Enregistrement ; - Consultation ; - Transmission.
L'installation de caméras MANTRA IVOIRE S.A	- Collecte ; - Stockage ; - Enregistrement ; - Consultation ; - Transmission.
L'installation de caméras OLAM IVOIRE S.A (Site Anyama)	- Collecte ; - Stockage ; - Enregistrement ; - Consultation ; - Transmission.

Fait à Abidjan, le 22 Décembre 2022

Le Président

ARTCI

Dr COTY Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

ANNEXE 4 : PRESCRIPTIONS ET DELAIS D'EXECUTION

POINTS D'ANALYSE	PRESCRIPTIONS	DELAIS D'EXECUTION
La légitimité et la licéité des traitements	L'Autorité de Protection prescrit au Groupe OLAM de procéder au recueil du consentement préalable des personnes concernées. Il recueillera comme ci-dessous : ➢ Dans le cadre de la gestion des programmes et projets : o Mettre à la disposition des personnes concernées, un formulaire de recueil du consentement préalable pour les traitements à effectuer. Les formulaires devront être signés par les producteurs de cacao et leurs ménages. ➢ Dans le cadre du recrutement et de la gestion du personnel, par : o la mise à disposition, lors de l'entretien d'embauche, d'un formulaire de recueil de consentement préalable ; o l'insertion des clauses de consentement préalable dans les contrats de travail proposés à la signature des salariés ; o tout autre moyen laissant preuve écrite. ➢ Dans le cadre de la gestion d'application métier : o Permettre à l'utilisateur de donner son consentement par le biais de case à cocher comportant les mentions « j'accepte » et « je refuse »	**60 jours**
La finalité des traitements	RAS	RAS

Les délais de conservation	- **Concernant la conservation des données relatives à la gestion du personnel** : L'autorité prescrit au Groupe OLAM de conserver les données traitées, pendant toute la durée du contrat de travail. En cas de rupture du contrat de travail, les données traitées devront être conservées pendant une période supplémentaire de : - trente (30) ans pour les données liées à la gestion du personnel, la formation et la paie ; - trois (03) mois pour les mots de passe ; - un (01) an pour les données de connexion ; - trois (03) ans pour toutes les autres données. Pour la gestion du recrutement, les données traitées peuvent être conservées pendant une période d'un (01) an, à compter du dernier contact avec la personne concernée. - **S'agissant de la conservation des données relatives à la gestion des programmes et projets** : L'Autorité de Protection prescrit au Groupe OLAM de conserver les données traitées, pendant toute la durée des programmes et projets et sur une période supplémentaire de dix (10) ans à compter de la fin du programme, pour les besoins statistiques et d'évaluation des projets. - **S'agissant de la conservation des données relatives à la gestion d'applications métier** : L'Autorité de Protection prescrit la conservation des données pendant toute la durée de l'utilisation de l'application. Pour les analyses statistiques, les données devront être conservées pendant une période de dix (10) ans maximum. En cas de contentieux, l'Autorité de Protection prescrit que les données traitées soient conservées jusqu'au règlement définitif du contentieux.	**12 mois**

	- **Pour l'archivage électronique** L'Autorité de Protection prescrit au Groupe OLAM d'élaborer une politique d'archivage et de procéder à un archivage électronique des données. Conformément aux dispositions du décret n°2016-851 du 19 Octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique.	
La proportionnalité des données	En application de l'article 21 de la loi relative à la protection des données à caractère personnel, l'Autorité de Protection prescrit que le Groupe OLAM ne collecte pas et ne traite pas les données suivantes : ➢ Dans le cadre de la gestion des programmes et projets : Sont interdits, la collecte et le traitement des données suivantes : o les données relatives à l'origine raciale et ethnique ; o la nationalité ➢ Dans le cadre de la gestion d'application métier : Sont interdits, la collecte et le traitement des données suivantes : o L'origine raciale et ethnique ➢ Dans le cadre de la gestion financière : Sont interdits, la collecte et le traitement des données suivantes : o Les données médicales ➢ Dans le cadre de la gestion des données sensibles : L'Autorité de Protection prescrit au Groupe OLAM, d'élaborer et de mettre en œuvre une politique de gestion des données sensibles. Dans ce cadre, il devra : o faire l'inventaire des données sensibles traitées ; o analyser la proportionnalité des données sensibles traitées ;	**30 jours**

	○ épurer sa base de données des informations sensibles disproportionnées et conserver les données pertinentes ; ○ sécuriser les données sensibles traitées ; ○ définir les accès aux données sensibles ; ○ procéder au recueil du consentement sur un formulaire distinct. ○ réaliser une étude d'impact relative à la protection des données personnelles	
La transparence du traitement	L'Autorité de Protection prescrit au Groupe OLAM de faire preuve de transparence. La transparence requiert que les personnes concernées soient informées de : - l'identité du responsable du traitement et le cas échéant, celle de son représentant dûment mandaté ; - la finalité du traitement ; - les catégories de données concernées ; - les destinataires auxquels les données sont susceptibles d'être communiquées ; - l'existence et des modalités d'exercice de leur droit d'accès et de rectification ; - la durée de conservation des données ; - l'éventualité de tout transfert de données à destination de pays tiers. L'information se fera par le biais de : - mentions légales sur les formulaires, contrats et sur le site internet du Groupe OLAM, - affiches dans tous les lieux où la société opère des traitements de données à caractère personnel ; - messages véhiculés par voie de presse, et en langues locales, par le canal de la Radio nationale et des radios de proximité.	**90 jours**
Le système informatique	D'une manière générale, l'Autorité de Protection prescrit au Groupe OLAM la mise en œuvre des mesures suivantes : - La réalisation d'une analyse de risque formelle axée sur les données à caractère personnel au cœur du système d'information. Cette analyse pourra s'appuyer sur les	**90 jours**

	normes existantes telle que la norme ISO/CEI 27005 qui fournit des lignes directrices traitant spécifiquement de la gestion des risques dans le contexte de la Sécurité des systèmes d'information. - La diffusion de la charte informatique à l'ensemble du personnel. - La mise en place des restrictions sur les ports USB des postes de travail ou l'utilisation de supports amovibles chiffrés, surtout pour les sauvegardes sur des disques durs externes. - La mise en place d'une politique de mot de passe sur les postes de travail, imposant des règles de complexité (longueur minimale de 8 caractères, utilisation de chiffres, symboles et lettres minuscules et majuscules), ainsi qu'une fréquence de renouvellement (chaque 3 ou 4 mois par exemple). - La revue régulière des habilitations et des accès des utilisateurs en fonction de leur profil.	
Les destinataires des données traitées	L'Autorité de Protection prescrit au Groupe OLAM de : - communiquer les données traitées uniquement aux destinataires habilités ; - entamer auprès l'Autorité de Protection, les formalités préalables requises pour les traitements qu'elle opère.	**30 jours**
L'Exactitude des données	L'Autorité de Protection prescrit au Groupe OLAM de : mettre à jour les fichiers physiques et détruire les informations inexactes et celles qui ont été conservées au-delà de la période de conservation définie.	**12 mois**
Les sous-traitants	Dans le cadre de ses activités, le Groupe OLAM est amené à procéder à des échanges de fichiers contenant des données à caractère personnel avec des tiers. Il est donc tenu :	**12 mois**

	- d'inclure des clauses relatives à la protection des données à caractère personnel dans les contrats passés avec ses sous-traitants ; - de contracter uniquement avec des sous-traitants capables d'apporter des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements à effectuer. Il incombe au Groupe OLAM et aux sous-traitants de veiller au respect de ces mesures.	
Le correspondant à la protection	L'Autorité de Protection prescrit au Groupe OLAM d'informer son personnel sur les missions du Correspondant. L'activité du Correspondant doit être relayée efficacement au sein des directions.	**30 jours**
Les droits d'accès, de rectification, d'effacement et d'opposition.	L'Autorité de Protection prescrit au Groupe OLAM de communiquer aux personnes concernées, les contacts du Correspondant à la protection, auprès duquel celles-ci pourront exercer leurs droits d'accès, de rectification, d'effacement et d'opposition.	**30 jours**
La formation du personnel	L'Autorité de Protection prescrit au Groupe OLAM de : - former son personnel sur la protection des données à caractère personnel ; - mettre à la disposition du personnel, des outils pédagogiques concernant la protection des données à caractère personnel.	**90 jours**
Les procédures	L'Autorité de Protection prescrit au Groupe OLAM : - d'élaborer une charte de protection des données à caractère personnel ; - d'élaborer une procédure de gestion des droits des personnes concernées ; - d'élaborer une procédure de gestion des incidents en cas de violation des données personnelles ; - d'intégrer des clauses de recueil du consentement et de transparence dans ses procédures ; - d'élaborer une procédure de gestion des plaintes des personnes concernées ; - de conformer les procédures existantes à la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.	**120 jours**

La biométrie	L'Autorité de Protection prescrit au Groupe OLAM : - d'éviter que l'usage de la biométrie ait pour finalité le contrôle des temps de présence des employés ; - d'utiliser des matériels biométriques sans base de données ; - de faire des formations sur l'usage de la biométrie ; - de soumettre à l'ARTCI, un rapport d'activité relatif à l'usage de la biométrie par la société par le Groupe OLAM .	**30 Jours**
Les transferts	L'Autorité de Protection prescrit au Groupe OLAM de soumettre à l'ARTCI, des Règles d'Entreprise Contraignantes (BCR) pour approbation.	**60 Jours**

Fait à Abidjan, le 22 Décembre 2022

Le Président

ARTCI

Dr COTY Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0825

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

EN DATE DU 22 DECEMBRE 2022

PORTANT AUTORISATION DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL PAR NSIA ASSURANCES

Conseil de Régulation : 31 Av Nogués, 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 Code CIMA ;

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 l'Ordonnance 2009-385 du 1er décembre 2009 portant règlementation bancaire ;

Vu l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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°2016-851 du 19 Octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

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°2021- 916 du 22 Décembre 2021 portant adoption du référentiel général de sécurité des systèmes d'information et du plan de protection des infrastructures critiques ;

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 de 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 des Télécommunications/tic de Côte d'Ivoire en date du 03 septembre 2014 portant adoption des règles de conduite relatives au traitement et à la protection des données à caractère personnel (DCP) ;

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°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 ;

Par les motifs suivants :

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par NSIA ASSURANCES, entreprise exerçant dans le domaine des assurances ;

Considérant que NSIA ASSURANCES entend mettre en œuvre une assurance de responsabilité civile scolaire.

Considérant que l'article 47 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 est chargée de recevoir les déclarations et d'octroyer les autorisations, pour la mise en œuvre de traitements de données à caractère personnel ;

L'Autorité de Protection est compétente, pour examiner la demande d'autorisation de traitements initiée par NSIA ASSURANCES ;

- **Sur la recevabilité de la demande d'autorisation**

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 qu'en l'espèce, NSIA ASSURANCES voudrait collecter les données à caractère personnel des élèves et des parents d'élèves des établissements scolaires ;

Ledit traitement doit être autorisé par l'Autorité de protection, pour être mis en œuvre ;

Considérant qu'aux termes de l'article 7 précité, la demande d'autorisation est présentée par le responsable du traitement ou son représentant légal ;

Que l'article 1 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, définit le responsable du traitement comme étant la personne physique ou morale, publique ou privée, 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 ;

Considérant que NSIA ASSURANCES envisage mettre en œuvre une assurance de responsabilité civile scolaire.

Qu'à cet effet, NSIA ASSURANCES va collecter, traiter, stocker, et communiquer des données à caractère personnel de ses clients ;

L'Autorité de Protection en conclut que NSIA ASSURANCES a la qualité de Responsable du traitement.

Considérant qu'aux termes de l'article 9 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la demande d'autorisation doit contenir les mentions minimums relatives à la dénomination sociale de la personne morale, au responsable du traitement, à son siège social, à l'identité de son représentant légal, à son numéro d'immatriculation au registre du commerce et du crédit mobilier, à son numéro de déclaration fiscale, aux finalités du traitement, à la durée de conservation des données traitées, aux dispositions prises pour assurer la sécurité des traitements, à la protection et à la confidentialité des données traitées ;

Considérant que lesdites mentions figurent dans la demande d'autorisation formulée par NSIA ASSURANCES et qu'elle satisfait aux conditions de forme exigées par les articles 7 et 9 de la Loi n°2013-450 relative à la protection des données à caractère personnel ;

En conséquence, l'Autorité de Protection déclare, la demande de NSIA ASSURANCES, recevable en la forme.

- **Sur la légitimité et la licéité du traitement**

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 que NSIA ASSURANCES indique qu'elle procédera au recueil du consentement préalable de ses clients à travers des contrats, avant toute collecte de données ;

Cependant, NSIA ASSURANCES n'a pas transmis de copie du contrat qu'elle entend faire signer à ses clients ;

L'Autorité de Protection ne peut considérer le traitement projeté par NSIA ASSURANCES licite et légitime, que si la demanderesse produit un contrat comportant une clause de recueil de consentement exprès, libre éclairé et spécifique ;

Toutefois, elle prescrit à NSIA ASSURANCES de lui faire parvenir une copie du contrat qu'elle entend faire signer à ses clients pour analyse.

- **Sur la finalité**

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 qu'en l'espèce, NSIA ASSURANCES procède au traitement de données à caractère personnel de ses clients afin de mettre en œuvre une assurance de responsabilité civile scolaire ;
L'Autorité de Protection considère que cette finalité est déterminée, explicite et légitime.

- **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 qu'en l'espèce, NSIA ASSURANCES a indiqué qu'elle conservera les données traitées pendant douze (12) mois ;

L'autorité de Protection, au regard de la nature des données traitées et de la finalité du traitement, considère que ce délai n'est pas excessif.

Toutefois, l'Autorité de Protection prescrit à NSIA ASSURANCES de conserver les données collectées pendant la durée de la relation client et une durée de dix (10) ans à compter de la fin de la relation contractuelle avec les clients, conformément à l'article 24 de l'Acte Uniforme portant organisation et harmonisation des comptabilités des entreprises.

- **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 qu'en l'espèce, NSIA ASSURANCES indique que le traitement concerne les données suivantes :

- **les données d'identification :** nom, prénom, adresse, date et lieu de naissance le nom et prénom du père et de la mère, numéro de téléphone du parent
- **les données de vie scolaire** : scolarité, formation, matricule, l'école, la classe ;
- **les données de santé** : données relatives aux soins, facture du soin, justificatif de soin, acte de décès de la partie tierce ;

Il y a lieu de constater que les données collectées, telles qu'elles sont décrites dans la demande d'autorisation, sont pertinentes, adéquates, et non excessives au regard de la finalité.

- **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, selon lesquelles la demande d'autorisation adressée à l'Autorité de Protection doit contenir les destinataires habilités à recevoir communication des données traitées ;

Considérant qu'en l'espèce, NSIA ASSURANCES indique qu'elle communique les données collectées aux :

- services internes de NSIA ASSURANCES ;
- aux centres de santé ;
- au Trésor public Ivoirien ;
- au ministère de l'éducation nationale.

L'Autorité de Protection considère ces partenaires susvisés comme destinataires de données et prescrit également, que les données traitées soient communiquées, aussi :

- au Procureur de la République ;
- aux Officiers de Police Judiciaire munis d'une réquisition ;
- aux agents assermentés de l'Autorité de Protection habilités, dans le cadre de l'exécution de leurs missions ;
- aux autorités et Administrations publiques Ivoiriennes dans le cadre de leurs missions.

- **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 NSIA ASSURANCES de faire preuve de transparence vis à vis des personnes concernées qui devront notamment être informées :

- 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.

Considérant que NSIA ASSURANCES indique dans son formulaire de demande d'autorisation que les personnes concernées seront informées à travers :

- des affiches présentes dans leur locaux ;
- l'envoi d'un courrier personnalisé aux personnes concernées ;
- un communiqué de l'association des parents d'élèves et les réseaux sociaux.

L'Autorité de Protection considère dès lors que le principe de transparence est respecté.

- **Sur les droits d'accès direct, d'opposition, de rectification 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 NSIA ASSURANCES indique que les droits d'accès direct, d'opposition, de rectification, d'effacement, de portabilité, de retrait du consentement donné, et de suppression, pourront être exercés auprès d'elle-même.

L'Autorité de Protection conclut que les droits d'accès direct, d'opposition et de rectification des personnes concernées sont respectés.

- **Sur les mesures de sécurité**

Considérant qu'en application de l'article 41 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le responsable du traitement et le sous-traitant prennent toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient détruites, déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance ;

Qu'en vue de respecter cette exigence de la loi, NSIA ASSURANCES a mis en place des mesures spécifiques afin de garantir la confidentialité, l'intégrité et la disponibilité des données collectées.

Considérant qu'au vu des éléments techniques fournis par NSIA ASSURANCES dans son formulaire de demande d'autorisation, il en résulte qu'elle a pris toutes les mesures nécessaires en vue d'assurer la sécurité des données ;

L'Autorité de Protection considère que les mesures de sécurité logique et physique nécessaires sont garanties.

Toutefois, l'Autorité de Protection prescrit à NSIA ASSURANCES de :

- maintenir à jour les systèmes d'exploitation et les applications utilisés afin d'être moins vulnérable aux différentes attaques ;
- Utiliser des mots de passe d'une longueur minimale de 10 caractères, composés de nombres, majuscules, minuscules, symboles et caractères spéciaux.
- Installer un système de détection d'intrusion afin de repérer des activités anormales ou suspectes ou aussi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

Après en avoir délibéré,

DECIDE :

Article 1 :

NSIA ASSURANCES est autorisée à effectuer la collecte, et l'enregistrement, le traitement, le stockage et la communication des données à caractère personnel ci-après :

- **les données d'identification :** Nom, prénom, adresse, date et lieu de naissance, le nom du père ou de la mère de l'élève, le numéro de téléphone du parent ;
- **les données de vie scolaire :** scolarité, formation matricule, l'école, la classe ;
- **les données de santé :** données relatives aux soins, facture de soin, justificatif de soin, acte de décès de la partie tierce.

Les données non mentionnées ne devront aucunement faire l'objet d'un quelconque traitement de la part de NSIA ASSURANCES.

Article 2 :

Les données traitées par NSIA ASSURANCES ne peuvent être utilisées à des fins autres que celles précisées dans la demande d'autorisation.

Toute réutilisation de ces données à d'autres fins doit faire l'objet d'une autorisation préalable de l'Autorité de protection.

Article 3 :

NSIA ASSURANCES est tenue de produire un contrat comportant une clause de recueil du consentement exprès, libre éclairé et spécifique des personnes concernées.

Article 4 :

NSIA ASSURANCES est autorisée à communiquer les données traitées :

- aux services internes de NSIA ASSURANCES ;
- aux centres de santé ;
- au trésor public Ivoirien ;
- au ministère de l'éducation nationale ;
- aux Officiers de Police Judiciaire munis d'une réquisition ;
- aux Agents assermentés de l'Autorité de Protection habilités, dans le cadre de l'exécution de leurs missions ;
- aux Agents habilités de l'administration publique dans le cadre de leurs missions.

Il est interdit à NSIA ASSURANCES de transférer, sans autorisation préalable de l'Autorité de protection, les données collectées vers des pays tiers, hors de la CEDEAO.

Article 5 :

Les données sont conservées par NSIA ASSURANCES pendant un délai de dix (10) ans après la fin de la relation contractuelle.

En cas de litige, les données sont conservées jusqu'à la fin de la procédure judiciaire, lorsque la décision de justice rendue est devenue définitive.

Article 6 :

NSIA ASSURANCES informe les personnes concernées de leurs droits d'accès direct, d'opposition, d'effacement, de portabilité, de retrait du consentement donné, de rectification et de suppression à travers les mentions légales contenues dans les formulaires.

NSIA ASSURANCES est tenue de définir une procédure de gestion des droits des personnes concernées.

Article 7 :

Conformément à l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, NSIA ASSURANCES est tenue d'établir pour le compte de l'Autorité de Protection un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

NSIA ASSURANCES communique ce rapport à l'Autorité de protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 8 :

L'Autorité de Protection procède à des contrôles auprès de la NSIA ASSURANCES afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 9 :

La présente décision entre en vigueur à compter de la date de sa notification à NSIA ASSURANCES.

Article 10 :

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

Fait à Abidjan, le 22 Décembre 2022
En deux (2) exemplaires originaux

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

ARTCI

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0826

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 22 DECEMBRE 2022

PORTANT AUTORISATION DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL PAR

LA BGFI BANK CÔTE D'IVOIRE

Conseil de Régulation : 31 Av Nogués, 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 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°2015-532 du 20 juillet 2015 portant Code du travail ;

Vu la Loi n°2017-803 du 07 décembre 2017 d'orientation de la société et de l'information ;

Vu l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

Vu l'Ordonnance n°2009-385 du 1er décembre 2009 portant réglementation bancaire ;

Vu le Décret n°2012-934 du 19 septembre 2012 portant organisation et fonctionnement 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° 2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le Décret n°2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

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°2020-218 du 29 janvier 2020 portant création, organisation et fonctionnement du Centre National de veille et de Réponse aux incidents de sécurité informatique dénommé CI-CERT ;

Vu le Décret n°2021-916 du 22 décembre 2021 portant organisation du Référentiel général de sécurité des systèmes d'information et du plan de Protection des infrastructures critiques ;

Vu le Décret n°2022-265 du 13 avril 2022 portant nomination du Directeur Général de l'Autorité 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 de Côte d'Ivoire, en abrégé 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 de 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 aux conditions de traitement des données à caractère personnel (DCP) ;

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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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°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 données à caractère personnel;

Vu le Rapport d'audit de protection des données personnelles de la BGFI Bank Côte d'Ivoire ;

Par les motifs suivants :

Considérant que conformément à l'article 53 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, les responsables du traitement doivent procéder à la mise en conformité des traitements qu'ils opèrent avec ladite loi ;

Considérant que pour faciliter cette mise en conformité, l'Autorité de Protection a par décision n°2017-0354 du 26 octobre 2017 défini la 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 ;

Considérant que la BGFI Bank Côte d'Ivoire, une société anonyme avec Conseil d'Administration au capital social de 20.000.000.000 FCFA dont le siège social est sis à Marcory Boulevard Valéry Giscard d'Estaing, 01 BP 11563 Abidjan 01, téléphone (+225) 27 21 56 91 56, a saisi l'Autorité de Protection d'une demande de mise en conformité ;

Que par ailleurs, la BGFI Bank Côte d'Ivoire a effectué son audit de protection des données personnelles ;

Considérant les recommandations contenues dans le rapport d'audit de protection des données personnelles ;

Après en avoir délibéré,

DECIDE :

Article 1 :

BGFI Bank Côte d'Ivoire est autorisée à effectuer les traitements des données mentionnées dans l'annexe 1 de la présente décision.

Les données non mentionnées dans l'annexe 1 ne devront aucunement faire l'objet d'un quelconque traitement, de la part de BGFI Bank Côte d'Ivoire.

Article 2 :

BGFI Bank Côte d'Ivoire est autorisée à effectuer les traitements énumérés dans l'annexe 3 de la présente décision.

Article 3 :

BGFI Bank Côte d'Ivoire est autorisée à transférer vers le Gabon, les données énumérées dans l'annexe 2 de la présente décision.

Article 4 :

La BGFI Bank Côte d'Ivoire est autorisée à communiquer les données traitées uniquement aux destinataires habilités, notamment :

- aux services internes de la BGFI Bank Côte d'Ivoire suivant leurs niveaux d'habilitation ;
- au bureau d'Information sur le Crédit (BIC) ;
- à la caisse Générale de Retraite des Agents de l'Etat (CGRAE) ;
- à la banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) ;
- à la Direction Générale des Impôts (DGI) ;
- aux officiers de police judiciaire munis d'une réquisition;
- à la Caisse National de Prévoyance Sociale (CNPS) ;
- aux avocats et intermédiaires de justice ;
- à la Cellule Nationale du Traitement de l'Information Financière (CENTIF) ;
- aux autorités publiques ivoiriennes habilitées agissant dans le cadre de l'exercice de leurs missions ;
- au Procureur de la république ;
- aux officiers de police judiciaire munis d'une réquisition ;
- aux agents assermentés de l'Autorité de Protection (ARTCI) habilités, dans le cadre de l'exécution de leurs missions.

Article 5 :

L'Autorité de Protection interdit à la BGFI Bank Côte d'Ivoire de transférer sans autorisation préalable de l'Autorité de Protection, les données traitées vers des pays tiers, autre que le Gabon.

La BGFI Bank Côte d'Ivoire est tenue avant tout transfert de données hors de la Côte d'Ivoire, de les stocker sur le territoire de la République de Côte d'Ivoire.

Article 6 :

Conformément à l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la BGFI Bank Côte d'Ivoire doit s'assurer que ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle relatives aux traitements de données qu'ils opèrent.

Il incombe à la BGFI Bank Côte d'Ivoire ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

Article 7 :

Les traitements de données autorisés dans la présente décision correspondent aux finalités listées dans l'annexe 3 de la présente décision.

Article 8 :

La BGFI Bank Côte d'Ivoire est tenue de mettre en œuvre les prescriptions énoncées dans l'annexe 4 de la présente décision. Elle le fait dans les délais prévus dans ladite annexe.

La mise en œuvre desdites prescriptions fera l'objet d'un contrôle par l'Autorité de Protection.

L'Autorité de Protection délivrera une attestation de conformité à la BGFI Bank Côte d'Ivoire lorsque toutes les prescriptions auront été mises en œuvre.

Article 9 :

En application de l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la BGFI Bank Côte d'Ivoire est tenue d'établir, pour le compte de l'Autorité de Protection, un rapport annuel sur le respect des dispositions de l'article 41 de ladite loi.

La BGFI Bank Côte d'Ivoire communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 10 :

L'Autorité de Protection procède à des contrôles auprès de la BGFI Bank Côte d'Ivoire, afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 11 :

La finalité du dispositif biométrique est limitée au contrôle d'accès des zones sensibles de la banque (salles serveurs, coffre-fort, zone à accès limité).

Article 12 :

La BGFI Bank Côte d'Ivoire est tenue de procéder au paiement des frais de dépôts de demande d'autorisation auprès du Greffe de l'ARTCI, conformément à la décision n°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel.

L'Autorité de Protection lui délivrera une facture à cet effet.

Article 13 :

La présente Décision entre en vigueur à compter de la date de sa notification à la BGFI Bank Côte d'Ivoire.

Article 14 :

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

Fait à Abidjan, le 22 Décembre 2022
En deux (2) exemplaires originaux

Le Président

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

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

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

CONSEIL DE REGULATION

REPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0828

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

EN DATE DU 22 DECEMBRE 2022

PORTANT AVERTISSEMENT ET MISE EN DEMEURE DE LA SOCIETE CRYPTONEO EN MATIERE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Conseil de Régulation : 31 Av Nogués, 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 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 l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication ;

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°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°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°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°2022-0738 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 05 mai 2022 portant approbation de la liste des contrôles en matière de protection des données à caractère personnel pour l'année 2022

Vu le Procès-verbal de contrôle n° 003/07/2022 du mardi 19 juillet 2022 ;

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, énonce 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 la société CRYPTONEO a été identifiée par la Décision n°2022-0738 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 05 mai 2022 portant approbation de la liste des contrôles en matière de protection des données à caractère personnel pour l'année 2022, comme un responsable du traitement à contrôler ;

Considérant que la société CRYPTONEO, située à Abidjan- Cocody-II Plateaux, 7ème tranche, est une entreprise qui fournit des prestations de sécurité électronique, certification électronique, signature électronique, horodatage, archivage, etc.

Le 19 juillet 2022, en application de la décision n°2022-0738 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 05 mai 2022 portant approbation de la liste des contrôles en matière de protection des données à caractère personnel pour l'année 2022, des agents assermentés de l'Autorité de Protection ont mené une opération de contrôle sur place au sein des locaux de la société CRYPTONEO.

Cette mission avait pour objet de vérifier le respect par la société CRYPTONEO 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, 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 CRYPTONEO et ses sous-traitants.

Considérant que lors du contrôle, l'Autorité de Protection a effectué les contrôles suivants :

- Contrôle de l'espace AE (Autorité d'Enregistrement) ;
- Contrôle des Ressources humaines ;
- Contrôle de la sécurité physique.

Considérant qu'à l'issue du contrôle, la copie du procès-verbal n° 003-07/2022 a été remise à la société CRYPTONEO.

II. Motifs de la Décision :

A) Sur le manquement à l'obligation de conformité avec la Loi n°2013 -450 du 19 juin 2013 relative à la protection des données personnelles

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 personnelles 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 personnelles 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 CRYPTONEO a communiqué aux agents de l'Autorité de Protection, une attestation de prestation produite par un cabinet d'accompagnement datée du 18 juillet 2022 attestant avoir entamé *« le processus de mise en conformité avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel et le Règlement Général de la protection des données à caractère personnel* » ;

Considérant que l'attestation de formation produite par la société CRYPTONEO est postérieure à la décision n°2022-0738 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 05 mai 2022 portant approbation de la liste des contrôles en matière de protection des données à caractère personnel pour l'année 2022 et à la lettre de l'ARTCI portant information pour le contrôle ;

Considérant qu'au moment du contrôle effectué par l'Autorité de Protection, la société CRYPTONEO n'avait introduit aucune demande de mise en conformité et ne dispose pas d'autorisation unique de traitement 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 personnelles ;

L'Autorité de Protection considère que la société CRYPTONEO n'a pas respecté les dispositions des articles 53 de la Loi n°2013 -450 du 19 juin 2013 relative à la protection des données personnelles et les dispositions des article 2 et 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 personnelles ;

B) Sur le manquement à l'obligation d'obtenir une autorisation de traitement

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 qu'en l'espèce, la société CRYPTONEO collecte et stocke entre autres données à caractère personnel, le numéro de téléphone, carte nationale d'identité, les images des visiteurs et des membres de son personnel ;

Qu'en application des dispositions précitées, lesdits traitements doivent être autorisés par l'Autorité de Protection, pour être mis en œuvre ;

Considérant que selon l'article 7 précité de la même loi, la demande d'autorisation est présentée par le responsable du traitement ou son représentant légal ;

Que l'article 1 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, définit le responsable du traitement comme étant la personne physique ou morale, publique ou privée, 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 ;

Considérant que lors du contrôle, le Responsable du traitement n'a pu fournir les autorisations de traitement pour les points de contrôles effectués ;

L'Autorité de Protection considère que la société CRYPTONEO n'a pas respecté les dispositions de l'article 7 précité.

C) 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, la société CRYPTONEO a transmis un formulaire de « *consentement du travailleur relative au traitement de ses données personnelles par CRYPTONEO conformément à la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel* » ;

Considérant que l'analyse de ce formulaire montre qu'il est conçu pour un recueil du consentement de plusieurs finalités ;

Qu'ainsi dès que la personne concernée donne son consentement, il accepte la collecte de ses données pour diverses finalités différentes. Qu'une seule action de consentement permet ici l'acceptation de plusieurs usages différents des données personnelles.

Que dès lors, le consentement n'est donc pas spécifique car il englobe plusieurs finalités différentes.

Que ce formulaire de consentement ne permet pas de recueillir le consentement de manière libre, spécifique, éclairé et univoque ;

Considérant par ailleurs que lors du contrôle, la société CRYPTONEO n'a pu fournir un motif de dérogation 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 ne satisfont pas au principe de la légitimité.

D) 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 pu constater que les finalités pour lesquelles les données étaient collectées étaient déterminées et explicites,

Considérant que pour que la finalité d'un traitement de données soit légitime, il est nécessaire que, 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 ;

Que non seulement les traitements de données personnelles opérées par la société CRYPTONEO ne se fondent pas sur un consentement valide mais aussi et surtout il n'existe aucun motif de dérogation à l'exigence du consentement ;

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

E) 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, la société CRYPTONEO a indiqué :

- Une conservation des dossiers de demande de certificat pendant sept (07) ans à compter de la date d'expiration du certificat ;
- Une conservation des données biométriques des agents de la société CRYPTONEO pendant tout le temps de présence des employés et la suppression de ces données au départ du salarié ;
- Une conservation des données des agents et salariés de la société CRYPTONEO pendant toute la durée de présence et pendant une durée supplémentaire de dix (10) ans à compter du départ du salarié ;
- Une conservation des données des agents et salariés non actifs dans les cartons d'archives ;
- Une durée de conservation indéfinie pour les registres d'accès à la salle du coffre-fort ;
- Une durée de conservation indéfinie pour le registre visiteur et employé ;
- Une suppression immédiate des données biométriques en cas de départ du salarié ;
- Une conservation des enregistrements de vidéosurveillance pendant une période d'un (01) mois ;

Considérant que la société CRYPTONEO n'a pu fournir à l'Autorité de Protection, les durées de conservation pour tous les autres points de contrôles ;

Considérant que les délais de conservations des données des agents à compter de leur départ sont insuffisants au regard de la pratique décisionnelle de l'Autorité de Protection ;

Considérant que la durée de conservation indéfinie des registres d'accès à la salle du coffre-fort est excessive au regard de la finalité ;

Considérant que la conservation indéfinie des données des agents et salariés non actifs dans les cartons d'archives est excessive ;

Dès lors, l'Autorité de Protection, au regard de la nature des données traitées considère que les durées de conservation évoquées sont inadéquates.

F) 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, la société CRYPTONEO a indiqué collecter les données biométriques dans le cadre du contrat de travail ;

Considérant que l'article 3 du décret n°2018-454 du 09 mai 2018 relatif au Registre National des Personnes Physiques, dispose que l'authentification des données biographiques et biométriques des personnes physiques relève de la compétence exclusive de l'Office National de l'Etat Civil et de l'Identification (ONECI) ;

Conformément à l'article 3 du décret n°2018-454 du 09 mai 2018 relatif au Registre National des Personnes Physiques, l'authentification et le stockage des données biométriques relèvent exclusivement de la compétence de l'Office National de l'Etat Civil et de l'Identification (ONECI) ;

Considérant que le recours à un dispositif de biométrie et partant, la collecte de données biométriques, doit avant tout répondre à un véritable impératif de sécurité et cela lorsqu'il n'y a plus d'autre alternative ;

Que la biométrie ne doive, par conséquent, être utilisée qu'en dernier recours, lorsqu'il n'existe aucun autre moyen pour atteindre les finalités du traitement envisagé ;

Considérant que l'analyse du formulaire de recueil de consentement du travailleur de la société CRYPTONEO fait ressortir un consentement unique à la fois pour les données des ressources humaines et pour l'empreinte digitale.

Que l'absence de distinction entre le consentement pour l'empreinte digitale et celui des données des ressources humaines entraine une collecte systématique des données biométriques des travailleurs, ce qui est contraire au principe de proportionnalité des données.

L'Autorité de Protection considère que la collecte systématique de l'empreinte digitale dans le cadre des ressources humaines est disproportionnée.

G) 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 identifiés ;

Considérant que le site internet de la société CRYPTONEO est hébergé chez MAGIC ONLINE en France ;
Considérant que les demandes de certificats SSL sont transmises au format « CSR » à l'entreprise GLOBAL SIGN basée en France ;

Que par ailleurs, le fichier CSR peut être décodé afin d'extraire des données à caractère personnel ;

Considérant que ni le site internet de CRYPTONEO, ni les formulaires de demandes de certificats ne comportent de mentions d'information relatives aux transferts de données ;

Considérant les dispositions de l'article 6.8 du cahier de charges de la société CRYPTONEO qui dispose que sauf autorisation de l'ARTCI, il est interdit à la société CRYPTONEO de transférer les données à caractère personnel à destination d'un pays tiers ;

Considérant que la société CRYPTONEO 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 société CRYPTONEO ne sont pas en conformité avec la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

H) 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 :

- 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 :

- l'identité du Responsable du traitement et le cas échéant, celle de son représentant dûment mandaté ;
- le fait que la société CRYPTONEO soit placée sous vidéosurveillance ;
- la finalité du traitement;
- les catégories de données concernées ;
- les destinataires auxquels les données sont susceptibles d'être communiquées;
- l'existence et des modalités d'exercice des droits de la personne concernée;
- la durée de conservation des données ;
- le numéro de l'Autorisation délivrée par l'Autorité de Protection.

Considérant que la société CRYPTONEO a installé un dispositif de vidéosurveillance ;

Considérant que la société CRYPTONEO ne dispose que d'un pictogramme ne contenant pas toutes les mentions ci-dessus évoquées ;

Considérant que la société CRYPTONEO ne dispose pas d'autorisation de traitement de données à caractère personnel pour la vidéosurveillance ;

Par conséquent, l'Autorité de Protection considère que le traitement effectué au moyen de la vidéosurveillance n'est pas conforme à la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

I) Sur le dispositif biométrique

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 des données à caractère personnel comportant des données biométriques est soumis à autorisation préalable de l'Autorité de Protection, avant toute mise en œuvre ;

Considérant que la société CRYPTONEO ne dispose pas d'autorisation de traitement pour le dispositif de biométrie ;

Considérant qu'au moment du contrôle, aucune formalité préalable n'a été effectuée par la société CRYPTONEO ;

Par conséquent, l'Autorité de Protection considère que le traitement effectué au moyen de la biométrie n'est pas conforme à la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

J) Sur la gestion des ressources humaines

Considérant que la société CRYPTONEO ne dispose pas d'autorisation de traitement de données pour les ressources humaines ;

L'Autorité de Protection considère que les traitements effectués pour la gestion des ressources humaines ne sont pas conformes à la loi n° n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

K) 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 la société CRYPTONEO dispose de plusieurs registres qui retracent les mouvements effectués dans certains endroits de l'entreprise et pour accéder à certaines informations ;

Considérant les articles 9 et 12 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Considérant que les pages des registres ne contiennent pas de mentions relatives aux droits des personnes concernées ;

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

L) 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 le contrôle a révélé l'implémentation des mesures de sécurité suivantes :

- Protection physique des équipements et des serveurs mettant en œuvre le traitement grâce notamment à un contrôle d'accès biométrique ;
- Définition de politiques de sécurité, et de mots de passe, profils d'habilitation, charte informatique etc. ;
- Utilisation de mots de passe forts ;
- Sécurisation des postes de travail utilisés pour le traitement ;
- Sauvegardes quotidiennes des données sur des supports amovibles.

Considérant que bien que la charte informatique prévoie le renouvellement des mots de passe tous les six mois, l'application de cette mesure n'est pas imposée sur les postes de travail mais plutôt laissée à l'attention des utilisateurs.

Considérant par ailleurs, que les supports amovibles utilisés pour les sauvegardes de données ne font pas l'objet de chiffrement.

L'Autorité de Protection considère que le niveau de sécurité du système d'information reste perfectible.

M) Sur les procédures internes de la société CRYPTONEO

Considérant que les Conditions Générales d'Utilisation (CGU) jointes aux formulaires de demande de certificat comportent des mentions relatives à la protection des données personnelles des clients ;

Que ces mentions ne contiennent pas les coordonnées du Correspondant à la protection des données ou du service auprès duquel exercer les droits des personnes concernées ;

Qu'enfin, les mentions d'information ne sont pas directement visibles sur les formulaires mais plutôt à la fin des Conditions Générales d'Utilisation (CGU) ;

Considérant également que les procédures internes de la société CRYPTONEO communiquées lors du contrôle ne contiennent pas de mesures spécifiques à la protection des données personnelles des clients ;

L'Autorité de Protection considère que les procédures internes et les formulaires ne sont pas conformes à la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

N) Sur les obligations contenues dans le cahier des charges de la société CRYPTONEO

Considérant l'article 6.7 du cahier de charges de la société CRYPTONEO qui dispose que la société CRYPTONEO adresse à l'Autorité de Protection, un rapport annuel sur les traitements de données personnelles ;

Considérant qu'au moment du contrôle, la société CRYPTONEO n'a pas communiqué à l'Autorité de Protection de rapport annuel sur les traitements de données personnelles ;

L'Autorité de Protection considère que la société CRYPTONEO n'a pas respecté les dispositions de l'article 6.7 du cahier de charges de la société les traitements de données personnelles

Considérant enfin que l'Autorité de Protection, à travers le contrôle effectué constate :

- **L'absence d'autorisation de traitement de données pour la société CRYPTONEO ;**
- **L'absence de mise en conformité à la loi relative à la protection des données à caractère personnel pour la société CRYPTONEO ;**
- **L'absence d'autorisation de transferts de données à destination d'un pays tiers ;**
- **L'absence d'autorisation de traitement des données personnel pour les sous-traitants de la société CRYPTONEO ;**
- **Le non-respect des principes de la légitimité, de la proportionnalité, de la durée limitée de la conservation des données, des droits des personnes concernées ;**
- **Le non-respect de l'information des personnes et de la transparence ;**
- **L'absence d'autorisation pour le dispositif de vidéosurveillance ;**
- **L'absence d'autorisation pour le dispositif de biométrique ;**
- **Affiche ou de pictogramme conforme pour la vidéosurveillance ;**
- **L'absence de procédure relative aux droits des personnes concernées ;**
- **Le non-respect des dispositions des articles 6.7 et 6.8 du cahier des charges de la société CRYPTONEO ;**
- **L'absence de mentions relatives aux droits des personnes concernées et aux principes de la protection des données personnelles dans procédures internes et les formulaires de demande de certificat.**

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 société CRYPTONEO :

- **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 constatés dans les trente (30) jours à compter de la notification de la présente décision ;**

- **une mise en demeure de se mettre en conformité** avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel **dans les soixante (60) jours à compter de la réception de la présente décision.**

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 CRYPTONEO.

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 22 Décembre 2022
En deux (2) exemplaires originaux

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

Autorité de Régulation des Télécommunications / TIC de Côte d'Ivoire
ARTCI
Le Président
15

SMC

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

CONSEIL DE REGULATION

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2022-0713
DE L'AUTORITE DE PROTECTION
DE LA REPUBLIQUE DE COTE D'IVOIRE
EN DATE DU 1er FEVRIER 2022
PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL
PAR K'ORIGINS

L'AUTORITE DE PROTECTION,

Vu la Loi n°2010-72 du 30 Septembre 2010 portant interdiction de la traite et les pires formes d travail des enfants en côte d'Ivoire ;

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°2014-390 du 20 juin 2014 d'orientation sur le développement durable ;

Vu la Loi n°2015-532 du 20 juillet 2015 portant Code du travail ;

Vu la Loi n°2015-537 du 20 juillet 2015 d'orientation agricole de Côte d'Ivoire ;

Vu l'Ordonnance n° 2000-583 du 17 août 2000 fixant les objectifs de l'action économique de l'Etat en matière de commercialisation de café et du cacao modifiée par Ordonnance N° 2001-46 du 31 janvier 2001 ;

Vu l'Ordonnance n° 2001-46 du 31 janvier 2001 modifiant l'article 11 de l'Ordonnance n°2000-583 du 17 août 2000 fixant les objectifs économiques de l'action de l'Etat en matière de commercialisation du café et du cacao ;

Vu l'Ordonnance N° 2001-47 du 31 janvier 2001 relative à la redevance professionnelle en matière de café et de cacao ;

Vu l'Ordonnance N° 2001-666 du 24 octobre 2001 modifiant l'ordonnance N° 2000-583 du 17 août 2000 fixant les objectifs économiques de l'action de l'Etat en matière de commercialisation du café et du cacao ;

Vu l'Ordonnance n°2008-225 du 05 Août 2008 portant aménagement du taux du droit proportionnel d'enregistrement sur les actes de confirmation de vente de café et cacao ;

Vu l'Ordonnance n°2008-259 du 19 septembre 2008 Modifiant et complétant l'ordonnance n°2000-583 du 17 août 2000 fixant les objectifs de l'action économique de l'Etat en matière de commercialisation du café et du cacao, telle que modifiée par les ordonnances n ° 2001-46 du 31 janvier 2001 et n ° 2001-666 du 24 octobre 2001 ;

Vu l'Ordonnance n°2011-481 du 28 décembre 2011 fixant les règles relatives à la commercialisation du café et du cacao ;

Vu l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications et aux Technologies de l'Information et de la Communication/TIC ;

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°2012-1008 du 17 Octobre 2012 fixant les modalités de commercialisations du cacao et du café;

Vu le Décret N°2012-1009 du 17 octobre 2012 fixant les conditions d'exercice de la profession d'acheteur de produits café et cacao ;

Vu le Décret N°2012-1010 du 17 octobre 2012 Règlementant la profession d'exportateur de café et de cacao ;

Vu le Décret N°2012-1013 du 17 octobre 2012 relatif à la tierce détention en matière de café-cacao ;

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°2014- 290 du 21 Mai 2014 portant application de la loi n°2010-272 du 30 Septembre 2010 portant interdiction de la traite et les pires formes de travail des enfants en côte d'Ivoire ;

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 autorisation traitement des données à caractère personnel ;

Vu le Décret n° 2016-483 du 07 juillet 2016 portant nomination de Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

Vu le Décret n°2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;

Vu le Décret N°2017-321 du 24 mai 2015 relatif à la mise en œuvre des projets de certification et de programmes de durabilité dans la filière café-cacao ;

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 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 l'Arrêté n° 2017-016 MPS/CAB du 02 juin 2017 déterminant la liste des travaux légers autorisés aux enfants dont l'âge est compris entre treize (13) et seize (16) ans ;

Vu l'Arrêté n°445/MINADER/CAB du 25 juillet 2018 déterminant les mentions devant figurer dans les contrats relatifs à la mise en œuvre des projets de certification et de programmes de durabilité dans la filière Café-Cacao ;

Vu l'Arrêté n°444/MINADER/CAB du 25 juillet 2018 déterminant la liste de manquements donnant lieu au retrait de l'agrément pour la mise en œuvre des projets de certification et de programmes de durabilité dans la filière Café-Cacao, ainsi que pour l'achat du café ou du cacao certifié ou durable ;

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 conditions au traitement des données à caractère personnel (DCP) ;

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°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;

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°2019-0494 du Conseil de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;

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 de l'activité :

- du correspondant à la protection des données, personnes morales ;
- de formation en matière de protection des données à caractère personnel ;
- d'audit en matière de protection des données à caractère personnel ;

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 données à caractère personnel ;

Vu la Résolution n°2021-161 du 30 juin 2021 portant désignation du Directeur Général par Intérim de l'Autorité de Régulation des Télécoms/TIC de Côte d'Ivoire (ARCTI) ;

Vu le Rapport d'audit de protection des données personnelles de K'ORIGNS ;

Par les motifs suivants :

Considérant que conformément à l'article 53 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, les responsables du traitement doivent procéder à la mise en conformité des traitements qu'ils opèrent avec ladite loi ;
Considérant que pour faciliter cette mise en conformité l'Autorité de protection a, par décision n°2017-0354 du 26 octobre 2017 définit la 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 ;

Considérant que K'ORIGINS est une Société Anonyme (SA) spécialisée dans le domaine du développement durable, en Côte d'Ivoire et dans la sous-région Ouest Africaine, qui a pour objectif de préserver la biodiversité et la durabilité par des projets qui améliorent la qualité de vie de ses bénéficiaires, dont le siège social est sis au II Plateaux Vallons, 3ème tranche, Lot 1723 ilot 162, 25 BP 327 Abidjan 25, téléphone (+225) 27 22 41 56 60 ;

Considérant que K'ORIGINS a saisi l'Autorité de protection d'une demande de mise en conformité ;
Considérant que K'ORIGINS a désigné un correspondant à la protection et a procédé à la formation de son personnel ;

Que par ailleurs, K'ORIGINS a effectué son audit de protection des données personnelles ;

Considérant les recommandations contenues dans le rapport d'audit de protection des données personnelles ;

Après en avoir délibéré,

DECIDE :

Article 1 :

K'ORIGINS est autorisée à effectuer les traitements des données mentionnées dans l'annexe 1 de la présente décision.

Les données non mentionnées dans l'annexe 1 ne devront aucunement faire l'objet d'un quelconque traitement, de la part de K'ORIGINS.

Article 2 :

K'ORIGINS est autorisée à effectuer les traitements énumérés dans l'annexe 2 de la présente décision.

Article 3 :

K'ORIGINS est autorisée à transférer vers la Hollande, les données énumérées dans l'annexe 3 de la présente décision.

Article 4 :

K'ORIGINS est autorisée à communiquer les données traitées uniquement aux destinataires habilités, notamment :

- aux agents suivant leurs habilitations et partenaires des projets basés en Côte d'Ivoire ;
- au conseil du café cacao ;
- les autorités publiques ivoiriennes habilitées agissant dans le cadre de l'exercice de leurs missions ;
- le Procureur de la république ;
- les officiers de police judiciaire munis d'une réquisition;
- les sous-traitants suivant leur domaine d'activités.

Article 5 :

L'Autorité de protection interdit à K'ORIGINS de transférer sans autorisation préalable de l'Autorité de protection, les données traitées vers des pays tiers, autre que la Hollande.

K'ORIGINS est tenue avant tout transfert de données hors de la Côte d'Ivoire, de les stocker sur le territoire de la République de Côte d'Ivoire.

Article 6 :

Conformément à l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, K'ORIGINS doit s'assurer que ses sous-traitants apportent des garanties suffisantes au regard des mesures de sécurité technique et organisationnelle relatives aux traitements de données qu'ils opèrent.

Il incombe à K'ORIGINS ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

Article 7 :

Les traitements de données autorisés dans la présente décision correspondent aux sept (07) finalités suivantes :

- la gestion des projets de durabilité ;
- la gestion juridique ;
- la gestion des dossiers administratifs ;
- la gestion financière et de comptabilité ;
- la gestion des Ressources Humaines ;
- la gestion de la logistique des projets ;
- la communication des données vers la Hollande.

Les traitements afférents aux finalités ci-dessus sont listés dans l'annexe 4 de la présente décision.

Article 8 :

K'ORIGINS est tenue de mettre en œuvre les prescriptions énoncées dans l'annexe 5 de la présente décision. Elle le fait dans les délais prévus dans ladite annexe.

La mise en œuvre desdites prescriptions fera l'objet d'un contrôle par l'Autorité de Protection.

L'Autorité de protection délivrera une attestation de conformité à K'ORIGINS, lorsque toutes les prescriptions auront été mises en œuvre.

Article 9 :

En application de l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, K'ORIGINS est tenue d'établir, pour le compte de l'Autorité de protection, un rapport annuel sur le respect des dispositions de l'article 41 de ladite Loi.

K'ORIGINS communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 10 :

L'Autorité de Protection procède à des contrôles auprès de K'ORIGINS, afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 11 :

K'ORIGINS est tenue de procéder au paiement des frais de dépôts de demande d'autorisation auprès du Greffe de l'ARTCI, conformément à la Décision n°2016-0201 de l'Autorité de protection de la République de Côte d'Ivoire fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel.

L'Autorité de Protection lui délivrera une facture à cet effet.

Article 12 :

La présente Décision entre en vigueur à compter de la date de sa notification à K'ORIGINS.

Article 13 :

Le Directeur Général par Intérim est chargé de l'exécution de la présente décision, qui sera publiée au Journal Officiel de la République de Côte d'Ivoire et sur le site internet de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire.

Fait à Abidjan, le 1er février 2022
En deux (2) exemplaires originaux

Le Président

ARTCI

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL