DECISION N°2025-1233

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

EN DATE DU 02 MAI 2025

PORTANT AVERTISSEMENT ET MISE EN DEMEURE DE L'INSTITUTION DE PREVOYANCE SOCIALE-CAISSE GENERALE DES AGENTS DE L'ETAT (IPS-CGRAE) EN MATIERE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

(AGENCE DE SAN PEDRO)

Conseil de Régulation : 31 Av Nogués, Imble Broadway 2ème étage 17 BP 110 Abj 17 Tél: +225 27 20 34 43 04 - Fax: +225 27 20 34 43 02
Siège Direction Générale : Marcory Anoumabo, 18 BP 2203 Abj 18 Tél: +225 27 20 34 43 73 / 74 - Fax: + 225 27 20 34 43 75
www.artci.ci

L'AUTORITE DE PROTECTION,

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

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

Vu la Loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques ;

Vu la Loi n°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/TIC de Côte d'Ivoire (ARTCI) ;

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

Vu le Décret n°2014-106 du 12 mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique ;

Vu le Décret n°2015-79 du 04 février 2015 fixant les modalités de dépôt des déclarations, de présentation des demandes, d'octroi et de retrait des autorisations pour le traitement des données à caractère personnel ;

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

Vu le Décret n°2019-947 du 13 novembre 2019 portant nomination du Président 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°2022-783 du 12 Octobre 2022 portant renouvellement partiel du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/ TIC Côte d'Ivoire, en abrégé ARTCI ;

Vu 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 portant règlement intérieur ;

Vu la Décision n°2014-0020 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications /TIC de Côte d'Ivoire en date du 03 septembre 2014 portant adoption des règles de conduites relatives au traitement et à la protection des données à caractères personnel ;

Vu la Décision n°2014-0021 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 03 septembre 2014 portant conditions et critères applicables à la limitation du traitement des données à caractère personnel ;

Vu la Décision n°2014-0022 du Conseil de Régulation de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire en date du 03 septembre 2014 portant conditions de la suppression des liens vers les données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communication électronique accessibles au public ;

Vu la Décision n°2017-354 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Vu la Décision n°2020-0581 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 30 juillet 2020 fixant les critères et les conditions d'exercice des activités de :

- correspondant à la protection des données, personne morale ;
- audit de conformité ;
- formation ;

Vu la Décision n°2021-0676 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 04 Août 2021 portant procédure de contrôle en matière de protection des données à caractère personnel ;

Vu la Décision n°2023-0920 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 20 Juillet 2023 portant approbation de la liste des contrôles en matière de protection des données à caractère personnel pour l'année 2023 ;

Vu les Procès-verbaux de contrôle n° 013/05/2024 des 13, 14, 15, 16 mai 2024.

Par les motifs suivants,

I. Faits et procédure

Considérant que l'article 46 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel dispose que, l'Autorité de Protection veille à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de ladite loi et de ses décrets d'application ;

Considérant qu'aux termes des articles 47 et suivants de la loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, l'Autorité de Protection est chargée de procéder par le biais d'agents assermentés, à des vérifications portant sur tout traitement de données à caractère personnel et de prononcer des sanctions administratives et pécuniaires à l'égard des responsables du traitement qui ne se conforment pas à ses dispositions ;

Considérant la décision n°2021-0676 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 04 Août 2021 portant procédure de contrôle en matière de protection des données à caractère personnel ;

Considérant que l'IPS-CGRAE a été identifiée par la décision n°2023-0920 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 20 Juillet 2023 portant approbation de la liste des contrôles en matière de protection des données à caractère personnel pour l'année 2023 comme un responsable du traitement à contrôler ;

Considérant que l'IPS-CGRAE a été informée de la mission de contrôle en matière de protection des données à caractère personnel qui se tiendrait dans ses locaux sis à San Pedro, les 13, 14, 15, 16 mai 2024 ;

Cette mission avait pour objet de vérifier le respect par l'IPS-CGRAE de l'ensemble des dispositions de la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ainsi que celles de ses sous-traitants ;

Ainsi, les agents assermentés ont effectué un contrôle sur les traitements de données à caractère personnel des clients, du personnel des visiteurs mis en œuvre par l'IPS-CGRAE et ses sous-traitants ;

Considérant que les contrôles de l'Autorité de Protection ont porté sur les activités :

- des Ressources Humaines ;
- de l'Infirmerie ;
- du Système d'information ;
- du Chef de section accueil ;
- du Chef de section des prestations sociales ;
- du Gestionnaire de traitements des réclamations ;
- du Correspondant à la protection des données ;
- du Directeur d'agence ;
- du respect des principes de la protection des données personnelles ;

Considérant qu'à l'issue du contrôle, une copie des procès-verbaux de contrôle n° 013/05/2024 des 13, 14, 15, 16 mai 2024 contradictoirement dressés et signés, a été remise à l'IPS-CGRAE.

II. Motifs de la Décision :

A) Sur les manquements aux obligations de conformité et d'autorisations de traitement avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données personnelles

Considérant qu'aux termes de l'article 7 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le traitement portant sur un numéro national d'identification ou tout autre identifiant de la même nature, notamment les numéros de téléphone est soumis à autorisation préalable de l'Autorité de Protection, avant toute mise en œuvre ;

Considérant que l'article 53 de ladite loi dispose que : « *les responsables de traitement de données à caractère personnel disposent d'un délai de six (06) mois, à compter de la date de l'entrée en vigueur de la présente loi, pour se mettre en conformité avec ses dispositions* » ;

Considérant que l'article 2 de la décision n°2017-354 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel dispose que : « *la mise en conformité implique que les mesures techniques, organisationnelles et juridiques, nécessaires pour la protection des données à caractère personnel ont été prises par le Responsables du traitement* » ;

Considérant que l'article 4 de la décision susmentionnée dispose que : « (...) *la demande de mise en conformité est adressée à l'Autorité de Protection* » ;

Considérant qu'au moment du contrôle effectué par l'Autorité de Protection, l'IPS-CGRAE ne disposait pas :

- **d'autorisations de traitement au sens de l'article 7 de loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel et de ses textes d'application ;**
- **d'autorisation unique de traitement au sens de l'article 53 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel et de la décision n°2017-354 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 26 octobre 2017 portant procédure de mise en conformité des responsables du traitement avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.**

Par conséquent, l'Autorité de Protection considère que **l'IPS-CGRAE n'a pas respecté les dispositions des articles 7 et 53 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel**.

B) Sur le non-respect du principe de la légitimité et licéité des traitements

Considérant que conformément aux dispositions de l'article 14 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, le traitement

de données à caractère personnel est considéré comme légitime si la personne concernée donne expressément son consentement préalable ;

Considérant toutefois que le consentement doit être exprès, non équivoque, libre, spécifique et éclairé ;

Que la personne concernée doit avoir été suffisamment informée par le responsable du traitement, avant de donner librement son consentement, afin d'être en mesure d'une part, de comprendre la portée et les conséquences de son consentement, et d'autre part, les avantages et les inconvénients du traitement ;

Considérant que lors du contrôle et après analyse des documents communiqués, l'Autorité de Protection a constaté sans que la liste ne soit exhaustive :

- **l'absence de recueil du consentement des salariés, des clients, des fournisseurs et des parties prenantes pour les traitements de données ne bénéficiant pas de dérogations à l'exigence du consentement (vidéosurveillance, biométrie du data center, biométrie de contrôle de présence, registre d'entrée pour les sous-traitants, fournisseurs et la géolocalisation, etc... ...) ;**

- **l'absence de consentement pour le traitement de données personnelles liés à « macgrae.ci » et « i-reclamation » ;**

- **L'absence de dispositions relatives à la protection des données personnelles dans la procédure de traitement des réclamations et requêtes ;**

- **L'absence de case à cocher pour le consentement sur la fiche de contact, fiche de demande de domiciliation bancaire, fiche de réclamation/requête client ;**

Considérant que le responsable du traitement n'a pas fourni à l'Autorité de Protection, les preuves du consentement ou les dérogations à l'exigence du consentement préalable, des salariés et des fournisseurs ;

Dès lors, l'Autorité de Protection considère que **tous les traitements opérés ne satisfont pas totalement au principe de la légitimité prévus à l'article 14 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel**.

C) Sur les finalités

Considérant l'article 16 de la loi relative à la protection des données à caractère personnel qui dispose que les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités ;

Considérant que lors du contrôle, l'Autorité de Protection a constaté que les finalités pour lesquelles les données étaient collectées étaient déterminées et explicites mais illégitimes en l'absence d'autorisation de traitement de données ;

Dès lors, l'Autorité de Protection considère que **les finalités sont déterminées et explicites mais illégitimes**.

D) Sur la période de conservation des données traitées

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

Considérant que lors du contrôle et après analyse des documents communiqués, l'Autorité de Protection a constaté sans que la liste ne soit exhaustive :

- **L'absence d'une politique de conservation des données validées ;**
- **La conservation des données biométriques indéfiniment ;**
- **La durée de conservation et de suppression des données du coffre-fort au départ des agents de l'IPS-CGRAE n'est pas définie ;**
- **L'absence de délai de suppression des données en cas de départ de l'agent de l'IPS-CGRAE ;**
- **Les données biométriques (accès au data center) sont conservées indéfiniment ;**
- **Le salarié gère la durée d'utilité administrative des documents dans son coffre-fort ;**

Dès lors, l'Autorité de Protection considère que **le principe de la conservation limitée des données est partiellement respecté**.

E) Sur la proportionnalité des données collectées

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

Considérant que lors du contrôle et après analyse des documents communiqués, l'Autorité de Protection a constaté sans que la liste ne soit exhaustive :

- **La collecte de données sensibles ;**

- **L'absence d'une procédure de gestion des données sensibles ;**

- **L'absence d'analyse d'impact à la vie privée ;**

- **L'absence d'inventaire des données sensibles.**

Considérant entre autres le Responsable du traitement n'a pu fournir de manière précise à l'Autorité de Protection, les textes qui encadrent la collecte desdites données ;

Par conséquent, l'Autorité de Protection considère que **le principe de la proportionnalité n'est pas respecté.**

F) Sur les destinataires ou catégories de destinataires habilités à recevoir communication des données

Considérant les dispositions de l'article 9 de la loi n°2013-450 relative à la protection des données à caractère personnel, le responsable du traitement est tenu d'indiquer les destinataires habilités à recevoir communication des données traitées ;

Considérant que les destinataires internes et externes doivent être clairement identifiés ;

Qu'à l'issue du contrôle et après analyse des documents, l'Autorité de Protection constate sans que la liste ne soit exhaustive, les informations aux destinataires suivants :

- **Le cabinet Raynald et Fadiga pour les recrutements ;**

- **La société MCI, assureur de la CGRAE ;**

- **La société MICROSOFT pour l'hébergement des données (CLOUD) ;**

L'Autorité de Protection considère que **les destinataires des données internes ou externes ne sont pas totalement identifiés.**

G) Sur la transparence des traitements

Considérant qu'aux termes des articles 18 et 28 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, la transparence implique l'information obligatoire et claire des personnes concernées par le responsable du traitement ;

Qu'il s'agit en l'espèce pour le responsable du traitement de faire preuve de transparence vis-à-vis des personnes concernées qui devront notamment être informées. Les affiches ou des pictogrammes doivent indiquer, d'une façon claire et visible, les informations suivantes :

- l'identité du Responsable du traitement et le cas échéant, celle de son représentant dûment mandaté ;
- la finalité du traitement ;
- les catégories de données concernées ;
- les destinataires auxquels les données sont susceptibles d'être communiquées ;

- l'existence et des modalités d'exercice de leur droit d'accès et de rectification ;
- la durée de conservation des données ;
- l'éventualité de tout transfert de données à destination de pays tiers.

Considérant que lors du contrôle et après analyse des documents, l'Autorité de Protection a constaté sans que la liste ne soit exhaustive :

- **les formulaires et les fiches de contact et fiches de prestations sociales ne comportent pas les mentions relatives à la protection des données personnelles ;**

- **l'existence de mentions d'informations sur le dispositif de vidéosurveillance ;**

- **l'absence de politique de protection des données personnelles affichée dans les locaux et sur le site internet ;**

- **l'absence de charte de protection des données personnelles ;**

- **l'existence d'un pictogramme contenant la mention suivante « pour votre sécurité, cet établissement est sous vidéosurveillance » ;**

Par conséquent, l'Autorité de Protection considère que **le principe de la transparence n'est pas respecté.**

H) Sur les droits des personnes concernées

Considérant que les articles 9 et 29 à 34 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel prescrivent que le responsable du traitement doit indiquer dans sa demande, la fonction de la personne ou le service auprès duquel s'exercent les droits reconnus aux personnes concernées, notamment les droits d'accès, de rectification, de suppression ;

Considérant que l'Autorité de Protection a constaté sans que la liste ne soit exhaustive :

- L'existence d'un correspondant à la protection des données personnelles ;

- **l'absence de procédure d'exercice des droits des personnes concernées validée ;**

- **l'absence de formulaire d'exercice des droits des personnes concernées validée.**

L'Autorité de Protection considère **que les droits des personnes concernées ne sont pas respectés**.

I) Sur les mesures de sécurité

Considérant que l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel dispose que le responsable du traitement est tenu de prendre toute précaution au regard de la nature des données et, notamment, pour empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Considérant que lors du contrôle et après analyse des documents communiqués, l'Autorité de Protection a constaté sans que la liste ne soit exhaustive :

- L'existence de politique spécifique à la gestion des accès au système d'information ;
- L'existence d'une politique de gestion des habilitations informatiques ;
- L'existence d'une procédure de maintenance préventive des équipements informatiques ;
- L'existence d'une cartographie des risques ;
- L'existence d'une politique de sécurité et d'information ;
- L'existence d'un dispositif de vidéosurveillance ;
- **La société SAESEM assure la sécurité des locaux** ;
- **L'absence de plan de continuité ;**
- Les mesures prises pour l'accès au DATACENTER sont le système d'accès par badge, biométrie, reconnaissance faciale, digit code ;
- Le data center dispose d'un système de contrôle incident avec porte ignifuge ;
- La politique de mot de passe est incluse dans la politique de sécurité du système d'information ;
- **Le site web est géré de façon hybride par l'IPS-CGRAE et le prestataire Propulse Groupe.**

Par conséquent, l'Autorité de Protection considère que **les mesures de sécurité sont partiellement mise en œuvre.**

J) Sur les sous-traitants

Considérant que l'article 40 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel dispose que le Responsable du traitement est tenu de choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements à effectuer.

Qu'il incombe au responsable du traitement ainsi qu'aux sous-traitants de veiller au respect de ces mesures.

Considérant qu'à l'issue du contrôle, l'Autorité de Protection a constaté que le Responsable du traitement a recours à des sous-traitants, prestataires et fournisseurs de services dont :

- **Les sous-traitants et les prestataires du Cabinet Raynald et Fadika, Novatec, Arel Technology, Sarafina, Vigassistance, Saesem ne disposent pas d'autorisations de traitement ou de mise en conformité ;**

- **Les contrats passés avec les sous-traitants ne comportent aucune disposition relative à la protection des données personnelles ;**

Considérant qu'au moment du contrôle, les prestataires et fournisseurs de services ne disposaient pas d'autorisations de traitement et/ou de décisions de mise en conformité avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;

Que les sous-traitants n'ont entrepris aucune démarche auprès de l'Autorité de protection en vue d'obtenir une autorisation de traitement ou une décision de mise en conformité ;

Considérant que l'hébergement des données à destination de la France, constitue un transfert de données à destination d'un pays hors espace CEDEAO ;

Considérant qu'au moment du contrôle, l'IPS-CGRAE n'a pu fournir à l'Autorité de Protection, la preuve de l'autorisation de transfert de données à destination du cloud de MICROSOFT ;

Dès lors, l'Autorité de Protection considère que le transfert de données à destination du pays tiers ne respecte pas les dispositions de l'article 7 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

Enfin, l'Autorité de Protection considère que l'IPS-CGRAE **n'a pas pris de garanties suffisantes dans le choix de ses sous-traitants.**

K) Sur les logiciels utilisés

Considérant que l'Autorité de protection a constaté l'utilisation de plusieurs logiciels dont :

- **CEGID pour la paie et la gestion des absences ;**
- **SIG-CGRAE pour la gestion des prestations sociales ;**
- **E-réclamation et macgrae ;**

Considérant que l'IPS-CGRAE ne dispose pas d'autorisation de traitement de données pour les traitements de données opérés par le biais de ces logiciels ;

Par conséquent, l'Autorité de protection considère que **les traitements de données opérés par le biais des logiciels sont illégitimes.**

L) Contrôle du site internet de l'IPS-CGRAE

Considérant que l'Autorité de Protection a effectué des contrôles sur le site de l'IPS-CGRAE ;

Considérant qu'au moment du contrôle, l'analyse du site a permis de faire sortir les non-conformités suivantes :

- **L'existence de cookies ;**

- **L'absence de politique de cookies, de conditions générales d'utilisation, du contact du correspondant, de la politique de confidentialité, de protection des données personnes, et de mentions légales ;**

- **L'absence de recueil de consentement pour les candidatures spontanées, les cookies, la newsletter ;**

L'Autorité de Protection considère que les mesures prises pour le site internet de l'IPS-CGRAE sont insuffisantes.

M) Sur les procédures

Considérant que l'Autorité de Protection a constaté au moment du contrôle :

- **L'existence d'une procédure de recrutement datée et signée en 2020. Les aspects liés à la protection des données personnelles ne sont pas pris en compte ;**

- Une copie du contrat à durée déterminée signée le 04 avril 2024 a été communiquée. Elle contient une clause sur le secret professionnel. **Toutefois, elle ne contient pas de clauses relatives à la protection des données personnelles ;**

- **Le synopsis de formation dispensé par le correspondant à la protection ne contient pas le détail des modules sur la protection des données personnelles ;**

- L'existence d'une politique de gestion des accès au système d'information signée qui définit la gestion des mots de passe. **Toutefois, elle ne spécifie pas le nombre de caractères, la fréquence de renouvellement de ceux-ci, la durée de suppression de compte en cas de départ d'un employé ;**

- **L'existence d'une politique de gestion des habilitations informatiques ;**

- **L'existence d'une procédure de maintenance préventive des équipements informatiques signée. Elle prend en compte les exigences de la norme ISO 27001 et le référentiel ;**

- L'existence d'une cartographie des risques. **Toutefois, elle ne prend pas en compte les risques spécifiques à la protection des données personnelles ;**

- L'existence d'une politique de sécurité de l'information signée. **Elle est axée sur les exigences des normes internationales ISO/IEC 27002, 27005 ;**

Par conséquent, l'Autorité de Protection considère que les mesures relatives à la protection des données personnelles sont insuffisantes.

Après en avoir délibéré,

DECIDE :

Article 1 :

Conformément aux dispositions de l'article 49 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel et l'article 17 de la décision n°2021-0676 de l'Autorité de Protection de la République de Côte d'Ivoire en date du 04 Août 2021 portant procédure de contrôle en matière de protection des données à caractère personnel, l'Autorité de Protection prononce à l'égard de l'IPS-CGRAE :

- **un avertissement pour non-respect des obligations découlant de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel** ;

- **une mise en demeure de corriger toutes les non-conformités observées dans les soixante (60) jours à compter de la réception de la présente décision** ;

- **une mise en demeure de procéder à sa mise en conformité avec la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel dans un délai de soixante (60) jours à compter de la réception de la présente.**

Article 2 :

Si l'IPS-CGRAE ne s'est pas conformée à la présente mise en demeure, l'Autorité de Protection prononcera l'une des mesures prévues par l'article 51 de la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

Article 3 :

Les agents assermentés de l'Autorité de Protection effectueront des contrôles afin de s'assurer du respect de la présente décision conformément à la décision n°2021-0676 de l'Autorité de Protection en date du 04 août 2021 portant procédure de contrôle en matière de protection des données à caractère personnel.

Article 4 :

La présente décision prend effet à compter de la date de sa notification à l'IPS-CGRAE.

Article 5 :

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

Fait à Abidjan, le 02 Mai 2025
En deux (2) exemplaires originaux

Le Président

Dr Coty Souleïmane DIAKITE
COMMANDEUR DE L'ORDRE NATIONAL

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