ARTCI
AUTORITE DE REGULATION DES TELECOMMUNICATIONSITIC DE COTE D'IVOIRE

REPUBLIQUE DE COTE D'IVOIRE
Union - Discipline - Travail

CONSEIL DE REGULATION

DECISION N° 2016-0203

DU CONSEIL DE REGULATION

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

EN DATE DU 22 NOVEMBRE 2016

FIXANT LES CONDITIONS DE L'EXERCICE DE L'ACTIVITE D'AUDIT DES TRAITEMENTS DES DONNEES A CARACTERE PERSONNEL

L'AUTORITE DE PROTECTION,

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

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°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°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 (ARTCI) ;

Vu le Décret 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 ;

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°2013-332 du 22 mai 2013 portant nomination du Directeur Général 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°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°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°2016-0201 de l'Autorité de protection de la République de de Côte d'Ivoire en date du 22 novembre 2016, fixant les frais de dossiers et d'agrément en matière de protection de données à caractère personnel.

Par les motifs suivants :

Considérant que conformément à l'article 47 de la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel , l'Autorité de protection est chargée :

- de déterminer les garanties indispensables et les mesures appropriées pour la protection des données à caractère personnel ;

- de faire des propositions susceptibles « ... » d'améliorer le cadre législatif et règlementaire concernant le traitement des données à caractère personnel ;

Considérant que l'Autorité de protection, dans l'exercice de ses missions, doit veiller à ce que l'activité d'audit de traitement de données à caractère personnel, objet d'une demande d'agrément permette effectivement d'aboutir au respect des exigences de la loi sur la protection des données à caractère personnel;

-

Que ce faisant l'exercice de l'activité d'audit des traitements de données à caractère personnel doit être soumise à des exigences particulières ;

Après en avoir délibéré,

DECIDE :

Article 1 :

La présente décision fixe les conditions et les critères de l'exercice de l'activité d'audit des traitements de données à caractère personnel.

Article 2 :

Le Conseil de régulation adopte les conditions et les critères d'exercice de l'activité d'audit des traitements de données à caractère personnel annexés à la présente décision.

Article 3 :
La demande d'agrément pour l'exercice de l'activité d'audit des traitements de données à caractère personnel est adressée à la Direction Générale de l'autorité de protection, assurée par l'ARTCI.

Article 4 :

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

Article 5 :

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 22 novembre 2016
en deux (2) exemplaires originaux

Le Président

Dr Lémassou FOFANA
OFFICIER DE L'ORDRE NATIONAL

ANNEXE :
CONDITIONS ET CRITERES DE L'EXERCICE DE L'ACTIVITES D'AUDIT DE TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL

Un audit est défini comme un processus systématique, indépendant et documenté en vue d'obtenir des preuves et de les évaluer de manière objective pour déterminer dans quelle mesure des critères prédéterminés sont satisfaits.

Le présent référentiel définit les critères et les moyens permettant à l'Autorité de régulation des télécommunications de Côte d'Ivoire dans sa mission d'Autorité de protection des données à caractère personnel de déterminer si la procédure d'audit de traitement de données à caractère personnel faisant l'objet d'une demande de label permet effectivement d'atteindre un tel objectif.

Les demandeurs doivent démontrer qu'ils satisfont les exigences du référentiel en fournissant des explications et des éléments de preuve. La démonstration proposée doit indiquer en quoi la procédure d'audit évaluée y répond de manière spécifique et précise.

Audit	Processus systématique, indépendant et documenté en vue d'obtenir des preuves et de les évaluer de manière objective pour déterminer dans quelle mesure des critères prédéterminés sont satisfaits
Audité	Organisme qui est audité
Auditeur	Personne possédant la compétence nécessaire pour réaliser un audit
Commanditaire de l'audit	personne demandant un audit - Le commanditaire peut être l'audité ou tout autre organisme qui a le droit réglementaire ou contractuel de demander un audit
Compétence	Qualités personnelles et capacité démontrées à appliquer des connaissances et des aptitudes
Conclusions d'audit	Résultat d'un audit fourni par l'équipe d'audit après avoir pris en considération les objectifs de l'audit et tous les constats d'audit
Critères d'audit	Ensemble de politiques, procédures ou exigences déterminées

Equipe d'audit	Un ou plusieurs auditeurs réalisant un audit, assistés, si nécessaire, par des experts techniques
Expert technique	Personne apportant à l'équipe d'audit des connaissances ou une expertise spécifique
Plan d'audit	Description des activités et des dispositions nécessaires pour réaliser un audit
Preuve d'audit	Enregistrements, énoncés de faits ou autres informations, qui se rapportent aux critères d'audit et sont vérifiables.
Procédure d'audit	Description de l'ensemble du processus de gestion des audits mise en œuvre par le requérant
Programme d'audit	Ensemble d'un ou plusieurs audits planifiés dans un laps de temps et dans un but déterminés. Un programme d'audit comprend toutes les activités nécessaires pour la planification, l'organisation et la réalisation des audits.
Rapport d'audit	Document réalisé par l'équipe d'audit et remis à l'audité, qui fournit un enregistrement complet, concis, précis et clair de l'audit.

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.

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 un diplôme de maîtrise en droit des affaires ou équivalent dans le secteur du droit au minimum.

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 un diplôme de Bac+4 ou équivalent dans le domaine de l'informatique ou des systèmes d'information au minimum.

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

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 d'audit de sécurité technique (intrusion, investigation, détection de vulnérabilités techniques...) de trente (30) jours, en une ou plusieurs fois, au minimum, au cours des deux (2) dernières années.

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 (personnes interrogées, vérifications effectuées, données contrôlées...) sont suffisamment représentatifs.

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 (contenant au minimum : 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), est émis dans les délais convenus à moins qu'une nouvelle date d'émission ne soit fixée, est approuvé selon la procédure retenue et 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 (documentation fournie, plan d'audit, preuves d'audit, rapport d'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.

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 permet de déterminer la loi nationale de protection des données applicable à chaque traitement se trouvant dans le champ de l'audit.

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 excessive 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.