



DECRET D/2026/ **0159** /PRG/SGG

**PORTANT PROCÉDURES D'AUDIT, DE CONTRÔLE ET DE
CERTIFICATION DES SYSTÈMES D'INFORMATION RELATIFS
AUX TRANSACTIONS ÉLECTRONIQUES**

LE PRÉSIDENT DE LA RÉPUBLIQUE,

Vu la Constitution de la République de Guinée ;

Vu la Loi L/2016/035/AN du 28 juillet 2016 relative aux Transactions Électroniques en République de Guinée ;

Vu la Loi L/2016/036/AN du 28 juillet 2016 modifiant et complétant certaines dispositions de la Loi N°017/AN du 8 septembre 2005 relative aux services de la Poste ;

Vu la Loi N°2015/018/AN du 13 août 2015 relative aux Télécommunications et aux Technologies de l'Information en République de Guinée ;

Vu la Loi L/2018/025/AN du 03 juillet 2018 portant organisation générale de l'Administration publique en République de Guinée ;

Vu l'Acte Additionnel A/SA.2/01/10 de la CEDEAO du 16 février 2010 relatif à la Protection des Données Personnelles dans l'espace CEDEAO ;

Vu la Directive C/DIR.1/08/11 de la CEDEAO sur la lutte contre la cybercriminalité dans l'espace CEDEAO ;

CONSIDÉRANT l'essor rapide des services de transactions électroniques en République de Guinée et la nécessité impérieuse de garantir la sécurité, la fiabilité et l'intégrité des systèmes d'information qui les supportent ;

CONSIDÉRANT la nécessité d'établir un cadre procédural clair, uniforme et opposable pour l'audit périodique des systèmes d'information des acteurs du secteur des transactions électroniques ;

CONSIDÉRANT les engagements internationaux de la République de Guinée en matière de cybersécurité et de protection des données personnelles dans l'espace CEDEAO ;

CONSIDÉRANT qu'il convient de conférer à l'Autorité de Régulation des Postes et Télécommunications (ARPT) les instruments procéduraux lui permettant d'exercer pleinement sa mission de supervision, de contrôle et de certification des systèmes d'information relatifs aux transactions électroniques ;



DÉCRÈTE :

CHAPITRE I : DISPOSITIONS GÉNÉRALES

Article 1er : Définitions

Au sens du présent décret, on entend par :

ARPT : Autorité de Régulation des Postes et Télécommunications.

Agrément de prestataire : Autorisation délivrée par l'ARPT à une personne morale, l'habilitant à réaliser des audits de sécurité conformément aux dispositions du présent décret.

Action corrective : Mesure prise pour éliminer la cause d'une non-conformité détectée et prévenir sa récurrence.

Audit : Processus périodique, méthodique, indépendant et documenté permettant d'évaluer le niveau de conformité d'un système d'information aux exigences du référentiel de l'ARPT en matière de sécurité.

Audité : Organisme responsable de tout ou partie d'un système d'information faisant l'objet d'un audit.

Certification : Processus d'évaluation et de validation de la conformité d'un système d'information aux normes techniques de sécurité et de performance définies par le référentiel de l'ARPT.

Certificat de conformité : Attestation formelle délivrée par l'ARPT, prouvant qu'une entité satisfaite aux conditions fixées par le référentiel général de sécurité.

Chiffrement : Technique consistant à transformer des données numériques en un format inintelligible au moyen d'algorithmes cryptographiques, afin de protéger leur confidentialité.

Conformité : Respect des exigences établies par les lois, règlements, référentiels applicables et politiques internes en vigueur.

Constat d'audit : Élément factuel observé, mesuré ou vérifié au cours de l'audit, servant de base aux conclusions de l'auditeur.

Échange de Données Informatisées (EDI) : Transfert électronique structuré d'informations entre systèmes électroniques, selon une norme convenue.

Expert auditeur : Auditeur titulaire d'une certification professionnelle reconnue par l'ARPT dans le domaine de la sécurité des systèmes d'information.

Infrastructures critiques : Installations physiques et systèmes d'information et de communication dont l'arrêt ou la destruction est susceptible d'avoir de graves incidences sur la santé, la sécurité, le bien-être social ou économique des citoyens, ou le fonctionnement continu des services de l'État.

Non-conformité majeure : Écart critique ou systémique compromettant la fiabilité, la sécurité ou la disponibilité du système audité.



Non-conformité mineure : Écart ponctuel ou isolé sans effet significatif sur la sécurité ou la performance globale du système.

Plan d'audit : Description formelle des activités, des ressources, des échéances et des méthodes utilisées lors d'un audit.

Prestataire d'Audit (PA) : Organisme agréé par l'ARPT, habilité à fournir des prestations d'audit de sécurité des systèmes d'information conformément aux exigences réglementaires en vigueur.

Rapport d'audit : Document formel présentant les constats, conclusions, recommandations et actions proposées à l'issue d'une mission d'audit.

Risque : Combinaison de la probabilité qu'une menace exploite une vulnérabilité d'un système d'information et de la gravité de l'impact potentiel qui en résulte sur la disponibilité, l'intégrité et la confidentialité dudit système.

Sécurité des Systèmes d'Information (SSI) : Ensemble des moyens techniques, organisationnels, juridiques et humains mis en oeuvre pour prévenir l'accès non autorisé, le mauvais usage, la modification ou le détournement d'un système d'information.

Système de Management de la Sécurité de l'Information (SMSI) : Ensemble de politiques, procédures et contrôles permettant de gérer de manière systématique la sécurité de l'information au sein d'une organisation.

Transaction Électronique : est une opération réalisée à distance à l'aide de moyens électroniques, sans contact physique direct entre les parties. Plus simplement, c'est tout échange, paiement ou transfert d'informations effectué via des technologies numériques (internet, téléphone, carte bancaire, etc.)

Article 2 : Objet

Le présent décret a pour objet de définir la procédure d'audit de sécurité, de contrôle et de certification des systèmes d'information des transactions électroniques, en application des articles 44 et 46 de la Loi L/2016/035/AN du 28 juillet 2016 relative aux Transactions Électroniques en République de Guinée.

Article 3 : Missions d'audit et de certification

La mission d'audit consiste en l'examen régulier, approfondi et indépendant des réseaux et systèmes informatiques des personnes morales de droit public et privé, établies en République de Guinée et exerçant des activités de transactions électroniques, quel que soit le type de support utilisé.

La mission de certification vise à attester formellement que le système d'information d'une entité est conforme aux référentiels de sécurité, de gestion et de réglementation en vigueur, et qu'il présente les garanties suffisantes de fiabilité, de performance et de gestion des risques.



CHAPITRE II : ORGANISMES SOUMIS À L'AUDIT DE SÉCURITÉ

Article 4 : Champ d'application

Sont soumis à l'audit de sécurité périodique obligatoire, toute entreprise ou établissement public ou privé, légalement constitué en République de Guinée et exerçant des activités de transactions électroniques.

Les modalités d'application différenciées selon la taille, la nature et le volume d'activité des entités concernées sont fixées par décision de l'ARPT, qui établit à cet effet une classification des entités par niveaux de criticité.

Sont également soumis au présent décret les prestataires établis hors du territoire guinéen qui offrent des services de transactions électroniques à des résidents en République de Guinée, dans les conditions fixées par décision de l'ARPT.

Toute entité soumise au présent décret qui cesse, suspend ou transfère son activité de transactions électroniques en informe l'ARPT dans un délai de trente (30) jours calendaires. L'ARPT statue sur les suites à donner aux obligations d'audit en cours.

CHAPITRE III : PROCÉDURE D'AUDIT DE SÉCURITÉ

Article 5 : Périodicité de l'audit

L'audit de sécurité des organismes visés à l'article 4 du présent décret est réalisé tous les trois (3) ans, sous réserve des dispositions particulières applicables aux entités classées à un niveau de criticité élevé, fixées par décision de l'ARPT.

À l'issue d'un audit de conformité concluant, l'ARPT délivre à l'organisme audité un certificat de conformité dans les conditions prévues à l'article 13 du présent décret.

En cas de non-conformité constatée, un contrôle de suivi est effectué dans un délai compris entre trois (3) et douze (12) mois suivant la date de l'audit, afin de vérifier que les recommandations ont été mises en oeuvre et que le système d'information satisfait aux exigences légales et réglementaires applicables. Ce délai est fixé par décision motivée de l'ARPT.

L'organisme audité transmet à l'ARPT son plan d'action correctif dans le délai imparti à compter de la notification de non-conformité et le met en oeuvre après validation par l'ARPT.

À défaut de transmission ou de mise en oeuvre dans les délais prescrits, des sanctions sont susceptibles d'être appliquées conformément aux dispositions du Chapitre IV du présent décret.

Nonobstant ce qui précède, après délivrance d'un certificat de conformité, un contrôle intermédiaire est réalisé auprès de l'organisme concerné dans les dix-huit (18) mois suivants, afin de s'assurer du maintien de la conformité aux exigences légales et réglementaires de sécurité.



Toute entité entrant nouvellement dans le champ d'application du présent décret dispose d'un délai de douze (12) mois à compter de la date d'entrée dans ce champ pour réaliser son premier audit de sécurité.

En cas d'incident de sécurité majeur ou de modification substantielle de l'architecture du système d'information, l'ARPT peut ordonner, par décision motivée, un audit exceptionnel en dehors du cycle périodique. Cette décision est notifiée à l'entité concernée au moins quinze (15) jours ouvrés avant le début de la mission.

Article 6 : Autorité compétente

Les missions d'audit de sécurité des systèmes d'information des transactions électroniques sont dévolues à l'ARPT, qui en assume la responsabilité réglementaire.

Article 7 : Délégation aux Prestataires d'Audit

Le choix du prestataire chargé de la réalisation de l'audit relève de l'entité auditée, à condition que ledit prestataire soit préalablement agréé par l'ARPT.

Pour être agréé, tout prestataire doit satisfaire aux conditions cumulatives suivantes :

- être une personne morale régulièrement constituée conformément à la législation guinéenne ou étrangère applicable ;
- présenter des garanties suffisantes d'indépendance à l'égard des entités susceptibles d'être auditées ;
- justifier d'une assurance en responsabilité civile professionnelle en cours de validité, couvrant les missions d'audit de sécurité des systèmes d'information ;
- disposer en son sein d'au moins un expert auditeur titulaire d'une certification professionnelle reconnue par l'ARPT dans le domaine de la sécurité des systèmes d'information.

Tout PA est tenu de déclarer à l'ARPT, préalablement à toute mission, toute situation susceptible de créer un conflit d'intérêts avec l'entité auditée. L'ARPT peut, par décision motivée notifiée avant le début de la mission, récuser le PA concerné et désigner un PA de substitution.

Les conditions et procédures complémentaires régissant l'obtention de l'agrément des PA sont fixées par décision de l'ARPT.

Article 8 : Programme annuel d'audit

L'ARPT établit chaque année, au plus tard le 30 septembre, le programme des audits de sécurité à réaliser au cours de l'année suivante, dans le cadre du plan stratégique triennal qu'elle définit.



Ce programme est communiqué en temps utile aux entités concernées par les audits à venir.

Le programme peut être modifié par l'ARPT. Toute modification doit être motivée et notifiée aux organismes concernés au moins trois (3) mois avant la date d'audit initialement prévue.

Article 9 : Périmètre de l'audit

L'audit de sécurité sur site porte notamment sur les éléments suivants :

- L'analyse et l'évaluation des risques résultant de l'exploitation des vulnérabilités et failles du système d'information ;
- Les aspects organisationnels, incluant le mode de gestion de la fonction de sécurité, des procédures de sécurité et la disponibilité et l'utilisation des outils de sécurisation ;
- Les aspects techniques de la sécurité de l'ensemble des composantes du système informatique, notamment par la réalisation de tests de résistance aux cybermenaces.

Article 10 : Rapport d'audit

À l'issue de chaque mission d'audit, le PA produit un rapport d'audit final ainsi qu'un procès-verbal de réunion de clôture, lesquels constituent les documents probants de la mission.

Article 11 : Contenu du rapport d'audit

Le rapport d'audit contient au minimum les éléments suivants :

- Un résumé exécutif présentant les principales conclusions de l'examen des documents et les recommandations prioritaires ;
- Une description et une évaluation complètes de la sécurité du système d'information, incluant les mesures mises en oeuvre depuis le dernier audit et les insuffisances constatées dans l'application des recommandations antérieures ;
- Une description de la démarche méthodologique utilisée ;
- Une description détaillée des mesures de sécurité recommandées, assortie d'un calendrier de mise en oeuvre indicatif.

Le rapport d'audit provisoire est transmis par le PA à l'entité auditée et à l'ARPT dans un délai de dix (10) jours ouvrés suivant la fin des opérations d'audit sur site.

L'entité auditée dispose d'un délai de dix (10) jours ouvrés pour formuler ses observations écrites au PA.

À compter de la réception des observations, le PA dispose d'un délai de sept (7) jours ouvrés pour organiser la séance de clôture, à l'issue de laquelle le rapport d'audit final est transmis à l'ARPT.



Article 12 : Confidentialité et conservation des rapports d'audit

Les rapports d'audit provisoires et finaux sont classifiés au niveau « Confidentiel ». Leur transmission entre le PA, l'entité auditée et l'ARPT s'effectue par voie sécurisée, garantissant leur intégrité et leur confidentialité.

Toute divulgation non autorisée du rapport d'audit ou de son contenu engage la responsabilité civile et, le cas échéant, pénale de son auteur.

Les rapports d'audit sont conservés par l'ARPT pendant une durée minimale de cinq (5) ans à compter de leur date de transmission. L'entité auditée est tenue de conserver ses propres exemplaires pendant la même durée.

Les modalités techniques de transmission et de conservation sécurisée des rapports d'audit sont fixées par décision de l'ARPT.

Article 13 : Délivrance du certificat de conformité

En cas de conformité totale, l'ARPT délivre à l'entité auditée un certificat de conformité dans un délai raisonnable à compter de la réception du rapport d'audit final.

En cas de non-conformité mineure, l'ARPT délivre le certificat de conformité dès que l'entité auditée a corrigé les réserves identifiées, dans un délai maximal de deux (2) mois à compter de la notification des observations.

En cas de non-conformité majeure, un nouvel audit de vérification est réalisé aux frais de l'entité auditée dans un délai de quatre-vingt-dix (90) jours calendaires à compter de la notification. Le certificat de conformité n'est délivré qu'à l'issue de cet audit concluant à la mise en conformité.

En cas de non-conformité, qu'elle soit mineure ou majeure, l'ARPT en informe l'autorité sectorielle compétente.

Le certificat de conformité est valable jusqu'à la date du prochain audit périodique obligatoire, telle que définie à l'article 5 du présent décret.

Le certificat de conformité peut être suspendu ou retiré par décision motivée de l'ARPT, en cas d'incident de sécurité majeur survenu postérieurement à sa délivrance ou en cas de manquement grave aux obligations du présent décret. La décision de suspension ou de retrait est notifiée à l'entité concernée et, le cas échéant, à l'autorité sectorielle compétente.

Article 14 : Obligation de notification des incidents

Tout organisme public ou privé soumis au présent décret est tenu d'informer l'ARPT de toute attaque, intrusion ou perturbation susceptible d'affecter le bon fonctionnement de son système d'information relatif aux transactions électroniques, dans un délai n'excédant pas soixante-douze (72) heures à compter du moment où il en prend connaissance.



Lorsque l'incident est susceptible d'affecter les données ou les services d'un nombre significatif d'utilisateurs, une notification initiale est adressée à l'ARPT dans les vingt-quatre (24) heures, suivie d'un rapport complet dans un délai de soixante-douze (72) heures.

Les modalités de notification, le format du rapport d'incident et les critères de qualification d'un incident comme « majeur » sont fixés par décision de l'ARPT.

Article 15 : Assistance de l'ARPT

L'ARPT apporte assistance et appui technique aux opérateurs de transactions électroniques afin de leur permettre de prendre les mesures nécessaires pour faire cesser toute perturbation affectant la sécurité ou la disponibilité de leur système d'information.

Article 16 : Obligation d'audit et mise en demeure

Les entités soumises à l'audit de sécurité périodique obligatoire en application de l'article 4 du présent décret, qui n'ont pas procédé à cet audit dans les délais impartis, font l'objet d'une mise en demeure de l'ARPT leur enjoignant de s'y conformer dans un délai de trente (30) jours à compter de la date de notification.

À l'expiration de ce délai, en l'absence de réalisation de l'audit dans les conditions prescrites, l'ARPT informe l'autorité sectorielle compétente du refus de l'entité de se soumettre à ses obligations légales et prend les mesures prévues aux articles 17 et 18 du présent décret.

CHAPITRE IV : SANCTIONS

Article 17 : Astreintes et sanctions pécuniaires

Le présent article institue deux régimes de sanction distincts et non cumulables pour les mêmes faits :

- 1. Astreinte de contrainte :** L'ARPT inflige une astreinte journalière de cinquante millions de francs guinéens (50 000 000 GNF) à l'encontre des entités visées à l'article 4 qui refusent ou s'abstiennent d'exécuter l'audit de sécurité périodique obligatoire. Cette astreinte court à compter de l'expiration du délai de mise en demeure prévu à l'article 16 et ne peut excéder la somme de quatre milliards cinq cents millions de francs guinéens (4 500 000 000 GNF). Elle cesse de courir dès l'engagement effectif de la procédure d'audit.
- 2. Sanction pécuniaire punitive :** Lorsqu'un ou plusieurs manquements aux dispositions du présent décret sont constatés, après une mise en demeure restée infructueuse, il est infligé au contrevenant une sanction pécuniaire dont le montant est proportionnel à la gravité du manquement et aux avantages qui en ont été tirés, sans pouvoir excéder la somme de trois milliards de francs guinéens (3 000 000 000 GNF). Ce régime ne peut se cumuler avec l'astreinte de contrainte pour les mêmes faits.



En cas de récidive, le montant de la sanction prononcée au titre du point 2 est porté au double.

Les sanctions prononcées dans le cadre du présent article font l'objet d'une publication sur le site de l'ARPT et dans un journal de la République de Guinée, sauf décision contraire motivée du Conseil National de Régulation des Postes et Télécommunications.

Article 18 : Sanctions applicables aux Prestataires d'Audit

En cas de manquement d'un Prestataire d'Audit agréé à ses obligations au titre du présent décret, notamment en cas de rapport inexact, incomplet ou transmis hors délai, de non-déclaration d'un conflit d'intérêts, ou de violation des règles de confidentialité prévues à l'article 12, l'ARPT peut prononcer, selon la gravité du manquement et après respect de la procédure contradictoire prévue à l'article 11, l'une des sanctions suivantes :

- un avertissement formel ;
- une suspension temporaire de l'agrément pour une durée ne pouvant excéder douze (12) mois ;
- un retrait définitif de l'agrément.

Ces sanctions sont notifiées au PA concerné et publiées sur le site de l'ARPT.

CHAPITRE V : RECOURS CONTRE LES DÉCISIONS DE L'ARPT

Article 19 : Voies de recours

Les décisions rendues par l'ARPT dans le cadre du présent décret peuvent faire l'objet des recours suivants :

- 1. Recours gracieux :** Toute entité s'estimant lésée par une décision de l'ARPT peut adresser un recours gracieux au Directeur Général de l'ARPT dans un délai de deux (2) mois à compter de la notification de la décision contestée. Le Directeur Général dispose d'un délai de trente (30) jours pour y répondre. Le silence gardé à l'issue de ce délai vaut décision de rejet.
- 2. Recours hiérarchique :** En cas de rejet du recours gracieux, l'entité peut formuler un recours hiérarchique devant le Conseil National de Régulation des Postes et Télécommunications dans un délai de soixante (60) jours à compter de la notification du rejet ou de l'expiration du délai de réponse. Le Conseil de Régulation statue dans un délai de quarante-cinq (45) jours.
- 3. Recours contentieux :** Les décisions du Conseil National de Régulation des Postes et Télécommunications peuvent être déférées devant la juridiction administrative compétente dans les conditions du droit commun.



Le recours n'est pas suspensif, sauf pour les sanctions pécuniaires. Toutefois, le sursis à exécution de la décision peut être accordé lorsque celle-ci est susceptible d'entraîner des conséquences manifestement excessives. Dans ce cas, la demande de sursis est présentée au Premier Président de la Cour d'Appel, statuant comme en matière de référé.

Article 20 : Recouvrement des pénalités

Les pénalités prononcées dans le cadre du présent décret sont recouvrées et perçues par l'ARPT, conformément à la réglementation en vigueur relative au recouvrement des créances publiques.

CHAPITRES VI : DISPOSITIONS DIVERSES ET FINALES

SECTION 1 : DISPOSITIONS DIVERSES

Article 21 : Obligations déclaratives des Prestataires d'Audit

Les activités d'audit de sécurité exercées par les Prestataires d'Audit agréés font l'objet d'une déclaration annuelle auprès de l'ARPT, dont les modalités sont fixées par décision de l'ARPT.

En cas de cessation d'activité, le PA en informe l'ARPT au plus tard trente (30) jours calendaires avant la date effective de cessation, afin de permettre à l'ARPT de prendre les dispositions nécessaires à la continuité des missions en cours.

Article 22 : Composition du dossier de déclaration d'ouverture

La déclaration d'intention d'ouverture d'un service d'audit de sécurité des systèmes d'information comprend les informations et pièces suivantes :

- L'identité et le statut juridique du demandeur ;
- Les types d'audit de sécurité des systèmes d'information proposés ;
- Les caractéristiques des logiciels et équipements utilisés pour les missions d'audit ;
- Les certifications professionnelles des experts composant l'équipe d'audit, reconnues par l'ARPT ;
- L'attestation d'assurance en responsabilité civile professionnelle en cours de validité.

SECTION 2 DISPOSITIONS TRANSITOIRES

Article 23 : Régime transitoire

Les entités visées à l'article 4 du présent décret qui exercent leurs activités à la date d'entrée en vigueur du présent décret disposent d'un délai de dix-huit (18) mois pour se conformer à l'ensemble de ses dispositions.



Durant cette période transitoire, l'ARPT élabore et met à disposition des entités concernées un programme d'accompagnement à la mise en conformité, comprenant notamment la publication de sa décision relative à la classification des entités par niveau de criticité et de sa décision relative aux conditions d'agrément des Prestataires d'Audit.

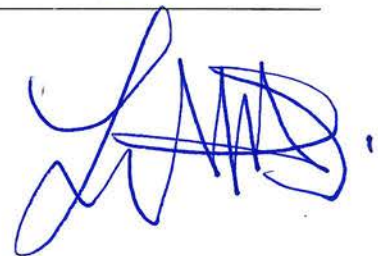
Les entités qui, à l'expiration du délai transitoire, n'ont pas réalisé leur premier audit de sécurité sont soumises aux dispositions des articles 17 et 18 du présent décret.

SECTION 3 : DISPOSITIONS FINALES

Article 24 : Entrée en vigueur

Le présent décret, qui prend effet à compter de la date de sa signature, sera enregistré et publié au Journal Officiel de la République de Guinée.

Conakry, le 21 MAI 2026



Président Mamadi DOUMBOUYA