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.