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

CONSEIL DE REGULATION

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2020-0530

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

EN DATE DU 28 JANVIER 2020

PORTANT AUTORISATION DE TRANSFERT DE DONNEES A CARACTERE PERSONNEL

PAR LE CABINET BAH BLESSON & COMPANY SARL

VERS L'IRLANDE

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/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°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°2014-106 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°2014-105 du 12 mars 2014 portant définition des conditions de fourniture des prestations de cryptologie ;

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° 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 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°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°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° 2020-0529 de l'Autorité de protection de la République de Côte d'ivoire en date du 28 janvier 2020 portant autorisation de traitement de données à caractère personnel par le cabinet Bah Blesson & Company sarl

Par les motifs suivants :

Considérant la demande d'autorisation de transfert de données à caractère personnel introduite par le Cabinet Bah Blesson & Company, Société à Responsabilité Limitée SARL, au capital de cinq millions (5 000 000) de francs CFA, sis à Abidjan, Plateau à la rue du Dr Crozet, 18 BP 2884 Abidjan 18, immatriculé au Registre du commerce et du crédit mobilier sous le numéro CI-2016-B-27079, CC : N°1652341 ;

Considérant que le Cabinet Bah Blesson & Company est un Cabinet Conseil en Management ;

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 transfert initiée par le Cabinet Bah Blesson & Company :

- **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 (03) mois ;

Considérant que, le Cabinet Bah Blesson & Company est une personne morale de droit ivoirien dûment immatriculée au Registre du Commerce et du Crédit Mobilier, 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 Directeur Général daté de moins de trois (03) mois ;

Il convient de noter que la demande de transfert présentée par le Cabinet Bah Blesson & Company est accompagné 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 que la demande de transfert du Cabinet Bah Blesson & Company est recevable en la forme.

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

L'Autorité de protection constate que le transfert envisagé par le Cabinet Bah Blesson & Company concerne les données dont le traitement a été autorisé par la décision n°2020-0529 du 28 janvier 2020 :

- **Les données d'identification :** nom, prénom, email ; téléphone mobile ;
- **Les données de connexion :** E-mail, nom d'utilisateur, mot de passe ;
- **Les données bancaires :** numéro de carte bancaire ; zip code ;

Considérant que les données sus-citées sont traitées dans le cadre de la gestion des clients et des usagers de la plateforme « business info », traitement autorisé par la décision n° 2020-0529 du 28 janvier 2020 ;

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

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

Considérant qu'en l'espèce, la demande de transfert soumise par le Cabinet Bah Blesson & Company à l'Autorité de protection, a pour finalité de communiquer les données traitées à la société MICROSOFT IRELAND OPERATIONS LIMITED, en Irlande ;

Qu'en effet, la société MICROSOFT IRELAND OPERATIONS LIMITED, est son sous-traitant ;

L'Autorité de protection en déduit que la finalité existe et qu'elle 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°450-2013 relative à la protection des données à 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 à 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 l'Irlande, pays de l'Union Européenne soumis au Règlement Général sur la Protection des données (RGPD) ;

Considérant que l'Irlande a une Autorité de protection, dénommée Data Protection Commissioner (DPC) ;

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

L'Autorité de protection considère que le Cabinet Bah Blesson & Company a apporté des garanties nécessaires à la protection des données transférées à la société MICROSOFT IRELAND OPERATIONS LIMITED, en Irlande ;

En conséquence, le cabinet Bah Blesson & Company SARL peut être autorisé à transférer vers l'Irlande, les données telles que mentionnées dans le dossier de demande de transfert.

Toutefois, l'Autorité de protection prescrit à la demanderesse de lui fournir le numéro de déclaration / autorisation de la société MICROSOFT IRELAND OPERATIONS LIMITED, auprès de l'Autorité de protection de l'Irlande (DPC), 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 le demandeur indique que les personnes concernées pourront faire valoir leurs droits d'accès direct, d'opposition, de rectification et de suppression auprès du cabinet Bah Blesson & Company SARL ;

Considérant par ailleurs que la DPC de l'Irlande 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 Cabinet Bah Blesson & Company 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 à 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 Cabinet Bah Blesson & Company SARL 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 Data Protection Commissioner (DPC) 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 Cabinet Bah Blesson & Company SARL est autorisé à transférer les données collectées vers la société MICROSOFT IRELAND OPERATIONS LIMITED, conformément à la décision n°2020-0529 du 28 janvier 2020.

Le transfert des données traitées devra respecter les conditions de communication des données prévues à l'article 4 de la décision n°2020-0529 du 28 janvier 2020.

Les données non mentionnées ne devront faire l'objet d'aucun traitement de la part du Cabinet Bah Blesson & Company.

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.

Article 2 :

Le Cabinet Bah Blesson & Company SARL 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 Cabinet Bah Blesson & Company SARL, 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 3 :

Le Cabinet Bah Blesson & Company 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.

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

Il 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 4 :

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 Cabinet Bah Blesson & Company SARL établit un rapport annuel sur le transfert de données à caractère personnel vers les pays tiers.

Le Cabinet Bah Blesson & Company SARL communique ce rapport à l'Autorité de Protection, au plus tard le 31 janvier de l'année suivant l'exercice écoulé.

Article 5 :

L'Autorité de protection procède à des contrôles auprès du Cabinet Bah Blesson & Company SARL, afin de vérifier le respect de la présente disposition, dont la violation donnera lieu à des sanctions, conformément à la règlementation en vigueur.

Article 6 :

La présente décision entre en vigueur à compter de la date de sa notification au Cabinet Bah Blesson & Company SARL.

Article 7 :

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 28 janvier 2020
En deux (2) exemplaires originaux

Le Président

Dr DIAKITE Coty Souleïmane
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°2020-0536

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 03 MARS 2020

PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL PAR LA SOCIETE SUNU ASSURANCES VIE 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 / TIC ;

Vu le Code des Assurances de la CIMA ;

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°2019-372 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 de Membres du Conseil de Régulation 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°2014-0021 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 30 septembre 2014 portant conditions de la suppression des liens vers les données à caractère personnel, des copies ou des reproductions de celles-ci existants dans le service de communication électronique accessible 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 du 26 octobre 2017 portant vérification préalable ;

Vu la Décision n°2017-0354 du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Vu le rapport d'audit de situation de la société SUNU Assurances Vie 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 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, définit les étapes du processus de mise en conformité ;

Considérant que la société SUNU Assurances Vie Côte d'Ivoire, **Société Anonyme,** au capital de **2 000 000 000 FCFA**, immatriculée au Registre du Commerce et du Crédit Mobilier sous le numéro **CI.ABJ 1985 B-92922**, sise à Abidjan, 9 av. Houdaille, 01 BP 2016 Abidjan 01 COTE D'IVOIRE, Tél. : (225) 20 31 04 00 Fax : (225) 20 22 37 60, E-mail : cotedivoire.vie@sunu-group.com, a saisi l'Autorité de protection d'une demande de mise en conformité ;

Considérant que SUNU Assurances Vie, Correspondant à la protection, personne morale agréé par l'Autorité de protection, a effectué l'audit de situation de la société SUNU Assurances Vie Côte d'Ivoire, qui a fait ressortir un niveau de conformité avec la Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, moyen.

Considérant toutefois les recommandations et prescriptions faites par l'Autorité de protection dans le rapport définitif d'audit de situation et sous réserve de l'application de ces recommandations et prescriptions ;

Considérant que la société SUNU Assurances Vie Côte d'Ivoire s'engage à mettre en œuvre les recommandations et prescriptions formulées dans le rapport définitif d'audit de situation, en vue d'apporter des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements qu'elle effectue ;

Que la société SUNU Assurances Vie Côte d'Ivoire s'engage à veiller au respect de ces mesures ;

Après en avoir délibéré,

DECIDE :

Article 1 :

La société SUNU Assurances Vie Côte d'Ivoire est autorisée à effectuer le traitement 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 la société SUNU Assurances Vie Côte d'Ivoire.

Article 2 :

La société SUNU Assurances Vie Côte d'Ivoire est autorisée à effectuer les traitements énumérés dans l'annexe 2 de la présente décision.

Article 3 :

La société SUNU Assurances Vie Côte d'Ivoire est autorisée à transférer les des données énumérées dans l'annexe 3, aux sociétés de réassurance avec lesquelles elle est liée par un contrat t.

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

Article 4 :

La société SUNU Assurances Vie 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 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 clients de la société SUNU Assurances Vie Côte d'Ivoire, les sociétés de réassurance dans le respect des clauses contractuelles qui les lient.

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, la société SUNU Assurances Vie 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 société SUNU Assurances Vie Côte d'Ivoire ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

Article 6 :

Les traitements de données autorisés dans la présente décision ont pour finalités :

- La gestion de la relation clients ;
- La gestion commerciale ;
- La gestion des ressources humaines ;
- La gestion juridique ;
- La gestion informatique ;
- La gestion de la communication de la société ;
- La gestion administrative de la société ;
- La sécurité des personnes et des biens au sein et aux alentours des locaux ;
- Le contrôle d'accès ;

Les traitements afférents aux finalités ci-dessus sont listés dans l'annexe 4 de la présente décision.

Article 7 :

La société SUNU Assurances Vie Côte 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 la société SUNU Assurances Vie 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, la société SUNU Assurances Vie 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 société SUNU Assurances Vie 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 la société SUNU Assurances Vie 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 10 :

La société SUNU Assurances Vie Côte d'Ivoire est tenue de procéder au paiement des frais de dépôt 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 SUNU Assurances Vie 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 03 Mars 2020
En deux (2) exemplaires originaux

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

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

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

ANNEXE 1
CONSEIL DE REGULATION

DONNEES AUTORISEES AUX TRAITEMENTS

- **Etat-civil, Identité, Données d'identification :**	nom, prénom, date et lieu de naissance, photographie, sexe, image, numéro de plaque d'immatriculation.
- **Vie personnelle :**	Situation familiale, habitude de vie, numéro d'appartement, taille, poids.
- **Vie professionnelle :**	Profession, fonction, formation, catégorie professionnelle, expérience professionnelle, service, poste occupé, distinction, curriculum vitae, emploi précédent.
- **Informations d'ordre économique et financier :**	situation financière, revenus liés à sa profession, salaire, RIB, bulletin de salaire .
- **Données sensibles :**	filiation
- **Données de connexion :**	Email
- **Données de localisation :**	Adresse
- **Numéro d'identification national :**	Numéro de téléphone, numéro de CNI.
- **Données médicales :**	pathologie, affections, antécédents familiaux, examens médicaux, données relatives aux soins, numéro de police.

Fait à Abidjan, le 03 Mars 2020

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

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

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

ANNEXE 2
CONSEIL DE REGULATION

LISTE DES TRAITEMENTS

1. Entrée en Relation-clients
2. Proposition de produits d'assurance aux entreprises
3. Propositions de produits d'assurance aux Particuliers
4. Propositions de produits d'assurance par le biais des banques
5. Enregistrements des souscriptions
6. Validation et modification des contrats d'assurance
7. Collecte des données de santé
8. Communication des données de santé
9. Rédaction de courriers
10. Rédaction des rapports et contrats
11. Communication externe
12. Communication interne
13. Gestion des Rachats : partiel / total
14. Gestion des sinistres déclarés
15. Gestion du Bureau Direct
16. Remises de chèques
17. Collecte de données informatiques
18. communication de données informatiques
19. Consultation et Conservation des images des caméras
20. Gestion des serveurs
21. Gestion du parc informatique : Configuration et installation (maintenance) téléassistance
22. modifications de données informatiques
23. Vidéosurveillance
24. Assistance aux utilisateurs dans leurs taches
25. Emission de chèques
26. Gestion des systèmes d'accès (badges)
27. Support web
28. Gestion du recouvrement
29. Réassurance
30. Conduite de missions d'audit
31. Lutte anti blanchiment
32. conservation provisoire de pièces d'identité
33. enregistrement de données d'identification
34. Communication de dossiers
35. Conservation des dossiers des prospects, assurés, Personnel de SUNU
36. Scannage de tous les dossiers physiques
37. collecte et distribution du courrier

38. Constitution de dossiers pour appels d'offre
39. Collecte de documents
40. Encaissement des loyers
41. Rédaction de contrats de bail
42. Collecte de dossiers de stage
43. Collecte de dossiers de candidature pour emploi
44. Etablissement de polices d'assurance
45. Gestion des déclarations CNPS
46. Gestion de la rémunération
47. Gestion des missions
48. Gestion des compétences
49. Gestion des congés et permissions
50. Gestion des départs de l'entreprise
51. Gestion des impôts sur les Traitements et Salaires (ITS)
52. Rédaction de contrats de stage
53. Rédaction de contrats de travail
54. Transfert

Fait à Abidjan, le 03 Mars 2020

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

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

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

CONSEIL DE REGULATION

ANNEXE 3

DONNEES AUTORISEES AU TRANSFERT

- **Etat-civil, Identité, Données d'identification :** Nom, prénom, date et lieu de naissance, numéro de police.

- **Vie personnelle :** Habitude de vie, situation familiale.

- **Vie professionnelle :** Situation professionnelle.

- **Informations d'ordre économique et financier :** Revenu, situation financière.

- **Données médicales :** Pathologie, affection, antécédents familiaux, données relatives aux soins.

Fait à Abidjan, le 03 Mars 2020

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

RTCI

CONSEIL DE REGULATION

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

ANNEXE 4

LISTE DES TRAITEMENTS PAR FINALITES

FINALITES	TRAITEMENTS
La gestion de la relation clients	- Entrée en Relation-clients - Proposition de produits d'assurance aux entreprises - Propositions de produits d'assurance aux Particuliers - Propositions de produits d'assurance par le biais des banques
La gestion commerciale	- Enregistrements des souscriptions - Gestion des Rachats : partiel / total - Gestion des sinistres déclarés - Gestion du Bureau Direct Remises de chèques - Emission de chèques - Validation et modification des contrats d'assurance - Collecte des données de santé - Communication des données de santé - Gestion du recouvrement - Réassurance
La gestion juridique	- Rédaction de courriers - Rédaction des rapports et contrats - Constitution de dossiers pour appels d'offres
La gestion des ressources humaines	- Collecte de dossiers de stage - Collecte de dossiers de candidature pour emploi - Etablissement de polices d'assurance - Gestion des déclarations CNPS - Gestion de la rémunération - Gestion des missions - Gestion des compétences - Gestion des congés et permissions - Gestion des départs de l'entreprise - Gestion des impôts sur les Traitements et Salaires (ITS) - Rédaction de contrats de stage - Rédaction de contrats de travail
La gestion informatique	- Collecte de données informatiques - Communication de données informatiques - Consultation et Conservation des images des caméras - Gestion des serveurs - Gestion du parc informatique : Configuration et installation (maintenance) téléassistance

	- Modifications de données informatiques - Assistance aux utilisateurs dans leurs taches - Support web
La sécurité des personnes et des biens au sein et aux alentours de ses locaux	- Vidéosurveillance
Le contrôle d'accès	- Gestion des systèmes d'accès (badges)
La gestion administrative de la société	- Conduite de missions d'audit - Lutte anti blanchiment - conservation provisoire de pièces d'identité - enregistrement de données d'identification Communication de dossiers - transfert - Conservation des dossiers des prospects, assurés, Personnel de SUNU - Scannage de tous les dossiers physiques - collecte et distribution de courriers - Collecte de documents - Encaissement des loyers - Rédaction de contrats de bail
La gestion de la communication de la société	- Communication externe - Communication interne

Fait à Abidjan, le 03 Mars 2020

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

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

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

CONSEIL DE REGULATION
ANNEXE 5

PRESCRIPTIONS ET DELAIS D'EXECUTION

POINTS D'ANALYSE	PRESCRIPTIONS	DELAIS D'EXECUTION
La légitimité et la licéité des traitements	Concernant le recueil du consentement des personnes concernées : ➢ dans le cadre de la gestion de la clientèle : - mettre à la disposition des personnes concernées, un formulaire de recueil du consentement préalable pour les traitements à effectuer. Les formulaires devront être mis à disposition lors de l'entrée en relation clientèle ; - insérer des clauses de consentement préalable dans les conditions générales de prestation de services ou dans les contrats proposés aux clients ; ➢ dans le cadre du recrutement et de la gestion du personnel : - mettre à disposition, lors de l'entretien d'embauche, un formulaire de recueil du consentement préalable ; - insérer des clauses de consentement préalable dans les contrats de travail proposés à la signature du personnel ; - par tous autres moyens laissant preuve écrite.	**60 jours**
La finalité des traitements	RAS	RAS
Les délais de conservation	➢ Concernant la conservation des données relatives à la gestion du personnel : 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 :	**6 mois**

	- 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 de la clientèle : Les données traitées peuvent être conservées pendant toute la durée de la relation client. En cas de cessation de la relation client, une période supplémentaire de dix (10) ans est autorisée, à compter de la date de cessation de la relation client, conformément à l'article 24 de l'Acte Uniforme portant organisation et harmonisation des comptabilités des entreprises. ➢ Concernant l'archivage électronique : - Elaborer une politique d'archivage - Procéder à un archivage électronique des données conformément aux dispositions du n°2016-851 du 19 Octobre 2016. ➢ Concernant les données biométriques : - Communiquer la base de données biométriques à l'Office National de l'Identification ; - Effacer de la base de données, les données biométriques collectées ; - Mener une étude d'impact vie privée	
La proportionnalité des données	➢ Dans le cadre de la gestion des ressources humaines Sont interdits, la collecte et le traitement des données suivantes : - La filiation des agents ;	**RAS**

	- Le casier judiciaire des agents ; - Les empreintes digitales des agents pour l'accès aux services généraux, le contrôle de présence, l'identification des agents pour la fourniture de service. ➢ La gestion des données sensibles - Faire l'inventaire des données sensibles traitées ; - Analyser la proportionnalité des données sensibles traitées ; - Epurer sa base de données des informations sensibles disproportionnées et conserver les données pertinentes ; - Sécuriser les données sensibles ; - Définir les accès aux données sensibles ; - Procéder au recueil du consentement sur un formulaire distinct.	
La transparence des traitements	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 leurs droits d'accès et de rectification ; - la durée de conservation des données ; - l'éventualité de tout transfert de données à destination de pays tiers.	**60 jours**
	L'information se fera par le biais de : - mentions légales sur les formulaires, contrats et sur le site internet de la société SUNU Assurances Vie Côte d'Ivoire , - affiches dans tous les lieux où sont opérés des traitements de données à caractère personnel ;	

	Diminuer la possibilité que les caractéristiques des sites web soient exploitées pour porter atteinte aux données à caractère personnel	
Le système informatique	La société SUNU Assurances Vie Côte d'Ivoire doit mettre en œuvre les 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 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 limitation des risques afin que des personnes non autorisées n'accèdent pas physiquement aux données à caractère personnel (liste des personnes autorisées, authentification des collaborateurs et des visiteurs, trace des accès, alerte en cas d'effraction, etc.). - la mise en place d'une étude d'impact (PIA) pour les données sensible, afin de maîtriser les risques que les traitements du cabinet médical font peser sur les droits et libertés des personnes concernées - Rendre les données à caractère personnel incompréhensibles à toute personne non autorisée à y avoir accès (chiffrement symétrique ou asymétrique, utilisation d'algorithmes publics réputés forts, certificat d'authentification, etc.). - La formalisation du PRA (Plan de Reprise d'Activité) ou du PCA (Plan de Continuité d'Activité), le diffuser auprès des personnels concernés (internes, externes, prestataires) et tester régulièrement son efficacité. - Disposer d'une organisation opérationnelle permettant de détecter et de traiter les événements susceptibles d'affecter les libertés et la vie privée des personnes concernées (définition des responsabilités, plan de réaction, qualifier les violations, etc.). - Assurer l'enregistrement et l'imputabilité des consultations et actions des utilisateurs du traitement, afin de pouvoir fournir des preuves dans le cadre d'enquêtes (système de journalisation, protection, analyse, conservation, etc.). - La mise à jour de la charte informatique en prenant en compte les DCP et la diffuser à l'ensemble des utilisateurs ;	**90 jours**

	- Limiter la vraisemblance des menaces liées aux opérations de maintenance sur les matériels et logiciels (contrat de sous-traitance, télémaintenance, accord de l'utilisateur, effacement des données, etc.). - Effacer de façon sécurisée ou bien détruire physiquement les supports de stockage mis au rebut contenant les DCP. - Réaliser une veille sur les vulnérabilités découvertes dans les logiciels (y compris les firmwares) utilisés en exploitation, et les corriger dès que possible.	
Les destinataires des données traitées	La société SUNU Assurances Vie Côte d'Ivoire doit : - Communiquer les données traitées uniquement aux destinataires habilités ;	**Sans délai**
Exactitude des données	La société SUNU Assurances Vie Côte d'Ivoire doit : - 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 ; - mettre à jour périodiquement les fichiers informatiques contenant les données à caractère personnel.	**06 mois**
Les sous-traitants	La société SUNU Assurances Vie Côte d'Ivoire doit : - inclure des clauses relatives à la protection des données à caractère personnel dans les contrats passés avec ses sous-traitants ; - 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 à la société SUNU Assurances Vie Côte d'Ivoire et aux sous-traitants de veiller au respect de ces mesures.	**12 mois**
La vidéosurveillance	La société SUNU Assurances Vie Côte d'Ivoire doit : - Obtenir une autorisation pour l'utilisation d'un système de vidéosurveillance ; - Requérir l'accord du personnel pour la mise en place du dispositif de vidéosurveillance - informer les personnes concernées de l'existence d'un dispositif de vidéosurveillance, au moyen d'affiches placées à hauteur de vue dans les zones filmées par les caméras, et de pictogrammes placés de façon visible, aux entrées et aux sorties des locaux sous surveillance. - Les affiches et pictogrammes doivent indiquer, d'une façon claire et visible, les informations	

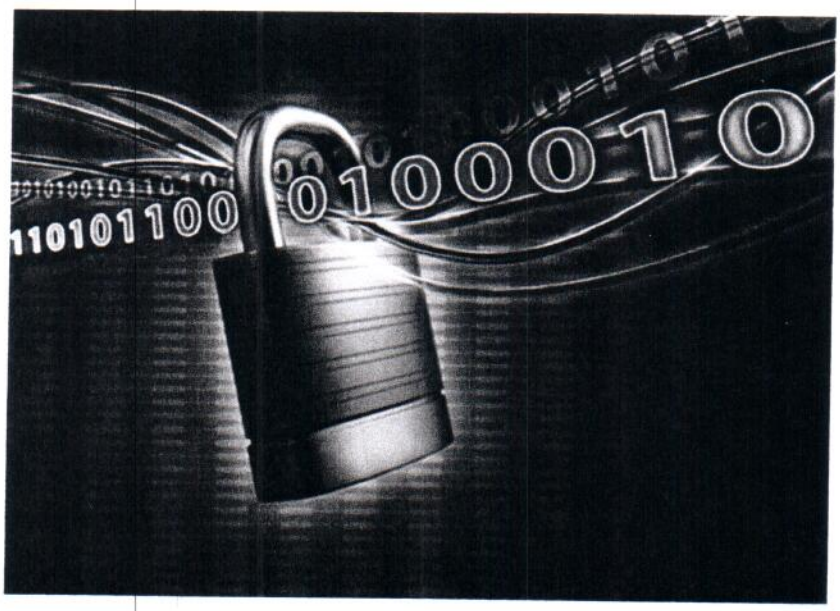
	suivantes : - Le nom du responsable du traitement ; - Le fait que l'établissement est placé sous vidéosurveillance ; - La finalité du dispositif (la sécurité des biens et des personnes) ; - Les coordonnées du contact pour l'exercice, par les personnes concernées, des droits d'accès, de rectification et d'opposition ; - Le numéro de l'autorisation octroyée par l'Autorité de protection. - Veiller à ce que les caméras pouvant filmer les zones de circulation ne portent pas atteinte à la vie privée des personnes concernées ; - Ne pas diriger ses caméras de vidéosurveillance sur les postes de travail de ses employés ; - Ne pas poser les caméras de vidéosurveillance dans les toilettes, les lieux de pause ou de repos de ses employés. La société SUNU Assurances Vie Côte d'Ivoire doit également conserver les données collectées pendant une durée **de trente (30) jours**. En cas d'incidents, les données collectées devront être conservées pendant une période **d'un (01) an,** à compter de la dernière sauvegarde mensuelle.	
Le correspondant à la protection	La société SUNU Assurances Vie Côte d'Ivoire doit mettre à la disposition du Correspondant, les outils adéquats pour l'exercice de ses fonctions. Elle doit en outre, favoriser la désignation d'un chargé de la protection au sein de toutes les autres directions.	**30 jours**
les droits d'accès, de rectification, d'effacement et d'opposition	La société SUNU Assurances Vie Côte d'Ivoire doit 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	La société SUNU Assurances Vie Côte d'Ivoire doit : - former son personnel sur la protection des données à caractère personnel. - Relayer efficacement l'action du Correspondant au sein des directions.	**90 jours**

Les procédures	La société SUNU Assurances Vie Côte d'Ivoire doit : - élaborer une charte de protection des données à caractère personnel ; - établir une politique de sécurité et de confidentialité ; - élaborer une procédure de gestion des droits des personnes concernées ; - intégrer des clauses de recueil du consentement et de transparence dans les procédures ; - d'élaborer une procédure de gestion des plaintes des personnes concernées ; - Conformer les procédures existantes à la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.	**90 jours**
La déclaration des fichiers	La société SUNU Assurances Vie Côte d'Ivoire doit introduire une demande d'autorisation de traitements de données à caractère personnel auprès de l'Autorité de protection	

Fait à Abidjan, le 03 Mars 2020

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL



MISE EN CONFORMITE DE SUNU ASSURANCES VIE C.I AVEC LA LOI 2013-450 DU 19 JUIN 2013 RELATIVE A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

1. Contexte

Les traitements de données à caractère personnel opérés par les entreprises, dans le cadre de leurs activités, sont soumis aux formalités préalables et au respect des différents principes prévus par la Loi n°2013-450 du 19 juin 2013, relative à la protection des données à caractère personnel.

Aux termes de l'article 53 de ladite Loi, les responsables du traitement ont l'obligation de se mettre en conformité avec ses dispositions.

Pour répondre donc à cette exigence, la Société SUNU Assurances Vie Côte d'Ivoire a décidé de démarrer son processus de mise en conformité. Ce processus, conformément à la décision de l'autorité de protection, comprend la désignation d'un correspondant à la protection des données à caractère personnel agréé par l'ARTCI.

C'est dans ce cadre que la société AS CONSULTING, spécialisée dans la prestation de services informatiques et agréée par l'autorité de protection, a été désignée par SUNU Assurances Vie Côte d'Ivoire comme correspondant pour l'accompagner dans ce processus de mise en conformité. Une démarche qui va dans le sens des objectifs de cet assureur.

Créée le 1er janvier 1985 par le groupe UAP International, la société devient AXA Vie Côte d'Ivoire suite à sa fusion avec le groupe AXA, en 1998. Aujourd'hui, entrée dans les filiales du Groupe SUNU, elle a pris la même dénomination pour devenir SUNU Assurances Vie Côte d'Ivoire.

Leader, depuis 2011, de l'assurance Vie en Côte d'Ivoire et dans les 11 pays de la zone CIMA, SUNU Assurances Vie Côte d'Ivoire se positionne comme un pionnier dans la bancassurance avec des produits innovants et une efficacité opérationnelle reconnue.

Le domaine de prédilection de la société est le segment des entreprises, auxquelles sont proposées des produits de retraite et de prévoyance collectives, ainsi que des indemnités de fin de carrière.

2. Enjeux

La Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, rend les entreprises responsables de la protection des données qu'elles manipulent (données des clients, données du personnel, etc.).

L'image d'une entreprise peut être négativement affectée, lorsque celle-ci est incapable de communiquer aux personnes concernées, les données qu'elles demandent ou lorsqu'une faille de sécurité a été rendue publique.

La mise en conformité implique que l'entreprise est en mesure de démontrer qu'elle a pris les dispositions techniques, organisationnelles et juridiques nécessaires à la protection des données qu'elle détient.

La Loi relative à la protection des données à caractère personnel est génératrice de changements au sein de l'entreprise qui doit :

- désigner un correspondant à la protection ;
- élaborer une data gouvernance en lien avec la stratégie de l'entreprise et en accord avec la règlementation.

Il s'agit d'une approche dynamique et permanente de la gestion de la protection des données à caractère personnel.

Une telle approche suppose la compréhension de la nouvelle gouvernance des données à caractère personnel, telle que définie par la Loi.

Il est donc primordial pour l'entreprise de former son personnel et d'effectuer un état des lieux des traitements, des données manipulées, des moyens, et des risques. Cet état des lieux permettra de détecter les dysfonctionnements éventuels, et d'élaborer une stratégie intégrant les exigences de conformité de la Loi.

Il est en outre important de définir l'échelle des responsabilités au sein de l'entreprise (Correspondant, DSI, RSSI...) et dans un périmètre plus large (sous-traitants, hébergeurs cloud, co-responsables de traitements, etc.).

La nouvelle gouvernance des données personnelles implique également la maitrise des données (nature, volume, localisation, niveau de criticité, cycle de vie, etc.), ainsi que la maitrise de techniques de sécurité telles que l'anonymisation, la pseudonymisation, le chiffrement, la traçabilité, la détection de fuite, etc.

Par ailleurs, une analyse de conformité permettra de mesurer les écarts entre l'existant et les exigences réglementaires.

En vue de faciliter la mise en conformité des entreprises avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, l'Autorité de protection a défini, par décision n°2017-0354 du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, une procédure dite « processus de mise en conformité ». Cette procédure permet à l'entreprise de se conformer à la loi et d'intégrer dans ses pratiques, la culture de la protection des données.

Cette procédure, en plus de permettre à l'entreprise de se conformer à ses obligations règlementaires, intègre la culture de la protection des données à caractère personnel au sein des entreprises.

Le processus de mise en conformité se déroule selon les étapes suivantes :

- la sensibilisation et la formation de l'ensemble du personnel ;
- le diagnostic des activités et processus métiers ;
- l'inventaire des données à caractère personnel et la classification des données traitées ;
- l'inventaire des traitements effectués y compris les transferts de données à l'étranger ;
- l'identification et la classification des supports de traitements ;

- l'analyse des critères relatifs aux données traitées ;
- l'analyse d'écarts ;
- la définition d'un plan d'actions correctives ;
- la déclaration des traitements et le dépôt de la demande d'autorisation.

A l'issue de cette procédure, une autorisation unique de traitement de données est délivrée à l'entreprise. Une attestation de conformité est également délivrée au responsable du traitement après correction des écarts constatés.

La mise en conformité est le point de départ d'un contrat de confiance entre l'entreprise et ses partenaires.

3. Méthodologie

La méthodologie adoptée correspond à celle définie dans l'annexe de la décision N°2017-0354 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 Octobre 2017, portant procédure de mise en conformité. Tout d'abord, les responsables des différents services et directions ont suivi une formation sur les notions de protection des données à caractère personnel. Ensuite, un audit de situation a été mené pour se faire une idée de l'état de conformité de l'entreprise, en ce qui concerne la protection de ses données.

3.1. La formation du personnel

La formation du personnel a eu lieu le mardi 21 Novembre 2017 au siège de SUNU Assurances Vie Côte d'Ivoire. Elle a été faite par M. SEKA Adiko Yves Florent, Directeur Technique de AS CONSULTING.

Elle avait pour objectifs de faire connaitre et comprendre :

- Les enjeux de la mise en conformité avec la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- Les différents principes de la protection des données à caractère personnel ;
- La notion de consentement préalable, sa nécessité dans le contexte de mise en œuvre d'un traitement et les exceptions qui lui sont applicables ;
- Le contenu des données dites sensibles ;
- Les différents régimes et formalités préalables pour le traitement des données à caractère personnel ;
- Les conditions et les modalités de transfert des données à caractère personnel hors de l'espace CEDEAO ;
- L'exercice des droits des personnes concernées par le traitement des données à caractère personnel ;
- Les obligations du responsable du traitement ;
- Le statut et la composition de l'Autorité de protection des données à caractère personnel ;

- Les missions et les pouvoirs de l'Autorité de protection des données à caractère personnel ;
- Les sanctions pouvant être mises en œuvre par l'Autorité de protection des données à caractère personnel ;
- Le statut, le profil et les missions du Correspondant à la protection des données à caractère personnel ;

Quinze (15) collaborateurs de la société SUNU Assurances Vie Cote d'Ivoire ont participé à la formation *(Voir liste de présence en annexe PP.38-41)*. Ils sont repartis dans les directions et services suivants :

- Direction Comptable et Financière
- Direction des Prestations
- Service du Contrôle de Gestion
- Direction Administrative et Juridique
- Direction des Systèmes d'Informations
- Département Marketing et Business Développement
- Département Commercial Bancassurance
- Direction Etude et Actuariat
- Département Communication et Relations Clients
- Direction Production et Encaissement
- Service Archives
- Département Audit Interne et Conformité

3.2. L'audit de situation

L'audit de situation s'est réalisé selon les étapes ci-après :

1- La réalisation des interviews :

Les agents ont été soumis à une série de questions de type ouvert et fermé *(Voir en annexe PP.38-41)*. Cela a permis de faire un diagnostic des activités de chaque direction et service, afin d'identifier celles liées aux traitements de données à caractère personnel ;

2- L'analyse et l'identification des données à caractère personnel ;

3- L'évaluation et le rapprochement des données conformément aux critères DCP :

Une analyse a été faite pour déceler les écarts entre les traitements et les critères relatifs à ladite loi.

4. Règles en vigueur

4.1. Le droit applicable à SUNU Assurances Vie Côte d'Ivoire cadre légal et institutionnel

4.1.1. Le cadre légal

Le cadre légal des traitements opérés par SUNU Assurances Vie Côte d'Ivoire est constitué par les textes suivants :

4.1.1.1.Textes régionaux

- Le traité CIMA du 10 juillet 1992, instituant une organisation intégrée de l'industrie des assurances dans les Etats africains ;
- L'Acte additionnel A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel ;
- L'Acte additionnel A/SA.2/01/10 du 16 février 2010 sur les transactions électroniques ;
- L'Acte Uniforme révisé relatif aux droits des Sociétés Commerciales et des Groupements d'Intérêt Economique ;
- Le règlement n°007/CIMA/PCMA/PCE/2018 Modifiant et Complétant le Régime du contrat d'Assurance.

4.1.1.2.Textes nationaux

- **Lois**

- Loi N° 2016-992 du 14 novembre 2016 relative à la lutte contre le blanchissement des capitaux et le financement du terrorisme ;
- La Loi n°2015-532 du 20 juillet 2015portant Code du travail ;
- La Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- La Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité ;
- La Loi n°2013-546 du 30 juillet 2013 relative aux Transactions électroniques.

- **Décrets**

- 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 ;

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

- 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 ;

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

- Décret n°2019-947 du 13 novembre2019 portant nomination du Président de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

- 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) ;

- Décret n°2019-372 du 24 Avril 2019 portant nomination du Directeur Général de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire .

- **Arrêté**

- 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.

- **Décisions de l'Autorité de protection**

- 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 ;

- 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 ;

- 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 ;

- la Décision n°2017-0352 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 Octobre 2017 portant autorisation de contrôle du respect des obligations en matière de données à caractère personnel ;

- la Décision n°2017-0353 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 Octobre 2017portant vérification préalable ;

- 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 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

4.1.2. Le cadre institutionnel

Conformément à l'article 46 de la Loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, les missions de l'Autorité de protection ont été confiées à l'Autorité en charge de la Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI).

Créée par l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications/TIC, l'ARTCI est une Autorité Administrative Indépendante, dotée de la personnalité juridique, de l'autonomie financière et de pouvoirs spéciaux. Elle est composée d'un Conseil de Régulation, d'un collège de sept (7) membres, et d'une Direction Générale.

En sa qualité d'Autorité de protection, l'ARTCI est chargée :

- d'informer les personnes concernées et les responsables du traitement de leurs droits et obligations ;
- de recevoir les déclarations et d'octroyer les autorisations pour la mise en œuvre de traitements des données à caractère personnel, ou de les retirer dans les cas prévus par la loi ;
- de recevoir les réclamations et les plaintes relatives à la mise en œuvre des traitements de données à caractère personnel et d'informer les auteurs de la suite accordée à celles-ci ;
- de déterminer les garanties indispensables et les mesures appropriées pour la protection des 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 loi ;
- d'élaborer des règles de conduite relatives aux traitements et à la protection des données à caractère personnel.

4.2. Les principes généraux applicables

Les principes sont brièvement développés ci-après :

4.2.1. La légitimité du traitement

Ce principe signifie que le consentement sans ambiguïté de la personne concernée est exigé préalablement à tout traitement de données à caractère personnel.

En effet, le traitement de données à caractère personnel est considéré comme légitime si la personne concernée donne expressément son consentement préalable.

Cependant, il peut être dérogé à cette exigence pour les motifs suivants.

- l'exécution d'une mission effectuée dans l'intérêt public ;
- le respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- l'exécution d'un contrat auquel la personne concernée est partie ;
- la sauvegarde des intérêts vitaux de la personne concernée.

4.2.2. La finalité du traitement

Ce principe définit le lien entre les données et les traitements. Les données à caractère personnel ne peuvent être recueillies et traitées que « pour des finalités déterminées, explicites et légitimes » et leur utilisation ultérieure doit toujours être compatible avec ces finalités.

Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime, correspondant aux missions du responsable du traitement.

4.2.3. La pertinence et la proportionnalité des données

Les données personnelles doivent être adéquates, pertinentes et non excessives, au regard des finalités pour lesquelles elles sont traitées. Seules doivent être traitées les informations pertinentes et nécessaires pour atteindre la finalité définie par le responsable du traitement.

4.2.4. La conservation limitée des données

Les données traitées doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées.

4.2.5. L'exactitude des données

Tous les efforts doivent être faits pour que les données traitées soient correctes et actuelles. Si ce n'est pas le cas, les données personnelles doivent être rectifiées, mises à jour ou bien effacées.

4.2.6. L'obligation de Transparence

Le responsable du traitement doit fournir à la personne concernée, l'information nécessaire relative aux données qu'il traite. Il doit lui assurer la possibilité d'un contrôle personnel. Le responsable du traitement doit avertir la personne concernée dès la collecte des données et en cas de transmission de ses données à des tiers.

En cas de demande de la personne concernée, le responsable du traitement doit fournir des renseignements quant aux données personnelles enregistrées et quant à leur utilisation, et effacer les informations dont le traitement ne serait pas conforme à la loi.

4.2.7. L'obligation de sécurité et de confidentialité

Le responsable du traitement est astreint à une obligation de sécurité. Il doit prendre les mesures nécessaires pour garantir l'intégrité, la confidentialité des données et éviter leur divulgation.

Le responsable du traitement ne peut communiquer les données traitées qu'à des destinataires légitimes ou habilités à en prendre connaissance.

4.2.8. Le respect des droits des personnes concernées

Les personnes concernées ont un droit :

- à l'information ou au questionnement,
- d'accès,
- d'opposition,
- de rectification,
- à l'oubli,
- à la portabilité.

4.3. Les règles applicables à SUNU Assurances Vie Côte d'Ivoire

Outre les principes généraux à respecter, SUNU Assurances Vie Côte d'Ivoire a l'obligation de :

- désigner un correspondant à la protection ;
- introduire une demande d'autorisation pour les traitements relatifs aux données à caractère personnel qu'elle opère.

4.3.1. La désignation d'un Correspondant à la protection des données à caractère personnel

Aux termes de l'article 9 de la loi 2013-450 du 19 juin 2013 relative à la protection des données la désignation d'un correspondant à la protection fait partie des conditions minimum de recevabilité d'une demande d'autorisation de traitement de données à caractère personnel. La désignation du correspondant obéit aux conditions 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.

La désignation du correspondant à la protection des données doit être approuvée par l'Autorité de protection, lorsqu'il s'agit d'une personne physique.

Le correspondant à la protection peut également être une personne morale qui dispose d'un agrément à la fonction de correspondant délivré par l'ARTCI.
Le correspondant est chargé d'assurer, d'une manière indépendante, le respect de la Loi. Il bénéficie des qualifications requises pour exercer ses missions. Il tient une liste des traitements effectués, immédiatement accessible à toute personne en faisant la demande, et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions. Le correspondant peut saisir l'Autorité de protection des difficultés qu'il rencontre dans l'exercice de ses missions.

4.3.2. La demande d'autorisation de traitement

SUNU Assurances Vie Côte d'Ivoire sera soumise à une autorisation de traitement conformément à l'article 7 de la loi 2013-450 du 19 juin 2013, en raison des objets, des finalités particulières mais aussi de l'existence de flux transfrontaliers de données liés aux traitements qu'elle effectue.

5. Etat des lieux de la protection des données à caractère personnel

L'état des lieux de la protection des données à caractère personnel de SUNU Assurances Vie Côte d'Ivoire comporte les étapes suivantes :

- l'organisation générale de SUNU Assurances Vie Côte d'Ivoire ;
- l'inventaire des traitements ;
- l'état de la conformité.

Les résultats qui suivent et les commentaires intègrent les différents entretiens menés avec les directions.

5.1. Sur l'organisation générale de SUNU Assurances Vie Côte d'Ivoire

5.1.1. Identification des activités impliquant le traitement de données à caractère personnel

La première partie du diagnostic des activités et processus métiers visait à se faire une idée du niveau de connaissance de l'activité des assurances et des données personnelles. Le questionnaire a porté sur les points suivants :

✓ *Existence pour chaque activité d'un seul et unique responsable*

Il existe effectivement un seul et unique responsable pour chaque activité, au sein des différents services et directions.

✓ *L'effectif total des directions / services interviewés*

Un entretien a été mené avec chaque responsable des directions et services. L'objectif était de connaître le nombre de personnes susceptibles de manipuler les données à caractère personnel dans chaque direction ou service. Ces entretiens ont relevé que les directions et services interviewés disposent d'un effectif de total de 137 personnes.

✓ *Les activités de la direction/service liés aux traitements des données personnelles*

Les activités des services /directions liés aux traitements de données *(voir PP. 17-23)*

5.1.2. Existence d'un chargé de la protection des données

Aucun agent de SUNU Assurances Vie Côte d'Ivoire n'a été désigné responsable des questions liées à la protection des données personnelles. Néanmoins un point focal existe. Celui-ci joue le rôle d'interface entre la Direction SUNU Assurances Vie Côte d'Ivoire et AS CONSULTING.

5.1.3. Risques liés aux processus métiers et connaissance des règles de la protection des données personnelles

✓ *Existence d'un fichier listant les activités impliquant les traitements des données à caractère personnel*

Il n'existe pas de fichiers listant spécifiquement les activités impliquant les traitements des données à caractère personnel.

✓ *Connaissance des règles de base à appliquer en matière de protection des données personnelles*

De façon générale, seuls les représentants des services et directions qui ont participé à la formation ont une connaissance des règles de base en matière de protection des données. En somme quinze (15) personnes sur un effectif total de cent trente-sept (137).

✓ *Connaissance des responsabilités et des sanctions pénales, financières et administratives en cas de non-respect de la règlementation*

La formation a permis aux différents participants de connaître les peines encourues en cas de non-respect de la règlementation.

5.1.4. Identification des risques propres à chaque direction

Il n'existe pas une identification et une évaluation des risques liés aux traitements des données personnelles au sein des différents services et directions.

5.1.5. Activités de contrôle interne

Aucun service et direction ne disposent de procédures de contrôle interne pour assurer la maîtrise des risques liés à la protection des données personnelles.

5.1.6. Recensement des fichiers et des traitements

5.1.6.1. Sur l'existence d'un recensement des fichiers contenant des données à caractère personnel détenus par les directions

Les directions et services ne disposent pas d'un recensement des fichiers et des traitements contenant des données personnelles.

5.1.6.2. Sur les supports utilisés pour le recensement des fichiers contenant des données personnelles.

Les services et directions utilisent des supports numériques (fichiers WORD, EXCEL, etc.), pour le recensement des fichiers contenant des données personnelles.

5.1.6.3. Sur l'actualisation des fichiers

Les services et directions actualisent régulièrement leurs fichiers.

5.1.7. Connaissance en matière de protection des données à caractère personnel

✓ *Formation en matière de protection des données à caractère personnel*

Les agents des directions et services ayant participé à la formation, en début du processus de conformité, ont une assez bonne notion des enjeux de la protection de données.

✓ *Existence d'un dispositif de formation en interne prenant en compte les modules DCP*

Quand bien même SUNU Assurances Vie Côte d'Ivoire est consciente des enjeux qu'implique la nouvelle loi, il n'existe aucun dispositif de formation en interne pour mieux outiller ses agents.

5.1.8. Sécurité

5.1.8.1. Analyse des risques et existence d'une charte informatique

La charte informatique existe, mais doit être mise à jour en prenant en compte l'analyse de risque liée aux données à caractère personnel au sein de SUNU Assurances Vie Côte d'Ivoire.

5.1.8.2.Sécurité physique

Tous les services et directions ont leurs accès protégés par des portes verrouillées. Mais, aucun système d'alarme anti-intrusion n'est installé.

5.1.8.3.Sécurité logique

Les deux (2) points forts de la sécurité logique sont les suivants :

- Le système d'exploitation, l'anti-virus et les logiciels sont maintenus à jour ;
- La politique de mot de passe est rigoureuse pour les administrateurs et utilisateurs ;

5.1.8.4.Authentification

Le système d'authentification implémenté au sein de l'entreprise se caractérise par :

- L'attribution d'un identifiant unique pour chaque utilisateur ;
- Les mots de passe utilisateur sont régulièrement renouvelés ;
- Les mots de passe respectent les règles de complexité ;
- Les profils d'habilitation sont définis pour chaque utilisateur.

5.1.8.5.Gestion des accès

Les permissions d'accès qui sont régulièrement mises à jour et supprimés en cas de départ de l'utilisateur de SUNU Assurances Vie Côte d'Ivoire.

5.1.8.6.Sauvegarde et maintenance

Des sauvegardes régulières sont effectuées sur des supports de stockage et conservées dans un endroit sûr. Par ailleurs, les interventions de maintenance sont enregistrées dans une main courante ; et une procédure de continuité (restauration) n'existe pas pour être testée à fréquence régulière.

5.1.8.7.Réseau

La sécurité du réseau est dévolue à la Direction des Systèmes d'Information. Celle-ci a limité les flux réseaux au strict nécessaire afin d'éviter toute intrusion malveillante. En plus, les accès distants des appareils nomades sont sécurisés par VPN *(Virtual Private Network : réseau privé virtuel)*.

5.2. Inventaire des traitements

L'inventaire des traitements effectués a permis d'identifier cinquante-quatre (**54) traitements,** répertoriés dans le tableau ci-après :

Départements /Services	N°	Traitements des DCP	Finalité	Données collectées
1-Département Communication et Relation Clients. 2-Dir. Commerciale et Réseau Particuliers 3-Direction des Prestations.	1	Entrée en Relation-clients	Informer et orienter les clients	1-Nom, Prénoms, Adresse Date, lieu de naissance, numéro de police 2-Habitude de vie, Situation familiale 3-Situation professionnelle 4-Revenus, Situation financière 5-Pathologie, affection, Antécédents familiaux, Données relatives aux soins 6-numéro de téléphone
	2	Proposition de produits d'assurance aux entreprises	- Satisfaire et fidéliser la clientèle - réaliser, Développer / Accroitre les ventes.	1-Nom, prénoms, Adresse Date, lieu de naissance 2-Habitude de vie, Situation familiale 3-Situation professionnelle 4-Revenus, Situation financière 5-Pathologie, affection, Antécédents familiaux, Données relatives aux soins 6-Numéro de téléphone, 7-Adresse électronique
	3	Propositions de produits d'assurance aux Particuliers		
	4	Propositions de produits d'assurance par le biais des banques		
	5	Enregistrements des souscriptions	Réaliser des ventes	1-Nom, prénoms Adresse, Date, lieu de naissance, Signature 2-Habitude de vie, Situation familiale 3-Situation professionnelle 4-Revenus, Situation financière 5-Pathologie, affection, Antécédents familiaux, Données relatives aux soins 6-Numéro de téléphone
1-Direction Production et Encaissements 2-Dir. Etude et actuariat	6	Validation et modification des contrats d'assurance	Accepter les couvertures d'assurance et mettre à jour les contrats	1-Nom, prénom Adresse Date, lieu de naissance, numéro de police 2-Habitude de vie, Situation familiale 3-Situation professionnelle 4-Revenus,Situation financière, téléphone mobile 5-Pathologie, affection, Antécédents familiaux, Données relatives aux soins
Cabinet médical	7	Collecte des données de santé	Suivi optimal des patients	1- Traitements médicaux 2- Pathologies
	8	Communication des données de santé	Transmettre les données aux patients et organismes concernés	

Départements /Services	N°	Traitements des DCP	Finalité	Données collectées
Dir. Adm et Juridique	9	Rédaction de courriers	Assurer les correspondances	1-Nom, prénoms 2- Numéro de téléphone 3-Fonction
	10	Rédaction des rapports et contrats	Rédiger les rapports et contrats	
Direction de la communication et Relation Clients	11	Communication externe	Faire de la communication publicitaire - Communication institutionnelle	1-Nom, prénoms, Photographie, voix 2-Fonction 3-numéro de téléphone, email
	12	Communication interne	Communiquer avec le personnel	'Email, numéro de téléphone fixe
Direction des Prestations.	13	Gestion des Rachats : partiel / total	Effectuer les rachats	1-Nom, prénoms, Adresse Date, lieu de naissance, 2-Numéro de police 3-Numéro de téléphone
	14	Gestion des sinistres déclarés	Régler les sinistres	1-Nom, prénoms, Adresse Date, lieu de naissance, numéro de police 2-Habitude de vie, Situation familiale 3-Situation professionnelle 4-Revenus,Situation financière 5-Pathologie, affection, Antécédents familiaux, Données relatives aux soins 6- numéro de téléphone
	15	Gestion du Bureau Direct	Gérer le suivi et le monitoring de tous les portefeuilles clients échus, suspendus,...	
	16	Remises de chèques	valeur de rachat du contrat	1- Nom, prénoms, Adresse Date, lieu de naissance, 2- Numéro de police
Direction des systèmes d'information	17	Collecte de données informatiques	Gérer les données informatiques de SUNU Assurances Vie CI	1- Identifiants des terminaux 2- Identifiants de connexions
	18	communication de données informatiques	Faciliter les échanges de courriers électroniques	
	19	Consultation et Conservation des images des caméras	- Elucider des incidents - Base de données visuelle des personnes ayant accès aux locaux	Images, numéro de plaques d'immatriculation
	20	Gestion des serveurs	Assurer le bon fonctionnement des équipements de stockage	1-Adresse IP, logs, Numéro de téléphone, adresse mail 2-Nom, prénoms, Date, lieu de naissance, Numéro de police 3-Situation personnelle, Dossiers clients

Départements /Services	N°	Traitements des DCP	Finalité	Données collectées
				4- Catégorie professionnelle, Numéro de Sécurité sociale, Scolarité, formation, distinctions, 5- Fichiers Impayés 6- Numéro de téléphone
	21	Gestion du parc informatique : Configuration et installation (maintenance) téléassistance	Assurer le bon fonctionnement des équipements informatiques	1-Adresse IP, logs, Numéro de téléphone, adresse email 2-Nom, prénoms, Date, adresse, lieu de naissance, Numéro de police 3-Situation personnelle, Dossiers clients 4- Catégorie professionnelle, Numéro de Sécurité sociale, Scolarité, formation, Distinctions, 5- Fichiers Impayés
	22	modifications de données informatiques	Assurer la maintenance du système informatique	1- Identifiants des terminaux 2- Identifiants de connexions
	23	Vidéosurveillance	Veiller à la sécurité des biens et des personnes de l'entreprise	Images, numéro de plaques d'immatriculation
	24	Assistance aux utilisateurs dans leurs taches	Faciliter l'utilisation des outils au personnel	1-Adresse IP, logs, Numéro de téléphone, adresse email 2-Nom, prénoms, Date, adresse, lieu de naissance, Numéro de police 3-Situation personnelle, Dossiers clients 4- Catégorie professionnelle, Numéro de Sécurité sociale, Scolarité, formation Distinctions, 5- Fichiers Impayés
	25	Emission de chèques	Editer les lettres-chèques émises en règlement des paiements des assurés et des bénéficiaires contractuels	Nom, prénoms
Direction des systèmes d'informations	26	Gestion des systèmes d'accès (badges)	Contrôler les accès aux différents paliers et bureaux	1-Adresse IP, logs, 2-Nom, prénoms, Date, adresse, lieu de naissance, Numéro de police 3-Situation personnelle, Dossiers clients 4- Catégorie professionnelle, Numéro de Sécurité sociale, Scolarité, formation Distinctions, 5- Fichiers Impayés 6- Numéro de téléphone

Départements /Services	N°	Traitements des DCP	Finalité	Données collectées
	27	Support web	Aider à l'utilisation et fonctionnement des Réseaux	1-Adresse IP, logs, Numéro de téléphone 2-Nom, prénoms, Date, adresse, lieu de naissance, Numéro de police 3-Situation personnelle, Dossiers clients 4- Catégorie professionnelle, Numéro de Sécurité sociale, Scolarité, formation Distinctions, 5- Fichiers Impayés
Direction Production Encaissements	28	Gestion du recouvrement	faire le recouvrement des primes échues non encaissées	1-Nom, prénoms, Adresse Date, lieu de naissance, numéro de police 2-Numéro de compte
	29	Réassurance	Réassurer les dossiers dont les capitaux sont importants	1-Nom, prénoms, Adresse Date, lieu de naissance, numéro de police 2-Habitude de vie, Situation familiale 3-Situation professionnelle 4-Revenus, Situation financière 5-Pathologie, affection, Antécédents familiaux, Données relatives aux soins
Dpt. Audit interne et Conformité	30	Conduite de missions d'audit	Effectuer des contrôles internes	1-Nom, prénoms 2- Service ou poste occupé
	31	Lutte anti blanchiment	Effectuer les contrôles sur la légalité des opérations des assurés et prospects	1-Nom, prénoms, Date, lieu de naissance, Adresse, Numéro de police 2- Situation matrimoniale, 3-Situation professionnelle 4-Situation économique (Tranche de revenu annuel, patrimoine etc.) 5-Numéro de téléphone
Service des Moyens généraux	32	conservation provisoire de pièces d'identité	contrôler l'accès au siège	-Nom, prénoms, Date, lieu de naissance, numéro de la pièce d'identité, photographie, taille, poids de la personne concernée, Nom et prénoms, date de naissance de l'un des parents de la personne concernée 2-Fonction de la personne concernée

Départements /Services	N°	Traitements des DCP	Finalité	Données collectées
Service des Moyens généraux	33	enregistrement de données d'identification	Base de données des visiteurs	1-Nom, prénoms, Date, lieu de naissance, numéro de la pièce d'identité, photographie, taille, poids de la personne concernée, Nom et prénoms, date de naissance de l'un des parents de la personne concernée 2-Fonction
Service Archives	34	Communication de dossiers	Transmettre les dossiers aux services qui les sollicitent	1-Nom, prénoms, Date, lieu de naissance, Adresse, Numéro de police 2- Situation matrimoniale , Habitude de vie 3-Situation professionnelle, Scolarité, formation Distinctions 4-Situation économique 5-Numéro de téléphone
	35	Conservation des dossiers des prospects, assurés, Personnel de SUNU	Constituer une Base de données de tous les dossiers	1-Nom, prénoms, Date, lieu de naissance, Adresse, Numéro de police 2- Situation matrimoniale , Habitude de vie 3-Situation professionnelle, Scolarité, formation Distinctions 4-Situation économique 5-Numéro de téléphone
	36	Scannage de tous les dossiers physiques	Numériser les archives	1-Nom, prénoms, Date, lieu de naissance, Adresse, Numéro de police 2- Situation matrimoniale , Habitude de vie 3-Situation professionnelle, Scolarité, formation Distinctions 4-Situation économique 5-Numéro de téléphone
Service courrier	37	collecte et distribution du courrier	Transmettre les courriers aux services et personnes concernées	1-Nom, prénoms, Photographie, voix 2-Fonction 3-numéro de téléphone, email
1- Service Juridique et Fiscal 2- Dir. Production et Encaissement	38	Constitution de dossiers pour appels d'offre	Obtenir des marchés	1-Nom, prénoms, Adresse, Date, lieu de naissance 2-Situation professionnelle 3- Situation matrimoniale 4- numéro de téléphone
Service Patrimoine Immobilier	39	Collecte de documents	Constituer une base donnée contractuelle	1-CNI, adresse, adresse 2- RIB, Bulletin de salaire,

Départements /Services	N°	Traitements des DCP	Finalité	Données collectées
				3- Fonction 4- numéro de téléphone
	40	Encaissement des loyers	encaisser le loyer	1-Nom et prénoms, 2-Numéro d'appartement
	41	Rédaction de contrats de bail	Entrer en relation contractuelle	
Service Ressources Humaines	42	Collecte de dossiers de stage	Recruter des stagiaires	1-Nom Prénoms, , Date, lieu de naissance, Photographie, sexe , Numéro de la pièce d'identité de la personne concernée Nom , prénoms 2 -Expérience professionnelle , CV, Formation 3-Numéro de téléphone, email
	43	Collecte de dossiers de candidature pour emploi	Recruter des employés	1-Nom Prénoms, , Date, lieu de naissance, Photographie, sexe ,Numéro de la pièce d'identité de la personne concernée Nom , prénoms , statut marital 3 -Expérience professionnelle , emploi précédent, CV, Formation 4-examens Médicaux 5-Numéro de téléphone, email
	44	Etablissement de polices d'assurance	Assurer les salariés	1-Nom Prénoms, Numéro de téléphone, Date, lieu de naissance, 2- Catégorie professionnelle, numéro de sécurité sociale 3- Salaire
	45	Gestion des déclarations CNPS	satisfaire aux dispositions sociales vigueur en CI	1-Nom Prénoms, Numéro de téléphone, Date, lieu de naissance, 2- Catégorie professionnelle, numéro de sécurité sociale 3- Salaire
	46	Gestion de la rémunération	Effectuer la paie du personnel	1-Nom Prénoms, Date, lieu de naissance, 2- Catégorie professionnelle, date d'entrée, matricule 3- Salaire
Service Ressources Humaines	47	Gestion des missions	Gérer les envois en missions des agents	1-Nom Prénoms, Date, lieu de naissance, 2- Poste occupé et Direction d'origine
	48	Gestion des compétences	Evaluer les travailleurs	1-Nom Prénoms, Date, lieu de naissance, 2- Catégorie professionnelle, Service poste occupé par l'agent
	49	Gestion des congés et permissions	Apporter des réponses aux demandes de départ en congés	1-Nom Prénoms 2-service poste occupé par l'agent

Départements /Services	N°	Traitements des DCP	Finalité	Données collectées
			et aux demandes de permission du personnel	
	50	Gestion des départs de l'entreprise	Gérer les fins de contrats des agents et stagiaires	1-Nom Prénoms, Date, lieu de naissance, 2- Catégorie, Poste occupé 3-Salaire
	51	Gestion des impôts sur les Traitements et Salaires (ITS)	satisfaire aux dispositions fiscales en vigueur en CI	1-Nom Prénoms, Numéro de téléphone, Date, lieu de naissance, 2- Catégorie professionnelle, matricule 3- Salaire
	52	Rédaction de contrats de stage	Etablir un lien contractuel avec le nouveau stagiaire	1-Nom Prénoms, Date, lieu de naissance, Photographie, sexe 2-Numéro de la pièce d'identité de la personne concernée Nom, prénoms
	53	Rédaction de contrats de travail	Etablir un lien contractuel avec le salarié	1-Nom Prénoms, , Date, lieu de naissance, Photographie, sexe Numéro de la pièce d'identité de la personne concernée Nom , prénoms 2-Examens Médicaux 3-Numéro de téléphone
Dir. Production et Encaissement	54	Transfert	Réassurer les dossiers dont les capitaux sont importants *(pour des clients se trouvant à l'étranger)*	1-Nom, prénoms, Adresse Date, lieu de naissance, numéro de police 2-Habitude de vie, Situation familiale 3-Situation professionnelle 4-Revenus, Situation financière 5-Pathologie, affection, Antécédents familiaux, Données relatives aux soins

5.3. Etat de la conformité : Evaluation

L'évaluation générale de **SUNU Assurances Vie Cote d'Ivoire** a donné **un taux de conformité avec la loi de 52 %**, selon le détail ci-après :

ENTITE	Note obtenue	Barème ARTCI	% Conformité
Cabinet médical	440	700	**63%**
Dir. Adm et Juridique	372	690	**54%**
Dir. Centrale fonctionnelle	255	600	**43%**
Dir. Commerciale Réseau Particuliers	325	600	**54%**
Dir. Comptable et Financière	265	600	**44%**
Dir. des prestations	345	600	**58%**
Dir. des Systèmes d'information	364	700	**52%**
Dir. Etude et actuariat	325	600	**54%**
Dir. Générale	325	600	**54%**
Dir. Production et Encaissement	342	601	**57%**
Dpt. Audit interne et Conformité	330	600	**55%**
Dpt. Clientèle Corporate	380	700	**54%**
Dpt. Commercial Bancassurance	290	600	**48%**
Dpt. Commercial Canaux alternatifs	275	600	**46%**
Dpt. Communication et Relations Clients	325	700	**46%**
Service Archives	255	600	**43%**
Service Contrôle de gestion	245	600	**41%**
Service Courrier	255	600	**43%**
Service des Moyens généraux	385	700	**55%**
Service Juridique et fiscal	385	685	**56%**
Service Patrimoine Immobilier	335	600	**56%**
Service Ressources humaines	377	600	**63%**
Total général	7195	13876	**52%**

6. Analyse

6.1. Sur la légitimité et la licéité des traitements

Aux termes de l'article 14 de la loi n°2013-450 du 19 juin relative à la protection des données à caractère personnel, le traitement des données à caractère personnel est considéré comme légitime si la personne concernée donne expressément son consentement.

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 :

- au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

- à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande ;

- à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée.

Considérant que la société SUNU Assurances Vie Côte d'Ivoire procède elle-même à la collecte des données ; qu'il s'agit là d'une collecte directe des données à caractère personnel ;

Considérant que SUNU Assurances Vie Côte d'Ivoire indique qu'elle procède par recueil du consentement préalable par le biais de formulaires signés par les clients et aussi par des pré-imprimés ;

Considérant que dans le cadre de son activité d'assurance, que la société SUNU Assurances Vie Côte d'Ivoire est soumise au une règlementation en vigueur, en l'occurrence le code CIMA.

En somme, le correspondant estime qu'au travers de ces dérogations, les traitements opérés par SUNU Assurances Vie Côte d'Ivoire, dans le cadre de son activité, sont légitimes. Par contre, en ce qui concerne les autres traitements, qui n'entrent pas dans le cadre de ses activités-métier telles que la vidéosurveillance, la gestion des accès par badges, etc., un effort reste à faire.

6.2. Sur la finalité des traitements

Aux termes de l'article 16 de la loi n°2013-450 du 19 juin relative à la protection des données à caractère personnel 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, SUNU Assurances Vie Côte d'Ivoire collecte les données à caractère personnel pour les finalités suivantes :

- Informer et orienter les clients
- Satisfaire et fidéliser la clientèle ;
- Réaliser, Développer / Accroitre les ventes ;
- Réaliser des ventes ;
- Accepter les couvertures d'assurance et mettre à jour les contrats ;
- Suivi optimal des patients ;
- Transmettre les données aux patients et organismes concernés ;
- Assurer les correspondances ;
- Rédiger les rapports et contrats ;
- Faire de la communication publicitaire - Communication institutionnelle ;
- Communiquer avec le personnel ;
- Effectuer les rachats ;

- Régler les sinistres ;
- Gérer le suivi et le monitoring de tous les portefeuilles clients échus, suspendus ;
- valeur de rachat du contrat ;
- Gérer les données informatiques de SUNU Assurances Vie CI ;
- Faciliter les échanges de courriers électroniques ;
- Elucider des incidents ;
- Base de données visuelle des personnes ayant accès aux locaux ;
- Assurer le bon fonctionnement des équipements de stockage ;
- Assurer le bon fonctionnement des équipements informatiques ;
- Assurer la maintenance du système Informatique ;
- Veiller à la sécurité des biens et des personnes de l'entreprise ;
- Faciliter l'utilisation des outils au personnel ;
- Editer les lettres-chèques émises en règlement des paiements des assurés et des bénéficiaires contractuels ;
- Contrôler les accès aux différents paliers et bureaux ;
- Aider à l'utilisation et fonctionnement des Réseaux ;
- faire le recouvrement des primes échues non encaissées ;
- Réassurer les dossiers dont les capitaux sont importants ;
- Effectuer des contrôles internes ;
- Effectuer les contrôles sur la légalité des opérations des assurés et prospects ;
- contrôler l'accès au siège ;
- Base de données des visiteurs ;
- Transmettre les dossiers aux services qui les sollicitent ;
- Constituer une Base de données de tous les dossiers ;
- Numériser les archives ;
- Transmettre les courriers aux services et personnes concernées ;
- Obtenir des marchés ;
- Constituer une base donnée contractuelle ;
- encaisser le loyer ;
- Entrer en relation contractuelle ;
- Recruter des stagiaires ;
- Recruter des employés ;
- Assurer les salariés ;
- satisfaire aux dispositions sociales vigueur en CI ;
- Effectuer la paie du personnel ;
- Gérer les envois en missions des agents ;
- Evaluer les travailleurs ;
- Apporter des réponses aux demandes de départ en congés et aux demandes de permission du personnel ;
- Gérer les fins de contrats des agents et stagiaires ;
- satisfaire aux dispositions fiscales en vigueur en CI ;
- Etablir un lien contractuel avec le nouveau stagiaire
- Etablir un lien contractuel avec le salarié ;
- Réassurer les dossiers dont les capitaux sont importants (pour des clients se trouvant à l'étranger).

Il convient d'estimer qu'il y a une finalité déterminée, explicite et légitime pour tous les traitements de SUNU Assurances Vie Côte d'Ivoire.

6.3. Sur les délais de conservation

Considérant qu'aux termes de l'article 16 alinéa 3 de la loi n°2013-450 du 19 Juin relative à la protection des données à caractère personnel qui dispose que les données collectées doivent être conservées pendant une période qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées ;

Considérant qu'en l'espèce, SUNU Assurances Vie Côte d'Ivoire, dans le cadre de ses activités, respecte les délais conformément à la règlementation telle que prévue par le code CIMA. Par contre, ces délais ne sont pas définis dans une politique d'archivage, ce qui ne permet pas à tout le personnel d'avoir connaissance des différentes durées de conservation.

En somme, le correspondant conclut que la politique d'archivage n'étant pas formalisée, cela pourrait amener certains départements, directions, et services de SUNU Assurances Vie Côte d'Ivoire à conserver les données pendant une période qui peut excéder la période nécessaire aux finalités pour lesquelles elles ont été collectées.

6.4. Sur la proportionnalité des données traitées

Considérant qu'aux termes de l'article 16 alinéa 2 de la loi n°2013-450 du 19 juin relative à la protection des données à caractère personnel qui dispose que les données collectées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement ;

Considérant qu'en l'espèce, SUNU Assurances Vie Côte d'Ivoire traite les données telles que :

a. Les données d'identification : le nom, le prénom, la date et lieu de naissance, la photographie, sexe, la nationalité, numéro Carte Nationale d'Identité ;

b. Les données de vie personnelle : situation familiale et professionnelle, habitude de vie ;

c. Information d'ordre économique et financier : situation financière, revenus liés à sa profession, salaire ;

d. Les données de localisation : adresse, numéro de téléphone, e-mail ;

e. Données relatives aux soins : pathologie, affections, antécédents familiaux, examens médicaux.

Pour ce qui est des données relatives aux soins, considérées par la loi comme des données sensibles au terme de l'article 21 (loi N°2013-450 du 19 juin 2013), donc interdites de collecte. Mais dès lors que le code CIMA permet la collecte des données sensibles pour évaluer les risques que l'assureur prend en charge, ce qui fonde l'exercice de l'activité de SUNU Assurances Vie Côte d'Ivoire ; Ces données ne paraissent pas excessives.

Au regard de tout ce qui précède, le correspondant à la protection estime que les données collectées au sein de SUNU Assurances Vie Côte d'Ivoire sont adéquates, pertinentes et non excessives.

6.5. Sur la transparence des traitements

Considérant qu'aux termes des dispositions de 28 de la loi n°2013-450 du 19 juin relative à la protection des données à caractère personnel qui dispose que le responsable du traitement est tenu de fournir à la personne dont les données font l'objet d'un traitement, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes :

- son identité et, le cas échéant, celle de son représentant dûment mandaté ;

- la ou les finalité(s) déterminée(s) du traitement auquel les données sont destinées ;

- les catégories de données concernées ;

- le ou les destinataire(s) auxquels les données sont susceptibles d'être communiquées ;

- la possibilité de refuser de figurer sur le fichier en cause ;

- l'existence d'un droit d'accès aux données concernant la personne et d'un droit de rectification de ces données ;

- la durée de conservation des données ;

- l'éventualité de tout transfert de données à destination de pays tiers.

En l'espèce, SUNU Assurances Vie Côte d'Ivoire n'apporte pas la preuve, au moyens de ses formulaires de collecte et affichage que toutes ces dispositions sont respectées avant toute collecte.

En somme, le correspondant à la protection en déduit que les personnes concernées ne sont pas informées sur leurs données, sur les destinataires, ainsi que de leurs droits, avant tout traitement.

6.6. Sur les mesures de sécurité

Considérant qu'aux termes des dispositions de l'article 41 de la loi n°2013-450 du 19 juin relative à la protection des données à caractère personnel, le responsable de 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 les données stockées sur des supports papiers et celles qui le sont sur supports informatiques ;

Qu'il en ressort des différents documents que SUNU Assurances Vie Côte d'Ivoire prend des mesures nécessaires en vue d'assurer la sécurité des données, telles que :

- L'existence de mot de passe robuste et de politique d'accès ;
- L'existence d'une DMZ ;
- Logiciel de sécurité Firewall ;
- La sauvegarde des codes sources une fois par an ;
- Niveaux d'habilitation en fonction de la hiérarchie ;
- Mesure de blocage du poste de travail après 5 minutes d'inactivité ;
- L'existence de casier et d'armoire à clef pour document papier.

En conclusion, le correspondant considère que quand bien même un effort est fait dans le sens de la protection logique, des insuffisances ont été relevées au niveau des mesures de sécurité physique. En effet, certains dossiers des assurés de SUNU Assurances Vie Côte d'Ivoire sont stockés sur des meubles à portée de tous, dans les bureaux. Aussi, il convient de noter que des chèques et autres fichiers afférents aux assurés de SUNU Assurances Vie Côte d'Ivoire transitent par le biais des coursiers sans précautions particulières pour la protection de ces documents. Ces manquements pourraient porter atteintes à la vie privée des personnes concernées.

6.6.1. Sur le système informatique

En plus des éléments signifiés au point 5.1.8 sur la sécurité, *(voir annexe PP.38-41)*

6.6.2. Sur les destinataires des données traitées

Les destinataires des données sont identifiés *(voir annexe PP.38-41)*.

6.6.3. Sur l'exactitude des données

Les données sont mises à jour après demande faite de la personne concernée.

6.6.4. Les sous-traitants

Au terme des dispositions de l'article 40 de la loi N°2013-450 du 19 juin 2013, 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.

Lorsque le traitement est mis en œuvre pour le compte du responsable du traitement, celui-ci choisi un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect de ces mesures.

Considérant qu'en l'espèce, dans le cadre de ses activités, SUNU Assurances Vie Côte d'Ivoire a recours à des sous-traitants dans les domaines suivants :

- Installation de caméras ;
- Maintenance informatique ;
- Société de gardiennage ;
- Publicité et organisations d'événements.

Considérant que ces sous-traitants ne disposent pas d'autorisation de l'ARTCI et qu'en sus les contrats de sous-traitance n'intègrent pas des clauses spécifiques aux données à caractère personnel,

En conclusion, le correspondant estime que ces insuffisances pourraient constituer un manquement au principe de garantie suffisante qui incombe au responsable de traitement (SUNU Assurances Vie Côte d'Ivoire).

6.7. Vidéosurveillance

Aux termes de l'article 1er, *paragraphe* 44 de la loi n°2013-450 du 19 Juin relative à la protection des données à caractère personnel dispose en matière de définition que toute activité faisant appel à des moyens techniques ou électroniques en vue de détecter, d'observer, de copier ou d'enregistrer les mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile ;

Considérant qu'en l'espèce, les traitements réalisés par SUNU Assurances Vie Côte d'Ivoire ont pour finalité la sécurité des biens et du personnel. La surveillance des locaux, dans le hall, le Sous-sol et la salle des machines et que seule la direction de sécurité en a accès.

Il convient d'estimer qu'il y a une finalité déterminée, explicite et légitime. Par contre, les constats suivants ont été relevés :

- SUNU Assurances Vie Côte d'Ivoire ne dispose pas d'une autorisation pour ce traitement auprès de l'ARTCI ;
- Il n'existe pas de consentement éclairé, déterminé et explicite de la part des salariés ;
- Aucune affiche, ni de pictogramme pour informer les visiteurs de l'existence d'un tel dispositif et vers qui exercer leurs droits n'est disponible près des caméras de vidéosurveillance.

6.8. Correspondant et chargé de la protection des données personnel

Un correspondant personne morale a été désigné, en l'occurrence AS CONSULTING et sa prise de fonction a été effective *(voir courrier de désignation en annexe PP.38-41)*, mais il n'est pas connu de tous les salariés et client de SUNU Assurances Vie Côte d'Ivoire. Le correspondant estime, à cet effet, que des sessions soient organisées afin de le faire connaitre des clients et autres partenaires de SUNU Assurances Vie Côte d'Ivoire.

6.9. Sur les droits d'accès, de rectification, d'effacement et d'opposition

Considérant qu'aux termes des dispositions des articles 28 à 33 et 38 de la loi n°2013-450 du 19 juin relative à la protection des données à caractère personnel qui reconnaît l'exercice de certains droits reconnus aux personnes concernées de la part du responsable de traitement portant sur les données à caractère personnel ;

Qu'en l'espèce, avec SUNU Assurances Vie Côte d'Ivoire, ces droits ne sont pas réellement exercés par les personnes concernées.

En somme, le correspondant à la protection en déduit que les personnes concernées ne sont pas informées sur l'existence du correspondant auprès de qui ils peuvent exercer leurs droits, avant tout traitement.

6.10. Connaissance en matière de protection de données à caractère personnel

De façon générale, seules les personnes ayant suivi la formation au sein de SUNU Assurances Vie Côte d'Ivoire (15 personnes) ont connaissance de la protection des données à caractère personnel.

Il importe donc à SUNU Assurances Vie Côte d'Ivoire de vulgariser sur un plus grand nombre, les connaissances en matière de données à caractère personnel.

6.11. Procédures de SUNU Assurances Vie Côte d'Ivoire

Dans le cas d'espèce, les procédures internes au sein de SUNU Assurances Vie Côte d'Ivoire n'intègre pas les données à caractère personnel. Le correspondant estime qu'un effort doit être fait à ce niveau, afin d'intégrer à ces procédures les principes de base avant tout traitement de données à caractère personnel.

6.12. Formalités préalables aux traitements des données à caractère personnel

Aucune formalité n'a été effectuée à ce jour. Cet audit est justement le cadre mis en place pour pouvoir les remplir.

7. Recommandations

Principe	N° Reco	Points d'amélioration	Recommandation
Sécurité	R1	Aucun système d'alarme anti-intrusion n'est installé	Limiter les risques afin que des personnes non autorisées n'accèdent pas physiquement aux données à caractère personnel (liste des personnes autorisées, authentification des collaborateurs et des visiteurs, trace des accès, alerte en cas d'effraction, etc.).
	R2	Aucune analyse des menaces et de leur impact sur DCP n'est menée	Mettre en place une étude d'impact (PIA) pour les données sensible, afin de maîtriser les risques que les traitements du cabinet médical font peser sur les droits et libertés des personnes concernées
	R3	Des mesures de chiffrement des supports de stockage amovibles et les ordinateurs portables ne sont pas implémentées	Rendre les données à caractère personnel incompréhensibles à toute personne non autorisée à y avoir accès (chiffrement symétrique ou asymétrique, utilisation d'algorithmes publics réputés forts, certificat d'authentification, etc.).
	R4	Des mesures pour assurer la continuité d'activité n'existent pas et ne sont pas régulièrement testées	Formaliser le PRA (Plan de Reprise d'Activité) ou le PCA (Plan de Continuité d'Activité), le diffuser auprès des personnels concernés (internes, externes, prestataires) et tester régulièrement son efficacité.
	R5	En cas d'accès frauduleux à leurs données les personnes concernées ne sont pas notifiées	Disposer d'une organisation opérationnelle permettant de détecter et de traiter les événements susceptibles d'affecter les libertés et la vie privée des personnes concernées (définition des responsabilités, plan de réaction, qualifier les violations, etc.).
	R6	Inexistence d'un système de journalisation	Assurer l'enregistrement et l'imputabilité des consultations et actions des utilisateurs du traitement, afin de pouvoir fournir des preuves dans le cadre d'enquêtes (système de journalisation, protection, analyse, conservation, etc.).
	R7	La charte informatique n'est pas à jour et diffusée à l'ensemble du personnel	Mettre à jour la charte informatique en prenant en compte les DCP et la diffuser à l'ensemble des utilisateurs
	R8	L'accord de l'utilisateur n'est pas recueilli avant toute opération de maintenance sur son poste de travail	Limiter la vraisemblance des menaces liées aux opérations de maintenance sur les matériels et logiciels (contrat de sous-traitance, télémaintenance, accord de l'utilisateur, effacement des données, etc.).
	R9	Les données des matériels en fin d'utilisation ne sont pas détruites	Effacer de façon sécurisée ou bien détruire physiquement les supports de stockage mis au rebut contenant les DCP
	R10	Les mises à jour critiques ne sont pas instantanément installées	Réaliser une veille sur les vulnérabilités découvertes dans les logiciels (y compris les firmwares) utilisés en exploitation, et les corriger dès que possible.
Durées de conservation des données	R11	Inexistence d'une procédure de destruction des données au-delà de la durée de conservation	Formaliser la procédure de destruction de données en adéquation avec la finalité du traitement et/ou des contraintes légales
	R12	Les délais de conservation ne sont pas contrôlés	Une fois la durée de conservation atteinte, supprimer les données sans délai

Principe	N° Reco	Points d'amélioration	Recommandation
	R13	Les données ne sont pas mises à jour périodiquement	Maintenir la qualité des données pour éviter des calculs à partir de données erronées ou obsolètes.
	R14	Les entités manquent d'information sur la durée légale de conservation des DCP	Mettre à disposition des entités et du personnel, toutes les informations utiles concernant la durée de conservation des données
	R15	Les entités ne s'assurent pas de l'exactitude des données recueillies	Maintenir la qualité des données pour éviter des calculs à partir de données erronées ou obsolètes.
	R16	Les procédures d'archivage des fichiers ne sont pas documentées	Formaliser l'ensemble des modalités de conservation et gestion d'archives électroniques contenant des données à caractère personnel
	R17	La politique d'archivage n'est pas formalisée	Définir et formaliser la politique d'archivage des DCP et la communiquer au personnel ayant en charge le traitement des DCP
	R18	Une durée de conservation n'est pas définie pour chaque donnée collectée	Réduire la gravité des risques en s'assurant que les données à caractère personnel ne seront pas conservées plus que nécessaire.
Droit des personnes concernées	R19	Inexistence de procédure de gestion des droits de la personne concernée	Formaliser la procédure garantissant aux personnes concernées leurs droits (d'accès, d'opposition, de rectification, d'effacement et à la portabilité)
	R20	Les personnes concernées ne peuvent pas accéder à l'intégralité de leurs DCP	Garantir aux personnes concernées la possibilité de prendre connaissance des données à caractère personnel qui les concernent
	R21	Les personnes concernées ne peuvent pas accéder, et de manière illimitée, aux copies de leur DCP	Garantir aux personnes concernées la possibilité d'accéder de manière illimitée aux copies des données à caractère personnel qui les concernent
	R22	Les personnes concernées ne sont pas informées de la procédure de gestion de leurs droits	Mettre en place un processus permettant d'informer les personnes concernées de la procédure de gestion de leurs droits.
	R23	Les personnes concernées ne sont pas informées de leur droit d'accès, de rectification et d'opposition	Garantir l'information aux personnes concernées sur leur droit d'accès, de rectification et d'opposition
Transparence	R24	L'entité ne dispose pas de la preuve de l'information des personnes concernées	Disposer de la preuve de l'information aux personnes concernées
	R25	L'entité ne dispose pas d'une charte de protection des DCP	Mettre en place une charte de protection des DCP et la diffuser à l'ensemble du personnel

Principe	N° Reco	Points d'amélioration	Recommandation
	R26	Les personnes concernées ne sont pas informées du traitement à effectuer et des finalités avant toute collecte de données	Garantir l'exhaustivité de l'information aux personnes concernées concernant les DCP avant toute collecte de données
Confidentialité	R27	Les entités ne disposent pas d'une autorisation de transfert.	Respecter les obligations en matière de formalités préalables au traitement des données, obtenir auprès de l'ARTCI préalablement une autorisation de transfert des données liée au DCP.
	R28	Manque d'information sur l'autorisation de traitement du destinataire	S'assurer que le destinataire dispose d'une autorité de protection et d'une législation sur la protection des DCP.
Légitimité et Licéité	R29	Inexistence d'un processus de recueil du consentement des personnes concernées	Mise en place d'un processus de recueil du consentement des personnes concernées, vérifier que le traitement ne repose pas sur une autre base légale que le consentement.
	R30	Le consentement donné de la personne concernée n'est pas éclairé	Permettre un choix libre, spécifique et éclairé
	R31	Le consentement donné de la personne concernée n'est pas exprès	La loi impose que les données soient collectées et traitées de manière loyale et licite.
Sous-traitance	R32	Les contrats de sous-traitance	Etre conforme à l'article 20 de la loi 2013-450 du 19 juin 2013 relative à la sous-traitance : Exiger du sous-traitant la transmission de sa Politique de Sécurité des Systèmes d'Information (PSSI) ainsi que de toutes les preuves de ses certifications en matière de sécurité de l'information et annexer ces documents au contrat. S'assurer que les mesures issues de sa PSSI sont conformes avec les recommandations de l'ARTCI en matière.
Formation	R33	15 personnes sur 137 salariés ont été formées sur les notions de DCP	Former et sensibiliser le personnel de SUNU assurance vie Côte d'Ivoire sur les notions de protection des DCP via des sessions de formations ou le système « E-learning »
Site internet	R34	Les mentions légales et la sécurité du site internet de SUNU assurance vie Côte d'ivoire	Diminuer la possibilité que les caractéristiques des sites web soient exploitées pour porter atteinte aux données à caractère personnel

8. Tableau récapitulatif des résultats obtenus

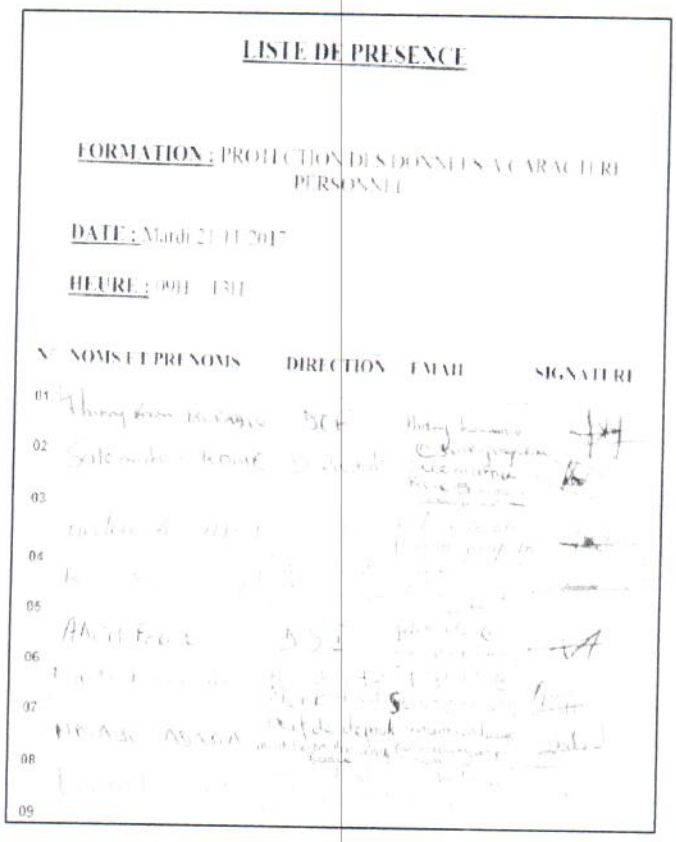
(Voir 5.3 Etat de la conformité : Evaluation)

9. Conclusion

L'Audit de situation de la Société SUNU Assurances Vie Côte d'Ivoire a révélé un niveau de conformité moyen (52%) avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

Sur la base du résultat obtenu, l'Autorité de protection pourra autoriser les traitements de données à caractère personnel opérés par la Société SUNU Assurances Vie Côte d'Ivoire.

L'Autorité de protection lui délivrera un certificat de conformité, lorsque la Société SUNU Assurances Vie Côte d'Ivoire aura effectivement mis en œuvre les actions correctives recommandées dans le présent rapport d'audit.



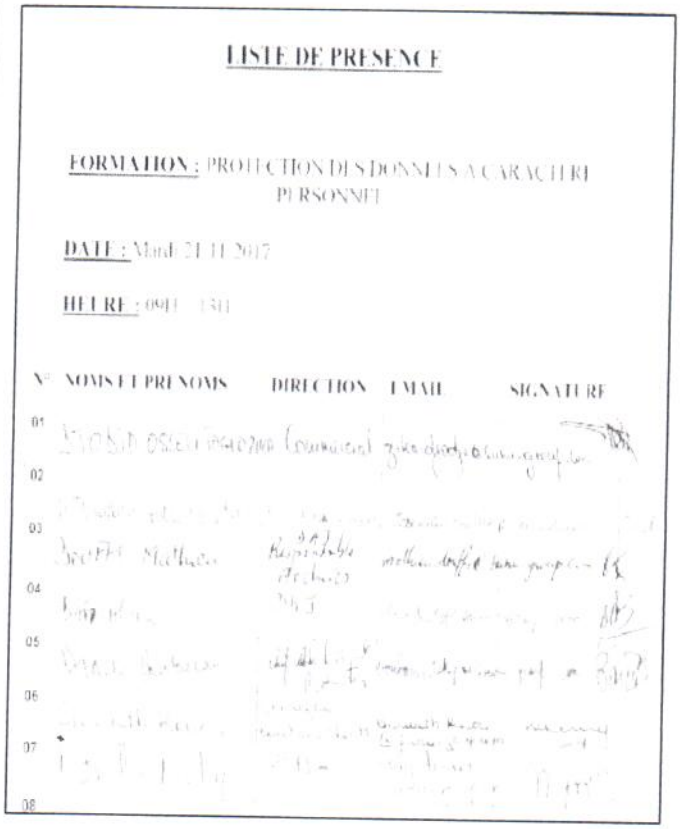
LISTE DE PRESENCE

FORMATION : PROTECTION DES DONNEES A CARACTERE PERSONNEL

DATE : Mardi 21 11 2017

HEURE : 09H - 13H

N°	NOMS ET PRENOMS	DIRECTION	EMAIL	SIGNATURE
01				
02				
03				
04				
05				
06				
07				
08				
09				



LISTE DE PRESENCE

FORMATION : PROTECTION DES DONNEES A CARACTERE PERSONNEL

DATE : Mardi 21 11 2017

HEURE : 09H - 13H

N°	NOMS ET PRENOMS	DIRECTION	EMAIL	SIGNATURE
01				
02				
03				
04				
05				
06				
07				
08				

10. Annexes

1- *Fiche de présence à la formation (voir P .7)*

2- *a/ Questionnaire de type ouvert (voir P.7)*

LEGITIMITE ET LICEITE DU TRAITEMENT

N/A : Non appliqué P/R : Pas de Réponse

CRITERE	APPLIQUE (OUI/NON)	COMMENTAIRES ET OBSERVATIONS	NOTE	BAREME
Le consentement des personnes a-t-il été requis pour l'utilisation des données ?	Oui		40	40
Le consentement donné est-il expresse ?	Oui		15	15
Le consentement donné est-il éclairé ?	**Non**		0	10
Disposez-vous de la preuve du consentement des personnes concernées ? (si oui préciser comment)	Oui		5	5
Avez-vous mis en place un processus de recueil du consentement des personnes concernées ? (si oui décrire le processus)	Oui		5	5
Etes-vous dans un cas d'exception prévu par la loi relative à la protection des données à caractère personnel ? Lequel ?		**Code de déontologie de la medecine**		
Les données sont-elles collectées pour une finalité clairement définie ? Laquelle ?	Oui	donner un avis médical	10	10
La finalité est-elle explicite ?	Oui		5	5
La finalité est-elle légitime ?	Oui		5	5
Les données sont-elles utilisées à d'autres fins?	Non		5	5
			90	100

QUESTIONS POUR LE DIAGNOSTIC DES ACTIVITES ET PROCESSUS METIER

1) Combien de personnes composent la direction ?

2) En quoi consiste votre activité ?

3) Existe-t-il une liste descriptive à jour de vos activités ?

4) Pour chaque activité existe-t-il un seul et unique responsable qui a le contrôle sur toutes ces activités et qui a les moyens d'assumer ses responsabilités ?

5) Quelles sont les activités de la direction qui implique un traitement de données à caractère personnel ?

6) Existe-t-il un recensement des activités liées au traitement des données à caractère personnel ?

7) Existe-t-il au sein de la direction un recensement de tous les fichiers sur support informatique ou manuels qui contiennent des données personnelles ?

8) Les fichiers recensés sont-ils régulièrement actualisés ? à quelle fréquence ?

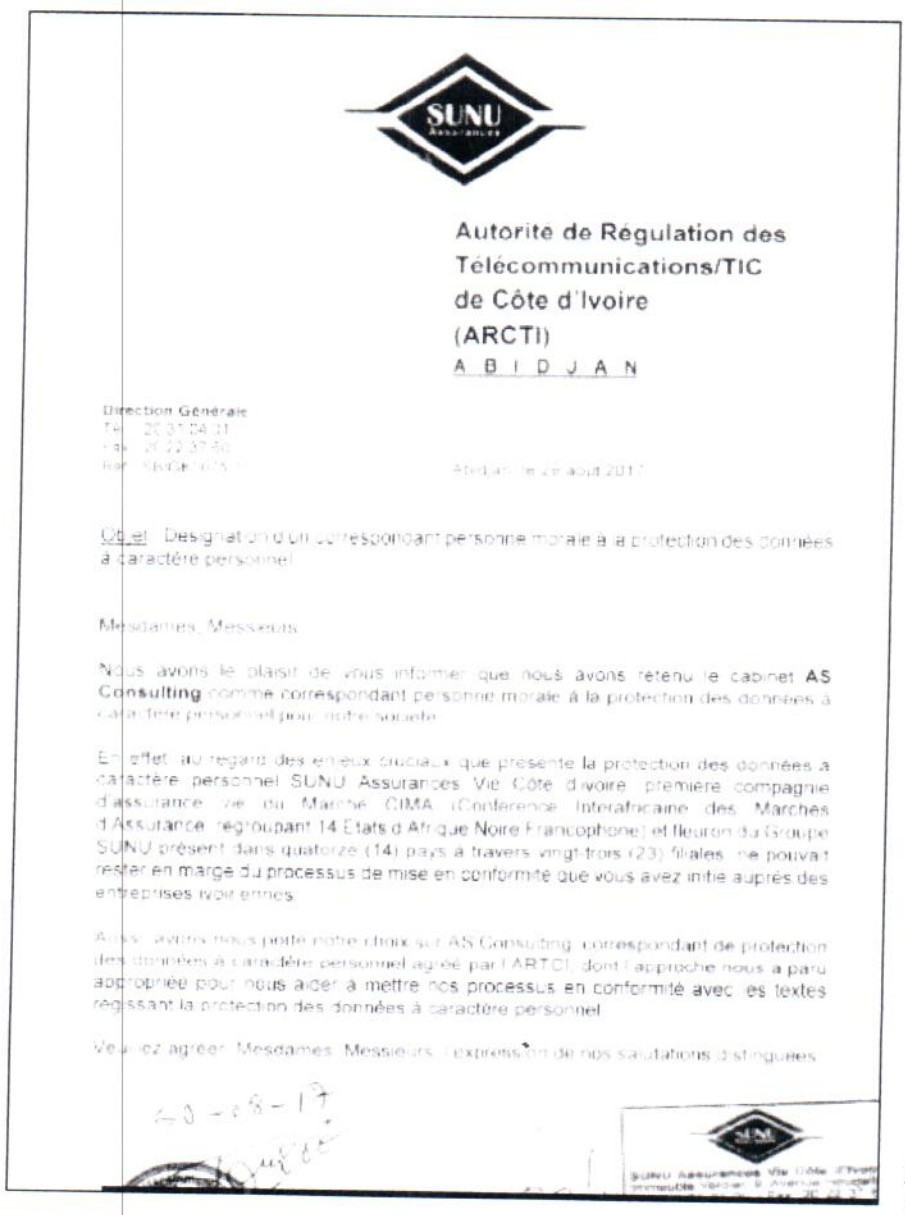
2- *b/ Questionnaire de type fermé (voir P.7)*

3- *Sécurité/système informatique (par traitement)*

TRAITEMENTS DES DCP	DESTINATAIRES
Constitution de dossiers pour appels d'offre	Entreprises partenaires (prospects)
Proposition de produits d'assurance aux entreprises	Laboratoires médicaux, Service médical VERDIER, Dr Production, Dr prestation, Actuariat
Enregistrements des souscriptions	Banques, Dr Production
Propositions de produits d'assurance par le biais des banques	Dr prestations, Dr production
Propositions de produits d'assurance aux Particulierss	Dr prestations, Dr production, Banques
Entrée en Relation-clients	Assurés, Banques, Dr Prestations, Dr Production
Gestion des sinistres déclarés	Dr prestation
Gestion des Rachats : partiel / total	Assurés
Remises de chèques	Assurés
Gestion du Bureau Direct	Assurés, Dr production
Validation et modification des contrats d'assurance	Assurés, Dr prestation, Dr reseaux Particulierss
Collecte de données informatiques	Direction Informatique Vie Groupe SUNU PARTICIPATION (Sénégal)
communication de données informatiques	
modifications de données informatiques	
Réassurance	(Entreprise partenaire)
Transfert s pour appel d'offre	
Rédaction de contrats de stage	Direction Admini. et Juridique,
Collecte de dossiers de candidature pour emploi	
Rédaction de contrats de travail	
Gestion des impôts sur les Traitements et Salaires (ITS)	
Gestion des déclarations CNPS	
Gestion de la rémunération	
Gestion des accompétences	
Gestion des congés et permissions	
Scanage de tous les dossiers physiques	
Consultation des images des caméras	
Conservation des images des caméras	
Gestion des départs de l'entreprise	
Gestion des serveurs	
Gestion des missions	
Gestion des systèmes d'accès (badges)	
Conservation des dossiers des prospects, assurés	
Personnel de SUNU	
Scanage de tous les dossiers physiques	
Gestion du parc informatique : Configuration et installation, maintenance, assistance	
Collecte de dossiers des Clients	
Emission de chèques	
enregistrement de données d'identification	
Support web	
conservation provisoire de pièces d'identité	
Conduite de missions d'audit	
Assistance aux utilisateurs dans leurs taches	
Lutte anti blanchiment	
Emission de chèques	
Rédaction de courriers	
conservation des rapports et représentation du DG	
Conduite de missions d'audit	
Gestion des compétences	
Validation des congés	
Collecte de documents	
Communication externe	

TRAITEMENTS DES DCP	SECURITE & ARCHITECTURE INFORMATIQUE
Collecte de dossiers de candidature pour emploi	Direction Admini. et Juridique, Impots CNPS, DG SUNU
Rédaction de contrats de travail	
Gestion des impôts sur les Traitements et Salaires (ITS)	
Gestion des déclarations CNPS	Physique: Armoires, Logique: Mot de passe
Gestion de la rémunération	Direction Admini. et Juridique, CNPS, DG SUNU
Gestion des accompétences	Direction Admini. et Juridique, Dr comptabilité, DG SUNU, Banques
Gestion des congés et permissions	Direction Admini. et Juridique, DG SUNU
Scanage de tous les dossiers physiques	Physique: Armoires, Logique: Mot de passe
Consultation des images des caméras	Mot de passe
Conservation des images des caméras	Existence d'une DMZ
Gestion des départs de l'entreprise	Existence d'une DMZ
Gestion des serveurs	Direction Admini. et Juridique, DG SUNU, Direction de l'ipent
Gestion des missions	Logiciel de sécurité firewall physique
Gestion des systèmes d'accès (badges)	SFTP Sunucloud
Conservation des dossiers des prospects, assurés	Les niveaux d'habilitation sont fonction de la hiérarchie
Personnel de SUNU	-SFTP:Sunucloud
Scanage de tous les dossiers physiques	-Sauvegarde des codes source une fois par an
Gestion du parc informatique : Configuration et installation, maintenance, assistance	Tous services
Collecte de dossiers des Clients	-Existence d'une politique d'accèes
Emission de chèques	-Mise à jour antivirus et systèmes à partir du serveur de l'antivirus
enregistrement de données d'identification	Dr Prestation
Support web	Les niveaux d'habilitation sont fonction de la hiérarchie ; sont tracées
conservation provisoire de pièces d'identité	Respo moyens généraux
Conduite de missions d'audit	-SFTP Sunucloud
Assistance aux utilisateurs dans leurs taches	Caisse, DG, CENTIF
Lutte anti blanchiment	Les niveaux d'habilitation sont fonction de la hiérarchie
Emission de chèques	Chef de Département Audit Interne -
Rédaction de courriers	-SFTP Sunucloud
conservation des rapports et représentation du DG	Etablissement d'un régistre pour les sorties
Conduite de missions d'audit	DG, Entreprises partenaires
Gestion des compétences	Casier de bureau
Validation des congés	Utilisateur Unique sur le serveur
Collecte de documents	DG, RH
Communication externe	les dossiers physiques non informatisés (seule la responsable y a la compta a accès aux autrance , le service juridique en cas de désaccords)
	Tous services, les assurés, les prospects, les institutions étatiques
	-Mot de passe
Rédaction de contrats de bail	Consultation exclusivement au bureau de la Responsable du Service Immeubles
Encaissement des loyers	Consultation exclusivement au bureau de la Responsable du Service Immeubles
Rédaction de courriers	Accès limité au bureau, mot de passe sur les ordinateurs
Rédaction des rapports et représentation du DG	Accès limité au bureau, Mot de passe sur les ordinateurs
gestion des compétences	Accès limité au bureau, Mot de passe sur les ordinateurs
Validation des congés	Mot de passe les ordinateurs, Accès limité au bureau

4- *Sécurité / données* *Les destinaires des traitées*



Autorité de Régulation des
Télécommunications/TIC
de Côte d'Ivoire
(ARCTI)
A B I D J A N

Direction Générale
Tél : 20 31 04 31
Fax : 20 22 37 40
Réf : SUNU/DG/[illegible]

Abidjan, le 29 août 2017

Objet : Désignation d'un correspondant personne morale à la protection des données à caractère personnel

Mesdames, Messieurs,

Nous avons le plaisir de vous informer que nous avons retenu le cabinet **AS Consulting** comme correspondant personne morale à la protection des données à caractère personnel pour notre société.

En effet, au regard des enjeux cruciaux que présente la protection des données à caractère personnel SUNU Assurances Vie Côte d'Ivoire, première compagnie d'assurance vie du Marché CIMA (Conférence Interafricaine des Marchés d'Assurance regroupant 14 Etats d'Afrique Noire Francophone) et fleuron du Groupe SUNU présent dans quatorze (14) pays à travers vingt-trois (23) filiales, ne pouvait rester en marge du processus de mise en conformité que vous avez initié auprès des entreprises ivoiriennes.

Aussi, avons nous porté notre choix sur AS Consulting, correspondant de protection des données à caractère personnel agréé par l'ARTCI, dont l'approche nous a paru appropriée pour nous aider à mettre nos processus en conformité avec les textes régissant la protection des données à caractère personnel.

Veuillez agréer, Mesdames, Messieurs, l'expression de nos salutations distinguées.

23-08-17

SUNU Assurances Vie Côte d'Ivoire

5- *Courrier de désignation de AS CONSULTING comme correspondant de SUNU Assurances Vie Côte d'Ivoire*

ARTCI

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

CONSEIL DE REGULATION

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2020-0537

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 03 MARS 2020

PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL PAR

LA SOCIETE SACO

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

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°2010-272 du 30 Septembre 2010 portant interdiction de la traite et les pires formes de travail des enfants en côte d'Ivoire

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°2011-481 du 28 décembre 2011 fixant les règles relatives à la commercialisation du café et du 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°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° 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° 2001-47 du 31 janvier 2001 relative à la redevance professionnelle en matière de café et de cacao ;

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° 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 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°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°2019-372 du 24 avril 2019 portant nomination du Directeur Général 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°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°2012-1008 du 17 Octobre 2012 fixant les modalités de commercialisations du cacao et du café ;

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°2019-372 du 24 Avril 2019 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°2014-0021 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 du 26 octobre 2017 portant vérification préalable ;

Vu la décision n°2017-0354 du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Vu le rapport d'audit de situation de la société SACO.

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 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, définit les étapes du processus de mise en conformité ;

Considérant que la société Africaine de Cacao (SACO) SA, Société Anonyme avec Administrateur Général, au capital de 25.695.651.316 FCFA, immatriculée au Registre du Commerce et du Crédit Mobilier sous le numéro CI-ABJ-1962-B-2396, sise à

Abidjan, Zone 4, 6 Rue Pierre et Marie Curie, 01 BP 1045 Abidjan 01, Tél. : 21 75 02 00, a saisi l'Autorité de protection d'une demande de mise en conformité ;

Considérant que SACO, Correspondant à la protection, personne morale agréé par l'Autorité de protection, a effectué l'audit de situation de la société SACO, qui a fait ressortir un niveau de conformité avec la Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, moyen ;

Considérant toutefois les recommandations et prescriptions faites par la société SACO dans le rapport définitif d'audit de situation et sous réserve de l'application de ces recommandations et prescriptions ;

Considérant que la société SACO s'engage à mettre en œuvre les recommandations et prescriptions formulées dans le rapport définitif d'audit de situation, en vue d'apporter des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements qu'elle effectue ;

Que la société SACO s'engage à veiller au respect de ces mesures ;

Après en avoir délibéré,

DECIDE :

Article 1 :

La société SACO est autorisée à effectuer le traitement 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 la société SACO.

Article 2 :

La société SACO est autorisée à effectuer les traitements énumérés dans l'annexe 2 de la présente décision.

Article 3 :

La société SACO 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 ;
- les officiers de police judiciaire munis d'une réquisition;
- les clients de la société SACO, dans le respect des clauses contractuelles qui les lient.

Article 4 :

La société SACO est autorisée à communiquer à la maison mère en Suisse, les données énumérées dans l'annexe 3.

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, la société SACO 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 société SACO ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

Article 6 :

Les traitements de données autorisés dans la présente décision ont pour finalités :

- Les achats et opération cacao
- Le monitoring et évaluation
- La durabilité
- La gestion de la qualité
- La gestion juridique
- La gestion des ressources humaines
- La gestion de l'informatique
- La gestion de la logistique
- Les archives
- La gestion administrative et financière de la société
- La communication des données à la maison mère

Les traitements afférents aux finalités ci-dessus sont listés dans l'annexe 4 de la présente décision.

Article 7 :

La société SACO 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 la société SACO, 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 SACO 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 SACO 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 SACO, 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 société SACO 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 SACO.

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 03 Mars 2020
En deux (2) exemplaires originaux

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

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

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

CONSEIL DE REGULATION
ANNEXE 1

DONNEES AUTORISEES AUX TRAITEMENTS

- **Etat-civil, Identité, Données d'identification :**	Nom, prénom, sexe, âge, date et lieu de naissance. nationalité, photo, image vidéo, extrait de naissance.
- **Vie personnelle :**	Situation matrimoniale, nombre d'enfants et âge des enfants, certificat de résidence.
- **Vie professionnelle :**	Date d'embauche, fonction, numéro matricule, numéro CNPS, curriculum vitae, signature, niveau d'études, catégorie professionnelle.
- **Informations d'ordre économique et financier :**	Revenu, numéro de compte bancaire, salaire.
- **Données biométriques :**	Empreinte digitale
- **Données de localisation : (déplacements, données GPS, GSM, etc.)**	Adresse géographique, coordonnées GPS, localisation des plantations cartographie de la plantation, géolocalisation de la flotte automobile.
- **Numéro d'identification national :**	Numéro de téléphone, numéro de CNI, numéro de passeport.
- **Infractions, condamnations, mesures de sureté :**	Casier judiciaire.
- **Données médicales :**	Fiche d'examen médical, analyse médicale, pathologie, affection, antécédents familiaux.
- **Données de connexion :**	email.

Fait à Abidjan, le 03 Mars 2020

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

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

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

ANNEXE 2

CONSEIL DE REGULATION

LISTE DES TRAITEMENTS

1. Achat des fèves
2. Achat cacao
3. Coordination service durabilité
4. Application KATCHILE
5. Formation sur la cacoculture
6. Monitoring et évaluation
7. Plant manager usine
8. Qualité assurance
9. Qualité fèves
10. Qualité usine
11. Up & down stream team
12. Création profil du salarié
13. Gestion administrative des ressources humaines
14. Gestion des carrières et recrutement
15. Gestion de la paie et rémunération
16. Formation
17. Contrat de travail et embauche
18. Contrôle d'accès biométrique
19. Vidéosurveillance
20. Gestion des assurances et sinistres
21. Gestion des contentieux
22. Gestion des contrats
23. Archivage papier
24. Comptabilité
25. Contrôle de gestion
26. Trésorerie
27. Achat : procurement
28. Géolocalisation
29. Sécurité domicile cadre
30. Import
31. Sécurité & HSE
32. Transfert de données vers la suisse

Fait à Abidjan, le 03 Mars 2020

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

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

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

CONSEIL DE REGULATION
ANNEXE 3

DONNEES AUTORISEES AU TRANSFERT

- **Etat-civil, Identité, Données d'identification :**	Nom, prénom, sexe, âge, date et lieu de naissance, nationalité, photo, image vidéo, extrait de naissance.
- **Vie personnelle :**	Situation matrimoniale, nombre d'enfants et âge des enfants, certificat de résidence.
- **Vie professionnelle :**	Date d'embauche, fonction, numéro matricule, numéro CNPS, curriculum vitae, signature, niveau d'études, catégorie professionnelle.
- **Informations d'ordre économique et financier :**	Revenu, numéro de compte bancaire, salaire.
- **Données de localisation : (déplacements, données GPS, GSM, etc.)**	Adresse géographique, coordonnées GPS, localisation des plantations cartographie de la plantation, géolocalisation de la flotte automobile.
- **Numéro d'identification national :**	Numéro de téléphone, numéro de CNI, numéro de passeport.
- **Infractions, condamnations, mesures de sureté :**	Casier judiciaire.
- **Données médicales :**	Fiche d'examen médical, analyse médicale, pathologie, affection, antécédents familiaux.
- **Données de connexion :**	email.

Fait à Abidjan, le 03 Mars 2020

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

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

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

CONSEIL DE REGULATION

ANNEXE 4

LISTE DES TRAITEMENTS PAR FINALITES

FINALITES	TRAITEMENTS
Achats et opération cacao	- Achat fèves - Achat cacao - Coordination service durabilité - communication
Monitoring et évaluation	- partenariat
La durabilité	- Application KATCHILE - Formation sur la cacaoculture - Communication (échange de mail et appel) - Coordination du service durabilité
La gestion de la qualité	- Plant manager usine - Qualité assurance - Qualité fèves - Qualité usine - Usine : up & down (stream team)
La gestion juridique	- Gestion des assurances et sinistres - Gestion des contentieux (sociaux) - Rédaction des contrats - Communication (échange de mail et appel)
La gestion des ressources humaines	- Création du profil salarié - Gestion administrative ressources humaines - Gestion des carrières - Recrutement - Gestion paie et rémunération - Infirmerie - Formation - Coordination ressources humaines - Attribution des matricules - Contrat de travail et note d'embauche
La gestion de l'informatique	- - Création et gestion des profils des salariés - Traitement générique

La gestion de la logistique	- Achat : procurement - Géolocalisation des véhicules - Sécurité domicile cadres - Import - Biométrie - vidéosurveillance
Archives	- archivage papier
La gestion administrative et financière de la société	- Comptabilité - Contrôle de gestion - trésorerie
La communication des données à la maison mère	- Transfert de données en Suisse

Fait à Abidjan, le 03 Mars 2020

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

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

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

CONSEIL DE REGULATION
ANNEXE 5

PRESCRIPTIONS ET DELAIS D'EXECUTION

POINTS D'ANALYSE	PRESCRIPTIONS	DELAIS D'EXECUTION
La légitimité et la licéité des traitements	Concernant le recueil du consentement des personnes concernées : ➢ dans le cadre de la gestion de la clientèle : - mettre à la disposition des personnes concernées, un formulaire de recueil du consentement préalable pour les traitements à effectuer. Les formulaires devront être mis à disposition lors de l'entrée en relation clientèle ; - insérer des clauses de consentement préalable dans les conditions générales de prestation de services ou dans les contrats proposés aux clients ; ➢ dans le cadre du recrutement et de la gestion du personnel : - mettre à disposition, lors de l'entretien d'embauche, un formulaire de recueil du consentement préalable ;	**60 jours**
	- insérer des clauses de consentement préalable dans les contrats de travail proposés à la signature du personnel ; - par tous autres moyens laissant preuve écrite.	
La finalité des traitements	RAS	RAS

Les délais de conservation	➢ Concernant la conservation des données relatives à la gestion du personnel : 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 de la clientèle : Les données traitées peuvent être conservées pendant toute la durée de la relation client. En cas de cessation de la relation client, une période supplémentaire de dix (10) ans est autorisée, à compter de la date de cessation de la relation client, conformément à l'article 24 de l'Acte Uniforme portant organisation et harmonisation des comptabilités des entreprises. ➢ Concernant l'archivage électronique : - Elaborer une politique d'archivage - Procéder à un archivage électronique des données conformément aux dispositions du n°2016-851 du 19 Octobre 2016.	**6 mois**
	➢ Concernant les données biométriques : - Communiquer la base de données biométriques à l'Office National de l'Identification ; - Effacer de la base de données, les données biométriques collectées ; - Mener une étude d'impact vie privée	

La proportionnalité des données	➢ Dans le cadre de la gestion des ressources humaines Sont interdits, la collecte et le traitement des données suivantes : - La filiation des agents ; - Le casier judiciaire des agents ; - Les empreintes digitales des agents pour l'accès aux services généraux, le contrôle de présence, l'identification des agents pour la fourniture de service. ➢ La gestion des données sensibles Elaborer et mettre en œuvre une politique de gestion des données sensibles. La société SACO devra : - Faire l'inventaire des données sensibles traitées ; - Analyser la proportionnalité des données sensibles traitées ; - Epurer sa base de données des informations sensibles disproportionnées et conserver les données pertinentes ; - Sécuriser les données sensibles ; - Définir les accès aux données sensibles ; - Procéder au recueil du consentement sur un formulaire distinct.	**RAS**
La transparence des traitements	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 ;	**60 jours**
	- l'existence et des modalités d'exercice de leurs droits 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 de la société SACO,	

	- affiches dans tous les lieux où sont opérés des traitements de données à caractère personnel ;	
Le système informatique	La société SACO doit mettre en œuvre les 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 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 ; - autoriser uniquement l'utilisation de supports amovibles chiffrés ; - implémenter le chiffrement des données communiquées par des canaux n'utilisant pas le protocole SSL ; - veiller à l'application effective de la politique de restriction des ports USB sur l'ensemble des postes de travail ; - informer les utilisateurs de la présence d'un système de journalisation ; cela pourrait se faire au moment de la diffusion de la charte informatique ; - enregistrer les interventions et les opérations de maintenance sur les postes de travail de manière à disposer de l'historique des accès.	**90 jours**
Les destinataires des données traitées	La société SACO - S.A doit : - Communiquer les données traitées uniquement aux destinataires habilités ;	**Sans délai**
Exactitude des données	La société SACO doit : - 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 ; - mettre à jour périodiquement les fichiers informatiques contenant les données à caractère personnel.	**06 mois**
Les sous-traitants	La société SACO doit : - inclure des clauses relatives à la protection des données à caractère personnel dans les contrats	**12 mois**

	passés avec ses sous-traitants ; - 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 à la société SACO et aux sous-traitants de veiller au respect de ces mesures.	
La vidéosurveillance	La société SACO doit : - Obtenir une autorisation pour l'utilisation d'un système de vidéosurveillance ; - Requérir l'accord du personnel pour la mise en place du dispositif de vidéosurveillance - informer les personnes concernées de l'existence d'un dispositif de vidéosurveillance, au moyen d'affiches placées à hauteur de vue dans les zones filmées par les caméras, et de pictogrammes placés de façon visible, aux entrées et aux sorties des locaux sous surveillance. - Les affiches et pictogrammes doivent indiquer, d'une façon claire et visible, les informations suivantes : - Le nom du responsable du traitement ; - Le fait que l'établissement est placé sous vidéosurveillance ; - La finalité du 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. - Veiller à ce que les caméras pouvant filmer les zones de circulation ne portent pas atteinte à la vie privée des personnes concernées ; - Ne pas diriger ses caméras de vidéosurveillance sur le poste de travail de ses employés ; - Ne pas poser ses caméras de vidéosurveillance dans les toilettes, les lieux de pause ou de repos de ses employés.	
	La société SACO doit également conserver les données collectées pendant une durée **de trente (30) jours**. En cas d'incidents, les données collectées devront être conservées pendant une période **d'un (01) an,** à compter de la dernière sauvegarde mensuelle.	
Le correspondant à la	La société SACO doit mettre à la disposition du Correspondant, les outils adéquats pour l'exercice de ses	**30 jours**

protection	fonctions. Elle doit en outre, favoriser la désignation d'un chargé de la protection au sein de toutes les autres directions.	
les droits d'accès, de rectification, d'effacement et d'opposition	La société SACO doit 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	La société SACO doit : - former son personnel sur la protection des données à caractère personnel. - Relayer efficacement l'action du Correspondant au sein des directions.	**90 jours**
Les procédures	La société SACO doit : - élaborer une charte de protection des données à caractère personnel ; - établir une politique de sécurité et de confidentialité ; - élaborer une procédure de gestion des droits des personnes concernées ; - intégrer des clauses de recueil du consentement et de transparence dans les procédures ; - d'élaborer une procédure de gestion des plaintes des personnes concernées ; - Conformer les procédures existantes à la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.	**90 jours**
La déclaration des fichiers	La société SACO doit introduire une demande d'autorisation de traitements de données à caractère personnel auprès de l'Autorité de protection	

Fait à Abidjan, le 03 Mars 2020

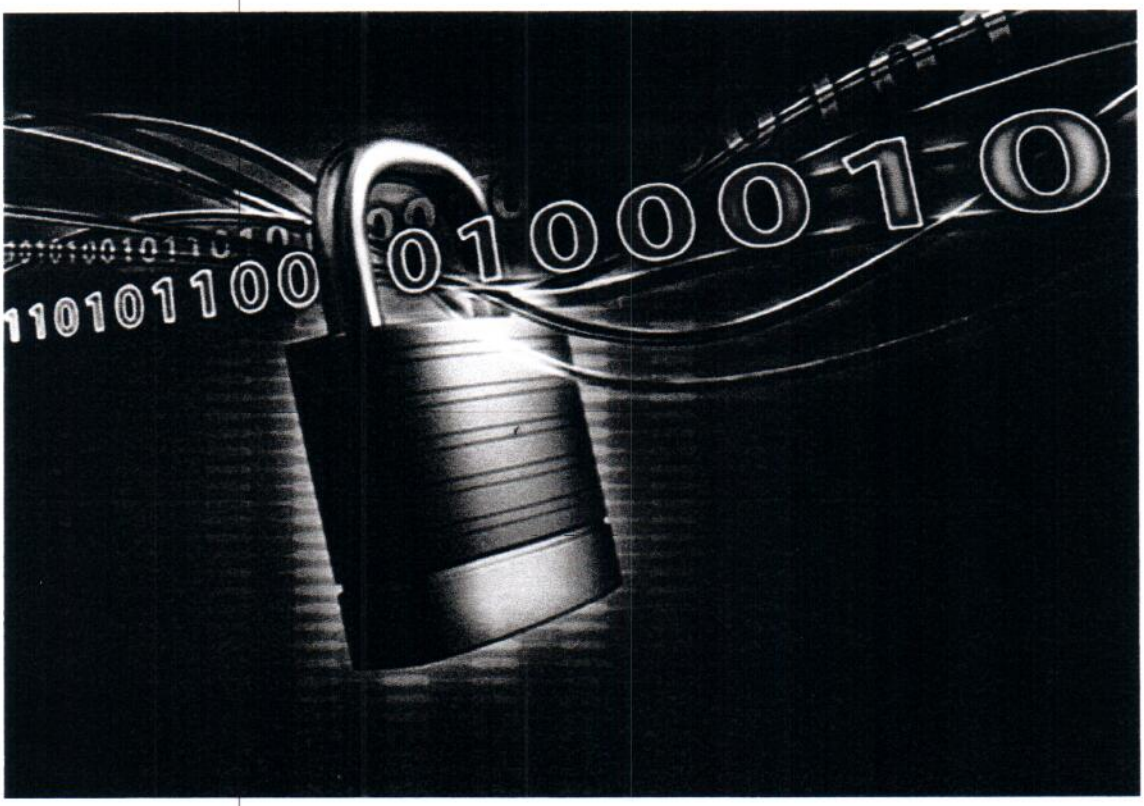
Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

SACO SOCIETE AFRICAINE DE CACAO
a Barry Callebaut company

Consulting

RAPPORT DEFINITIF D'AUDIT DE SITUATION



MISE EN CONFORMITE DE LA SOCIETE AFRICAINE DE CACAO (SACO) AVEC LA LOI 2013-450 DU 19 JUIN 2013 RELATIVE A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

1. Contexte

Les traitements de données à caractère personnel opérés par les entreprises, dans le cadre de leurs activités, sont soumis aux formalités préalables et au respect des différents principes prévus par la Loi n°2013-450 du 19 juin 2013, relative à la protection des données à caractère personnel.

Aux termes de l'article 53 de ladite Loi, les responsables du traitement ont l'obligation de se mettre en conformité avec ses dispositions.

Pour répondre donc à cette exigence, la Société Africaine de Cacao (SACO) a décidé de démarrer son processus de mise en conformité en accord avec la décision de l'autorité de protection, tendant à la désignation d'un correspondant à la protection des données à caractère personnel agréé par l'ARTCI.

C'est dans ce cadre que la société AS CONSULTING, spécialisée dans la prestation de services informatiques et agréé par l'autorité de protection, a été désignée comme correspondant par Société Africaine de Cacao (SACO) le 23 janvier 2018, pour l'accompagner dans ce processus de mise en conformité. Une démarche en adéquation avec les objectifs de la susdite.

Créée en 1964, la Société Africaine de Cacao en abrégé SACO est la filiale Ivoirienne du Groupe International BARRY CALLEBAULT.

Le domaine de prédilection de la société est l'achat et la transformation de fèves de cacao.

2. Enjeux

La Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, rend les entreprises responsables de la protection des données qu'elles manipulent (données des clients, données du personnel, etc.).

L'image d'une entreprise peut être négativement affectée, lorsque celle-ci est incapable de communiquer aux personnes concernées, les données qu'elles demandent ou lorsqu'une faille de sécurité a été rendue publique.

La mise en conformité implique que l'entreprise est en mesure de démontrer qu'elle a pris les dispositions techniques, organisationnelles et juridiques nécessaires à la protection des données qu'elle détient.

La Loi relative à la protection des données à caractère personnel est génératrice de changements au sein de l'entreprise qui doit :

- désigner un correspondant à la protection ;
- élaborer une data gouvernance en lien avec la stratégie de l'entreprise et en accord avec la règlementation.

Il s'agit d'une approche dynamique et permanente de la gestion de la protection des données à caractère personnel.

Une telle approche suppose la compréhension de la nouvelle gouvernance des données à caractère personnel, telle que définie par la Loi.

Il est donc primordial pour l'entreprise de former son personnel et d'effectuer un état des lieux des traitements, des données manipulées, des moyens, et des risques. Cet état des lieux permettra de détecter les dysfonctionnements éventuels, et d'élaborer une stratégie intégrant les exigences de conformité de la Loi.

Il est en outre important de définir l'échelle des responsabilités au sein de l'entreprise (Correspondant, DSI, RSSI...) et dans un périmètre plus large (sous-traitants, hébergeurs cloud, co-responsables de traitements, etc.).

La nouvelle gouvernance des données personnelles implique également la maitrise des données (nature, volume, localisation, niveau de criticité, cycle de vie, etc.), ainsi que la maitrise de techniques de sécurité telles que l'anonymisation, la pseudonymisation, le chiffrement, la traçabilité, la détection de fuite etc.

Par ailleurs, une analyse de conformité permettra de mesurer les écarts entre l'existant et les exigences réglementaires.

En vue de faciliter la mise en conformité des entreprises avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, l'Autorité de protection a définie, par décision n°2017-0354 du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, une procédure dite « processus de mise en conformité ».

Le processus de mise en conformité se déroule selon les étapes suivantes :

- la sensibilisation et la formation de l'ensemble du personnel ;
- le diagnostic des activités et processus métiers ;
- l'inventaire des données à caractère personnel et la classification des données traitées ;
- l'inventaire des traitements effectués y compris les transferts de données à l'étranger ;
- l'identification et la classification des supports de traitements ;
- l'analyse des critères relatifs aux données traitées ;
- l'analyse d'écarts ;
- la définition d'un plan d'actions correctives ;
- la déclaration des traitements et le dépôt de la demande d'autorisation.

A l'issue de cette procédure, une autorisation unique de traitement de données est délivrée à l'entreprise. Une attestation de conformité est également délivrée au responsable du traitement après correction des écarts constatés.

La mise en conformité est le point de départ d'un contrat de confiance entre l'entreprise et ses partenaires.

3. Méthodologie

La méthodologie adoptée correspond à celle définie dans l'annexe de la décision N°2017-0354 du 26 octobre 2017, portant procédure de mise en conformité. Tout d'abord, les responsables des différents services et directions ont suivi une formation sur les notions de protection des données à caractère personnel. Ensuite, un audit de situation a été mené pour se faire une idée de l'état des lieux de l'entreprise, en ce qui concerne la protection de ces données. Cet audit à consister en une série d'interviews avec les différents responsables de pôle afin de cerner au mieux les traitements de chaque direction et services sur les données à caractères personnel.

3.1. La formation du personnel

La formation du personnel a eu lieu le 13 février 2018 au siège de SACO. Elle a été faite par M. ASSOUA Silvère de l'ARTCI.

Elle avait pour objectifs de faire connaitre et comprendre :

- les enjeux de la mise en conformité avec la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- les différents principes de la protection des données à caractère personnel ;
- la notion de consentement préalable, sa nécessité dans le contexte de mise en œuvre d'un traitement et les exceptions qui lui sont applicables ;
- le contenu des données dites sensibles ;
- les différents régimes et formalités préalables pour le traitement des données à caractère personnel ;
- les conditions et les modalités de transfert des données à caractère personnel hors de l'espace CEDEAO ;
- l'exercice des droits des personnes concernées par le traitement des données à caractère personnel ;
- les obligations du responsable du traitement ;
- le statut et la composition de l'Autorité de protection des données à caractère personnel ;
- les missions et les pouvoirs de l'Autorité de protection des données à caractère personnel ;
- les sanctions pouvant être mises en œuvre par l'Autorité de protection des données à caractère personnel ;
- le statut, le profil et les missions du Correspondant à la protection des données à caractère personnel ;

16 personnes réparties **en 6 Directions et Services** de la société SACO ont participé à la formation *(Voir en annexe : liste de présence)* :

- Direction Générale
- Partenariat /MNI
- Durabilité
- Informatique
- Ressources Humaines

- Direction Juridique

3.2. L'audit de situation

L'audit de situation s'est réalisé selon les étapes ci-après :

Dans un premier temps, les responsables de la SACO (au nombre de 26, représentant 22 Directions et Services) ont été soumis à un questionnaire ; ces interviews se sont déroulées sur les sites de la Zone 4 et de Vridi. L'objectif était de faire un diagnostic des activités de chacune de ces entités services afin d'identifier celles liées au traitement de données à caractère personnel ;

A la suite de cela, les données recueillies ont été analysées afin d'identifier les données à caractère personnel

Pour finir, une évaluation suivie d'un rapprochement ont été menés pour déceler les écarts entre ces traitements et les critères relatifs à ladite loi.

4. Règles en vigueur

4.1. Le droit applicable à Société Africaine de Cacao (SACO) : cadre légal et institutionnel

4.1.1. Le cadre légal

Le cadre légal des traitements opérés par la Société Africaine de Cacao (SACO) est constitué par les textes suivants :

4.1.1.1.Textes régionaux

- l'Acte additionnel A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel ;
-
- l'Acte additionnel A/SA.2/01/10 du 16 février 2010 sur les transactions électroniques.
- L'Acte Uniforme révisé relatif aux droits des sociétés et des groupements d'intérêt économique.

4.1.1.2.Textes nationaux

- **Lois**

- 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 ;

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

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

- La Loi n°2013-546 du 30 juillet 2013 relative aux Transactions électroniques.

o **Ordonnance**

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

- L'ordonnance N°2011-481 du 28 décembre 2011 fixant les règles relatives à la commercialisation du café et du cacao ;

- 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 ;

- 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 ;

- 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 ;

- Ordonnance N° 2001-47 du 31 janvier 2001 relative à la redevance professionnelle en matière de café et de cacao ;

- 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 ;

- 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 ;

o **Décrets**

- 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 ;

- Le Décret n°2012-1008 du 17 Octobre 2012 fixant les modalités de commercialisations du cacao et du café ;

- 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 ;

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

- 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 ;

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

- 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 ;

- Décret N°2012-1013 du 17 octobre 2012 relatif à la tierce détention en matière de café-cacao ;

- Décret N°2012-1012 du 17 octobre 2012 fixant les modalités de conditionnement des cafés verts à l'exportation ;

- Décret N°2012-1011 du 17 octobre 2012 fixant les modalités de conditionnement du cacao à l'exportation ;

- Décret N°2012-1010 du 17 octobre 2012 Règlementant la profession d'exportateur de café et de cacao ;

- Décret N°2012-1009 du 17 octobre 2012 fixant les conditions d'exercice de la profession d'acheteur de produits café et cacao ;

- Décret N°2012-1008 du 17 octobre 2012 fixant les modalités de commercialisation du café et du cacao ;

- Décret N° 2012-86 du 20 janvier 2012 portant nomination du Directeur Général du Conseil de Régulation, de Stabilisation et de Développement de la Filière Café-Cacao, en abrégé « le Conseil du Café-Cacao » ;

- Décret N° 2012- 26 du 20 janvier 2012 portant nomination des membres du Conseil d'Administration du Conseil de Régulation, de Stabilisation et de Développement de la Filière Café-Cacao en abrégé « le Conseil du Café-Cacao » ;

- Décret N° 2012-07 du 16 janvier 2012 portant composition du Conseil d'Administration du Conseil de Régulation, de Stabilisation et de Développement de la Filière Café-Cacao ;

- Décret N° 2012-06 du 16 janvier 2012 portant dénomination de l'Organe de Gestion, de Développement, de Régulation de la Filière Café-Cacao et de Stabilisation des prix du Café et du Cacao ;

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

- Décret n°2019-947 du 13 novembre2019 portant nomination du Président de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

- 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) ;

- Décret n°2019-372 du 24 Avril 2019 portant nomination du Directeur Général de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;

- **Arrêté**

- 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 ;

- 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

- 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

- Arrêté Interministériel N° 017/MINAGRI/MPMEF du 11 janvier 2013 fixant le niveau des taxes et redevances au titre de la campagne café 2012/2013

- Arrêté N° 764 du 16 Novembre 2012 portant modification du Droit Unique de Sortie (DUS) sur les fèves de cacao et sur les produits dérivés du cacao

- Arrêté N° 691 du 03 Octobre 2012 portant modification du Droit Unique de Sortie (DUS) sur les fèves de cacao et sur les produits dérivés du cacao

- Arrêté N°009 MINAGRI/MEF du 3 OCT 2012 fixant le niveau des taxes et redevances au titre de la campagne principale cacao 2012-2013.

o **Décisions de l'Autorité de protection**

- 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 ;

- 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 ;

- 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.

- Décision n°2017-0353 du 26 octobre 2017 portant vérification préalable ;

- Décision n°2017-0354 du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

4.1.2. Le cadre institutionnel

Conformément à l'article 46 de la Loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, les missions de l'Autorité de protection ont été confiées à l'Autorité en charge de la régulation des télécommunications/TIC de Côte d'Ivoire (ARTCI).

Créée par l'Ordonnance n°2012-293 du 21 mars 2012 relative aux Télécommunications/TIC, l'ARTCI est une Autorité Administrative Indépendante, dotée de la personnalité juridique, de l'autonomie financière et de pouvoirs spéciaux. Elle est composée d'un Conseil de Régulation, collège de sept (7) membres, et d'une Direction Générale.

En sa qualité d'Autorité de protection, l'ARTCI est chargée :

- d'informer les personnes concernées et les responsables du traitement de leurs droits et obligations ;
- de recevoir les déclarations et d'octroyer les autorisations pour la mise en œuvre de traitements des données à caractère personnel, ou de les retirer dans les cas prévus par la loi ;
- de recevoir les réclamations et les plaintes relatives à la mise en œuvre des traitements de données à caractère personnel et d'informer les auteurs de la suite accordées à celle-ci ;
- de déterminer les garanties indispensables et les mesures appropriées pour la protection des 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 loi ;
- d'élaborer des règles de conduite relatives aux traitements et à la protection des données à caractère personnel.

4.2. Les principes généraux applicables

Les principes sont brièvement développés ci-après :

4.2.1. La légitimité du traitement

Ce principe signifie que le consentement sans ambiguïté de la personne concernée est exigé préalablement à tout traitement de données à caractère personnel.

En effet, le traitement de données à caractère personnel est considéré comme légitime si la personne concernée donne expressément son consentement préalable.

Cependant, il peut être dérogé à cette exigence pour les motifs suivants.

- l'exécution d'une mission effectuée dans l'intérêt public ;
- le respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- l'exécution d'un contrat auquel la personne concernée est partie ;
- la sauvegarde des intérêts vitaux de la personne concernée.

4.2.2. La finalité du traitement

Ce principe définit le lien entre les données et les traitements. Les données à caractère personnel ne peuvent être recueillies et traitées que « pour des finalités déterminées, explicites et légitimes» et leur utilisation ultérieure doit toujours être compatible avec ces finalités.

Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime, correspondant aux missions du responsable du traitement.

4.2.3. La pertinence et la proportionnalité des données

Les données personnelles doivent être adéquates, pertinentes et non excessives, au regard des finalités pour lesquelles elles sont traitées. Seules doivent être traitées les informations pertinentes et nécessaires pour atteindre la finalité définie par le responsable du traitement.

4.2.4. La conservation limitée des données

Les données traitées doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées.

4.2.5. L'exactitude des données

Tous les efforts doivent être faits pour que les données traitées soient correctes et actuelles. Si ce n'est pas le cas, les données personnelles doivent être rectifiées, mises à jour ou bien effacées.

4.2.6. L'obligation de Transparence

Le responsable du traitement doit fournir à la personne concernée, l'information nécessaire relative aux données qu'il traite. Il doit lui assurer la possibilité d'un contrôle personnel. Le responsable du traitement doit avertir la personne concernée dès la collecte des données et en cas de transmission de ses données à des tiers.

En cas de demande de la personne concernée, le responsable du traitement doit fournir des renseignements quant aux données personnelles enregistrées et quant à leur utilisation, et effacer les informations dont le traitement ne serait pas conforme à la Loi.

4.2.7. L'obligation de sécurité et de confidentialité

Le responsable du traitement est astreint à une obligation de sécurité. Il doit prendre les mesures nécessaires pour garantir l'intégrité, la confidentialité des données et éviter leur divulgation.

Le responsable du traitement ne peut communiquer les données traitées qu'à des destinataires légitimes ou habilités à en prendre connaissance.

4.2.8. Le respect des droits des personnes concernées

Les personnes concernées ont un droit :

- à l'information ou au questionnement,
- d'accès,
- d'opposition,
- de rectification,
- à l'oubli,
- à la portabilité.

4.3. Les règles applicables à Société Africaine de Cacao (SACO)

Outre les principes généraux à respecter, la Société Africaine de Cacao **(SACO)** à l'obligation de :

- désigner un correspondant à la protection ;
- introduire une demande d'autorisation pour les traitements qu'elle opère.

4.3.1. La désignation d'un Correspondant à la protection des données à caractère personnel

Aux termes de l'article 9 de la loi 2013-450 du 19 juin 2013 relative à la protection des données la désignation d'un correspondant à la protection fait partie des conditions minimum de recevabilité d'une demande d'autorisation de traitement de données à caractère personnel. La désignation du correspondant obéit aux conditions 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.

La désignation du correspondant à la protection des données doit être approuvée par l'Autorité de protection, lorsqu'il s'agit d'une personne physique.

Le correspondant à la protection peut également être une personne morale qui dispose d'un agrément à la fonction de correspondant délivré par l'ARTCI.
Le correspondant est chargé d'assurer, d'une manière indépendante, le respect de la Loi. Il bénéficie des qualifications requises pour exercer ses missions. Il tient une liste des traitements effectués, immédiatement accessible à toute personne en faisant la demande, et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions. Le correspondant peut saisir l'Autorité de protection des difficultés qu'il rencontre dans l'exercice de ses missions.

4.3.2. La demande d'autorisation de traitement/ la déclaration ou l'avis

En raison de son activité au quotidien, des finalités particulières mais aussi de l'existence de flux transfrontaliers de données, les traitements effectués par la Société Africaine de Cacao (SACO) sera soumise à autorisation, conformément à l'article 7 et 9 de la loi 2013-450 du 19 juin 2013.

En effet, La SACO, dans le cadre de ses activités, collecte notamment : le numéro de téléphone, les données biométriques et effectue des transferts des données à destination BARRY CALLEBAUT, l'entreprise mère, basée en Suisse (pays tiers au regard de ladite loi).

Tous les traitements, ci -dessus énumérés, étant soumis à une demande d'autorisation préalable, au terme de l'article 7 précité ; la SACO est donc assujetti au régime de l'autorisation

5. Etat des lieux de la protection des données à caractère personnel

L'état des lieux de la protection des données à caractère personnel de la **Société Africaine de Cacao (SACO)** comporte les étapes suivantes :

- l'organisation générale de la **Société Africaine de Cacao (SACO) ;**
- l'inventaire des traitements ;
- l'état de la conformité.

Les résultats qui suivent et les commentaires intègrent les différents entretiens menés avec les directions.

5.1. Sur l'organisation générale de la Société Africaine de Cacao (SACO)

5.1.1. Identification des activités impliquant le traitement de données à caractère personnel

La première phase du travail d'indentification des activités a consisté à se faire une idée du niveau de connaissance du domaine d'activité et des données à caractère personnels des directions et services. Le questionnaire a porté sur les points suivants :

✓ *Nombre de personnes par directions / services audités*

Les entretiens menés ont permis de relever que les directions et services audités disposent d'un effectif de 1170 personnes. Cet effectif se réparti comme suit :

Directions et Services	Effectif*
Achat : Procurement	4
Contrôle de gestion	6
Coordinatrice des archives	2
DAF	6
Direction Achat fèves	82
Direction Achat industriel / sécurité	30
Direction juridique	3
Direction Opération Cacao	134
DRH Administratif	4
DRH Paie	4
DRH Recrutement	4
DRH Responsable	4
Durabilité	500
Import	5
Infirmerie	1
IT : Informatique	4
Partenariat	2

Directions et Services	Effectif*
Plant Manager Usine	205
Qualité Assurance Afrique	45
Qualité Usine	20
Responsable Assurance Qualité	89
sécurité et HSE	6
Trésorerie	8
Usine Up & Down Stream	2
TOTAL	1 170

** ces effectifs sont issus de l'organigramme fourni par la SACO (actualisé le 23 nov. 2017) et des entretiens menés avec les différents responsables.*

✓ *Existence pour chaque activité d'un seul et unique responsable*

Hormis les archives, il existe effectivement un seul et unique responsable pour chaque activité, au sein des différents services et directions

✓ *Les activités de la direction/service liés aux traitements des données personnelles*

Les activités des services /directions liées aux traitements de données se répartissent comme présentées *aux PP.16-26.*

5.1.2. Existence d'un chargé de la protection des données

Il n'existe pas au sein de la SACO un chargé de la protection des données à caractère personnel. Néanmoins un point focal existe : il s'agit de la direction juridique, qui fait office d'interface entre la Direction de la SACO et AS CONSULTING (correspondant).

5.1.3. Risques liés aux processus métiers et connaissance des règles de la protection des données personnelles

Tous les responsables interrogés reconnaissent ne pas détenir de fichier listant spécifiquement les activités impliquant les DCP.

Pour ce qui est des règles de base à appliquer en matière de protection des données personnelles, seulement 7 responsables sur 24 interrogés, soit un taux de 29%, avouent les connaitre. Ces responsables appartiennent aux directions et services, qui sont en grande parties, concernées par les questions relatives aux DCP (direction Juridique, Ressources humaines et Durabilité).

Aussi, 6 responsables sur 24 affirment avoir connaissance des responsabilités et des sanctions pénales, financières et administratives en cas de non-respect de la règlementation.

5.1.4. Identification des risques propres à chaque direction

Dans l'ensemble, l'Identification des risques propres à chaque direction et services n'est pas effective. En effet, il n'y a que 3 responsables sur 24 qui la pratiquent.

5.1.5. Activités de contrôle interne

Seuls 2 responsables sur les 24 interrogés disposent de procédures de contrôle interne pour assurer la maîtrise des risques liés à la protection des données personnelles.

5.1.6. Recensement des fichiers et des traitements

5.1.6.1.*Sur l'existence d'un recensement des fichiers contenant des données à caractère personnel détenus par les directions*

Il n'existe pas au sein des services et directions, un recensement des fichiers listant spécifiquement les données à caractère personnel. Ces données personnelles se retrouvent incorporées aux autres données et éparpillées dans les autres fichiers.

5.1.6.2.*Sur les supports utilisés pour le recensement des fichiers contenant des données personnelles.*

Les supports utilisés pour le traitement des données personnelles de la SACO se répartissent comme suit :

Support de traitement des DCP
Boîtier électronique GPS
Dispositif biométrique (à trace)
Caméra (images)
Courrier électronique SACO
Dossier numérisé (Data Legal Base)
Fichier (WORD, EXCEL, PDF)
Infrastructure réseau informatique
Logiciel RH SUITE
Papier
Plateforme SUCCESS FACTOR
Poste de travail (PC, téléphone, etc.)

Smartphone de collecte "KATCHILE "
Système DMS (Formulaire)

5.1.6.3.Sur l'actualisation des fichiers

Plus de la moitié des directions et services, soit 15 sur 24 (63%), actualisent régulièrement leurs fichiers (voir annexe).

5.1.7. Connaissance en matière de protection des données à caractère personnel

15 agents ont été formés sur les notions des Données à Caractère Personnel (voir liste de présence), dans le cadre de la mise en œuvre du processus de conformité. Par contre, il n'existe pas encore de dispositif de formation au sein de la SACO sur le sujet.

5.1.8. Sécurité

5.1.8.1. Analyse des risques et existence d'une charte informatique

Il existe une charte informatique. Mais, celle-ci ne prend pas en compte les bonnes pratiques pour protéger les données à caractère personnel et aussi, elle n'est pas diffusée à l'ensemble du personnel.

5.1.8.2.Sécurité physique

La sécurité des locaux des locaux abritant les supports des traitements est assez bonne.

En effet, l'accès à l'entreprise est contrôlé par des agents de sécurité via un registre et des caméras de surveillance, les portes des différents bureaux sont fermées à clef. Mais sur ce dernier point, il faut souligner que le local contenant les archives dispose d'une clef utilisée par plusieurs personnes, ce qui n'est pas propice à une meilleure protection des données personnelles

5.1.8.3.Sécurité logique

La sécurité logique de la SACO repose sur repose sur la mise en œuvre d'un système de contrôle d'accès logique rigoureux s'appuyant sur un service d'authentification réputé fort, ainsi que des niveaux d'habilitation restreignant l'information aux seules personnes ayant droit

5.1.8.4.Authentification

Le système d'authentification mené au sein de la SACO se caractérise par :

- L'attribution d'un identifiant unique à chaque utilisateur ;
- Les mots de passe (utilisateur) sont régulièrement renouvelés ;
- Les mots de passe respectent les règles de complexité ;
- Des profils d'habilitation sont définis pour chaque utilisateur ;

5.1.8.5.Gestion des accès

Les accès aux applications et aux ressources informatiques, en général, sont régulièrement mis à jour et supprimés en cas de départ de l'utilisateur.

5.1.8.6.Sauvegardes et maintenance

La sauvegarde et la maintenance sont assurées à distance au niveau groupe Barry Callebaut, depuis le siège en Suisse.

5.1.8.7.Réseau

La sécurité du réseau est dévolue à la direction informatique. Celle-ci a limité les flux réseaux au strict nécessaire afin d'éviter toute intrusion malveillante. En plus, les accès distants des appareils nomades sont sécurisés par VPN.

5.2. Inventaire des traitements

L'inventaire des traitements effectués a permis d'identifier **42 traitements,** répertoriés dans le tableau ci-après (voir page **19-29**) :

Direction	Entité	Traitement	Finalités	Données collectées
Direction administrative et finance	Comptabilité	Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
		Analyse des fiches de paie des salariés	Expliquer les variations (dépassement ou économie) de la paie	- Nom et prénom - Matricule - Salaire
	Contrôle de gestion	Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
	Direction administrative et finance	Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
	Direction juridique	Gestion des assurances et sinistres	Formaliser et gérer les risques juridiques avec les parties prenantes	- Nom et prénom - Police (personnes physiques)
		Gestion des contentieux (sociaux)	Formaliser et gérer les relations juridiques avec les partenaires sociaux	- Nom et prénom - Matricule - Fonction
		Rédaction des contrats	Formaliser les relations juridiques avec les parties prenantes	- Nom et prénom - Matricule - Fonction
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone

Direction	Entité	Traitement	Finalités	Données collectées
	Informatique	Création et gestion des profils (mails)	- Crée les comptes utilisateurs (arrivée) et les supprimer (départ) de l'entreprise - Administrer les mails	- Nom et prénom - Fonction - Photo - Catégorie professionnelle - Service
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
	Trésorerie	Signature des ordres de paiement	signature des ordres de paiement	- CNI - Passeport - Certificat de résidence
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
Direction des ressources humaines	Direction des ressources humaines	Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
		Coordination RH (SUCCESS FACTOR)	- Recrutement - Gestion administrative - Paie	- CV - Nom et prénom - N° CNPS
	Infirmerie	Prévention	Prévenir les maladies et pathologie afin d'avoir des employés en bonne santé	- Nom, prénom - Matricule - Fiche d'examen médical

Direction	Entité	Traitement	Finalités	Données collectées
		Sensibilisation	Sensibiliser les collaborateurs afin d'avoir des employés en bonne santé	- Nom, prénom - Matricule
				- Nom, prénom - Date d'entrée - Date de naissance - Fiche d'examen médical
		Visite médicale	S'assurer de la bonne santé des candidats en vue de l'embauche	
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
	Recrutement et gestion des carrières	Formation (en interne-externe)	Assurer la formation des collaborateurs	- Nom, - Prénom - Matricule - Fonction - Service
		Gestion des carrières (SUCCESS FACTOR)	Faire le suivi de la carrière des collaborateurs	- Nom, - Prénom - Âge - Situation matrimoniale
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone

Direction	Entité	Traitement	Finalités	Données collectées
		Recrutement (SUCCESS FACTOR)	Recruter les futurs collaborateurs	- Nom, prénom - Date de naissance - Photo - CV - Numéro de téléphone - Fiche d'examen médical
	Paie et rémunération	Attribution des matricules	Créer en attribuant un code au nouveau salarié au sein de l'entreprise	- Nom, - Prénom - Matricule - Fonction - Service
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
		Création profil et gestion du salarié sur SAGE RH SUITE	Créer le profil du nouveau collaborateur pour qu'il ait accès et travail sur le Logiciel	- Nom, - Prénom - Matricule - Fonction - Service
		Gestion Paie et rémunération (SUCCESS FACTOR)	Assurer la rémunération des collaborateurs	- Matricule - Nom et prénom d'usage - Nombre d'enfant - Date de naissance - Numéro compte bancaire

Direction	Entité	Traitement	Finalités	Données collectées
		Afficher la note d'embauche	Faire connaitre le (la) nouvel(le) embauché(e) aux autres collaborateurs	- Nom - Prénom - Photo - Matricule - Fonction - Service
	Gestion administrative RH			
		Etablir le contrat de travail	Formaliser la relation juridique liant le collaborateur à l'entreprise	- CNI - Extrait de naissance - Casier judiciaire - Photo
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
		Gestion administratives RH (SUCCESS FACTOR)	Assurer la gestion administrative des salariés	- Nom - Prénom - Photo - Matricule - Fonction - Service
Direction Logistique Achat Sécurité	Achat : procurement	Mise à disposition de la main d'œuvre temporaire	S'assurer de la qualité du personnel sélectionné (Main d'œuvre Temporaire)	- Nom et prénom - CV - Numéro de téléphone
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone

Direction	Entité	Traitement	Finalités	Données collectées
		Géolocalisation des véhicules (sous-traitée)	- Retrouver les véhicules en cas de vol ou de braquage - Traçabilité des véhicules	- Données GPS
				- Localisation - Numéro de
	Direction Achat industriel / sécurité	Sécurité (Domicile cadres)	Assurer la sécurité du domicile des cadres de l'entreprise	téléphone des cadres (codés) - Nom et prénom - Fonction
		Sécurité (Site)	Assurer l'intégrité des biens de l'entreprise et des personnes qui y travaillent	- Nom et prénom - CNI
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
	Import	Transit Guichet Unique du Commerce Extérieur (GUCE)	Assurer le dédouanement des marchandises de l'entreprise	- Nom et prénom - CNI
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
	sécurité et HSE	Donnée biométrique (Empreinte digitale)	- S'assurer du pointage des collaborateurs - Surveillance du site - Prévention contre tous les risques	- Empreinte biométrique
		Vidéosurveillance	Surveiller le site pour prévenir tout acte de malveillances	- Image de caméra

Direction	Entité	Traitement	Finalités	Données collectées
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
				- Nom, prénom - Date de naissance - Sexe
Direction Qualité	Plant Manager Usine	Evaluation	Faire un feed-back du travailleur pour une amélioration continue	- Date d'entrée - Parcours professionnel CV) - photo
		Rémunération	Revalorisation salariale du travailleur	- Nom et prénom - Date de naissance - Sexe - Date d'entrée - Salaire
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
	Qualité Assurance Afrique	Mesures de performance	Connaitre la performance des travailleurs de l'usine (atteinte des objectifs)	- Nom et prénom - Fonction - Catégorie professionnelle - Signature
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone

Direction	Entité	Traitement	Finalités	Données collectées
	Qualité fèves	Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
			- Protection des produits (la sécurité alimentaire) - S'assurer que le personnel en contact avec les produits est en bonne santé	- C.V (appel si nécessaire de l'employeur)
	Qualité Usine	Food defense (sécurité alimentaire)		- Empreinte biométrique - Casier judiciaire - Image de vidéosurveillance - Analyse médicale
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
	Usine : Up & Down Stream Team	La traçabilité travaux usine	Planifier, noter et suivre la qualité des travaux du personnel	- Numéro flotte du personnel - Nom et prénom - Matricule - Numéro de l'équipe (si en groupe de travail)
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone

Direction	Entité	Traitement	Finalités	Données collectées
Direction R & D Durabilité	Durabilité	Application KATCHILE	- Connaitre les planteurs avec qui SACO travaille (jeunes, personnes âgées) - S'assurer de disposer du cacao (matière première principale de SACO) de matière durable. - Améliorer la situation de vie du planteur (éducation des enfants, santé)	- Nom et prénom - Sexe - Âge - Nombre d'enfants (âge, niveau d'étude, etc.)
		Formation sur la cacao culture	- Orienter les services de SACO aux planteurs (formation, construction d'écoles, comment prêter et à qui prêter)	- Nom et prénom - Sexe - Âge - Nombre d'enfants (âge, niveau d'étude, etc.)
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
Direction Usine site d'achats	Direction Achat fèves	Achat Fèves	Achat des fèves avec les commerciaux, coopératives, société, site d'achat	- CNI (du président et membres du conseil d'administration) - Nom et prénom des travailleurs - Numéro de téléphone
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone

Direction	Entité	Traitement	Finalités	Données collectées
		Achat cacao	- S'assurer de travailler avec des gens ou des structures légales (en règle vis-à-vis du conseil du café-cacao) en conformité avec les procédures de gestion de risques de la SACO	- CNI des responsables de la coopérative - Signature du responsable - Revenus, salaires - Données GPS de la plantation - Cartographie de la plantation
	Direction opération Cacao			
		Coordination du service durabilité	- Collecte d'informations socio-économiques liées aux planteurs pour évaluer l'impact liés l'activité - Géolocalisation et cartographie des plantations	- CNI des responsables de la coopérative - Signature du responsable - Revenus, salaires - Données GPS de la plantation - Cartographie de la plantation
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone

Direction	Entité	Traitement	Finalités	Données collectées
Monitoring & Evaluation	Partenariat	Reporting	- Rendre compte aux clients, donateurs, et autres organismes partenaires sur la gestion des projets et des fonds octroyés - Collecte des données pour avoir une évaluation sur l'impact des activités et sur les indicateurs (production et producteur)	- Nom et prénom - Les coordonnées GPS de la plantation
		Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
Projet Archives	Archives	Communication (échange de mail et appel)	Communication : - Interne (Entre collaborateurs) - Externe (Avec les parties prenantes)	- Mails - Numéro de téléphone
		Archivage papier	Superviser le projet d'archivage et archiver les documents papier provenant des services et directions de l'entreprise	Données de toute sorte (méconnues)
SACO	SACO	Transfert de données	Echanger les données entre les entités du groupe	Données issues de toutes les entités

5.3. Etat de la conformité : Evaluation

L'évaluation générale de **SACO** a donné **un taux de conformité avec la loi de 63%,** selon le détail ci-après :

Entité	Note obtenue	Barème*	% conformité
Contrôle de gestion	9	9	100%
Qualité fèves	5	5	100%
Direction administrative et finance	5	5	100%
Comptabilité	5	5	100%
Informatique	34	37	92%
Durabilité	39	43	91%
Achat : Procurement	9	10	90%
Qualité Assurance Afrique	13	15	87%
Direction juridique	29	35	83%
Partenariat	13	16	81%
Direction des ressources humaines	13	16	81%
Gestion administrative RH	27	34	79%
Paie et rémunération	29	37	78%
Recrutement et gestion des carrières	33	45	73%
Archives	7	10	70%
Qualité Usine	16	23	70%
Import	9	15	60%
Trésorerie	9	15	60%
Usine : Up & Down Stream Team	9	16	56%
Plant Manager Usine	13	27	48%
Direction opération Cacao	12	28	43%
sécurité et HSE	13	34	38%
Direction Achat fèves	8	23	35%
Direction Achat industriel / sécurité	19	61	31%
Infirmerie	17	65	26%
TOTAL GENERAL	395	629	63%

** La variation des barèmes est due, d'une part, à la spécificité de chaque direction et services et, d'autre part, aux traitements de ces directions et services sur les DCP.*

6. Analyse

6.1. Sur la légitimité et la licéité des traitements

Aux termes de l'article 14 de la loi n°2013-450 du 19 Juin relative à la protection des données à caractère personnel, le traitement des données à caractère personnel est considéré comme légitime si la personne concernée donne expressément son consentement ;

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 :

- soit au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

- à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande ;

- à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée.

Considérant que la Société Africaine de Cacao (SACO) procède elle- même à la collecte des données ; qu'il s'agit là d'une collecte directe des données à caractère personnel ;

Considérant que la Société Africaine de Cacao (SACO) indique qu'elle procède par recueil du consentement préalable par le biais de formulaires signés par les paysans et planteurs, et aussi ses salariés liés par des contrats de travail ;

En somme, le correspondant estime qu'au travers de ces dérogations, les traitements opérés par la Société Africaine de Cacao (SACO), dans le cadre de son activité, sont légitimes. Par contre, en ce qui concerne les autres traitements, qui n'entrent pas dans le cadre de ses activités-métier telles que la vidéosurveillance, la gestion des accès par badges, et de la biométrie, un effort reste à faire.

6.2. Sur la finalité des traitements

Aux termes de l'article 16 de la loi n°2013-450 du 19 Juin relative à la protection des données à caractère personnel 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 Société Africaine de Cacao (SACO) collecte les données à caractère personnel pour les finalités suivantes :

- Communication interne (Entre collaborateurs) et externe (Avec les parties prenantes) ;
- Expliquer les variations (dépassement ou économie) de la paie ;
- Formaliser et gérer les risques juridiques avec les parties prenantes et les partenaires sociaux ;
- Crée les comptes utilisateurs (arrivée) et les supprimer (départ) de l'entreprise ;
- Administrer les mails ;
- Signature des ordres de paiement ;
- Recrutement ;
- Gestion administrative ;
- Paie ;

- Prévenir et sensibiliser sur les maladies et pathologie afin d'avoir des employés en bonne santé ;
- S'assurer de la bonne santé des candidats en vue de l'embauche ;
- Assurer la formation des collaborateurs ;
- Faire le suivi de la carrière des collaborateurs ;
- Recruter les futurs collaborateurs ;
- Créer en attribuant un code au nouveau salarié au sein de l'entreprise ;
- Créer le profil du nouveau collaborateur pour qu'il ait accès et travaille sur le Logiciel ;
- Assurer la rémunération des collaborateurs ;
- Faire connaitre le (la) nouvel(le) embauché(e) aux autres collaborateurs ;
- Formaliser la relation juridique liant le collaborateur à l'entreprise ;
- Assurer la gestion administrative des salariés ;
- S'assurer de la qualité du personnel sélectionné (Main d'œuvre Temporaire) ;
- Retrouver les véhicules en cas de vol ou de braquage ;
- Traçabilité des véhicules ;
- Assurer la sécurité du domicile des cadres de l'entreprise ;
- Assurer l'intégrité des biens de l'entreprise et des personnes qui y travaillent ;
- Assurer le dédouanement des marchandises de l'entreprise ;
- S'assurer du pointage des collaborateurs ;
- Surveillance du site ;
- Prévention contre tous les risques ;
- Surveiller le site pour prévenir tout acte de malveillances ;
- Faire un feed-back du travailleur pour une amélioration continue ;
- Revalorisation salariale du travailleur ;
- Connaitre la performance des travailleurs de l'usine (atteinte des objectifs) ;
- Protection des produits (la sécurité alimentaire) ;
- S'assurer que le personnel en contact avec les produits est en bonne santé ;
- Planifier, noter et suivre la qualité des travaux du personnel ;
- Connaitre les planteurs avec qui SACO travaille (jeunes, personnes âgées) ;
- S'assurer de disposer du cacao (matière première principale de SACO) de matière durable.
- Améliorer la situation de vie du planteur (éducation des enfants, santé) ;
- Orienter les services de SACO aux planteurs (formation, construction d'écoles, comment prêter et à qui prêter) ;
- Achat des fèves avec les commerciaux, coopératives, société, site d'achat ;
- S'assurer de travailler avec des gens ou des structures légales (en règle vis-à-vis du conseil du café-cacao) en conformité avec les procédures de gestion de risques de la SACO ;
- Collecte d'informations socio-économiques liées aux planteurs pour évaluer l'impact liés l'activité :
- Géolocalisation et cartographie des plantations ;
- Rendre compte aux clients, donateurs, et autres organismes partenaires sur la gestion des projets et des fonds octroyés ;
- Collecte des données pour avoir une évaluation sur l'impact des activités et sur les indicateurs (production et producteur) ;

- Superviser le projet d'archivage et archiver les documents papier provenant des services et directions de l'entreprise ;
- Echanger les données entre les entités du groupe.

Considérant qu'en l'espèce, la Société Africaine de Cacao (SACO) collecte les données à caractère personnel de ses employés, des planteurs participant à des programmes de formation pour des besoins de suivi, sur les bonnes pratiques agricoles et de techniques appropriées, en vue de leurs apporter une solution à leurs différents besoins.

Considérant que les traitements réalisés par la Société Africaine de Cacao (SACO) ont pour finalité de répondre aux partenaires commerciaux que sont les planteurs, d'obtenir une meilleure pratique Agricole et une saine gestion de leurs plantations en vue d'une amélioration de vie de ces derniers tout en ayant une bonne qualité de cacao de façon parraine.

Il convient d'estimer qu'il y a une finalité déterminée, explicite et légitime pour tous les traitements de la Société Africaine de Cacao (SACO).

6.3. Sur les délais de conservation

Considérant qu'aux termes de l'article 16, les alinéas 3 et 4 de la loi n°2013-450 du 19 Juin relative à la protection des données à caractère personnel qui dispose que :

Elles doivent être conservées pendant une période qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées ;

Au-delà de cette période requise, les données ne peuvent faire l'objet d'une conservation qu'en vue de répondre spécifiquement à un traitement à des fins historique, statistiques ou de recherches en vertu des dispositions légales.

Considérant qu'en l'espèce, la Société Africaine de Cacao (SACO), dans l'ensemble de ses directions, départements et services, conservent les données collectées jusqu'à fin de la campagne cacaoyère et au besoin quelques années après campagne pour des données statistiques soit pendant un délai allant jusqu'à dix (10) ans pour certains, trente (30) ans pour d'autres ou même voir illimité dans certains cas.

En somme le correspondant conclut qu'il existe un délai indiqué dans les cas d'espèce. Néanmoins la Société Africaine de Cacao (SACO) est tenue de rendre ce délai formel (en projet) et pour qu'il soit connu dans l'ensemble de ses directions, départements et services.

6.4. Sur la proportionnalité des données traitées

Considérant qu'aux termes de l'article 16 alinéa 2 de la loi n°2013-450 du 19 Juin relative à la protection des données à caractère personnel qui dispose que les données collectées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ;

Considérant qu'en l'espèce la Société Africaine de Cacao (SACO) traite les données telles que :

a. Les données d'identification : le nom, le prénom, la date et lieu de naissance, la photographie, sexe, la nationalité, numéro Carte Nationale d'Identité, photographie ;

b. Les données de vie personnelle : situation familiale ;

c. Les données de vie professionnelle : le CV, situation professionnelle, formation, scolarité, distinction, données de livraison de cacao, pratiques professionnelles, participation aux formations, date d'entrée, numéro matricule,

d. Les données de localisation : les coordonnées GPS des plantations et villages, les coordonnées GPS des véhicules, cartographie des plantations, adresse, numéro de téléphone, E-mails ;

e. Les données de connexions : Identifiant des terminaux ;

f. Données relatives à la santé : pathologie, infections, antécédents familiaux dans la médecine du travail ;

Pour ce qui est des données relatives aux soins, considérées par la loi comme des données sensibles au terme de l'article 21 de la loi N°2013-450 du 19 juin 2013, donc interdites de collecte. Mais dès lors que c'est dans le cadre de la médecine du travail, la loi permet la collecte des données dites sensibles de ses travailleurs, par dérogations au principe du consentement, par ce que soit au respect d'une obligation légale à laquelle le responsable du traitement est soumis, soit à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises, soit à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée. Tel est le cas de la Société Africaine de Cacao (SACO) dans l'exercice de ses activités. Donc ces données ne paraissent pas excessives.

Au regard de tout ce qui précède, le correspondant à la protection estime que les données collectées au sein de la Société Africaine de Cacao (SACO) sont adéquates, pertinentes et non excessives.

6.5. Sur la transparence des traitements

Considérant qu'aux termes des dispositions des Articles 18 et 28 de la loi n°2013-450 du 19 juin relative à la protection des données à caractère personnel qui dispose que le responsable du traitement est tenu de fournir à la personne dont les données font l'objet d'un traitement, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes :

- son identité et, le cas échéant, celle de son représentant dûment mandaté ;

- la ou les finalité(s) déterminée(s) du traitement auquel les données sont destinées ;

- les catégories de données concernées ;

- le ou les destinataire(s) auxquels les données sont susceptibles d'être communiquées ;

- la possibilité de refuser de figurer sur le fichier en cause ;

- l'existence d'un droit d'accès aux données concernant la personne et d'un droit de rectification de ces données ;

- la durée de conservation des données ;

- l'éventualité de tout transfert de données à destination de pays tiers tel Barry Callebaut Sourcing AG, la société mère en suisse.

En l'espèce, la Société Africaine de Cacao (SACO) apporte la preuve, qu'au moyens de ses formulaires de consentements et affichages que ces dispositions sont observées avant toute collecte.

En somme, le correspondant à la protection en déduit que les personnes concernées sont informées sur leurs données, sur les destinataires, ainsi que de leurs droits, avant tout traitement. Mais un effort reste à faire au niveau de l'information à apporter aux salariés (les différents contrats de travail).

6.6. Sur les mesures de sécurité

Selon les dispositions de l'article 41 de la loi n°2013-450 du 19 Juin relative à la protection des données à caractère personnel, le responsable de 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, déformes, endommagées ou que des tiers non autorisés puissent en prendre connaissance ;

Considérant que les mesures de sécurité doivent couvrir les données stockées sur des supports papiers et celles qui le sont sur supports informatiques ;

Qu'il en ressort des différents documents que la Société Africaine de Cacao (SACO) prend des mesures nécessaires en vue d'assurer la sécurité des données, telles que :

- L'existence de mot de passe robuste et de politique d'accès ;
- Les accès distants des appareils nomades sont sécurisés par un VPN ;
- Logiciel de sécurité Firewall ;
- La sauvegarde des données sur un cloud du groupe Barry Callebaut Sourcing AG, en suisse la Société mère ;
- Niveaux d'habilitation en fonction de la hiérarchie ;
- Mesure de blocage du poste de travail après 5 minutes d'inactivité.

En conclusion, le correspondant considère que quand bien même un effort est fait dans le sens de la protection logique, des insuffisances ont été relevées au niveau des mesures de sécurité physique. En effet, dans le cadre de la conservation des archives de la Société Africaine de Cacao (SACO), les documents sont stockés dans les bureaux. Aussi, il convient de noter qu'en cas d'un incendie les risques de pertes des données à caractère personnel de la Société Africaine de Cacao (SACO) seraient énormes et sans précaution particulière pour la protection de ces documents. Ces manquements pourraient porter atteintes à la vie privée des personnes.

6.6.1. Sur le système informatique

Voir le point 5.1.8 sur la sécurité.

6.6.2. Sur les destinataires des données traitées

Les destinataires des données sont identifiés et des clauses de confidentialité sont introduites dans les contrats

6.6.3. Sur l'exactitude des données

Les données sont mises à jour périodiquement par plus de la moitié (63%) des responsables des directions et services (voir annexe)

6.6.4. Les sous-traitants

Au terme des dispositions de l'article 40 de la loi n°2013-450 du 19 juin 2013, 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.

Lorsque le traitement est mis en œuvre pour le compte du responsable du traitement, celui-ci choisi un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect de ces mesures.

Considérant qu'en l'espèce, dans le cadre de ses activités, de la Société Africaine de Cacao (SACO) a recours à des sous-traitants dans les domaines suivants :

- Société de gardiennage (site, domicile cadre) ;
- Main d'œuvre temporaire ;
- Géolocalisation de la flotte automobile.

Considérant que ces sous-traitants ne disposent pas d'autorisation de l'ARTCI et qu'en sus les contrats de sous-traitance n'intègrent pas des clauses spécifiques aux données à caractère personnel,

En conclusion, le correspondant estime que ces insuffisances pourraient constituer un manquement au principe de garantie suffisante qui incombe au responsable de traitement la Société Africaine de Cacao (SACO).

6.7. Vidéosurveillance

Aux termes de l'article 1er, *paragraphe* 44 de la loi n°2013-450 du 19 Juin relative à la protection des données à caractère personnel dispose en matière de définition que toute activité faisant appel à des moyens techniques ou électroniques en vue de détecter, d'observer, de copier

ou d'enregistrer les mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile ;

Considérant qu'en l'espèce, les traitements réalisés par la Société Africaine de Cacao (SACO) ont pour finalité la sécurité des biens et du personnel. La surveillance des locaux, dans les différents parcs autos, et les différentes installations et que seule la direction de la sécurité en a accès.

Il convient d'estimer qu'il y a une finalité déterminée, explicite et légitime. Par contre, les constats suivants ont été relevés :

- la Société Africaine de Cacao (SACO) ne dispose pas d'une autorisation pour ce traitement auprès de l'ARTCI ;
- Il n'existe pas de consentement éclairé, déterminé et explicite de la part des salariés ;
- Aucune affiche, ni de pictogramme pour informer les visiteurs de l'existence d'un tel dispositif et vers qui exercer leurs droits n'est disponible près des caméras de vidéosurveillance.

6.8. Correspondant et chargé de la protection des données personnel

Un correspondant personne morale a été désigné, en l'occurrence AS CONSULTING et sa prise de fonction a été effective. *(Voir courrier de désignation en annexe).)*, Mais il n'est pas connu de tous les salariés et clients de la Société Africaine de Cacao (SACO). Le correspondant estime, à cet effet, que des sessions soient organisées afin de le faire connaitre des clients et autres partenaires de la Société Africaine de Cacao (SACO).

6.9. Sur les droits d'accès, de rectification, d'effacement et d'opposition

Considérant qu'aux termes des dispositions des articles 9 et 28 à 38 de la loi n°2013-450 du 19 Juin relative à la protection des données à caractère personnel qui implique l'exercice de certain droits reconnus aux personnes concernées, notamment les droits d'accès, de rectification, effacement, opposition de la part du responsable de traitement portant sur les données à caractère personnel ;

- la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès ;

Considérant que la société Africaine de Cacao (SACO) n'indique pas les coordonnées du correspondant auprès de qui ces droits pourraient être exercés aux personnes concernées ;

Qu'en l'espèce, avec la Société Africaine de Cacao (SACO), ces droits ne sont pas réellement exercés par les personnes concernées.

En somme, le correspondant à la protection en déduit que les personnes concernées ne sont pas informées sur l'existence du correspondant auprès de qui ils peuvent exercer leurs droits, avant tout traitement.

6.10. Connaissance en matière de protection de données à caractère personnel

De façon générale, seules les personnes ayant suivi la formation au sein de la Société Africaine de Cacao (SACO) ont connaissance de la protection des données à caractère personnel.

6.11. Procédures de la Société Africaine de Cacao (SACO)

Dans le cas d'espèce, il n'y a que quelques procédures internes au sein de la Société Africaine de Cacao (SACO) qui intègre les données à caractère personnel. Le correspondant estime qu'un effort doit être fait à ce niveau, afin d'intégrer à ces procédures les principes de base avant tout traitement de données à caractère personnel.

6.12. Formalités préalables aux traitements des données à caractère personnel

Aucune formalité n'a été effectuée à ce jour. Cet audit est justement le cadre mis en place pour pouvoir les remplir.

La société SACO a obtenu par décision n°2016-0187 en date du 07 octobre 2016, une autorisation de traiter des données à caractère personnel.

7. Recommandations

Points d'analyse	Non-conformités constatées	N° Reco	Recommandations	Traitements concernés	Entité responsable de la mise en œuvre de la recommandation
				Création et gestion des profils (mails)	Informatique
Droit des personnes	Les personnes concernées ne sont pas informées de leurs droits à l'oubli. Elles ne peuvent donc pas l'exercer	R1	Définir et formaliser la procédure du droit à l'oubli conformément à l'article 36-Loi N°2013-450 du 19 juin 2013, puis la faire connaitre aux personnes concernées.	Création profil du salarié sur SAGE RH SUITE	Paie et rémunération
				Mesures de performance	Qualité Assurance Afrique
				Achat cacao	Direction opération Cacao
				Achat Fèves	Direction Achat fèves
				Evaluation	Plant Manager Usine
				Rémunération	
				Reporting	Partenariat
				Sécurité (Domicile cadres)	Direction Achat industriel / sécurité
				Sécurité (Site)	
				Gestion des assurances et sinistres	Direction juridique
				Gestion des contentieux (sociaux)	
				Food defense (sécurité alimentaire)	Qualité Usine
				La traçabilité travaux usine	Usine : Up & Down Stream Team

Points d'analyse	Non-conformités constatées	N° Reco	Recommandations	Traitements concernés	Entité responsable de la mise en œuvre de la recommandation
				Géolocalisation des véhicules (sous-traitée)	Direction Achat industriel / sécurité
				Vidéosurveillance	sécurité et HSE
				Prévention	Infirmerie
				Sensibilisation	
	Les personnes concernées ne sont pas informées de leurs droits d'accès, de rectification et d'opposition et ne peuvent donc pas les exercer	R2	Définir et formaliser la procédure des droits d'accès, de rectification et d'opposition conformément aux articles 29 à 34-Loi N°2013-450 du 19 juin 2013, puis les faire connaitre aux personnes concernées.	Signature des ordres de paiement	Trésorerie
				Transit Guichet Unique du Commerce Extérieur (GUCE)	Import
				Visite médicale	Infirmerie
				Achat cacao	Direction opération Cacao
				Achat Fèves	Direction Achat fèves
				Evaluation	Plant Manager Usine
				Rémunération	
				Sécurité (Domicile cadres)	Direction Achat industriel / sécurité
				Sécurité (Site)	
				Food defense (sécurité alimentaire)	Qualité Usine
				La traçabilité travaux usine	Usine : Up & Down Stream Team

Points d'analyse	Non-conformités constatées	N° Reco	Recommandations	Traitements concernés	Entité responsable de la mise en œuvre de la recommandation
				Création et gestion des profils (mails)	Informatique
				Gestion administratives RH	Gestion administrative RH
				Gestion des carrières	Recrutement et gestion des carrières
	Les personnes concernées ne sont pas informées de leurs droits à la portabilité. Elles ne peuvent donc pas l'exercer	R3	Définir et formaliser la procédure du droit à la portabilité conformément à l'article 38-Loi N°2013-450 du 19 juin 2013, puis la faire connaitre aux personnes concernées.	Gestion paie rémunération	Paie et rémunération
				Evaluation	Plant Manager Usine
				Food defense (sécurité alimentaire)	Qualité Usine
				Formation (en interne-externe)	Recrutement et gestion des carrières
				Rémunération	Plant Manager Usine
				Reporting	Partenariat
	Il n'existe pas de correspondant à la protection des données au sein de la SACO.	R4	Nommer un correspondant à la protection des données , auprès duquel les personnes concernées pourront exercer leurs droits légaux	-	Direction générale SACO

Points d'analyse	Non-conformités constatées	N° Reco	Recommandations	Traitements concernés	Entité responsable de la mise en œuvre de la recommandation
				Géolocalisation des véhicules (sous-traitée)	Direction Achat industriel / sécurité
				Création et gestion des profils (mails)	Informatique
Durée de conservation	Les durées sont formalisées (politique d'archivage), mais ne sont pas connues de tout le personnel	R5	Diffuser la politique d'archivage à tout le personnel de la SACO	Création profil du salarié sur SAGE RH SUITE	Paie et rémunération
				Coordination Ressources humaines	Direction des ressources humaines
				Prévention	Infirmerie
				Sensibilisation	
				Visite médicale	
				Mesures de performance	Qualité Assurance Afrique
				Coordination du service durabilité	Direction opération Cacao
				Evaluation	Plant Manager Usine
				Formation (en interne-externe)	Recrutement et gestion des carrières
				Rémunération	Plant Manager Usine
				Reporting	Partenariat
				Sécurité (Domicile cadres)	Direction Achat industriel / sécurité
				Sécurité (Site)	
				Rémunération et paie	Paie et rémunération
				La traçabilité travaux usine	Usine : Up & Down Stream Team

Points d'analyse	Non-conformités constatées	N° Reco	Recommandations	Traitements concernés	Entité responsable de la mise en œuvre de la recommandation
				Attribution des matricules	Paie et rémunération
				Achat Fèves	Direction Achat fèves
				Afficher la note d'embauche	Gestion administrative RH
				Etablir le contrat de travail	
				Rédaction des contrats	Direction juridique
				Signature des ordres de paiement	Trésorerie
				(GUCE)	Import
				Gestion des assurances et sinistres	Direction juridique
				Gestion des contentieux (sociaux)	
				Coordination Ressources humaines	Direction des ressources humaines
				Gestion administratives RH	Gestion administrative RH
				Gestion des carrières	Recrutement et gestion des carrières
				Gestion paie rémunération	Paie et rémunération
				Recrutement	Recrutement et gestion des carrières

Points d'analyse	Non-conformités constatées	N° Reco	Recommandations	Traitements concernés	Entité responsable de la mise en œuvre de la recommandation
Légitimité	Pas de consentement explicite de la part de la personne concernée (visiteurs, salariés, prestataires, fournisseurs, etc.).	R6	Recueillir le consentement des personnes au travers d'un contrat ou une fiche de consentement sur le traitement de leurs données à caractère personnel conformément aux dispositions de l'article 14 de la loi n°2013-450 du 19 Juin 2013.	Achat Fèves	Direction Achat fèves
				Sécurité (Site)	Direction Achat industriel / sécurité
				Achat cacao	Direction opération Cacao
Proportionnalité	Méconnaissance des données archivées	R7	Vérifier les documents à archiver [pour distinguer les données sensibles (sécurité accrue), des autres données] -> Justifier de la collecte de chaque donnée.	Archivage papier	Archives
Sécurité (Organisationnelle)	Accès aux locaux sont autorisés à plusieurs personnes	R8	Tenir à jour une liste des personnes (visiteurs, employés, employés habilités, stagiaires, prestataires, etc.) autorisées à pénétrer dans les locaux abritant les archives.	Archivage papier	Archives

Points d'analyse	Non-conformités constatées	N° Reco	Recommandations	Traitements concernés	Entité responsable de la mise en œuvre de la recommandation
	Aucun dispositif anti-intrusion n'est installé dans les locaux abritant les archives	R9	Installer un dispositif permettant d'être alerté en cas d'effraction.	Archivage papier	Archives
	Conservation des CNI (du président et membres du conseil d'administration) et des fournisseurs dont les contrats sont arrivés à terme	R10	Détruire les documents papier (CNI et autre) contenant des données et qui ne sont plus utiles à l'aide d'un broyeur approprié.	Achat Fèves	Direction Achat fèves
	Distinguer les documents papier contenant des DCP des autres documents	R11	Porter une mention visible et explicite dans les applications métiers permettant d'accéder à des données et permettant de les imprimer.	Coordination Ressources humaines	Direction des ressources humaines
				Etablir le contrat de travail	Gestion administrative RH
				Gestion des contentieux (sociaux)	Direction juridique
				Recrutement	Recrutement et gestion des carrières
				Rémunération et paie	Paie et rémunération
	Distinguer les documents papier contenant des DCP des autres documents	R12	Porter une mention visible et explicite sur chaque page des documents contenant des données sensibles.	Visite médicale	Infirmerie
	Données médicales devenues obsolètes	R13	Détruire les documents papier contenant des données médicales et qui ne sont plus utiles à l'aide d'un broyeur approprié.	Visite médicale	

Points d'analyse	Non-conformités constatées	N° Reco	Recommandations	Traitements concernés	Entité responsable de la mise en œuvre de la recommandation
	Il n'existe pas de trace de transmission des CNI (du président et membres du conseil d'administration et des fournisseurs) d'un responsable à un autre	R14	Garder une trace précise de la transmission des documents papier contenant des données.	Achat Fèves	Direction Achat fèves
	Il n'existe pas de trace de transmission des CV d'un responsable à un autre	R15	Garder une trace précise de la transmission des CV (des documents papier) contenant des données.	Mise à disposition de la main d'œuvre temporaire	Achat : Procurement
	L'accès au bureau de l'infirmier n'est protégé que par une porte (fermée à clef)	R16	Installer un dispositif permettant d'être alerté en cas d'effraction.	Visite médicale	Infirmerie
	L'archivage des documents est en projet par le biais d'un cabinet (la personne en charge des archives joue le rôle de coordonnateur) _	R17	Finaliser au plus vite le projet d'archivage et désigner en interne un responsable des archives (qui aura pour mission d'organiser le service et de mettre en place une politique d'archivage)	Archivage papier	Archives
	L'archivage des documents est en projet par le biais d'un cabinet (la personne en charge des archives joue le rôle de coordonnateur)	R18	Vérifier que les processus de gestion des archives sont bien définis et que les rôles en matière d'archivage sont identifiés.	Archivage papier	

Points d'analyse	Non-conformités constatées	N° Reco	Recommandations	Traitements concernés	Entité responsable de la mise en œuvre de la recommandation
	Les archives ne sont pas numérisées	R19	Numériser les archives papier (pour réduire les risques de disparition de données)	Archivage papier	
	Les CNI (du président et membres du conseil d'administration) des fournisseurs sont rangés dans des chemises ou des cartons (dans le bureau)	R20	Stocker les documents papier contenant des données dans un meuble sécurisé.	Achat Fèves	Direction Achat fèves
	les CV des prestataires sélectionnés sont rangés dans des chemises ou des cartons (dans le bureau)			Mise à disposition de la main d'œuvre temporaire	Achat : Procurement
	les CV des prestataires sélectionnés (qui ne sont plus utiles) restent entreposés dans le bureau	R21	Détruire les CV (documents papier) contenant des données et qui ne sont plus utiles à l'aide d'un broyeur approprié.	Mise à disposition de la main d'œuvre temporaire	
	La biométrie est utilisée à l'entrée de SACO	R22	Le dispositif biométrique doit être supprimé car excessif compte tenu de la finalité de celui-ci	Donnée biométrique (Empreinte digitale)	Sécurité et HSE

Points d'analyse	Non-conformités constatées	N° Reco	Recommandations	Traitements concernés	Entité responsable de la mise en œuvre de la recommandation
	Nécessité de mesures complémentaires de lutte contre les incendies	R23	Mettre en place des moyens de prévention, détection et protection contre l'incendie.	Archivage papier	
	Plusieurs personnes disposent d'une clef donnant accès aux archives	R24	Conserver une trace des accès après en avoir informé les personnes concernées.	Archivage papier	
	Protection des données médicales	R25	Mettre en place une étude d'impact (PIA) pour les données médicales, afin de maîtriser les risques que les traitements du service infirmerie font peser sur les droits et libertés des personnes concernées.	Visite médicale	Infirmerie
Sécurité (Sous-traitance)	Insuffisance dans l'application des bonnes pratiques en cas de sous-traitance	R26	Appliquer à ses prestataires les mêmes mesures que pour les salariés de l'organisme : formation aux enjeux de la protection des DCP, obligation de respecter les règles d'usage des ressources informatiques de l'organisme annexées au règlement intérieur.	Mise à disposition de la main d'œuvre temporaire	Achat : procurement

Points d'analyse	Non-conformités constatées	N° Reco	Recommandations	Traitements concernés	Entité responsable de la mise en œuvre de la recommandation
	Insuffisance dans l'application des bonnes pratiques en cas de sous-traitance	R27	Fournir à ses prestataires un poste de travail interne à l'organisme ou s'assurer que l'utilisation du poste de travail fourni par leur employeur est compatible avec les objectifs de sécurité de l'organisme.	Mise à disposition de la main d'œuvre temporaire	
	Insuffisance dans l'application des bonnes pratiques en cas de sous-traitance	R28	S'assurer que ses prestataires sont bien engagés auprès de leur employeur par une clause de confidentialité applicable aux organismes clients de leur employeur.	Mise à disposition de la main d'œuvre temporaire	
	Manque d'informations sur les garanties du sous-traitant (Société de gardiennage) à protéger les DCP.	R29	Déterminer contractuellement la répartition des responsabilités vis à vis des processus légaux visant à permettre l'exercice des droits des personnes.	Sécurité (Domicile cadres)	Direction Achat industriel / sécurité
				Sécurité (Site)	

Points d'analyse	Non-conformités constatées	N° Reco	Recommandations	Traitements concernés	Entité responsable de la mise en œuvre de la recommandation
	Méconnaissance des garanties des mesures sécuritaires relatives aux traitements des données de géolocalisation effectués par le sous-traitant.	R30	Exiger du sous-traitant la transmission de sa Politique de Sécurité des Systèmes d'Information (PSSI) ainsi que de toutes les preuves de ses certifications en matière de sécurité de l'information et annexer ces documents au contrat. S'assurer que les mesures issues de sa PSSI sont conformes avec les recommandations de l'ARTCI en matière.	Géolocalisation des véhicules (sous-traitée)	Direction Achat industriel / sécurité
	Méconnaissance des garanties des mesures sécuritaires relatives aux traitements des données de géolocalisation effectués par le sous-traitant.	R31	Préciser dans le contrat que le respect des obligations de l'article 20 et 40 de la loi 2013-450 du 19 juin 2013 est une obligation essentielle du contrat.	Géolocalisation des véhicules (sous-traitée)	
	Méconnaissance des garanties des mesures sécuritaires relatives aux traitements des données de géolocalisation effectués par le sous-traitant.	R32	Encadrer la relation de sous-traitance via un contrat conclu intuitu personæ.	Géolocalisation des véhicules (sous-traitée)	

Points d'analyse	Non-conformités constatées	N° Reco	Recommandations	Traitements concernés	Entité responsable de la mise en œuvre de la recommandation
Sécurité informatique (portant sur les données du traitement)	Des mesures de chiffrement des données à caractère personnel ne sont pas implémentées	R33	Rendre les données à caractère personnel incompréhensibles à toute personne non autorisée à y avoir accès (chiffrement symétrique ou asymétrique, utilisation d'algorithmes publics réputés forts, certificat d'authentification, etc.).	Traitement générique (concerne tous les traitements)	Informatique
Transparence	Les salariés ne sont pas informés de leurs droits, des destinataires, du transfert concernant le traitement de leurs données personnelles. Les personnes ne sont pas également informées de la durée de conservation de leurs données personnelles.	R34	Informer les salariés par tous moyens appropriés (avenant ou annexe au contrat de travail, note de service, etc.) et en des termes clairs et facilement compréhensibles sur les informations obligatoires à connaitre, conformément aux articles 28 de la loi N°2013-450 du 19 Juin 2013	Géolocalisation des véhicules (sous-traitée)	Direction Achat industriel / sécurité
				Vidéosurveillance	sécurité et HSE
				Visite médicale	Infirmerie
				Achat cacao	Direction opération Cacao
				Sécurité (Site)	Direction Achat industriel / sécurité
				Food defense (sécurité alimentaire)	Qualité Usine
				Recrutement	Recrutement et gestion des carrières
				Achat Fèves	Direction Achat fèves
Formation	Le personnel de la SACO est insuffisamment formé sur les notions des DCP	R35	Former et sensibiliser le personnel de SACO sur les notions de protection des DCP via des sessions de formations ou le système « E-learning »	-	SACO

8. Conclusion

L'Audit de situation de la Société Africaine de Cacao (SACO) a révélé un niveau de conformité moyen (63%) avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.
Sur la base du résultat obtenu, l'Autorité de protection pourra autoriser les traitements de données à caractère personnel opérés par la Société Africaine de Cacao (SACO).

L'Autorité de protection lui délivrera un certificat de conformité, lorsque la Société Africaine de Cacao (SACO) aura effectivement mis en œuvre les actions correctives recommandées dans le présent rapport d'audit.

9. Annexes

A. Courrier de désignation d'AS CONSULTING comme correspondant personne morale de la SACO

SACO SOCIETE AFRICAINE DE CACAO
a Barry Callebaut company

COPIE

Abidjan, le 23 janvier 2018

N/REF.: **AG/LB/HKB/Sma/n°0032/2018**

Monsieur le Directeur Général
de l'ARTCI

ABIDJAN

Objet : Désignation d'un Correspondant
à la protection des données à caractère personnel

Monsieur le Directeur Général,

Conformément aux dispositions de la loi N°2013-450 du 19 juin relative à la protection des données à caractère personnel, SACO a l'obligation de désigner un correspondant agréé à la protection de ses données à caractères personnel.

A cet effet, par courrier référencé N°17-01435 DG/DPDP/DCPD/CC-124-79, en date du 08 avril 2017, deux propositions de correspondant-personnes morales agréés par l'ARTCI, nous ont été faites. Notamment AS CONSULTING et ICT Consulting.

Après analyse des offres techniques et financières desdits correspondants, nous venons par la présente, porter à votre connaissance la désignation de la société AS CONSULTING en qualité de correspondant à la protection de données à caractère personnel.

Pour formaliser les relations entre les deux parties, un contrat de prestation de service a été signé. Ce contrat conclu pour une durée d'un an, ne prendra effet qu'à compter de l'approbation de l'ARTCI.

Vous souhaitant bonne réception des présentes, et restant à votre disposition pour tout complément d'information ;

Nous vous prions de recevoir, Monsieur le Directeur Général, nos salutations distinguées.

Loïc BIARDEAU
Administrateur Général

B. Fiche de présence à la formation

SACO
SOCIETE AFRICAINE DE CACAO

FICHE DE PRESENCE FORMATION

FORMATION : INTERNE [X] EXTERNE [ ]

Intitulé de la formation : Le recrutement des femmes à [illegible]

Période de la formation : [illegible]

Horaire : [illegible] à

Date de la formation : 13/11/2013

Formateur : [illegible] ASSOU ALICI **Signature :**

Personnes ayant suivi la formation

Mlle	NOMS & Prénoms	Catégorie	Fonction	Service	Emargement
1332	BAKAU Loc	DG	DG	DG	
1382	DJI KELABONE FLORENT	Cadre	DAC	COM	
	Hongnica Rose Antoine		Secrétaire	COM	
2015	[illegible]		[illegible]	BP	
2013	[illegible]		[illegible]	PP	
1421	Koulibaly Ousmane		IT	IT	
2014	Kouamé [illegible]		IT	IT	
1936	ASSOUMOU Jean-Jacques		RRH	DRH	
1317	MICHAEL Appia Charlotte		[illegible]	CCH	
2013	[illegible]		[illegible]	[illegible]	
1935	EWAH FREDERIC	Cadre	AM Comm	DRH	
2013	[illegible]	Cadre	HC BP	DRH	
2013	[illegible]	Cadre	Resp GG	[illegible]	
	[illegible]	ADJOINT	[illegible]	[illegible]	
1936	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]		[illegible]	[illegible]	

VISA DRH

C. Evaluation des interviews effectuées

Questions	Nombre Responsables ayant répondu positivement	Total responsables interrogés	% de réponses positives
Activités de contrôle interne	2	24	**8%**
Connaissance des règles de base à appliquer en matière de protection des données personnelles	7	24	**29%**
Connaissance des responsabilités et des sanctions pénales, financières et administratives en cas de non-respect de la règlementation	6	24	**25%**
Existence d'un fichier listant les activités impliquant les traitements des données à caractère personnel	0	24	**0%**
Existence pour chaque activité d'un seul et unique responsable	23	24	**96%**
Identification des risques propres à chaque direction	3	24	**13%**
Sur l'actualisation des fichiers	15	24	**63%**
Sur l'existence d'un recensement des fichiers contenant des données à caractère personnel détenus par les directions	3	24	**13%**

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

CONSEIL DE REGULATION

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

DECISION N°2020-0538

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

EN DATE DU 03 MARS 2020

PORTANT AUTORISATION DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL PAR SK AUTOMATE SARL

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 le Règlement n° 15/2002/CM/UEMOA du 19 Septembre 2002 relatif aux systèmes de Paiement dans les états membres de l'Union Economique et Monétaire Ouest Africaine (UEMOA) ;

Vu l'Instruction n°127-07-08 du 9 juillet 2008 fixant les modalités de mise en œuvre de la surveillance par la BCEAO des systèmes de paiement dans les Etats membres de l'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°2016-992 du 14 novembre 2016 relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme ;

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 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 ;

Par les motifs suivants :

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par la société SK AUTOMATE, Société à Responsabilité Limitée, au capital de cinq millions (5 000 000) de francs CFA, sise à Abidjan, Plateau. Rue

Delafosse, BP 2220 Abidjan 10, immatriculée au Registre du Commerce et du Crédit mobilier sous le numéro CI-ABJ-2015-B-9493 ;

Considérant que la société SK AUTOMATE SARL est une société de paiement électronique ;

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 la société SK AUTOMATE 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 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 ses bornes de paiement électroniques, les données à caractère personnel des utilisateurs dont le numéro de téléphone ;

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 la société SK AUTOMATE SARL met à la disposition des utilisateurs, des bornes de paiement électronique ;

Qu'à l'occasion de l'utilisation de ces bornes, elle procède à la collecte et la conservation de données personnelles ;

L'Autorité de protection en conclut que la société SK AUTOMATE SARL 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 société SK AUTOMATE 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 déclare la demande de la société SK AUTOMATE SARL, 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 société SK AUTOMATE SARL n'indique pas comment elle procédera au recueil du consentement préalable ;

L'Autorité de protection prescrit à la société SK Automate Sarl de :

- mettre en place des conditions générales permettant d'éclairer le consentement de l'usager ;
- prévoir un mécanisme de recueil de consentement sur les bornes de paiement électronique.

- **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 en vue d'offrir aux utilisateurs des services de paiements électroniques ;

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 société SK AUTOMATE SARL déclare que les données sont conservées selon les exigences des fournisseurs mais ne précise pas les délais de conservation des données traitées ;

L'Autorité de Protection, au regard de la nature des données traitées et de la finalité du traitement, prescrit que :

- **Pour le paiement** : les données soient conservées pendant le délai de **trente (30) jours** à compter de la date de l'opération de paiement. A la fin de ce délai, les données doivent être supprimées ;

- **Pour les réclamations ou litiges** : les données doivent être conservées pendant toute la durée du traitement de la réclamation ou du litige. A la fin du litige ou de la réclamation, les données doivent être supprimées.

- **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, SK AUTOMATE SARL indique que le traitement concerne les données suivantes :

- **les données de connexion :** Identifiants des terminaux, identifiants des connexions ;
- **les données d'identification** : le numéro de téléphone mobile ;

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 ;

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

- aux émetteurs de monnaie électronique avec lesquels la demanderesse est en relation contractuelle dans le respect des termes de leur contrat ;
- à ses agents habilités ;
- 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 des administrations publiques habilitées, dans le cadre de leurs missions.

Considérant qu'en l'espèce, la demanderesse affirme que les données traitées ne seront pas transférer vers l'étranger ;

L'Autorité de protection prescrit que les données traitées ne fassent l'objet d'aucun transfert vers un 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.

Que la demanderesse n'indique pas le moyen par lequel les personnes concernées seront informées de leurs droits, préalablement à toute collecte ;

L'Autorité de protection prescrit à la société SK Automate SARL de remplir cette formalité par :

- la programmation sur la plateforme, d'un message d'information à l'attention de ses usagers, qui s'affichera avant l'utilisation de la plateforme;

- l'élaboration de conditions générales d'utilisation des bornes de paiement électroniques ;

- l'insertion de mentions légales relatives à la protection des données à caractère personnel sur son site internet ;

- le biais d'affiches dans les locaux où les données sont collectées.

- **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 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 la demanderesse 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.

- **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 vérification préalable de l'Autorité de protection, le niveau de sécurité du système d'information de SK AUTOMATE SARL, lui permet de mettre en œuvre des traitements pour les finalités déclarées ;

Qu'il en résulte que la demanderesse 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 :

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

- **les données de connexion :** Identifiants des terminaux, identifiants des connexions ;
- **les données d'identification** : le numéro de téléphone.

Les données visées au présent article concernent les usagers des plateformes de paiement électronique de la société SK AUTOMATE SARL.

Les données non mentionnées au présent article ne devront aucunement faire l'objet d'un quelconque traitement de la part de la société SK AUTOMATE SARL.

Article 2 :

Les données traitées par la société SK AUTOMATE 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 :

La société SK AUTOMATE SARL a l'obligation de procéder au recueil du consentement préalable des personnes concernées. Elle devra en fournir la preuve à l'Autorité de protection.

Article 4 :

La société SK AUTOMATE SARL est autorisée à communiquer les données traitées

- aux émetteurs de monnaie électronique avec lesquels la demanderesse est en relation contractuelle dans le respect des termes de leur contrat ;
- à ses agents habilités ;
- 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 des administrations publiques habilitées, dans le cadre de leurs missions.

Il est interdit à la société SK AUTOMATE SARL de transférer, **sans autorisation préalable de l'Autorité de protection**, les données collectées vers un pays tiers.

Article 5 :

La société SK AUTOMATE SARL conserve l'ensemble des données traitées :

- **Pour le paiement** : pendant le délai de **trente** (**30**) **jours** à compter de la date de l'opération de paiement. A la fin de ce délai, les données doivent être supprimées ;

- **Pour les réclamations ou litiges** : pendant toute la durée du traitement de la réclamation ou du litige. A la fin du litige ou de la réclamation, les données doivent être supprimées.

Article 6

La société SK AUTOMATE 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 par :

- la programmation sur sa plateforme, d'un message d'information à l'attention de ses usagers, qui s'affichera avant l'utilisation de la borne de paiement électronique;

- l'élaboration de conditions générales d'utilisation des bornes de paiement électroniques ;

- l'insertion de mentions légales relatives à la protection des données à caractère personnel sur son site internet ;

- le biais d'affiches dans les locaux où les données sont collectées.

Article 7

La société SK AUTOMATE 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.

La société SK AUTOMATE SARL est tenue de définir une procédure de gestion des droits des personnes concernées.

Article 8 :

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

La société SK AUTOMATE SARL est tenue 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, la société SK AUTOMATE 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.

La société SK AUTOMATE SARL 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 société SK AUTOMATE 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 11 :

La société SK AUTOMATE 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 12 :

La présente décision entre en vigueur à compter de la date de sa notification à la société SK AUTOMATE SARL.

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 03 Mars 2020
En deux (2) exemplaires originaux

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

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

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

CONSEIL DE REGULATION

DECISION N°2020-0565

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

EN DATE DU 13 MAI 2020

PORTANT AUTORISATION DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL PAR LE CABINET SOLUTION DE MARKETING ET SERVICES

(SMS CABINET DE FORMATION)

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

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 des 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 de Membres Du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) ;

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°2016-0202 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les conditions d'exercice de l'activité de formation en matière de Protection des données à caractère personnel ;

Vu la décision n°2016-0203 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les conditions d'exercice de l'activité d'audit de traitement 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 ;

Par les motifs suivants :

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par le Cabinet de formation Solutions de Marketing et Services en abrégé (SMS), Entreprise Individuelle, sise à Abidjan-Cocody 7ème Tranche, 28 BP 1070 Abidjan 28, immatriculée au Registre du Commerce et du Crédit Mobilier sous le numéro CI-ABJ-2013-A-6288/ N°CC.132690 G ;

Considérant que le Cabinet Solutions de Marketing et Services (SMS) est un Cabinet de Formation ;

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 le Cabinet de Formation SMS ;

- **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 bénéficiaires de ses formations, dont les numéros de téléphones de ceux-ci ;

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 Cabinet de Formation SMS propose à ses clients, des formations multi sectorielles ;

Que lesdites formations nécessitent la collecte des données à caractère personnel des clients ;

L'Autorité de protection en conclut que le Cabinet de Formation SMS 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 Cabinet de Formation SMS, la demande d'autorisation 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 du Cabinet de Formation SMS 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 le Cabinet de Formation SMS procède à la collecte des données auprès des bénéficiaires de ses prestations de service ;

Considérant que le Cabinet de Formation SMS indique qu'il procédera au recueil du consentement préalable, par des mentions sur les listes de présence ;

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, pour qu'elle comprenne d'une part, la portée et les conséquences de son consentement, et d'autre part, les avantages et les inconvénients du traitement ;

Considérant cependant que les mentions contenues sur les listes de présence permettent aux personnes concernées d'avoir toutes ces informations avant l'accès aux formations dudit Cabinet ;

L'Autorité de protection considère le traitement comme légitime, licite et loyal ;

- **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 dans le cadre de la gestion des attestations de présences des participants à ses formations ;

Considérant, par ailleurs, que le Cabinet de Formations SMS est agréé FDFP sous le numéro : FDFP-CG/N°153-2019/HAB/NKJ/ALBB/kt ;

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, le Cabinet de Formation SMS a indiqué qu'il conservera les données traitées pendant toute la durée de la formation et sur une période **d'un (01) mois** après la formation ;

L'Autorité de Protection, au regard de la nature des données traitées et de la finalité du traitement, considère que le délai sus-indiqué n'est pas excessif.

- **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 de Formation SMS indique que le traitement concerne les données suivantes :

- **les données d'identification :** Nom, prénom, numéro de téléphone ;
- **les données de connexion :** E-mail ;
- **les données de vie professionnelle** : Situation professionnelle ;

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 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 qu'en l'espèce, le demandeur a précisé qu'il communiquera les données collectées à ses agents habilités et à l'ARTCI ;

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

- au Procureur de la République de Côte d'Ivoire ;
- 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 habilités de l'administration publique de Côte d'Ivoire, dans le cadre de leurs missions ;

Considérant par ailleurs que le demandeur mentionne dans sa demande qu'il n'effectuera aucun transfert de données ;

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 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 des mentions légales sur les listes de présences aux formations permettront aux personnes concernées d'être informées de leurs droits, préalablement à toute collecte ;

Considérant que l'insertion de mentions légales sur les listes de présence satisfait le principe de transparence ;

L'Autorité de protection prescrit, également au demandeur de remplir cette formalité par le biais de mentions légales sur son site internet (en création), ce qui permettra aux personnes concernées d'être informées de leurs droits, préalablement à toute collecte ;

- **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 par ailleurs que la demanderesse n'a pas désigné de correspondant à la protection ;

L'Autorité de protection prescrit au Cabinet de formation SMS 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 ;

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 du Cabinet de Formation SMS 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.

Après en avoir délibéré,

DECIDE :

Article 1 :

Le Cabinet de Formations SMS est autorisé à effectuer la collecte et l'enregistrement des données à caractère personnel ci-après :

- **les données d'identification :** Nom, prénom, numéro de téléphone ;
- **les données de vie professionnelle** : Situation professionnelle ;
- **les données de connexion** : Adresse Email ;

Les données visées au présent article concernent les clients, participants aux formations du Cabinet de Formations SMS.

Les données non mentionnées ne devront aucunement faire l'objet d'un quelconque traitement de la part du Cabinet du Cabinet de Formations SMS.

Article 2 :

Les données traitées par le Cabinet de Formations SMS 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 de Formations SMS a l'obligation de procéder au recueil du consentement préalable des personnes concernées, par l'insertion de mentions obligatoires sur ses listes de présence.

Article 4 :

Le Cabinet de Formations SMS est autorisé à communiquer les données traitées :

- au Procureur de la République de Côte d'Ivoire ;
- 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 habilités de l'administration publique de Côte d'Ivoire dans le cadre de leurs missions.

Il est interdit au Cabinet de Formations SMS de transférer, sans autorisation préalable de l'Autorité de protection, les données collectées vers des pays tiers.

Article 5 :

Les données sont conservées pendant toute la durée de la formation dispensée par le Cabinet de Formations SMS.

Les données sont supprimées dans un délais d'un (01) mois après la formation.

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

Article 6 :
Le Cabinet de Formations SMS 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.

Il le fait par le biais de mention sur ses formulaires.

Le Cabinet de Formations SMS est tenu de définir une procédure de gestion des droits des personnes concernées.

Article 7 :

Le Cabinet de Formations SMS 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 de Formations SMS veille au respect des dispositions de la Loi relative à la protection des données à caractère personnel par ses sous-traitants.

Le Cabinet de Formations SMS 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 Cabinet de Formations SMS 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 de Formations SMS 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 de Formations SMS, 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 Cabinet de Formations SMS.

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 13 Mai 2020
En deux (2) exemplaires originaux

Le Président

Dr DIAKITE Coty Souleïmane
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° 2020-0581

DE l'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE CÔTE D'IVOIRE

EN DATE DU 30 JUILLET 2020

FIXANT LES CRITERES ET LES CONDITIONS D'EXERCICE DES ACTIVITES DE :

- CORRESPONDANT A LA PROTECTION DES DONNEES, PERSONNE MORALE
- AUDIT DE CONFORMITE
- FORMATION

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 des 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 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 ;

Par les motifs suivants,

Considérant que la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel confie les missions d'Autorité de protection des données à caractère personnel à l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI).

Qu'à ce titre, elle est chargée de déterminer les garanties indispensables et les mesures appropriées pour la protection des données à caractère personnel et de faire des propositions susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire concernant le traitement des données à caractère personnel.

Considérant que pour favoriser l'émergence de nouveaux métiers, l'Autorité de Protection a mis en place un processus de mise en conformité qui implique

l'intervention de divers acteurs dont le Correspondant à la protection, le formateur et l'auditeur en matière de protection de données à caractère personnel.

Considérant que les responsables du traitement ont besoin de références et de repères leur permettant de choisir des services de qualité respectueux de la vie privée et de la protection des données personnelles.

Considérant que les prestataires en matière de protection des données personnelles doivent être un vecteur de confiance, justifier de compétences, de savoir-faire et d'habilitation.

Qu'il est indispensable, en matière de protection des données à caractère personnel, de fixer les critères et les conditions d'exercice des activités de Correspondant à la protection des données, personne morale, de formateur, et d'auditeur.

Après en avoir délibéré,

DECIDE :

Article 1 :

Les activités de :

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

sont soumises aux exigences prévues par les référentiels annexés à la présente décision.

Article 2 :

La procédure d'agrément comprend trois étapes :

- une analyse de dossiers et de documents justificatifs ;
- un test écrit de type Questions à Choix Multiples;
- un test oral de mise en situation sur une thématique, devant un jury. Le test oral concerne les agréments de formateurs et d'auditeurs.

Les postulants aux agréments de formateurs ou d'auditeurs devront renseigner les formulaires de demande d'agrément joints à la présente décision.

Article 3 :

Le Jury qui procède à l'évaluation du candidat conformément à la procédure décrite ci-dessus est composé de **trois** (**03**) personnes-ressources habilitées de l'Autorité de Protection.

Article 4 :

Le Directeur Général de l'ARTCI est chargé de l'exécution de la présente décision qui sera publiée sur le site internet de l'ARTCI et au journal Officiel de la République de Côte d'Ivoire.

Fait à Abidjan, le 30 Juillet 2020
en deux (2) exemplaires originaux

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

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

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

CONSEIL DE REGULATION

ANNEXES A LA DECISION 2020-0581

DE l'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE CÔTE D'IVOIRE

EN DATE DU 30 JUILLET 2020

FIXANT LES CRITERES ET LES CONDITIONS D'EXERCICE DES ACTIVITES DE CORRESPONDANT A LA PROTECTION DES DONNEES, PERSONNE MORALE, AUDIT DE CONFORMITE, FORMATION

ANNEXE 1 : CONDITIONS GENERALES POUR L'EXERCICE DES ACTIVITES DE CORRESPONDANTS PERSONNES MORALES, AGREMENT FORMATEUR ET AGREMENT AUDITEUR

Catégorie 1. Conditions préalables à remplir par le candidat à la certification

Exigence 1.1. Pour accéder à la phase d'évaluation, le candidat doit remplir les conditions préalables suivantes :

- être une personne morale de droit ivoirien;
- produire les justificatifs de régularité fiscale et de déclaration auprès des institutions de prévoyance sociale ;
- le personnel de l'entreprise, candidate à la certification doit exercer au moins depuis deux (2) ans des activités dans le domaine de la protection des données personnelles et produire les justificatifs et autres éléments probatoires, ou avoir suivi une formation de 35 heures sur la protection des données ;
- produire une police d'assurance couvrant les risques professionnels liés à l'activité de protection des données à caractère personnel ;
- disposer de personnel ayant au minimum le profil du correspondant, personne physique.

Catégorie 2. Compétences et savoir-faire du personnel de l'entreprise candidate affectés aux missions

Exigence 2.1. Le personnel de l'entreprise candidate connaît et comprend les principes de licéité du traitement, de limitation des finalités, de minimisation des données, d'exactitude des données, de conservation limitée des données, d'intégrité, de confidentialité et de responsabilité.

Exigence 2.2. Le personnel de l'entreprise candidate sait identifier la base juridique d'un traitement.

Exigence 2.3. Le personnel de l'entreprise candidate sait déterminer les mesures appropriées et le contenu de l'information à fournir aux personnes concernées.

Exigence 2.4. Le personnel de l'entreprise candidate sait établir des procédures pour recevoir et gérer les demandes d'exercice des droits des personnes concernées.

Exigence 2.5. Le personnel de l'entreprise candidate connaît le cadre juridique relatif à la sous-traitance en matière de traitement de données personnelles.

Exigence 2.6. Le personnel de l'entreprise candidate sait identifier l'existence de transferts de données hors CEDEAO, et sait déterminer les instruments juridiques de transfert susceptibles d'être utilisés.

Exigence 2.7. Le personnel de l'entreprise candidate sait élaborer et mettre en œuvre une politique ou des règles internes en matière de protection des données.

Exigence 2.8. Le personnel de l'entreprise candidate sait organiser et participer à des audits en matière de protection des données.

Exigence 2.9. Le personnel de l'entreprise candidate connaît le contenu du registre d'activités de traitement, la documentation des violations de données ainsi que la documentation nécessaire pour prouver la conformité à la réglementation en matière de protection des données.

Exigence 2.10. Le personnel de l'entreprise candidate sait identifier des mesures de protection des données dès la conception, et par défaut, adaptées aux risques et à la nature des opérations de traitement.

Exigence 2.11. Le personnel de l'entreprise candidate sait participer à l'identification des mesures de sécurité adaptées aux risques et à la nature des opérations de traitement.

Exigence 2.12. Le personnel de l'entreprise candidate sait identifier les violations de données personnelles nécessitant une notification à l'Autorité de Protection.

Exigence 2.13. Le personnel de l'entreprise candidate sait déterminer s'il est nécessaire ou non d'effectuer une analyse d'impact relative à la protection des données (AIPD), et sait en vérifier l'exécution.

Exigence 2.14. Le personnel de l'entreprise candidate sait dispenser des conseils en matière d'analyse d'impact relative à la protection des données ; en particulier sur la méthodologie, l'éventuelle sous-traitance et les mesures techniques et organisationnelles à adopter.

Exigence 2.15. Le personnel de l'entreprise candidate sait gérer les relations avec les Autorités de Protection, en répondant à leurs sollicitations et en facilitant leur action, en particulier l'instruction des plaintes et de contrôles.

Exigence 2.16. Le personnel de l'entreprise candidate sait élaborer, mettre en œuvre et est en capacité de dispenser des programmes de formation et de sensibilisation du personnel et des instances dirigeantes en matière de protection des données personnelles

Exigence 2.17. Le personnel de l'entreprise candidate sait assurer la traçabilité de ses activités, notamment à l'aide d'outils de suivi ou de bilan annuel.

PPK

ANNEXE 2 : REFERENTIEL D'EVALUATION DE L'ACTIVITE DE FORMATION

Exigences relatives au respect de loi du 19 juin 2013 sur la protection des données à caractère personnel par l'organisme de formation

L'organisme de formation met en place une démarche visant à s'assurer de la conformité à la loi n° 2013-450 du 19 juin 2013 sur la protection des données à caractère personnel de l'ensemble des traitements qu'il met en œuvre pour l'ensemble de ses activités, dont la formation.

L'organisme de formation procède aux formalités préalables relatives aux traitements mis en œuvre au titre de la gestion de son personnel et de l'ensemble de ses activités, dont la formation. L'organisme de formation informe, dans le respect des dispositions de la loi n° 2013-450 du 19 juin 2013 sur la protection des données à caractère personnel, les personnes concernées par les traitements qu'il met en œuvre.

L'organisme de formation met en place une procédure destinée à gérer les demandes et les réclamations des personnes dont il traite les données.

Exigences relatives à l'identification des besoins de formation

L'organisme de formation dispose d'une procédure pour tenir compte des besoins des apprenants et de leur commanditaire lors de la conception du contenu de la formation et du processus de formation ; par exemple : formulaire de recueil de besoin, étude de marché, réunion préparatoire à l'organisation de la formation.

L'organisme de formation dispose d'une procédure pour s'assurer que les méthodes et supports de formation utilisés sont appropriés pour atteindre les objectifs énoncés ; par exemple : consultation de professionnels de la protection des données, enquête de satisfaction.

L'organisme de formation dispose d'une procédure pour que le contenu de la formation et le processus de formation tiennent compte des résultats de la formation ; par exemple : évaluation des apprenants, analyse des questionnaires de satisfaction.

Exigences relatives au processus de conception de la formation

L'organisme de formation a mis au point et documenté un plan d'étude et les moyens d'évaluation appropriés de la formation.

L'organisme de formation dispose de méthodes de formation qui répondent aux objectifs et aux exigences du plan d'étude et tiennent compte des besoins des apprenants.

L'organisme de formation dispose de procédures destinées à revoir et mettre à jour le contenu de la formation, tant en fonction des besoins et retours des apprenants et de leur commanditaire, que de l'actualité, de l'évolution de la législation, de la réglementation et du développement des techniques.

SMK

Exigences relatives à la compétence et à l'évaluation des formateurs

L'organisme de formation dispose d'un agrément formation délivré par le Fonds Développement de la Formation Professionnelle (FDFP).

L'organisme de formation s'assure que son personnel et ses formateurs possèdent les compétences requises pour identifier les besoins des apprenants, concevoir la formation et délivrer son contenu ; par exemple : en auditionnant le formateur, ou en assistant à une session de formation.

L'organisme de formation s'assure que les formateurs ont une expérience professionnelle avérée de deux (2) ans au minimum dans le secteur de la protection des données en conformité avec la certification de compétences exigée par l'ARTCI.

L'organisme de formation s'assure que les formateurs ont effectué cinq (5) formations au minimum dans les deux dernières années.

L'organisme de formation met en place des dispositifs d'évaluation des compétences de son personnel et des intervenants. Ce processus est documenté.

L'organisme de formation s'assure que les procédures d'évaluation choisies et mises en œuvre fournissent des informations fiables sur les compétences de son personnel et des intervenants.

Exigences relatives aux conditions de réalisation de la formation

L'organisme de formation informe l'apprenant et son commanditaire des objectifs de la formation, de son format, des instruments pédagogiques utilisés et, le cas échéant, des critères d'évaluation utilisés pour l'évaluation.

L'organisme de formation informe l'apprenant et son commanditaire des prérequis comme les qualifications et l'expérience professionnelle nécessaires à l'apprentissage.

L'organisme de formation s'assure que les ressources de la formation sont disponibles et accessibles aux apprenants.

2. Référentiel d'évaluation du contenu du module principal de l'activité de formation

Exigences relatives à la présentation des principes et des définitions

La formation permet de comprendre et de connaître les notions de traitement, de fichier, de données à caractère personnel, de responsable de traitement et de destinataire.

La formation permet de comprendre et de connaître le champ d'application matériel et géographique de la loi n° 2013-450 du 19 juin 2013 sur la protection des données à caractère personnel.

Exigences relatives à la présentation des conditions de la légitimité et licéité des traitements

La formation permet de comprendre et de connaitre le fondement juridique du traitement et d'en savoir déterminer la base légale applicable.

La formation permet de comprendre et de connaître le principe de finalité des traitements.

La formation permet de comprendre et connaître le principe de pertinence et d'adéquation des données à la finalité poursuivie.

La formation permet de comprendre et de connaître le principe de la conservation limitée des données.

La formation permet de comprendre et de connaître le principe relatif à la sécurité et confidentialité des données.

La formation permet de comprendre et de connaître la notion de consentement, sa nécessité dans le contexte de mise en œuvre d'un traitement et les exceptions à son recueil.

La formation permet de comprendre et de connaître les données dites sensibles.

Exigences relatives à la présentation des droits des personnes à l'égard des traitements de données à caractère personnel

La formation permet de comprendre et de connaître le droit à l'information des personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement. La formation permet de comprendre et de connaître le droit d'opposition des personnes, les modalités de son exercice et les obligations qui en résultent pour le responsable de traitement.

La formation permet de comprendre et de connaître le droit d'accès dont disposent les personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement. La formation permet de comprendre et de connaître le droit de rectification, de suppression et droit à l'oubli dont disposent les personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement.

3. Référentiel d'évaluation du contenu des modules complémentaires de la formation

Exigences relatives à la présentation de l'Autorité de protection et de ses missions

La formation permet de comprendre et de connaître le statut et la composition de l'Autorité de Protection.

La formation permet de comprendre et connaître les différentes missions de l'Autorité de protection.

Exigences relatives à la présentation du rôle du correspondant à la protection des données à caractère personnel

La formation permet de comprendre et de connaître le statut du correspondant à la protection donnée à caractère personnel.

La formation permet de comprendre et de connaître les modalités et la procédure de désignation et révocation d'un correspondant à la protection des données à caractère personnel.

La formation permet de comprendre et de connaître les missions d'un correspondant à la protection des données à caractère personnel.

Exigences relatives à la présentation des formalités préalables à la mise en œuvre des traitements

La formation permet de comprendre et de connaître les différents régimes de formalités préalables.

La formation permet de comprendre et de connaître, pour les différents régimes, les modalités selon lesquelles les formalités doivent être accomplies auprès de l'Autorité de Protection, et la manière dont elle les instruit.

Exigences relatives à la présentation de l'encadrement des transferts de données hors des pays de la CEDEAO

La formation permet de comprendre et de connaître les différents moyens destinés à encadrer les transferts de données.

La formation permet de comprendre et de connaître les formalités préalables applicables à un transfert de données hors de la CEDEAO.

La formation permet de comprendre et de connaître les obligations du responsable de traitement concernant l'information des personnes concernées par le transfert hors des Etats de la CEDEAO.

Exigences relatives à la présentation du pouvoir de contrôle de l'Autorité de Protection

La formation permet de comprendre et de connaître le pouvoir de contrôle de l'Autorité de Protection.

Exigences relatives à la présentation du pouvoir de sanction de l'Autorité de Protection

La formation permet de comprendre et de connaître les différentes mesures pouvant être prononcées par l'Autorité de Protection, avertissement, mise en demeure, décision d'interruption, de verrouillage, ou d'interdiction du traitement.

La formation permet de comprendre et de connaître les différentes procédures de sanction pouvant être mises en œuvre par l'Autorité de Protection.

La formation permet de comprendre et de connaître le formalisme associé à une procédure de sanction ainsi que les droits et les obligations du responsable de traitement mis en cause.

ANNEXE 3 : REFERENTIEL D'EVALUATION DE L'ACTIVITES D'AUDIT DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL

1.1 Exigences relatives aux principes à respecter

Le requérant a mis en place une démarche visant à s'assurer de la conformité à la loi N°2013-450 du 19 juin 2013 de l'ensemble des traitements qu'il met en œuvre pour l'ensemble de ses activités, dont l'audit.

La procédure d'audit comprend l'engagement que les auditeurs respectent les principes de déontologie professionnelle, de présentation impartiale des résultats, de conscience professionnelle et d'indépendance.

1.2 Exigences relatives à tous les auditeurs

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les auditeurs ont une expérience professionnelle de cinq (5) ans au minimum.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les auditeurs ont suivi une formation à la méthodologie d'audit (principes, procédures et techniques d'audit, documents relatifs à l'audit, lois, réglementations et autres exigences applicables pertinentes pour la discipline...) de vingt (20) heures par an, au minimum, pour chacune des cinq dernières années.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les auditeurs ont participé à vingt (20) audits au minimum, depuis leur déclenchement jusqu'à leur clôture, dans les cinq (5) dernières années. Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les auditeurs ont neuf cents (900) jours d'expérience d'audit au minimum.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les auditeurs continuent à se perfectionner professionnellement.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les auditeurs sont évalués selon des critères et des méthodes définies dans le cadre de chaque audit et que les auditeurs qui ne satisfont pas à ces critères complètent leur formation ou leur expérience.

Les règles en vigueur au sein du cabinet d'audit permettent de déterminer la loi nationale de protection des données applicable à chaque traitement se trouvant dans le champ de l'audit.

1.3 Exigences relatives aux responsables d'équipe d'audit

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les responsables d'équipe d'audit ont participé à quatre (4) audits au minimum, depuis leur déclenchement jusqu'à leur clôture, dans les deux (2) dernières années.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les responsables d'équipe d'audit ont cent quatre-vingts (180) jours d'expérience d'audit au minimum en tant que responsable d'équipe d'audit au cours des deux (2) dernières années.

1.4 Exigences relatives aux auditeurs « juridiques »

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les auditeurs « juridiques » ont obtenu au minimum, un diplôme de maîtrise en droit des affaires ou équivalent dans le secteur du droit.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les auditeurs « juridiques » ont une expérience de deux (2) ans au minimum dans le domaine de la protection des données à caractère personnel ; exemple : conseil, contentieux, accomplissement de formalités préalables.

1.5 Exigences relatives aux auditeurs « techniques »

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les auditeurs « techniques » ont obtenu au minimum, un diplôme de niveau Bac+4 ou équivalent dans le domaine de l'informatique ou des systèmes d'information ou dans des domaines connexes.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les auditeurs « techniques » ont suivi une formation de trente (30) jours, en une ou plusieurs fois, au minimum, au cours des deux (2) dernières années sur les référentiels utiles au management de la sécurité des systèmes d'information : réglementation, normes, méthodes, bonnes pratiques, gestion des risques.

Les règles en vigueur au sein du cabinet d'audit permettent de s'assurer que les auditeurs « techniques » ont suivi une formation dans le domaine de la protection des données à caractère personnel.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les auditeurs « techniques » ont suivi une formation de trente (30) jours, en une ou plusieurs fois, au minimum, au cours des deux (2) dernières années, sur l'audit de sécurité technique : intrusion, investigation, détection de vulnérabilités techniques.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les auditeurs « techniques » ont une expérience de deux (2) ans au minimum dans le domaine de la sécurité des systèmes d'information.

1.6 Exigences relatives à la préparation des audits

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les responsabilités de chacun, les objectifs, le champ, les critères et le déroulement de l'audit sont définis avec le commanditaire en tenant compte des éventuels audits préalablement réalisés.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que la faisabilité de l'audit est étudiée et que les actions nécessaires sont prises en fonction de cette étude.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que l'équipe d'audit est constituée en fonction des compétences « juridiques » et « techniques » nécessaires pour atteindre les objectifs de l'audit et dans le respect des principes relatifs aux auditeurs.

La procédure d'audit prévoit l'insertion d'une clause particulière dans le contrat établi entre le prestataire et le commanditaire de l'audit, afin de garantir la confidentialité des données à caractère personnel qui pourraient, le cas échéant, être portées à la connaissance du prestataire dans le cadre de l'audit.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que la documentation examinée par l'auditeur est consultée dans les locaux de l'audité ou est anonymisée si elle est consultée hors des locaux de l'audité. Ce principe est inscrit dans la clause de confidentialité établie entre le prestataire et le commanditaire de l'audit.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que la documentation examinée par l'auditeur est adéquate pour réaliser l'audit et que le commanditaire de l'audit en est informé si ce n'est pas le cas. Pour qu'elle soit adéquate, elle comprend notamment les critères et les conclusions des éventuels audits préalablement réalisés, ainsi que les politiques internes relatives à la protection des données à caractère personnel, dans le champ de l'audit.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les instruments de recueil d'informations qui seront employés par l'équipe d'audit (questionnaires, guides d'entretien, logiciel d'analyse...) sont pertinents au regard des vérifications prévues et qu'ils sont éprouvés (des tests préliminaires ont été réalisés, des utilisations antérieures ont démontré leur justesse...).

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que les échantillonnages réalisés sont suffisamment représentatifs : personnes interrogées, vérifications effectuées, données contrôlées.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que le plan d'audit, la manière dont les actions d'audit seront menées et les circuits de communication sont validés avec les responsables des activités du champ de l'audit et leurs questions traitées.

Les règles en vigueur au sein du cabinet d'audit permettent d'assurer que le responsable de l'équipe d'audit élabore un plan d'audit validé par le commanditaire de l'audit. Ce plan d'audit contient notamment les objectifs de l'audit, les critères d'audit, les documents de référence, le champ d'audit, les dates, lieux, horaires et durée d'audit sur site, les rôles et responsabilités ainsi que la mise à disposition des ressources appropriées et, éventuellement, les objections de l'audité. Les critères d'audit tiennent compte des audits préalablement réalisés et des politiques internes relatives à la protection des données à caractère personnel.

1.7 Exigences relatives à la réalisation des audits

La procédure d'audit permet d'assurer que l'accès et l'utilisation de données à caractère personnel nécessitant une habilitation particulière sont réservés aux personnes dûment habilitées à le faire, et ce dans le respect de la loi et de la réglementation. Ce principe est inscrit dans le contrat établi entre le prestataire et le commanditaire de l'audit.

La procédure d'audit permet de vérifier que seules les personnes disposant d'une habilitation particulière ont effectivement accès aux données et peuvent les utiliser.

La procédure d'audit permet d'assurer que l'audité, et, si nécessaire, le commanditaire de l'audit, est informé de l'avancement et de toute difficulté rencontrée, de manière régulière.

La procédure d'audit permet d'assurer que les preuves d'audit sont constituées à partir d'une vérification « juridique » et « technique » des informations recueillies et consignées.

La procédure d'audit permet d'assurer que les données à caractère personnel collectées en tant que preuve sont soit anonymisées, soit uniquement consultables au sein des locaux de l'audité, tout en étant conservées de manière à assurer leur confidentialité.

Ce principe est inscrit dans la clause de confidentialité établie entre le prestataire et le commanditaire de l'audit. La procédure d'audit permet d'assurer que les constats d'audit sont élaborés en évaluant la conformité des preuves d'audit par rapport aux critères d'audit. La procédure d'audit permet d'assurer que l'équipe d'audit prépare les conclusions d'audit sur la base des constats d'audit. La procédure d'audit permet d'assurer que les preuves, les constats et les conclusions d'audit sont présentés à l'audité afin de vérifier sa compréhension et de faire reconnaître les preuves comme exactes et que toute divergence d'opinion subsistant à l'issue de la discussion est consignée.

1.8 Exigences relatives à la finalisation des audits

La procédure d'audit permet d'assurer que le rapport d'audit fournit un enregistrement complet, concis, précis et clair de l'audit. Le contenu minimal d'audit se présente comme suit : date du rapport d'audit, objectifs de l'audit, champ d'audit, commanditaire de l'audit, équipe d'audit, dates et lieux des

activités d'audit sur site, critères d'audit, constats d'audit et conclusions d'audit. Il est émis dans les délais convenus, à moins qu'une nouvelle date d'émission ne soit fixée, et approuvée selon la procédure retenue. Il est diffusé aux destinataires identifiés par le commanditaire de l'audit.

La procédure d'audit permet d'assurer que les documents relatifs à l'audit sont conservés de manière à préserver leur confidentialité ou détruits de manière définitive et sécurisée, s'ils ne sont plus utiles à l'issue de l'audit : documentation fournie, plan d'audit, preuves d'audit, rapport d'audit.

1.9 Exigences relatives aux bases de connaissances utilisées

La procédure d'audit s'appuie sur une base de connaissances en conformité avec la législation de Côte d'Ivoire.

La procédure d'audit s'appuie sur une base de connaissances reflétant l'état de l'art en matière de sécurité des systèmes d'information et dispose d'une méthode permettant de la mettre à jour régulièrement.

1.10 Exigences relatives à l'organisme audité

Le cabinet d'audit dispose d'une méthode permettant d'identifier la structure organisationnelle de l'organisme audité, les systèmes d'information, les flux d'information concernés et les normes juridiques spécifiques dans le champ de l'audit.

Les règles en vigueur au sein du cabinet d'audit permettent d'apprécier l'existence et l'efficacité de l'organisation et de la documentation pour gérer les traitements de données à caractère personnel dans le champ de l'audit.

La procédure d'audit permet d'apprécier, dans le cas où l'audité dispose d'un correspondant à la protection des données à caractère personnel, les moyens qui lui sont accordés pour réaliser sa mission et le bilan de celle-ci.

1.11 Exigences relatives à l'identification des traitements

La procédure d'audit décrit un processus méthodologique d'énumération de tous les traitements identifiés à l'intérieur du champ de l'audit.

La procédure d'audit contient un processus de détection des traitements éventuellement non identifiés par le responsable de traitement au sein du champ de l'audit.

La procédure d'audit permet le recours éventuel à des prestataires extérieurs.

La procédure d'audit permet d'identifier et de catégoriser l'ensemble des données à caractère personnel utilisées dans les traitements inclus dans le champ de l'audit.

La procédure d'audit permet de caractériser la responsabilité de l'organisme audité au regard des traitements au sein du champ de l'audit, en déterminant notamment si l'organisme est responsable de traitement ou sous-traitant au sens de la Loi n°2013-450 du 19 juin 2013.

La procédure d'audit contient une approche méthodologique pour réaliser un bilan des formalités préalables ou des éléments portés dans le registre du correspondant à la protection des données à caractère personnel le cas échéant permettant de vérifier leur exhaustivité et leur exactitude.

1.12 Exigences relatives à l'appréciation de la licéité des traitements

La procédure d'audit permet d'obtenir une description exacte des finalités des traitements inclus dans le champ de l'audit.

La procédure d'audit permet d'apprécier le fondement légal de chaque traitement inclus dans le champ de l'audit.

La procédure d'audit comprend une démarche particulière pour déterminer si les données à caractère personnel des traitements inclus dans le champ de l'audit sont pertinentes, adéquates et non excessives au regard des finalités identifiées.

La procédure d'audit permet d'évaluer si les données à caractère personnel utilisées sont toutes nécessaires au regard de la finalité recherchée et si certaines d'entre elles pourraient être partiellement ou totalement anonymisées tout en permettant d'atteindre la finalité désirée.

La procédure d'audit permet d'évaluer la qualité de la méthode de recueil des données à caractère personnel auprès de personnes concernées, notamment pour apprécier son caractère loyal et licite.

La procédure d'audit permet de s'assurer que les traitements confiés à des prestataires font l'objet d'un contrat de prestation de service.

La procédure d'audit permet de s'assurer que les contrats de prestation de services contiennent des dispositions relatives aux mesures de sécurité et des instructions claires données par le responsable de traitement à son prestataire.

La procédure d'audit dispose d'une méthode d'identification des flux de données hors des Etats membres de la CEDEAO.

La procédure d'audit permet de vérifier l'existence et la conformité des instruments juridiques permettant d'encadrer les transferts hors des Etats membres de la CEDEAO.

1.13 Exigences relatives à l'étude des personnes accédant aux données

La procédure d'audit dispose d'une méthode permettant de recenser et de catégoriser l'ensemble des personnes qui, en raison de leurs fonctions, sont chargées de traiter les données à caractère personnel qui sont incluses dans le champ de l'audit.

La procédure d'audit permet d'évaluer la politique d'habilitation appliquée à chaque personne ayant un accès légitime aux données identifiées, au regard du principe de limitation des accès au besoin d'en connaître.

1.14 Exigences relatives à l'analyse des durées de conservation

La procédure d'audit comprend une démarche particulière pour recenser les durées de conservation des données à caractère personnel utilisées.

La procédure d'audit comprend une démarche particulière pour déterminer si les durées de conservation sont adéquates.

La procédure d'audit prévoit des contrôles pertinents sur les systèmes d'information par des auditeurs « techniques » afin de vérifier si les durées de conservation appliquées sont conformes aux durées prévues.

La procédure d'audit prévoit des contrôles afin de vérifier que les données font l'objet d'une suppression effective à l'expiration de leur durée de conservation.

La procédure d'audit examine également la politique d'archivage des données à caractère personnel, le cas échéant, au regard des recommandations de l'ARTCI en la matière.

1.15 Exigences relatives à l'étude de la sécurité

La procédure d'audit permet d'analyser et d'évaluer la démarche mise en œuvre par les responsables de traitement pour assurer la confidentialité, l'intégrité et la disponibilité des données à caractère personnel entrant dans le champ de l'audit.

La procédure d'audit comprend une démarche particulière pour identifier les principaux risques que les traitements dans le champ de l'audit font peser sur les libertés et la vie privée des personnes concernées en cas d'atteinte à la sécurité des données à caractère personnel, en tenant compte des éventuels sous-traitants. Cette démarche permet notamment d'estimer ces risques en termes de gravité et de vraisemblance.

La procédure d'audit comprend une démarche particulière pour identifier les mesures de sécurité mises en œuvre et pour évaluer leur pertinence vis-à-vis des risques identifiés et estimés, notamment pour gérer les incidents de sécurité liés aux données à caractère personnel.

La procédure d'audit permet de déterminer si les mesures de sécurité identifiées sont correctement mises en œuvre et s'appuie sur des vérifications adéquates effectuées sur les systèmes d'information, réalisées par des auditeurs « techniques ».

1.16 Exigences relatives à l'étude du respect du droit des personnes

La procédure d'audit permet de vérifier que les personnes concernées disposent d'un droit d'accès, de rectification et le cas échéant d'un droit d'opposition.

La procédure d'audit permet de contrôler que les droits des personnes peuvent être exercés de manière effective, et dans des délais raisonnables.

La procédure d'audit permet de vérifier que les personnes disposent d'une information correcte, accessible et claire sur leurs droits.

1.17 Exigences relatives à l'étude des traitements particuliers

La procédure d'audit permet de déterminer le régime juridique dont relèvent les traitements au sein du champ de l'audit et d'étudier la conformité aux dispositions particulières afférentes en matière de protection des données à caractère personnel, notamment, l'utilisation de traitements soumis à autorisation préalable de l'Autorité de protection des données à caractère personnel.

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

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

CONSEIL DE REGULATION

DECISION N°2020-0609

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 16 NOVEMBRE 2020

PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL PAR LA FONDATION ICI

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

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°2010-272 du 30 septembre 2010 portant interdiction de la traite et des pires formes de travail des enfants

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 des 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 de 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 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 le rapport d'audit de protection des données personnelles de la FONDATION ICI.

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 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, défini les étapes du processus de mise en conformité ;

Considérant que la FONDATION ICI, a saisi l'Autorité de protection d'une demande de mise en conformité ;

Considérant que l'Autorité de protection a effectué l'audit de situation de la FONDATION ICI, qui a fait ressortir un niveau de conformité moyen avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Considérant, toutefois les prescriptions faites par l'Autorité de protection dans le rapport définitif d'audit en matière de protection des données personnelles et sous réserve de l'application de ces prescriptions ;

Considérant que la FONDATION ICI s'engage à mettre en œuvre les prescriptions formulées dans le rapport définitif d'audit en matière de protection des données personnelles, en vue d'apporter des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements qu'elle effectue ;

Que la Fondation ICI s'engage à veiller au respect de ces mesures ;

Après en avoir délibéré,

DECIDE :

Article 1 :

La FONDATION ICI 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 la FONDATION ICI.

Article 2 :

La FONDATION ICI est autorisée à effectuer les traitements énumérés dans l'annexe 2 de la présente décision.

Article 3 :

La FONDATION ICI 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, les officiers de police judiciaire munis d'une réquisition;
- les bailleurs de fonds, les partenaires techniques et financiers
- les coopératives ;
- les bénéficiaires des programmes ;
- le siège de la Fondation ICI à Genève ;
- la Banque ;
- le comité national de surveillance des actions de lutte contre la traite l'exploitation et le travail des enfants (CNS);
- les auditeurs externes ;
- les soumissionnaires d'appels d'offres retenus.

Article 4 :

La FONDATION ICI est autorisée à communiquer au siège en Suisse, les données énumérées dans l'annexe 3.

Avant tout transfert desdites données, la Fondation ICI est tenue 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, la FONDATION ICI 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 FONDATION ICI ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

Article 6 :

Les traitements de données autorisés dans la présente décision ont pour finalités :

- la gestion des programmes et projets de la Fondation;
- la gestion du suivi et évaluation ;
- la gestion des ressources humaines de la Fondation ;
- la gestion administrative et financière de la Fondation ;

- la gestion informatique ;
- la gestion de la communication de la Fondation;
- la communication de données au siège à Genève ;
- L'hébergement de données en France.

Les traitements afférents aux finalités ci-dessus sont listés dans l'annexe 4 de la présente décision.

Article 7 :

L'Autorité de protection notifie à la FONDATION ICI son rapport d'audit de protection des données personnelles.

La FONDATION ICI 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 la FONDATION ICI, 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 FONDATION ICI 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 FONDATION ICI 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 FONDATION ICI, 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 FONDATION ICI 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 FONDATION ICI.

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 16 Novembre 2020
en deux (2) exemplaires originaux

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL

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

DECISION N°2020-0610

DE L'AUTORITE DE PROTECTION

DE LA REPUBLIQUE DE COTE D'IVOIRE

EN DATE DU 16 NOVEMBRE 2020

PORTANT AUTORISATION DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL PAR WORLD COCOA FOUNDATION (WCF)

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/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°2013-333 du 22 mai 2013 portant nomination des Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire tel que modifié par les décrets n°2015-173 du 19 mars 2015 portant nomination d'un Membre du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire et 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°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°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 de 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°2017-0353 du 26 octobre 2017 portant vérification préalable ;

Vu la décision n°2017-0354 du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Vu le rapport d'audit de protection des données personnelles de la World Cocoa Foundation (WCF).

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 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, défini les étapes du processus de mise en conformité ;

Considérant que la World Cocoa Foundation, a saisi l'Autorité de protection d'une demande de mise en conformité ;

Considérant que l'Autorité de protection a effectué l'audit de situation de la World Cocoa Foundation, qui a fait ressortir un niveau de conformité avec la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, insuffisant;

Considérant toutefois les recommandations et prescriptions faites par l'Autorité de protection dans le rapport définitif d'audit de situation et sous réserve de l'application de ces recommandations et prescriptions ;

Considérant que la World Cocoa Foundation s'engage à mettre en œuvre les recommandations et prescriptions formulées dans le rapport définitif d'audit de situation, en vue d'apporter des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements qu'elle effectue ;

Que la World Cocoa Foundation s'engage à veiller au respect de ces mesures ;

Après en avoir délibéré,

DECIDE :

Article 1 :

La World Cocoa Foundation 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 la World Cocoa Foundation.

Article 2 :

La World Cocoa Foundation est autorisée à effectuer les traitements énumérés dans l'annexe 2 de la présente décision.

Article 3 :

La World Cocoa Foundation 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 ;
- les officiers de police judiciaire munis d'une réquisition;
- les clients de la World Cocoa Foundation, dans le respect des clauses contractuelles qui les lient.

Article 4 :

La World Cocoa Foundation est autorisée à communiquer au siège aux Etats Unis, à la succursale au Ghana et à l'hébergeur en Allemagne, les données énumérées dans l'annexe 3.

Avant tout transfert desdites données, la Fondation ICI est tenue 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, la World Cocoa Foundation 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 World Cocoa Foundation ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

Article 6 :

Les traitements de données autorisés dans la présente décision ont pour finalités :

- La gestion des ressources humaines ;
- La gestion du Programme relatif à la sécurité alimentaire et au genre ;
- La gestion des opérations et des Finances ;
- La gestion du Programme relatif à l'amélioration de la production cacaoyère ;
- L'installation de système de géolocalisation ;
- Les transferts de données aux USA, Allemagne et au Ghana.

Les traitements afférents aux finalités ci-dessus sont listés dans l'annexe 4 de la présente décision.

Article 7 :

L'Autorité de protection notifie à la World Cocoa Foundation son rapport d'audit de protection des données personnelles.

La World Cocoa Foundation 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 la World Cocoa Foundation, 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 World Cocoa Foundation 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 World Cocoa Foundation 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 World Cocoa Foundation, 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 World Cocoa Foundation 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 :

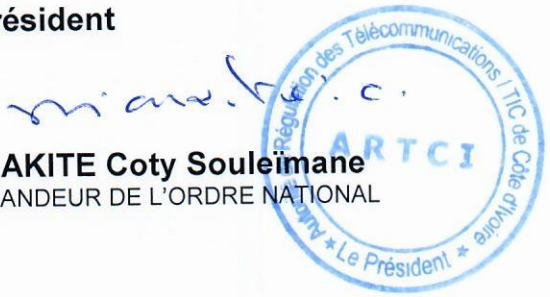
La présente décision entre en vigueur à compter de la date de sa notification à la World Cocoa Foundation.

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 16 Novembre 2020
en deux (2) exemplaires originaux

Le Président



Dr DIAKITE Coty Souleïmane
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°2020-0529

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

EN DATE DU 28 JANVIER 2020

PORTANT AUTORISATION DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL PAR LE CABINET BAH BLESSON & COMPANY

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/TIC ;

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°2014-106 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°2014-105 du 12 mars 2014 portant définition des conditions de fourniture des prestations de cryptologie ;

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° 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 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°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°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 le procès-verbal de vérification préalable en matière de protection de données à caractère personnel n°006/08/2018 ;

Par les motifs suivants :

Considérant la demande d'autorisation de traitement de données à caractère personnel introduite par le Cabinet Bah Blesson & Company, Société à Responsabilité Limitée, au capital de cinq millions (5 000 000) de francs CFA, sis à Abidjan, Plateau à la rue du Dr Crozet, 18 BP 2884 Abidjan 18, immatriculé au Registre du Commerce et du Crédit Mobilier sous le numéro CI-2016-B-27079, CC : N°1652341 ;

Considérant que Bah Blesson & Company est un Cabinet Conseil en Management ;

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 le Cabinet Bah Blesson & Company :

- **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 usagers de sa plateforme « Businessinfo.ci », 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 Cabinet Bah Blesson & Company propose aux usagers, une plateforme web mettant à disposition des informations financières fiables et légales sur toutes les entreprises en Côte d'Ivoire, dénommée « Business Info » ;

Que ladite plateforme est susceptible de collecter les données à caractère personnel des usagers ;

L'Autorité de protection en conclut que le Cabinet Bah Blesson & Company 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 Cabinet Bah Blesson & Company, la demande d'autorisation 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 du Cabinet Bah Blesson & Company, 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 le Cabinet Bah Blesson & Company procède à la collecte des données auprès des usagers de sa plateforme dénommée « Businessinfo.ci » ;

Considérant que le Cabinet Bah Blesson & Company indique qu'il procédera au recueil du consentement préalable, par des mentions dans les conditions générales d'utilisation de la plateforme « Business Info » ;

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 cependant que les mentions contenues dans les conditions générales d'utilisation ne permettent pas d'avoir toutes ces informations avant l'accès aux différents services ;

En outre, l'Autorité de protection prescrit que l'accès aux différents services de la plateforme « Business Info » soit subordonné à la présence de cases à cocher pour le 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 qu'en l'espèce, le demandeur procède au traitement de données à caractère personnel dans le cadre de la création et de la gestion des comptes utilisateurs des usagers et clients de la plateforme « Business Info » ;

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, le Cabinet Bah Blesson & Company a indiqué qu'il conservera les données traitées pendant toute la durée de souscription et sur une période de cinq (05) années ;

Considérant que le délai de conservation varie selon les différents services proposés, l'Autorité de protection prescrit que :

- les données soient conservées pendant toute la durée de l'utilisation de la plateforme « Business Info » ;
- Les données soient supprimées dans un délai de (5) cinq ans, en cas de dé-souscription ;
- les données soient supprimées dans un délai de douze (12) mois, en cas de désinstallation de la plateforme « Business Info » ;
- les données soient conservées jusqu'à la fin de la procédure judiciaire, lorsque la décision de justice rendue est devenue définitive, en cas de litige ;

- **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 Bah Blesson & Company indique que le traitement concerne les données suivantes :

- **les données d'identification :** Nom, prénom, adresse, numéro de téléphone ;
- **les données de connexion :** E-mail, nom d'utilisateur, mot de passe ;
- **les données bancaires :** numéro de carte bancaire ; zip code ;

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 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 qu'en l'espèce, le demandeur ne précise pas dans sa demande d'autorisation les destinataires desdites données ;

Considérant que pour le paiement de son service, le Cabinet Bah Blesson & Company interagit avec les prestataires de services que sont :

- STRIPE (stripe.com) ;
- API ;
- CinetPay qui regroupe Orange Money ; - MTN Mobile Money ; - Moov Money.

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

- à ses agents habilités ;
- 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 de l'administration publique dans le cadre de leurs missions.

Considérant par ailleurs que le demandeur mentionne dans sa demande qu'il effectuera un transfert de données vers son sous-traitant en Irlande ;

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 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 des mentions légales sur site internet permettront aux personnes concernées d'être informées de leurs droits, préalablement à toute collecte ;

L'Autorité de protection considère 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 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,

Il le fait par le biais de mentions sur son site internet ;

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

L'Autorité de protection prescrit au Cabinet Bah Blesson & Company 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 ;

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 le demandeur, et après vérification préalable de l'Autorité de protection, le niveau de sécurité du système d'information du Cabinet Bah Blesson & Company, lui permet de mettre en œuvre sa plateforme « Business Info » 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 :

Le Cabinet Bah Blesson & Company est autorisé à effectuer la collecte, et l'enregistrement des données à caractère personnel ci-après :

- **les données d'identification :** Nom, prénom, adresse, numéro de téléphone ;
- **les données de connexion :** E-mail, nom d'utilisateur, mot de passe ;
- **les données bancaires :** numéro de carte bancaire, zip code ;

Les données visées au présent article concernent les utilisateurs de la plateforme « Business Info » du Cabinet Bah Blesson et Company.

Les données non mentionnées ne devront aucunement faire l'objet d'un quelconque traitement de la part du Cabinet Bah Blesson & Company.

Article 2 :

Les données traitées par le Cabinet Bah Blesson & Company 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 Bah Blesson & Company a l'obligation de procéder au recueil du consentement préalable des personnes concernées, par l'insertion de mentions d'informations sur son site, indépendamment des conditions générales d'informations.

Article 4 :

Le Cabinet Bah Blesson & Company est autorisé à communiquer les données traitées :

- pour la fourniture de ses services, à ses agents habilités ;
- pour le paiement de ses services, aux prestataires que sont STRIPE (stripe.com), API, CinetPay qui regroupe : Orange Money, MTN Mobile Money, Moov Money ;
- 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 de l'administration publique dans le cadre de leurs missions.

Il est interdit au Cabinet Bah Blesson & Company de transférer, sans autorisation préalable de l'Autorité de protection, les données collectées vers des pays tiers.

Article 5 :

Les données sont conservées pendant toute la durée de l'utilisation de la plateforme : « Business Info » par l'usager.

Les données sont supprimées dans un délai de (05) cinq ans, en cas de dé-souscription ;

Les données seront supprimées dans un délai de douze (12) mois, en cas de désinstallation de la plateforme.

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

Article 6

Le Cabinet Bah Blesson & Company 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.

Il le fait par le biais de mention sur son site internet.

Le Cabinet Bah Blesson & Company est tenu de définir une procédure de gestion des droits des personnes concernées.

Article 7 :

Le Cabinet Bah Blesson & Company 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 Bah Blesson & Company veille au respect des dispositions de la Loi relative à la protection des données à caractère personnel par ses sous-traitants.

Le Cabinet Bah Blesson & Company 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 Cabinet Bah Blesson & Company 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 Bah Blesson & Company 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 Bah Blesson & Company, 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 Cabinet Bah Blesson & Company.

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 28 janvier 2020
En deux (2) exemplaires originaux

Le Président

Dr DIAKITE Coty Souleïmane
COMMANDEUR DE L'ORDRE NATIONAL