

DECISION N°2025-1234
DE L'AUTORITE DE PROTECTION
DE LA REPUBLIQUE DE CÔTE D'IVOIRE
EN DATE DU 02 MAI 2025
PORTANT AUTORISATION DE TRAITEMENT
DE DONNEES A CARACTERE PERSONNEL
PAR BUREAU VERITAS CÔTE D'IVOIRE

L'AUTORITE DE PROTECTION,

- Vu la Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- Vu la Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité ;
- Vu la Loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques ;
- Vu la Loi n°2015-532 du 20 juillet 2015 portant Code du travail ;
- Vu la Loi n°2024-352 du 06 juin 2024 relative aux communications électroniques ;
- Vu le Décret n°2012-934 du 19 septembre 2012 portant organisation et fonctionnement de l'Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI) ;
- Vu le Décret n°2014-105 du 12 mars 2014 portant définition des conditions de fourniture des prestations de cryptologie ;
- Vu le Décret n°2014-106 du 12 mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique ;
- Vu le Décret n°2015-79 du 04 février 2015 fixant les modalités de dépôt des déclarations, de présentation des demandes, d'octroi et de retrait des autorisations pour le traitement des données à caractère personnel ;
- Vu le Décret n°2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;
- Vu le Décret n°2019-947 du 13 novembre 2019 portant nomination du Président du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire ;
- Vu le Décret n°2019-985 du 27 Novembre 2019 portant nomination des Membres du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) ;
- Vu le Décret n°2021-916 du 22 décembre 2021 portant organisation du Référentiel général de sécurité des systèmes d'information et du plan de Protection des infrastructures critiques ;
- Vu le Décret n°2022-783 du 12 Octobre 2022 portant renouvellement partiel du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire, en abrégé ARTCI ;
- Vu le Décret n°2025-55 du 17 janvier 2025 portant nomination du Directeur Général de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) ;

- Vu l'Arrêté n°0099 MTND/CAB du 16 août 2024 modifiant l'Arrêté n°511/MPTIC/CAB du 11 novembre 2014 portant définition du profil et fixant les conditions d'emploi du correspondant à la protection des données à caractère personnel ;
- Vu la Décision n°2013-0003 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 20 septembre 2013 portant règlement intérieur ;
- Vu la Décision n°2014-0020 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 03 septembre 2014 portant adoption des règles de conduites relatives aux conditions au traitement des données à caractère personnel (DCP) ;
- Vu la Décision n°2014-0021 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 03 septembre 2014 portant conditions et critères applicables à la limitation du traitement des données à caractère personnel ;
- Vu la Décision n°2014-0022 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 03 septembre 2014 portant conditions de la suppression des liens vers les données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communication électronique accessibles au public ;
- Vu la Décision n°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 22 novembre 2016 fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel ;
- Vu la Décision n°2017-0354 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- Vu la Décision n°2019-0494 du conseil de régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 16 mai 2019 portant adoption d'un référentiel général de sécurité des systèmes d'information (RGSSI) ;
- Vu la Décision n°2021-0676 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 04 août 2021 portant procédure de contrôle en matière de données à caractère personnel ;
- Vu le Rapport d'audit de protection des données personnelles de **Bureau Veritas Côte d'Ivoire**.

Par les motifs suivants :

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

Considérant que pour faciliter cette mise en conformité l'Autorité de Protection a par décision n°2017-0354 du 26 octobre 2017, défini la procédure de mise en conformité des responsables du traitement avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Considérant que **le Bureau Veritas Côte d'Ivoire** est une société Anonyme Unipersonnelle, au capital de 1.482.140.000 de francs CFA ; immatriculée au RCCM sous le numéro CI-ABJ-2009-B-215339, sis au Plateau, Bd. Roume angle Rue Thomasset, 01 BP 1453 Abidjan 01 ; téléphone (+225) 27 20 31 25 00, a saisi l'Autorité de Protection d'une demande de mise en conformité ;

Considérant que **le Bureau Veritas Côte d'Ivoire** est spécialisé dans les services d'évaluation de conformité et de certification ;

Que par ailleurs, **le Bureau Veritas Côte d'Ivoire** a effectué sa formation et son audit de protection des données personnelles ;

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

Après en avoir délibéré,

DECIDE :

Article 1 :

Le Bureau Veritas Côte d'Ivoire est autorisé à traiter les données mentionnées dans l'annexe 1 de la présente décision.

Les données non mentionnées dans l'annexe 1 ne devront aucunement faire l'objet d'un quelconque traitement de la part du **Bureau Veritas Côte d'Ivoire**.

Article 2 :

Le Bureau Veritas Côte d'Ivoire est autorisé à communiquer les données traitées uniquement aux destinataires habilités, notamment :

- aux services internes du **Bureau Veritas Côte d'Ivoire** suivant leurs niveaux d'habilitation ;
- au groupe en France, en Allemagne, aux Pays-Bas ;
- à ses filiales au Ghana, au Nigeria, au Cameroun et au Kenya ;
- à la Caisse National de Prévoyance Sociale (CNPS) ;
- aux Autorités publiques ivoiriennes habilitées agissant dans le cadre de l'exercice de leurs missions ;
- au Procureur de la république ;
- aux Officiers de police judiciaire munis d'une réquisition ;

- aux Agents assermentés de l'Autorité de Protection (ARTCI) habilités, dans le cadre de l'exécution de leurs missions ;
- aux compagnies d'assurances, banques ;
- aux Sous-traitants et prestataires suivant leur domaine d'activités.

Article 3 :

Le **Bureau Veritas Côte d'Ivoire** est autorisé à effectuer des transferts de données vers la France, l'Allemagne, les Pays-Bas, le Ghana, le Nigeria, le Cameroun et le Kenya.

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

Tout autre transfert sera soumis à l'autorisation préalable de l'Autorité de Protection.

Article 4 :

Conformément à l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le Bureau Veritas 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 au **Bureau Veritas Côte d'Ivoire** ainsi qu'à ses sous-traitants, de veiller au respect de ces mesures.

Article 5 :

Les traitements de données autorisés dans la présente décision correspondent aux vingt-huit (28) finalités énumérées à l'annexe 3 de la présente décision.

Article 6 :

Le **Bureau Veritas Côte d'Ivoire** est tenu de mettre en œuvre les prescriptions énoncées dans l'annexe 4 de la présente décision. Elle le fait dans les délais prévus dans ladite annexe.

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

L'Autorité de Protection délivrera une attestation de conformité au **Bureau Veritas Côte d'Ivoire** lorsque toutes les prescriptions auront été mises en œuvre.

Article 7 :

En application de l'article 42 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le **Bureau Veritas Côte d'Ivoire** 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 Bureau Veritas 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 du **Bureau Côte d'Ivoire**, afin de vérifier le respect de la présente décision, dont la violation donnera lieu à des sanctions, conformément à la réglementation en vigueur.

Article 10 :

Le **Bureau Veritas Côte d'Ivoire** est tenu de procéder au paiement des frais de dépôts de demande d'autorisation auprès du Greffe de l'ARTCI, conformément à la décision n°2016-0201 de l'Autorité de Protection de la République de Côte d'Ivoire fixant les frais de dossiers et d'agrément en matière de protection des données à caractère personnel. L'Autorité de Protection lui délivrera une facture à cet effet.

Article 11 :

La présente décision entre en vigueur à compter de la date de sa notification au **Bureau Veritas 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 02 mai 2025
En deux (2) exemplaires originaux

Le Président

Coty Souleïmane DAKITE

Dr Coty Souleïmane DAKITE
COMMANDEUR DE L'ORDRE NATIONAL



**ANNEXE 1 : DONNEES AUTORISEES AUX TRAITEMENTS (BUREAU
VERITAS CÔTE D'IVOIRE)**

❖ Données ordinaires	
- Données d'identification :	Nom, prénoms, date et lieu de naissance, âge, signature, extrait de naissance, attestation d'identité, nationalité, sexe, extrait d'acte de mariage
- Données de la vie personnelle :	Situation matrimoniale, nombre d'enfants
- Données de la vie professionnelle :	Numéro CNPS, assurance, fiche de poste, Curriculum Vitae, nombre de contrat à durée indéterminée, qualification et parcours professionnel, fonction, carte d'assurance, numéro matricule, ancienneté, diplômes, date d'embauche, scolarisation des enfants, connaissances techniques, codes producteurs, niveau d'influence dans la société, vitesse, nombre de femmes (promotion du genre)
- Données d'informations d'ordre économique et financier :	Relevé d'identité bancaire (RIB), salaire, prime, bulletin de salaire, rémunération, dépenses effectuées
- Données de localisation :	Adresse géographique (lieu d'habitation et adresse de l'entreprise), coordonnées Global Positioning System (GPS) des véhicules
- Numéro d'identification national :	Numéro de téléphone, numéro de la Carte Nationale d'Identité (CNI), Numéro National d'Identification (NNI), numéro de passeport, numéro de la Couverture Maladie de Universelle (CMU), numéro du permis de conduire, numéro de la plaque d'immatriculation
- Données de connexion :	Adresse mail, identifiants de connexion, mot de passe
❖ Données sensibles	
- Données médicales :	Certificat médical, antécédents médicaux, examens physiques et paraclinique, diagnostic, prescription, arrêt maladie, radiographie
- Autres données sensibles :	Filiation
- Données biométriques :	Vidéo, image, photo
- Infractions, condamnations mesures de sûreté :	Casier judiciaire

Fait à Abidjan, le 02 mai 2025

Le Président

M. Coty Souleimane Diakite
Le Président

Dr Coty Souleimane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL



**ANNEXE 2 : DONNEES AUTORISEES AU TRANSFERT
(BUREAU VERITAS CÔTE D'IVOIRE)**

<u>Catégories de données</u>	<u>Données</u>
❖ <u>Données ordinaires</u>	
Données d'identification :	Nom, prénoms, âge, sexe, photo, extrait de naissance, nationalité, signature
Données de la vie personnelle :	Nombre d'enfants, situation matrimoniale
Données professionnelles :	Numéro CNPS, matricule, assurance, fonction, ancienneté, qualifications professionnelles, vitesse des véhicules, code de producteur, type de contrat de travail, fiche de poste, nombre de femmes (promotion du genre), motif de réclamation
Données d'informations d'ordre économique et financier :	Relevé d'identité bancaire (RIB), rémunération, éléments variables du salaire, salaire de base, primes et bonus
Données de localisation :	Adresse géographique (lieu d'habitation), Global Positioning System des véhicules, adresse postale, localité
Numéro d'identification national :	Numéro de téléphone, numéro de la CNI, Numéro National d'Identification (NNI), Numéro du passeport
Données de connexion :	E-mail, identifiant, mot de passe
❖ <u>Données sensibles</u>	
- Données médicales :	Pathologies, informations sur l'état de santé
- Autres données sensibles:	Filiation

Fait à Abidjan, le 02 mai 2025

Le Président



Dr Coty Soulemane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

ANNEXE 3 : LISTE DES TRAITEMENTS PAR FINALITE (BUREAU VERITAS CÔTE D'IVOIRE)

FINALITES	TRAITEMENTS
1. la gestion des ressources humaines	- la collecte, l'analyse, l'organisation, la conservation
2. la gestion des activités de médecine du travail	- la collecte, l'analyse, l'enregistrement, le traitement
3. la gestion du système d'information	- la collecte, l'accès
4. la gestion des consultants, fournisseurs et prestataires de service	- la collecte, l'enregistrement, la vérification, l'analyse, la communication, le suivi, le stockage
5. le contrôle de la conformité des produits agricoles	- la collecte, l'enregistrement, la validation, le traitement, le suivi,
6. le traitement et transmission des offres de service	- la collecte, l'enregistrement, le traitement, la validation, l'envoi, le suivi
7. la gestion administrative et financière	- le traitement, la validation, enregistrement, le suivi
8. la prospection commerciale et la gestion de la relation client	- la collecte, l'intégration, le traitement, l'extraction, le suivi
9. la réalisation de l'audit environnemental	- la collecte, l'évaluation
10. la gestion de la documentation et des archives	- la collecte, le traitement, la communication, la destruction
11. la gestion du parc automobile	- le tracking
12. la sécurité des biens et des personnes au sein et aux alentours des locaux	- la collecte, la captation d'image, le stockage
13. l'installation de caméras embarquées dans les véhicules des chauffeurs	- l'analyse, le tracking
14. la gestion des activités Qualité, Hygiène, Sécurité, Environnement (QHSE)	- la collecte, le traitement, la transmission
15. la réalisation de prestations d'inspection de marchandises dans le cadre de contrats avec le gouvernement	- la collecte, l'analyse, la communication

16. la réalisation de prestation de certification internationales pour le compte des clients (normes ISO)	- la collecte, la conservation, le suivi
17. la réalisation de missions d'inspection sur les navires en service	- la collecte, la consultation, l'analyse, la validation, le suivi
18. la gestion des correspondances et l'expédition de colis	- le transfert
19. la gestion des activités industrielles	- la collecte, le traitement, l'enregistrement, le contrôle, la validation, le stockage
20. la gestion des activités d'expertise pétrolière	- la collecte, le contrôle, la vérification, le traitement
21. la géolocalisation des véhicules du parc automobile	- la collecte, le tracking
22. le transfert des données au groupe en France	- la collecte, la communication
23. le transfert des données au Pays-Bas	- la collecte, la communication
24. le transfert des données en Allemagne	- la collecte, la communication
25. le transfert des données au Cameroun	- la collecte, la communication
26. le transfert des données au Ghana	- la collecte, la communication
27. le transfert des données au Nigeria	- la collecte, la communication
28. le transfert des données au Kenya	- la collecte, la communication

Fait à Abidjan, le 02 mai 2025

Le Président



Dr Coty Souleimane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

ANNEXE 4

PRESCRIPTIONS ET DELAIS D'EXECUTION (BUREAU VERITAS CÔTE D'IVOIRE)

POINTS D'ANALYSE	PRESCRIPTIONS	DELAIS D'EXECUTION
<p>La légitimité et la licéité des traitements</p>	<p>Il est prescrit à Bureau Veritas Côte d'Ivoire (BVCI) de procéder au recueil du consentement préalable des personnes concernées. Elle le recueillera comme ci-dessous :</p> <ul style="list-style-type: none"> - Dans le cadre du recrutement et de la gestion du personnel : <ul style="list-style-type: none"> o mettre à disposition lors de l'embauche un formulaire de recueil de consentement préalable ; o mettre à disposition lors de l'entretien d'embauche un formulaire de recueil de consentement spécifique aux données sensibles (données de santé, filiation), la vidéosurveillance et la géolocalisation ; o insérer des clauses relatives au consentement préalable dans les contrats de travail proposés à la signature des salariés. - Dans le cadre de la gestion des données des clients, des consultants, des fournisseurs et des prestataires : <ul style="list-style-type: none"> o insérer des clauses relatives à la protection des données personnelles et de consentement préalable conforme aux exigences légales ; 	<p>60 jours</p>

	<ul style="list-style-type: none"> ○ mettre à la disposition des personnes concernées un formulaire de recueil de consentement préalable dans le cadre des audits de durabilité avant toute collecte de données ; ○ mettre à la disposition des personnes concernées un formulaire spécifique pour le traitement des données sensibles, les transferts de données et la prospection commerciale. 	
<p>Les délais de conservation</p>	<p>- Concernant la conservation des données relatives à la gestion du personnel:</p> <p>Il est prescrit à Bureau Veritas Côte d'Ivoire de conserver les données traitées, durant toute la durée de la relation contractuelle avec la personne concernée.</p> <p>En cas de rupture du contrat de travail, les données traitées devront être conservées pendant une période supplémentaire de :</p> <ul style="list-style-type: none"> ○ 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. <p>Pour la gestion du recrutement, il est prescrit à Bureau Veritas Côte d'Ivoire de conserver les données traitées pendant une période de deux (02) ans, à compter du dernier contact avec la personne concernée.</p> <p>Par ailleurs, les dossiers médicaux du personnel doivent uniquement être conservés et archivés par le personnel soignant (médecin du travail ou infirmier).</p>	<p>12 mois</p>

Handwritten mark

	<p>- S'agissant de la conservation des données relatives aux clients, fournisseurs, prestataires et autres partenaires commerciaux :</p> <p>Il est prescrit à Bureau Veritas Côte d'Ivoire de conserver les données traitées pendant une période de dix (10) ans, à compter de la fin de l'exercice au cours duquel les traitements ont été réalisés, conformément à l'article 24 de l'Acte Uniforme portant organisation et harmonisation des comptabilités des entreprises.</p> <p>Bureau Veritas Côte d'Ivoire conserve également les pièces et documents relatifs aux opérations effectuées, y compris les livres de comptes et les correspondances commerciales dix (10) ans après l'exécution de l'opération.</p> <p>En cas de contentieux, il est recommandé à Bureau Veritas Côte d'Ivoire de conserver les données traitées jusqu'au règlement définitif du contentieux.</p> <p>- Pour l'archivage :</p> <p>Il est prescrit à Bureau Veritas Côte d'Ivoire de mettre en œuvre une politique de gestion électronique des documents et d'élaborer une procédure d'archivage électronique des données qui devra obéir aux dispositions du décret n°2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique.</p> <p>Bureau Veritas Côte d'Ivoire est tenu de faire respecter la procédure d'archivage afin d'éviter que les documents physiques non utilisés dans le bureau des agents fassent l'objet d'accès non autorisé.</p>	
<p>La proportionnalité des données</p>	<p>Il est prescrit à Bureau Veritas Côte d'Ivoire de mettre en place une procédure de communication des données de santé (arrêts maladies, formulaire d'adhésion couverture maladie, résultats des visites médicales, etc..) afin de restreindre l'accès et la consultation de ces données uniquement aux personnes habilitées.</p>	<p>30 jours</p>

	<p>En application de l'article 21 de la loi relative à la protection des données à caractère personnel, il est prescrit à Bureau Veritas Côte d'Ivoire de ne pas collecter et traiter les données suivantes :</p> <ul style="list-style-type: none"> - les données relatives à la filiation des clients et du personnel figurant sur la carte d'identité ; - le casier judiciaire des agents collecté lors de la phase précontractuelle. <p>Il est également prescrit à Bureau Veritas Côte d'Ivoire de mettre en œuvre des mesures de pseudonymisation ou d'anonymisation des données des planteurs communiqués aux clients et autres partenaires dans le cadre des projets de durabilité.</p> <p>Il est prescrit à Bureau Veritas Côte d'Ivoire d'élaborer et de mettre en œuvre une politique de gestion des données sensibles. Dans ce cadre, elle devra :</p> <ul style="list-style-type: none"> o faire l'inventaire des données sensibles traitées ; o analyser la proportionnalité des données sensibles traitées ; o épurer sa base de données des informations sensibles disproportionnées et conserver les données pertinentes ; o sécuriser les données sensibles traitées ; o définir les accès aux données sensibles ; o procéder au recueil du consentement sur un formulaire distinct ; o réaliser une Analyse d'Impact relative à la Protection des Données (AIPD). 	
<p>La transparence des traitements</p>	<p>Il est prescrit à Bureau Veritas Côte d'Ivoire de faire preuve de plus de transparence en informant de manière concise les personnes concernées de :</p> <ul style="list-style-type: none"> - l'identité de Bureau Veritas Côte d'Ivoire et le cas échéant celle de son représentant dûment mandaté ; 	<p>90 jours</p>

	<ul style="list-style-type: none"> - la finalité du traitement ; - des catégories de données concernées ; - des 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. <p>Bureau Veritas Côte d'Ivoire le fera par le biais :</p> <ul style="list-style-type: none"> - de mentions légales sur ses formulaires, contrats et tout support de communication digitale ; - d'affiches dans tous les lieux où elle opère des traitements de données personnelles. 	
<p>Sur le système informatique</p>	<ul style="list-style-type: none"> - Il est prescrit à Bureau Veritas Côte d'Ivoire de mettre en œuvre les mesures suivantes : - Mettre en place une procédure de notification des violations de données personnelles, incluant un système de détection, une notification rapide et conforme aux autorités et parties concernées, ainsi qu'une évaluation et documentation des incidents pour prévenir leur récurrence ; - Implémenter des mesures de chiffrement systématique des données, en adoptant des algorithmes des protocoles de chiffrement forts (par exemple, AES-256 pour les données au repos et TLS pour les données en transit), et en mettant en place une gestion sécurisée des clés de chiffrement ; - Conserver les supports de stockage dans des lieux sûrs et accessibles uniquement aux personnes autorisées ; 	<p>90 jours</p>

Handwritten mark

	<ul style="list-style-type: none"> - Installer un système d'alarme anti-intrusion avec détection automatique des activités suspectes, telles que les tentatives d'accès non autorisé ; - Mettre en place un système de journalisation sécurisé enregistrant les accès, les activités des utilisateurs, ainsi que les modifications de données ou de configurations sensibles, en veillant à ce que ces journaux soient protégés contre la falsification, accessibles uniquement aux administrateurs autorisés, et à ce que les agents soient informés de leur existence ; - Élaborer et mettre en œuvre une politique "Clean Desk Policy" pour réduire les risques de fuite de données, incluant l'interdiction de laisser des documents confidentiels visibles, l'obligation de verrouiller les postes de travail inactifs, et l'utilisation de broyeurs pour détruire les documents sensibles ; - Organiser régulièrement des sessions de sensibilisation pour informer le personnel sur les bonnes pratiques de sécurité ; - Mettre en place un plan de continuité des activités pour minimiser l'impact des incidents de sécurité ; - Élaborer une politique de gestion des habilitations, incluant la mise à jour régulière des profils pour répondre aux changements organisationnels, ainsi qu'une politique de mots de passe définissant des règles de complexité, de renouvellement, et l'utilisation de l'authentification multi facteur ; - Implémenter les mesures de verrouillage des ports USB sur les PC professionnels ; - Mettre en place d'un système de verrouillage automatique de session ; - Réaliser une analyse des risques et d'impact prenant en compte les données à caractère personnel et le respecte des normes ISO/CEI 27005 et du Référentiel Général de Sécurité des Systèmes d'Information (RGSSI) de l'ARTCI. 	
Exactitude des données	<p>Il est prescrit à Bureau Veritas Côte d'Ivoire d'élaborer une procédure d'actualisation des données personnelles qu'elle traite.</p>	12 mois

Les procédures	<p>Il est prescrit à Bureau Veritas Côte d'Ivoire :</p> <ul style="list-style-type: none"> - de développer une stratégie de protection des données personnelles conforme aux exigences légales ; - d'adapter les procédures et politiques groupe en matière de protection des données personnelles à la loi Ivoirienne ; - d'élaborer une procédure de gestion et de communication des données sensibles (données de santé des agents, etc...) ; - d'élaborer une procédure d'archivage physique ; - d'élaborer une procédure d'actualisation des données ; - d'élaborer une procédure de notification des violations et incidents en matière de protection des données personnelles ; - d'intégrer à la cartographie des risques, les risques liés à la protection des données personnelles. 	120 jours
La vidéosurveillance	<p>Il est prescrit à Bureau Veritas Côte d'Ivoire :</p> <ul style="list-style-type: none"> - de requérir l'accord du personnel pour la mise en place du dispositif de vidéosurveillance ; - d'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. <p>Les affiches et pictogrammes doivent indiquer, d'une façon claire et visible, les informations suivantes :</p> <ul style="list-style-type: none"> - le nom du responsable du traitement ; - le fait que l'établissement est placé sous vidéosurveillance ; - la finalité du dispositif (sécurité des biens et des personnes) ; 	30 jours

	<ul style="list-style-type: none"> - 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 les caméras de vidéosurveillance sur le poste de travail des employés; - ne pas poser les caméras de vidéosurveillance dans les toilettes, les lieux de pause, de repas ou de repos des employés. <p>Bureau Veritas Côte d'Ivoire est tenu également de 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.</p> <p>Dans le cadre de l'installation des caméras embarquées, Bureau Veritas Côte d'Ivoire est tenu de :</p> <ul style="list-style-type: none"> - mettre à la disposition des salariés conducteurs un formulaire de recueil du consentement préalable spécifique ; - réaliser une Analyse d'Impact pour la protection des données pour le projet. <p>En cas de litige les données seront conservées jusqu'au règlement définitif du litige.</p>	
<p>La géolocalisation</p>	<p>Il est prescrit à Bureau Veritas Côte d'Ivoire de ne pas utiliser le dispositif de géolocalisation installé dans les véhicules mis à la disposition du personnel pour :</p> <ul style="list-style-type: none"> o contrôler l'employé en permanence ; o suivre la localisation en dehors du temps de travail (temps de pause, trajet domicile travail, etc...). <p>Bureau Veritas Côte d'Ivoire est tenu de réaliser une Analyse d'Impact relative à la Protection des Données (AIPD) pour tous les traitements impliquant la géolocalisation des agents et des prestataires.</p>	<p>90 jours</p>

Handwritten mark

	Bureau Veritas Côte d'Ivoire est tenu de s'assurer que son sous-traitant est conforme aux exigences légales applicables en matière de protection de données personnelles.	
Les sous-traitants	<p>Il est prescrit à Bureau Veritas Côte d'Ivoire :</p> <ul style="list-style-type: none"> - d'inclure dans ses contrats des clauses relatives à la protection des données ; - de contracter uniquement avec des sous-traitants capables d'apporter des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements à effectuer ; - d'inclure des clauses de responsabilité en matière de protection des données personnelles impliquant les données sensibles ; - de s'assurer de la conformité de ses sous-traitants avec les dispositions de la Loi relative à la protection des données personnelles. <p>Bureau Veritas Côte d'Ivoire et ses sous-traitants sont tenus de veiller au respect de ces mesures.</p>	30 jours
Transferts et communication de données	<p>Il est prescrit à Bureau Veritas Côte d'Ivoire :</p> <ul style="list-style-type: none"> - de communiquer les données traitées uniquement aux destinataires habilités ; - d'élaborer des règles contraignantes (BCR) pour l'encadrement des transferts des données intra-groupe. 	
Le correspondant à la protection	<p>Il est prescrit à Bureau Veritas Côte d'Ivoire :</p> <ul style="list-style-type: none"> - de mettre à la disposition du correspondant les ressources et les moyens nécessaires afin de mener à bien sa mission ; - d'informer l'ensemble du personnel de la désignation du correspondant à la protection et de ses missions. L'activité du correspondant doit-être relayée dans les services. 	30 jours

<p>Le respect des droits d'accès, de rectification, d'effacement et d'opposition</p>	<p>Il est prescrit à Bureau Veritas Côte d'Ivoire de mettre en place au niveau local une politique de gestion des droits des personnes concernées et de communiquer à ces personnes, les contacts du correspondant à la protection, auprès duquel celles-ci pourront exercer leurs droits d'accès, de rectification, d'effacement, d'opposition.</p>	<p>30 jours</p>
<p>La formation du personnel</p>	<p>Il est prescrit à Bureau Veritas Côte d'Ivoire de mettre en place une politique de formation et de sensibilisation de l'ensemble du personnel sur la protection des données personnelles.</p> <p>Elle devra également, mettre à la disposition du personnel des outils pédagogiques concernant la protection des données à caractère personnel. A titre d'exemples :</p> <ul style="list-style-type: none"> ✓ des guides individuels pour les différentes catégories d'acteurs ; ✓ des sessions de formation inscrites au catalogue de la Direction des Ressources Humaines ; ✓ la sensibilisation de l'ensemble du personnel ; ✓ des modules d'apprentissage en ligne (« e-learning ») ; ✓ la formation du correspondant à la protection et des chargés de protection des données personnelles, sanctionnée par un certificat. 	<p>90 jours</p>

Fait à Abidjan, le 02 mai 2025



Le Président
 Régulation des Télécommunications / TIC de Côte d'Ivoire
Le Président
 Dr Coty Soulemane DIAKITE
 COMMANDEUR DE L'ORDRE NATIONAL