Le cadre juridique du numérique en Côte d’Ivoire

Guide de référence et de mise en conformité pour les entreprises

Ministère de la Transition Numérique et de l’Innovation Technologique

Édition du 30 octobre 2026

Ce guide permet à une entreprise de repérer les règles qui encadrent ses usages numériques, de déterminer les formalités liées à son activité et d’organiser les preuves de sa conformité. Il s’adresse aux dirigeants, responsables juridiques, financiers, informatiques, commerciaux et des ressources humaines.

La conformité numérique se construit à partir des opérations réellement réalisées. Un fichier de paie, une boutique en ligne, une plateforme de mise en relation et un service de paiement n’entraînent pas les mêmes obligations. Plusieurs réglementations peuvent s’appliquer simultanément au même projet.

Le document couvre le socle transversal ivoirien, les principales interfaces communautaires et les activités réglementées les plus courantes. Pour un projet bancaire, sanitaire, audiovisuel, de transport ou de communications électroniques, les règles sectorielles doivent être examinées en complément avant le lancement.

Avertissement : *ce guide est un document d’information et d’orientation publié par le Ministère de la Transition Numérique et de l’Innovation Technologique. Il ne constitue pas un avis juridique et ne se substitue ni aux textes officiels, ni aux décisions des autorités compétentes, ni au conseil d’un professionnel. Les textes cités doivent être consultés dans leur version en vigueur ; l’état du droit présenté est celui du 30 octobre 2026.*

Sommaire

Synthèse pour la direction..... 3
1 Comprendre les sources du droit numérique..... 4
2 Identifier les autorités compétentes..... 5
3 Protéger les données personnelles..... 7
4 Encadrer la biométrie, la vidéosurveillance et le cloud..... 8
5 Organiser la cybersécurité et les audits..... 9
6 Réagir aux incidents et conserver les preuves..... 11
7 Vendre et contracter en ligne..... 12
8 Encadrer la prospection et les traceurs..... 14
9 Sécuriser la signature et les archives électroniques..... 15
10 Exploiter une plateforme ou un service de communications..... 16
11 Héberger des contenus et communiquer au public..... 17
12 Appliquer la fiscalité du numérique..... 18
13 Fournir des paiements et des services financiers numériques..... 19
14 Protéger les logiciels, les marques et les contenus..... 20
15 Encadrer les contrats informatiques et les achats..... 21
16 Gérer les usages numériques des salariés..... 22
17 Utiliser les avantages des startups et développer de nouveaux usages..... 23
18 Piloter les risques, les contrôles et les recours..... 25
19 Examiner les obligations connexes et internationales..... 26
20 Accomplir les démarches numériques auprès de l’État..... 27
Annexe A Questionnaire de qualification..... 31
Annexe B Plan de conformité sur 90 jours..... 32
Annexe C Registre des obligations et preuves..... 33
Annexe D Inventaire des traitements et transferts..... 33
Annexe E Grille de conservation..... 34
Annexe F Grille de revue des contrats numériques..... 35
Annexe G Cas pratiques..... 35
Annexe H Glossaire..... 36
Annexe I Maturité numérique et contexte économique..... 37
Annexe J Gouverner les usages de l’IA et la cybersécurité..... 40
Répertoire des textes et sources..... 43

Synthèse pour la direction

Les décisions à prendre en priorité

Une entreprise doit commencer par qualifier ses activités et ses flux de données. Cette qualification détermine les formalités auprès de l'ARTCI, le périmètre de l'audit de sécurité, les obligations de vente en ligne, les règles fiscales et, le cas échéant, les autorisations sectorielles. La conformité d'une plateforme ne se déduit ni de son immatriculation au RCCM ni du paiement de ses impôts.

Les premiers travaux doivent porter sur les traitements de données personnelles, les activités nécessitant une déclaration ou un agrément, la sécurité des systèmes, la facturation et les engagements contractuels. Les contrôles pratiques proposés dans ce guide sont des méthodes d'organisation. Ils ne remplacent pas les formalités prescrites par les textes.

La loi de protection des données et les règles de transactions électroniques constituent un socle ancien, complété par les textes de cybersécurité, la loi de communications électroniques de 2024 et les mesures fiscales annuelles. Les mises à jour les plus utiles aux entreprises concernent notamment les plateformes numériques, le rôle de l'ANSSI et la fiscalité de 2026. [R01, R05, R08, R10, R11, R22, R24]

Activité observée	Sujet à traiter	Preuve à réunir
Toute entreprise employant des salariés ou gérant des clients	Données personnelles et sécurité	Inventaire des traitements et formalités applicables
Site marchand ou vente par application	Information du client et contrat électronique	Mentions publiées et parcours de commande conservé
Plateforme de services numériques	Déclaration sectorielle à qualifier auprès de l'ARTCI	Récépissé correspondant à l'activité
Entreprise établie sur le territoire national	Audit réglementaire de sécurité selon le cadre ANSSI	Rapport du prestataire agréé et suivi des corrections
Émission de factures ou de tickets	FNE ou RNE et dispenses fiscales éventuelles	Factures certifiées ou justification de la dispense
Encaissement de fonds pour des tiers ou fourniture de paiements	Réglementation BCEAO et lutte contre le blanchiment	Agrément ou partenariat autorisé et périmètre contractuel
Jeune entreprise numérique innovante	Label startup et avantages effectivement ouverts	Arrêté de labellisation et dossier fiscal

Les changements à intégrer en 2026

L'ARTCI a rappelé le 4 avril 2025 que l'établissement et l'exploitation de plateformes de services numériques nécessitent un récépissé de déclaration préalable. Une société qui exploite une application doit vérifier sa qualification au regard du service fourni et de ce communiqué. [R11]

L'ANSSI rappelle un cycle d'audit de sécurité de trois ans. Le décret prévoit également un audit périodique dix-huit mois après l'obtention du certificat. L'entreprise doit suivre ces échéances, le périmètre des contrôles et l'agrément du prestataire. [R09, R44]

La FNE s'inscrit désormais dans le fonctionnement courant des entreprises concernées. Le dispositif comporte des dispenses et une distinction entre facture normalisée électronique et reçu normalisé

électronique. Une facture électronique peut être imprimée ; son origine et sa certification sont déterminantes. [R18, R19, R20]

L'annexe fiscale 2026 prévoit un régime fiscal pour certaines plateformes étrangères et précise les exonérations des startups numériques labellisées. Ces deux sujets doivent être examinés séparément de la TVA et de la FNE. [R21 à R25]

Comment utiliser le guide

La première partie expose les règles et leur articulation. Les annexes permettent d'ouvrir un chantier interne sans attendre : questionnaire d'assujettissement, registre des obligations, inventaire des traitements, grille de conservation et liste des clauses à négocier. Les références entre crochets renvoient au répertoire de sources cliquables en fin de document. Chaque chapitre s'ouvre sur un encadré « À retenir » qui en résume l'essentiel. Les annexes I et J apportent des repères sur la maturité numérique des entreprises et sur la gouvernance de l'IA et de la cybersécurité.

La mention « obligation » désigne une exigence issue du cadre cité. La mention « recommandation » désigne une mesure proposée pour faciliter sa mise en œuvre ou réduire un risque. Une fréquence interne de revue ou un calendrier de projet recommandé ne constitue pas un délai légal.

Éditions et mises à jour

Le présent guide est publié par le Ministère de la Transition Numérique et de l'Innovation Technologique. La présente édition, datée du 30 octobre 2026, en est la première. Le guide a vocation à être mis à jour au rythme de l'évolution des textes, notamment des lois de finances, des décisions de l'ARTCI, des référentiels de l'ANSSI et des textes de la BCEAO. Chaque nouvelle édition sera datée et ses principales évolutions seront signalées dans le tableau ci-dessous. La version en vigueur est consultable et téléchargeable dans l'espace Entreprises de la plateforme Agora Digital Côte d'Ivoire.

Édition	Date	Principales évolutions
Première édition	30 octobre 2026	Publication initiale : synthèse, vingt chapitres, dix annexes et répertoire de 75 textes et sources.

1 Comprendre les sources du droit numérique

> **À retenir**
>
> - Le droit du numérique combine des textes nationaux (données, cybercriminalité, transactions et communications électroniques), le droit commun et le droit communautaire (OHADA, UEMOA, OAPI).
> - Chaque obligation se qualifie à partir de cinq éléments : l'entité qui agit, le service rendu, les personnes concernées, les données utilisées et les territoires impliqués.
> - Une stratégie nationale fixe une orientation ; ce sont les textes et décisions applicables qui créent des obligations.

Un cadre composé de plusieurs niveaux

Le droit du numérique ne se limite pas à une loi unique. Les textes nationaux sur les données, la cybercriminalité, les transactions et les communications électroniques se combinent avec le droit des

contrats, la consommation, le travail, la fiscalité et la propriété intellectuelle. La loi n° 2017-803 du 7 décembre 2017 d'orientation de la société de l'information fournit également un cadre général. [R12]

Le droit communautaire intervient notamment à travers l'OHADA pour la vie commerciale et la comptabilité, l'UMOA et l'UEMOA pour les services financiers, et l'OAPI pour la propriété intellectuelle. La Convention de Malabo complète l'environnement continental : la liste officielle de l'Union africaine mentionne pour la Côte d'Ivoire une adhésion ou ratification le 8 mars 2023 et un dépôt le 3 avril 2023. Ces instruments doivent être lus selon leurs conditions d'application et leur articulation avec le droit interne. [R13, R14, R26, R29, R34]

Une loi peut être complétée par un décret, un arrêté, une décision du régulateur ou un cahier des charges. Une stratégie nationale fixe une orientation publique ; elle ne doit pas être traitée comme un catalogue autonome d'obligations sanctionnées. Une certification volontaire peut, quant à elle, devenir une exigence contractuelle dans un appel d'offres.

Déterminer le périmètre de chaque obligation

Le raisonnement doit partir de cinq éléments : l'entité qui agit, le service rendu, les personnes concernées, les données utilisées et les territoires impliqués. La localisation du siège ne résout pas à elle seule les questions de territorialité. Des prestations rendues depuis l'étranger à des clients ivoiriens peuvent notamment relever de règles fiscales locales. [R21 à R23]

Recommandation : établir une fiche de qualification par produit. Elle décrit le parcours client, les contrats, les paiements, les prestataires, les lieux d'hébergement et les autorités concernées. Une qualification doit être revue lorsqu'une fonctionnalité transforme l'activité, par exemple lorsqu'un site de petites annonces commence à encaisser des fonds pour ses vendeurs.

Les erreurs de méthode à éviter

Une autorisation de traitement de données ne vaut pas agrément pour fournir un service financier. Un contrat cloud ne dispense pas de vérifier les transferts de données. Une inscription fiscale n'autorise pas l'exploitation d'un réseau. Une déclaration de plateforme ne couvre pas nécessairement tous les services qui y sont proposés.

Les documents de conformité doivent porter une date, un périmètre et un responsable. Il est utile de distinguer le texte applicable, l'analyse de l'entreprise et la preuve d'exécution. Le simple rangement d'une loi dans un dossier ne démontre pas que les obligations correspondantes sont respectées.

2 Identifier les autorités compétentes

> **À retenir**
>
> - L'ARTCI intervient à la fois comme régulateur des communications électroniques et comme Autorité de protection des données personnelles.
> - L'ANSSI, créée en 2024, est compétente pour la cybersécurité et l'organisation des audits réglementaires.
> - DGI, BCEAO, CENTIF, OAPI et HACA interviennent selon l'activité : chaque démarche a son interlocuteur et son objet.

ARTCI et protection des données

L'Autorité de Régulation des Télécommunications et des TIC de Côte d'Ivoire intervient dans les communications électroniques. Elle assure également les missions d'Autorité de protection des données dans le cadre de la loi n° 2013-450. Les démarches de protection des données et les formalités de communications électroniques répondent à des objets distincts. [R01, R02, R10, R11]

Recommandation : conserver un dossier de correspondance par démarche. L'entreprise y range le formulaire transmis, les annexes, la preuve de dépôt, les demandes de complément, le récépissé ou l'autorisation et les éventuelles réserves. Un accusé de dépôt ne doit pas être confondu avec un titre autorisant la mise en œuvre lorsque celui-ci est requis.

ANSSI et sécurité des systèmes

L'Agence Nationale de la Sécurité des Systèmes d'Information intervient dans la cybersécurité et l'organisation des audits réglementaires. Le décret n° 2024-958 du 30 octobre 2024 porte création de l'agence. L'ordonnance n° 2024-950 du même jour a notamment abrogé l'article 50 de la loi sur les transactions électroniques qui attribuait des missions de sécurité et de certification à l'ARTCI. Les anciennes pages institutionnelles doivent donc être confrontées aux textes et indications opérationnelles actuels. [R07, R08, R09]

Une entreprise doit vérifier que le prestataire retenu pour un audit réglementaire dispose de l'agrément pertinent. Une prestation commerciale de test d'intrusion n'équivaut pas automatiquement à l'audit réglementaire. [R09]

Autorités fiscales, financières et sectorielles

La DGI pilote les règles fiscales, les déclarations et le dispositif FNE. La BCEAO encadre les services de paiement dans l'UMOA. La CENTIF intervient dans la lutte contre le blanchiment pour les personnes et activités assujetties. L'OAPI et les organismes nationaux compétents interviennent pour la propriété intellectuelle. La HACA encadre la communication audiovisuelle, y compris dans les conditions de son extension aux supports numériques. [R18, R26, R28, R29, R32]

Les autorités judiciaires et les services d'enquête compétents peuvent demander la communication ou la conservation de données selon les procédures applicables. La réponse doit être organisée sans divulgation excessive ni destruction des preuves. [R04]

Situation	Interlocuteur principal	Objet de la démarche
Création ou modification d'un traitement de données personnelles	ARTCI agissant comme Autorité de protection	Déclaration, autorisation et mise à jour
Exploitation d'une plateforme ou d'un service de communications	ARTCI	Qualification et titre sectoriel
Audit réglementaire et sécurité	ANSSI et PASSI agréé	Périmètre d'audit et certification éventuelle
Facturation et taxation numérique	DGI	FNE, RNE, TVA et impôts applicables
Service de paiement	BCEAO et autorités financières compétentes	Agrément, enregistrement et contrôle
Soupçon financier chez un assujetti	CENTIF	Déclaration et obligations de vigilance
Contenus audiovisuels	HACA	Qualification et obligations de l'éditeur

3 Protéger les données personnelles

> **À retenir**
>
> - Tout fichier de clients, de salariés ou de prospects constitue un traitement de données personnelles.
> - Le principe est la déclaration préalable auprès de l'ARTCI ; certains traitements, notamment biométriques, médicaux ou impliquant un transfert hors CEDEAO, exigent une autorisation.
> - L'entreprise doit pouvoir répondre aux demandes des personnes et prouver sa conformité dans la durée.

Reconnaître un traitement de données

Un nom, une adresse électronique nominative, une image, un numéro d'identification ou une information de santé peuvent être des données personnelles. La collecte, la consultation, la transmission, l'archivage et la suppression constituent des opérations de traitement. Le responsable du traitement détermine les finalités et les moyens ; le sous-traitant agit pour son compte. [R01, R02]

L'entreprise doit appliquer des finalités déterminées, une collecte proportionnée, une durée adaptée et des mesures de sécurité. L'information des personnes et l'exercice de leurs droits font partie du fonctionnement du traitement. Le consentement n'est pas à utiliser comme justification universelle : la licéité doit être appréciée au regard de la situation et de la loi. [R02]

L'article 14 de la loi n° 2013-450 pose le consentement exprès préalable comme principe. Il prévoit, pour un responsable dûment autorisé, des dérogations de nécessité liées notamment à une obligation légale, une mission d'intérêt public, un contrat ou des mesures précontractuelles demandées, ainsi qu'à la sauvegarde des droits et intérêts fondamentaux de la personne. La justification doit être rattachée au traitement précis. [R01]

Recommandation : commencer l'inventaire par les fichiers RH, la paie, le recrutement, le CRM, les comptes clients, les enregistrements d'appels, les caméras et les outils de prospection. Pour chacun, décrire l'objectif réel avant de lister les données. Une collecte « au cas où » est difficile à justifier.

Déclaration, autorisation et dispenses

L'article 5 de la loi n° 2013-450 pose le principe de la déclaration préalable. Les articles 6 et 8 prévoient des dispenses ou simplifications. L'article 7 soumet certains traitements à autorisation préalable, notamment ceux comportant des données biométriques, certaines données médicales et les transferts vers un pays tiers. Les autres catégories visées par cet article doivent également être examinées. [R01]

Le décret n° 2015-79 du 4 février 2015 précise les modalités des déclarations et demandes d'autorisation. Les informations du dossier comprennent notamment l'identité du responsable, les finalités, les données, les personnes concernées, les destinataires, la conservation, la sécurité et les sous-traitants ou transferts envisagés. [R03]

Recommandation : établir une fiche de décision par traitement avec trois rubriques : formalité retenue, justification et référence du titre obtenu. Toute dispense doit être documentée. La désignation d'un correspondant ne doit pas être interprétée comme une dispense générale de toutes les autorisations.

Organiser les droits des personnes

Les droits comprennent notamment l'information, l'accès, l'opposition, la rectification et, dans les conditions prévues, l'effacement. Une obligation légale de conservation peut justifier le maintien de

certaines données malgré une demande de suppression. L'entreprise doit expliquer la réponse et distinguer les données encore nécessaires de celles qui peuvent être effacées. [R02]

Recommandation : ouvrir un canal clairement indiqué dans les notices. Chaque demande reçoit un identifiant, une date, une vérification d'identité proportionnée, une recherche dans les systèmes concernés et une réponse conservée. La vérification d'identité ne doit pas conduire à collecter systématiquement une pièce complète lorsque cela n'est pas nécessaire.

La procédure interne doit associer l'équipe métier, le service juridique et les prestataires concernés. Le client ne devrait pas être renvoyé indéfiniment du responsable vers l'hébergeur. Le contrat du prestataire doit prévoir l'assistance nécessaire pour retrouver, extraire, rectifier et supprimer les informations.

Correspondant et responsabilité interne

L'Autorité de protection décrit les missions du correspondant, son indépendance et la notification de sa désignation. Elle mentionne également la tenue d'une liste des traitements et un rapport annuel. Les conditions de désignation et le profil doivent être examinés avec les textes applicables et les exigences de l'Autorité. [R02]

Recommandation : formaliser une lettre de mission, un accès aux décideurs, des moyens de travail et une procédure d'alerte. Le correspondant conseille et suit la conformité ; la direction demeure responsable des choix et des ressources. Une fonction affichée sans accès aux projets, aux contrats et aux incidents ne permet pas de piloter les risques.

Prouver la conformité dans la durée

Un dossier utile contient l'inventaire, les décisions de formalité, les notices, les contrats, les habilitations, les durées de conservation, les preuves de formation et les demandes des personnes. Le traitement doit être réexaminé en cas de nouvelle finalité, de nouveau destinataire, de transfert ou de modification substantielle.

Exemple d'application : avant de relier un logiciel RH à un outil d'analyse de productivité, l'entreprise doit réexaminer les objectifs, la proportionnalité, les accès, l'information des salariés et les formalités. L'existence d'un traitement RH régulier ne valide pas automatiquement cette nouvelle utilisation.

4 Encadrer la biométrie, la vidéosurveillance et le cloud

> **À retenir**
>
> - La biométrie, comme le pointage par empreinte, exige une autorisation préalable de l'ARTCI.
> - Une caméra qui permet d'identifier des personnes est un traitement de données à part entière.
> - Le recours au cloud impose de localiser serveurs, sauvegardes et accès, et d'encadrer les transferts hors CEDEAO.

Les dispositifs de contrôle des personnes

Les traitements biométriques nécessitent une autorisation préalable de l'ARTCI. Une solution de pointage proposée par un fournisseur ne peut donc pas être déployée sur la seule base d'un devis et du consentement des salariés. Il faut examiner la nécessité du dispositif et les modalités de collecte, de stockage et d'accès. [R02]

Recommandation : comparer le dispositif avec des moyens moins intrusifs, tels qu'un badge, avant de décider. Documenter les raisons du choix, les personnes concernées, les données effectivement conservées, les destinataires et la procédure de suppression au départ du salarié. Le fournisseur doit préciser si les données brutes ou des gabarits biométriques sont stockés.

Une caméra doit être analysée comme un traitement de données dès lors qu'elle permet d'identifier des personnes. L'entreprise doit préparer l'information des visiteurs et salariés, limiter les accès et justifier la couverture et la durée de conservation au regard de sa finalité. [R01, R02]

Recommandation : tenir un plan des caméras et un registre des extractions. Les zones filmées, les horaires et les droits de consultation doivent être validés avant l'installation. Un changement d'usage, par exemple le passage de la sécurité des locaux au suivi individuel permanent, appelle une nouvelle analyse.

Hébergement et transferts internationaux

La loi définit le pays tiers par référence aux États non membres de la CEDEAO et prévoit un encadrement des transferts, notamment à son article 7. Une solution cloud implique de localiser les serveurs, sauvegardes, équipes d'assistance et sous-traitants susceptibles d'accéder aux données. [R01]

La qualification doit porter sur le flux réel, y compris l'administration à distance depuis l'étranger. La présence d'une interface commerciale en Côte d'Ivoire ne prouve pas que toutes les données y sont traitées. Un contrat type de fournisseur international ne remplace pas la formalité ivoirienne applicable.

Recommandation : demander une liste des pays de traitement, la chaîne de sous-traitance et une procédure de notification des changements. Avant toute migration, examiner l'autorisation requise et la cohérence avec les engagements envers les clients. Une obligation générale d'hébergement exclusivement local ne doit pas être présumée : toute restriction de localisation doit être rattachée à un texte, un secteur ou un contrat précis.

Clauses et contrôles du fournisseur

Le contrat devrait préciser les instructions, la confidentialité, la sécurité, l'assistance aux demandes, la gestion des incidents, la réversibilité et le sort des sauvegardes. Il doit permettre de vérifier les engagements sans exiger des accès incompatibles avec la sécurité des autres clients.

Recommandation : distinguer la restitution des données et leur effacement. La restitution nécessite un format exploitable, un délai, une assistance et un coût. L'effacement doit couvrir les copies actives et prévoir le traitement des sauvegardes selon un cycle documenté. Un test de sortie réalisé avant la fin du contrat permet de vérifier que l'entreprise peut continuer son activité.

5 Organiser la cybersécurité et les audits

> **À retenir**
>
> - Les entreprises établies sur le territoire national font l'objet d'un audit réglementaire de sécurité selon un cycle de trois ans, réalisé par un PASSI agréé.
> - Le référentiel de l'ANSSI (RGSSI) compte 107 critères et trois niveaux, selon l'exposition et la sensibilité des données.
> - Les mesures de base (comptes individuels, authentification multifacteur, mises à jour, sauvegardes testées) doivent être vérifiables.

Le socle juridique

La loi n° 2013-451 du 19 juin 2013, modifiée notamment par la loi n° 2023-593 du 7 juin 2023, incrimine les atteintes aux systèmes et données. Les obligations de sécurité des données personnelles découlent aussi du cadre de protection des données. Il faut distinguer la sanction d'un attaquant, le manquement de l'entreprise à une obligation de sécurité et sa responsabilité contractuelle envers ses clients. [R01, R04, R06]

Le décret n° 2021-916 du 22 décembre 2021 adopte le Référentiel général de sécurité des systèmes d'information et le Plan de protection des infrastructures critiques. Le décret n° 2021-917 définit les procédures d'audit, de contrôle et de certification. Les exigences applicables doivent être rattachées à la version du référentiel et au périmètre effectivement retenu. [R08]

Audit réglementaire et prestataire agréé

L'ANSSI rappelle une périodicité de trois ans pour les organismes publics et entreprises privées établis sur le territoire national. L'audit réglementaire est réalisé par un PASSI agréé. Un audit volontaire ou un test technique ne le remplace pas nécessairement. L'entreprise doit vérifier le statut du prestataire et le périmètre couvert avant de signer. [R09]

L'article 4 du décret n° 2021-917 prévoit aussi un audit périodique obligatoire dix-huit mois après l'obtention du certificat. Le calendrier ne doit donc pas être réduit à un rendez-vous tous les trois ans. Les articles 11 et 13 organisent notamment la transmission du rapport sous dix jours ouvrés après la clôture et, en cas de rejet, la réalisation d'un nouvel audit par un autre PASSI sous trois mois. Les modalités pratiques sont à articuler avec les compétences actuelles de l'ANSSI. [R44]

Recommandation : préparer un cahier des charges qui identifie les systèmes, applications, sites, filiales, accès distants et prestations externalisées. Définir les règles de test, les autorisations, la protection des données et les conditions d'arrêt pour éviter une interruption de production.

Le rapport doit donner lieu à un plan de correction, avec un propriétaire, une priorité et une preuve de clôture pour chaque constat. Les vulnérabilités critiques ne doivent pas attendre le prochain cycle réglementaire. Un contrôle de la correction est particulièrement utile lorsque le défaut affecte l'authentification, les sauvegardes ou l'exposition d'une base de données.

Niveaux du référentiel révisé

Le RGSSI publié par l'ANSSI comporte 107 critères répartis en 16 domaines et trois niveaux. Le niveau 1 concerne des structures à faible exposition ; le niveau 2 vise les organismes traitant des données sensibles ou personnelles ; le niveau 3 concerne les données d'intérêt vital pour la nation. Chaque critère indique les niveaux auxquels il s'applique. La classification doit être documentée pour établir une grille d'audit cohérente. [R43]

La section B14 prévoit notamment, pour les niveaux désignés dans ses tableaux, un plan de réponse et des mécanismes d'alerte. Pour le niveau 3, elle prévoit une déclaration immédiate des incidents à l'ANSSI et la transmission de relevés techniques avec conservation minimale de six mois. Ces exigences spécifiques ne doivent pas être étendues indistinctement à tous les niveaux. [R43]

Mesures de sécurité recommandées

Les mesures ci-dessous constituent une base opérationnelle à ajuster aux risques et exigences applicables :

- Recenser les actifs et attribuer un responsable aux applications et données critiques.

- Utiliser des comptes individuels, limiter les privilèges et renforcer les accès sensibles par une authentification multifacteur.
- Maintenir les équipements et logiciels à jour et organiser le traitement des vulnérabilités.
- Séparer les environnements, protéger les accès d'administration et surveiller les événements utiles.
- Effectuer des sauvegardes protégées, conserver une copie suffisamment isolée et tester la restauration.
- Former les utilisateurs, notamment aux fraudes au changement de coordonnées bancaires et à l'hameçonnage.

Chaque mesure doit être proportionnée et vérifiable. Une politique annonçant des sauvegardes quotidiennes a peu de valeur si aucune restauration n'a été testée. Un compte d'administrateur partagé empêche d'attribuer les actions et rend les départs de personnel difficiles à sécuriser.

Continuité et responsabilité de la direction

Recommandation : définir les services qui doivent être rétablis en priorité, le temps d'interruption acceptable et la perte de données maximale supportable. Ces objectifs doivent être confrontés aux capacités réelles du fournisseur et aux résultats des exercices.

La direction doit arbitrer les risques résiduels. Un risque accepté doit être décrit, limité dans le temps et assorti d'un responsable. Une dérogation technique ne doit pas devenir une exonération implicite et permanente des obligations légales ou contractuelles.

6 Réagir aux incidents et conserver les preuves

> **À retenir**
>
> - En cas d'incident : contenir, préserver les preuves, puis évaluer les personnes et services touchés.
> - Les délais de notification se déterminent à partir des textes ivoiriens, du secteur et des contrats.
> - La remise en service suppose la correction de la cause et la vérification des accès.

Déclencher une réponse coordonnée

Une fuite de données, un rançongiciel, une compromission de messagerie et une fraude au paiement appellent des décisions rapides, mais différentes. L'objectif initial est de contenir l'incident, préserver les preuves, évaluer les personnes et services touchés et déterminer les obligations de communication.

Recommandation : constituer une cellule associant la direction, l'informatique, le juridique, le correspondant données, les finances et la communication selon le cas. Tenir une chronologie factuelle avec les décisions, les personnes consultées et les mesures prises. Distinguer ce qui est établi des hypothèses.

Le délai de notification de 72 heures prévu par le RGPD européen ne s'applique pas, en tant que tel, à toute entreprise ivoirienne. Les destinataires, délais et contenus doivent être déterminés à partir des textes ivoiriens, du secteur, des contrats et, le cas échéant, des règles étrangères réellement applicables.

Préserver des éléments utilisables

La loi sur la cybercriminalité prévoit des mécanismes de conservation, communication et collecte des données dans les enquêtes. Les articles 73 et suivants doivent être distingués de la conservation habituelle des journaux. Une demande de conservation peut imposer de protéger les données aussi longtemps que nécessaire pour la procédure concernée. [R04]

Recommandation : préserver les journaux pertinents, les courriels complets, les paramètres, les traces d'accès et les éléments de facturation. Décrire leur origine, la date de collecte, la personne qui les a extraits et les transferts successifs. Une capture d'écran isolée peut aider à comprendre un fait, mais ne remplace pas toujours les fichiers et métadonnées d'origine.

Les opérations de restauration ou de nettoyage doivent être coordonnées avec la préservation. Avant de réinstaller un poste compromis, déterminer quelles traces doivent être conservées. Les investigations doivent rester autorisées et proportionnées ; une entreprise ne doit pas tenter d'entrer sans droit dans le système d'un tiers pour récupérer des données.

Répondre aux autorités et aux partenaires

Recommandation : prévoir une procédure de vérification des réquisitions et demandes officielles, de leur périmètre et du canal de transmission. La réponse doit être tracée et limitée aux données demandées dans le cadre légal. Les demandes urgentes ne dispensent pas d'identifier l'auteur et le fondement.

Les contrats devraient imposer au prestataire une alerte assez rapide pour permettre à l'entreprise d'agir. Une clause doit préciser le contenu initial, les compléments, la conservation des preuves et l'assistance. Le délai contractuel convenu doit être identifié comme tel et distingué d'un délai légal.

Retour à la normale

Recommandation : conditionner la remise en service à la correction de la cause, la vérification des accès et la restauration contrôlée. Prévoir un suivi de la fraude et des comptes exposés. Le retour d'expérience doit déboucher sur des actions datées et sur la mise à jour des procédures, plutôt que sur un simple compte rendu.

7 Vendre et contracter en ligne

> **À retenir**
>
> - La loi n° 2013-546 impose d'identifier clairement le vendeur et d'afficher un prix complet.
> - La commande en ligne suit des étapes : conditions accessibles, vérification et correction de la commande, accusé de réception.
> - Pour la vente à distance, le consommateur dispose de dix jours ouvrables après la livraison pour retourner le produit.

Identifier le vendeur et informer le client

La loi n° 2013-546 encadre le commerce électronique. Ses articles 5 et 6 imposent notamment des informations accessibles sur l'identité du professionnel et une présentation claire du prix, précisant si taxes et livraison sont incluses. Les informations varient selon le statut, l'immatriculation et la réglementation de l'activité. [R05]

La loi n° 2016-412 du 15 juin 2016 relative à la consommation complète ce dispositif pour les relations entrant dans son champ. Une vente réalisée par messagerie ou réseau social ne perd pas sa nature commerciale du seul fait qu'elle ne passe pas par un site marchand classique. [R15]

Recommandation : préparer une fiche produit compréhensible indiquant les caractéristiques, le prix total, les conditions de livraison, les restrictions, les garanties et le traitement des réclamations. Les

informations importantes doivent être visibles avant l'engagement et cohérentes avec le message publicitaire.

Organiser la commande et son acceptation

Les articles 21 et 22 de la loi sur les transactions électroniques organisent notamment la mise à disposition des conditions contractuelles, la possibilité de vérifier la commande et corriger les erreurs, puis l'accusé de réception. Certaines règles connaissent des aménagements pour des échanges exclusivement entre professionnels. [R05]

Recommandation : conserver la version des conditions acceptées, la date, l'identification du compte, le contenu de la commande, son prix et les confirmations. La case d'acceptation des conditions de vente doit être distincte du choix de recevoir des publicités. Toute modification ultérieure des conditions doit rester traçable.

Exemple d'application : si un client conteste un abonnement, l'entreprise doit pouvoir produire l'offre affichée au jour de la souscription, le choix de durée, les modalités de renouvellement et la preuve de l'acceptation. Une copie des conditions actuelles ne démontre pas ce qui a été accepté plusieurs mois auparavant.

Garanties, rétractation et réclamations

L'article 11 de la loi n° 2016-412 prévoit, pour les opérations visées de vente à distance ou hors établissement, un délai de dix jours ouvrables à compter de la livraison pour retourner un produit au vendeur, en vue d'un échange ou remboursement, sans pénalités autres que les frais de retour. L'article 12 porte ce délai à trois mois si les informations d'identification qu'il exige n'ont pas été fournies, avec un mécanisme de retour au délai de dix jours lorsque l'information intervient pendant cette période. [R15]

Les articles 16 à 18 prévoient un régime distinct pour le démarchage, notamment la renonciation et la confirmation écrite après certaines sollicitations par téléphone ou messagerie électronique. Il faut qualifier le parcours de vente avant de fixer les conditions ; les règles sur le retour d'un produit ne doivent pas être transposées sans analyse à toute prestation de services. [R15]

Recommandation : adopter une procédure de réclamation décrivant les interlocuteurs, les justificatifs raisonnables, le retour, le remplacement, le remboursement et la preuve de règlement. Les délais commerciaux promis doivent être réalistes et suivis. Les conditions de vente ne doivent pas annoncer une exclusion générale de responsabilité sans examen de sa validité.

Cas des places de marché

Recommandation : identifier clairement qui vend, qui facture, qui encaisse, qui livre et qui traite le remboursement. L'opérateur doit expliquer son rôle aux utilisateurs et aligner les contrats vendeurs, les conditions clients et les flux financiers. Une présentation qui laisse croire que la plateforme vend elle-même peut créer un risque différent de celui d'un simple hébergement d'annonces.

Avant l'ouverture à des vendeurs tiers, vérifier la déclaration sectorielle de plateforme, les obligations liées aux contenus, les données personnelles, les commissions et l'éventuelle fourniture de services de paiement. Ces examens sont cumulatifs. [R04, R11, R26]

8 Encadrer la prospection et les traceurs

> **À retenir**
>
> - La prospection électronique vers une personne physique requiert son consentement préalable, sauf exception encadrée pour des clients existants.
> - Chaque message doit permettre de demander l'arrêt des envois.
> - Cookies et pixels peuvent constituer des traitements de données : ils doivent être recensés et maîtrisés.

Consentement et exception pour certains courriels

L'article 14 de la loi sur les transactions électroniques pose le principe du consentement préalable pour la prospection électronique utilisant les coordonnées d'une personne physique. Il prévoit une exception pour certains courriels, lorsque les coordonnées ont été recueillies directement et en connaissance de cause auprès de clients ou abonnés, pour des produits ou services analogues. L'article 15 impose des coordonnées permettant de demander l'arrêt des communications. [R05]

La loi de protection des données reconnaît aussi un droit d'opposition à la prospection. La loi sur la cybercriminalité comporte des incriminations relatives à la prospection et aux envois illicites. La mise en œuvre d'une exception doit donc être documentée et appréciée avec l'ensemble de ces dispositions. [R02, R04]

Recommandation : recueillir un choix explicite lorsqu'il est requis, conserver le texte présenté et la preuve du choix, puis synchroniser les oppositions entre les outils. L'achat d'un fichier ne démontre pas que les destinataires ont accepté les messages de l'entreprise. Le contrat du vendeur du fichier doit être contrôlé, mais ses garanties ne remplacent pas la vérification de la licéité.

Fichiers de suppression et prestataires marketing

Recommandation : tenir une liste d'opposition limitée aux données nécessaires pour éviter la réinscription accidentelle. Définir son accès et son usage. La suppression de tout historique sans conserver les moyens de respecter une opposition peut conduire à solliciter à nouveau la personne.

Les campagnes confiées à une agence doivent prévoir les instructions, la source des contacts, les listes d'opposition, les sous-traitants et le contrôle des envois. Les données ne devraient pas être réutilisées pour les campagnes d'autres clients sans examen juridique distinct.

Cookies, pixels et suivi publicitaire

Un identifiant de terminal ou un suivi en ligne peut entrer dans le champ des données personnelles selon les possibilités d'identification. La finalité, les destinataires, l'information et les formalités doivent être examinés. L'installation d'un bandeau inspiré d'un autre pays ne prouve pas, à elle seule, la conformité ivoirienne. [R01, R02]

Recommandation : recenser les traceurs techniques, statistiques et publicitaires ; vérifier leur déclenchement réel et les transferts qu'ils produisent. Prévoir une gestion compréhensible des choix et un moyen de les modifier. Les recommandations européennes ou les exigences des fournisseurs peuvent être utiles, mais leur statut doit être distingué d'une obligation locale.

9 Sécuriser la signature et les archives électroniques

À retenir

- L'écrit électronique est reconnu lorsque l'identité de l'auteur et l'intégrité du document sont garanties.
- Une image de signature collée dans un fichier n'offre pas les garanties d'une signature électronique fiable.
- Les documents électroniques se conservent en principe dix ans, dans des conditions d'accessibilité et d'intégrité.

Valeur juridique et fiabilité

La loi sur les transactions électroniques reconnaît l'écrit électronique sous conditions. L'identité de l'auteur et l'intégrité de l'écrit sont déterminantes. Les règles relatives à la signature supposent un procédé fiable et un lien avec l'acte ; une image de signature collée dans un fichier ne fournit pas nécessairement les garanties recherchées. [R05]

Le décret n° 2014-106 du 12 mars 2014 précise les conditions d'établissement et de conservation de l'écrit et de la signature électroniques. Le décret n° 2016-851 du 19 octobre 2016 porte sur l'archivage électronique. Ces textes doivent guider le choix d'une solution et la définition de la preuve attendue. [R16]

Recommandation : distinguer les actes selon leur enjeu. Pour une opération importante, vérifier les pouvoirs du signataire, l'authentification, l'intégrité, l'horodatage, les certificats utilisés, les traces et la possibilité de produire le dossier de preuve longtemps après la signature.

Conservation et accessibilité

L'article 40 de la loi n° 2013-546 prévoit une conservation électronique de dix ans, sous réserve des dispositions légales prévoyant un délai plus court, avec des conditions d'accessibilité et d'intégrité. Les exigences comptables OHADA doivent également être prises en compte pour les livres et pièces justificatives. [R05, R14]

Recommandation : construire une grille par catégorie documentaire. Définir l'événement de départ, la durée, le support, les accès, la destruction et la suspension en cas de contentieux. Les archives doivent rester lisibles malgré les changements de logiciels et de formats. La sauvegarde destinée à restaurer un système et l'archive destinée à conserver une preuve remplissent des fonctions différentes.

Choisir et quitter un prestataire de confiance

Recommandation : vérifier le statut du service, les conditions de certification et la capacité de validation future. Tester l'export d'un dossier signé avec ses preuves, sans dépendre exclusivement d'un lien temporaire dans le portail du fournisseur. Prévoir le sort des certificats expirés et la disponibilité des éléments nécessaires à la vérification.

L'entreprise doit décider qui peut engager une dépense, approuver un contrat et signer. Une authentification technique correcte ne remplace pas le pouvoir juridique. La matrice de délégation et l'administration des comptes de signature doivent être réconciliées lors des changements de fonction et des départs.

10 Exploiter une plateforme ou un service de communications

À retenir

- La loi n° 2024-352 distingue licence individuelle, autorisation générale, déclaration et régime libre.
- L'exploitation d'une plateforme de services numériques suppose un récépissé de déclaration préalable délivré par l'ARTCI.
- Réseaux radio, objets connectés et fréquences exigent une qualification avant tout déploiement.

Les régimes de la loi de 2024

La loi n° 2024-352 du 6 juin 2024 relative aux communications électroniques modernise le cadre sectoriel. Elle distingue notamment licence individuelle, autorisation générale, déclaration et régime libre. Le titre applicable dépend des activités, du réseau et des ressources utilisées. Une entreprise doit aussi examiner les obligations de son titre et de son cahier des charges. [R10]

Le régime d'autorisation générale vise notamment certaines activités de réseaux et services sans assignation de fréquences, des infrastructures d'accueil et des réseaux radioélectriques indépendants privés, sous réserve des exceptions prévues par la loi. La qualification technique doit donc précéder le choix du dossier administratif. [R10]

Plateformes numériques

Le communiqué de l'ARTCI du 4 avril 2025 rappelle l'exigence d'un récépissé préalable de déclaration pour l'établissement et l'exploitation d'une plateforme de services numériques. Il rappelle une définition large, fondée sur l'accès à des contenus, services et applications par les canaux de communication électronique, et avait fixé une échéance de régularisation au 30 avril 2025. [R11]

Recommandation : décrire à l'ARTCI le service précis plutôt que demander une validation abstraite du mot « application ». Mentionner les utilisateurs, la facturation, la connectivité, les partenaires, les contenus et la zone de fourniture. Le dossier doit refléter l'exploitation réelle et être revu si les fonctionnalités changent.

Réseaux privés, équipements et ressources

Recommandation : avant de déployer un réseau radio, des objets connectés ou une infrastructure de communications, vérifier les fréquences, l'équipement, les droits d'installation et le régime applicable. L'achat d'un matériel sur internet ne prouve pas qu'il peut être utilisé dans les mêmes conditions en Côte d'Ivoire.

Les activités de simple utilisation d'un service et celles de fourniture au public doivent être distinguées. Les projets multisites, Wi-Fi public, connectivité embarquée ou revente de capacité méritent une qualification spécifique. Le coût du titre, sa durée et les redevances doivent être intégrés au modèle économique après confirmation du régime.

Dossier permanent sectoriel

Recommandation : tenir un dossier contenant le titre, le cahier des charges, les redevances, les déclarations périodiques exigées, les incidents, les réclamations et les échanges avec le régulateur. Toute opération de cession ou de restructuration doit être examinée au regard des conditions de transfert du titre.

11 Héberger des contenus et communiquer au public

À retenir

- Les obligations dépendent du rôle effectivement joué : éditeur, hébergeur, plateforme ou fournisseur.
- Certaines données d'identification doivent être conservées trois ans (contributeurs) ou dix ans (abonnés).
- Une activité audiovisuelle en ligne relève du cadre de la HACA.

Responsabilités des intermédiaires

La loi sur la cybercriminalité organise des règles pour les personnes qu'elle vise comme prestataires techniques. Les obligations dépendent du rôle effectivement joué. L'article 53 prévoit trois ans pour les données permettant d'identifier les contributeurs à des contenus ; l'article 72 prévoit dix ans pour les données relatives aux abonnés des fournisseurs de services. Ces catégories ne se confondent pas avec toutes les données de trafic. [R04]

Recommandation : dresser une carte des rôles de l'entreprise : éditeur de ses propres contenus, hébergeur de contributions, opérateur de plateforme, vendeur ou fournisseur de communication. Les conditions d'utilisation et la procédure de traitement des signalements doivent correspondre à cette carte.

Modération et signalements

Recommandation : prévoir un canal de signalement, une qualification, une escalade et une conservation adaptée des éléments. Les décisions de retrait, de restriction ou de maintien doivent être motivées en interne. La procédure doit permettre de réagir aux contenus manifestement illicites et aux demandes judiciaires sans organiser une collecte illimitée de données.

Les contenus exposent à des risques distincts : atteinte à la réputation, haine, fraude, violation de droits d'auteur, divulgation de données ou publicité trompeuse. L'équipe chargée de la modération doit savoir quand transmettre un cas au juridique et quand préserver une preuve avant modification.

Audiovisuel, presse et réseaux sociaux

La loi n° 2017-868 du 27 décembre 2017 sur la communication audiovisuelle, modifiée par la loi n° 2022-979 du 20 décembre 2022, doit être examinée pour les services et contenus entrant dans son champ. La HACA présente cette évolution dans son répertoire. Une activité éditoriale audiovisuelle appelle donc une analyse distincte de la simple présence commerciale sur un réseau social. [R32]

La HACA a présenté une Charte des réseaux sociaux en octobre 2023. Ses principes peuvent orienter la politique éditoriale, mais leur portée doit être distinguée des dispositions législatives et réglementaires qui fondent les obligations et sanctions. [R33]

Recommandation : encadrer les prises de parole officielles, les partenariats d'influence, la validation des publicités, les droits sur les images et les réponses aux crises. Les créateurs externes doivent recevoir des instructions sur les droits, la transparence commerciale et l'usage des données.

12 Appliquer la fiscalité du numérique

À retenir

- Les factures et reçus normalisés électroniques (FNE, RNE) sont obligatoires, sous réserve des dispenses prévues.
- Les services numériques consommés en Côte d'Ivoire sont soumis à la TVA de 18 %, avec une immatriculation simplifiée pour les opérateurs non résidents.
- Depuis 2026, certaines plateformes étrangères réalisant au moins 50 millions FCFA de chiffre d'affaires avec des clients ivoiriens relèvent d'un régime d'imposition spécifique.

FNE, RNE et champ des dispenses

L'annexe fiscale 2025 a institué l'obligation de délivrance de factures et reçus normalisés électroniques. L'arrêté n° 0337 du 9 mai 2025 précise les modalités de mise en œuvre. La DGI distingue la génération directe, l'interfaçage par API et les terminaux d'émission de reçus normalisés électroniques. [R17, R18, R20]

La règle doit être lue avec les dispenses de l'article 145 du Livre de procédures fiscales. La DGI cite notamment les banques, assurances, pharmacies et certaines opérations de carburant et transport. Une dispense peut dépendre de l'opération ; elle ne doit pas être étendue sans analyse à toutes les prestations d'un même opérateur. [R18]

La FAQ officielle distingue aussi les loyers d'immeubles nus, les locations meublées, les commissions d'agences et les ventes de billets d'avion. Elle précise que les redevables de la taxe communale de l'entreprenant ne sont pas encore pris en charge. L'entreprise doit vérifier la version de ces précisions au moment de son inscription. [R18]

Organiser le circuit de facturation

Recommandation : cartographier les ventes, acomptes, avoirs, remises et remboursements. Définir le responsable de l'émission, le contrôle des identifiants clients, la séparation des droits, les rapprochements et l'archivage. Les intégrations API doivent être testées avec des cas normaux et des annulations, en tenant compte des communiqués DGI en vigueur.

La fin du système de facture normalisée physique a fait l'objet de communiqués successifs, notamment en décembre 2025 et janvier 2026. Elle ne signifie pas qu'une FNE ne peut jamais être imprimée. La facture doit être générée et certifiée selon le dispositif applicable. [R19, R20]

Le communiqué DGI de janvier 2026 précise que les FNE sont admises pour justifier les charges et déduire la TVA grevant les acquisitions concernées. Il rappelle l'accompagnement des tickets des magasins à rayons multiples par des RNE et lie l'inscription à la délivrance de l'attestation de régularité fiscale. Ces prescriptions doivent être articulées avec les dispenses légales. [R39]

Recommandation : vérifier les factures fournisseurs avant comptabilisation et traiter les anomalies. Les risques de rejet de justificatif, de rappel de TVA ou de pénalités doivent être appréciés selon la règle fiscale et l'irrégularité exacte. Les conséquences d'une non-conformité ne sont pas uniformes : elles dépendent de la règle en cause et de la nature de l'irrégularité.

TVA et prestations numériques internationales

Le dispositif issu notamment de l'article 7 de l'annexe fiscale 2022 encadre la TVA de services et commissions de plateformes en ligne. La contribution officielle ivoirienne à la CNUCED en 2026 décrit l'application du taux de 18 % à des services numériques consommés en Côte d'Ivoire et le mécanisme d'immatriculation simplifiée des opérateurs non résidents. [R21]

Recommandation : distinguer les ventes propres, commissions, abonnements, publicité et prestations cloud. Pour un achat étranger, examiner la territorialité, la facture, la TVA et les retenues éventuelles avec le responsable fiscal. L'absence d'établissement local du fournisseur ne suffit pas à conclure à une absence d'impôt.

Imposition de certaines plateformes étrangères en 2026

L'article 33 de l'annexe fiscale 2026 vise certaines plateformes sans installation professionnelle en Côte d'Ivoire réalisant un chiffre d'affaires annuel TTC d'au moins 50 millions de francs CFA dans leurs relations avec les clients ivoiriens. Les plateformes disposant d'une installation locale relèvent du traitement de droit commun décrit par la DGI. [R22]

La DGI indique un bénéfice forfaitaire de 10 % du chiffre d'affaires, imposé à 30 %, soit une charge correspondant à 3 % du chiffre d'affaires avant les ajustements prévus. Elle précise l'imputation de certaines retenues de l'article 92 du CGI, sans création de crédit. Ce régime doit être distingué de la TVA et examiné avec les conventions fiscales applicables. [R23]

Recommandation : suivre séparément les revenus ivoiriens, les critères de localisation, les retenues supportées et les déclarations. L'équipe financière doit disposer d'une analyse écrite du champ et des échéances. Les taux cités sont ceux du dispositif documenté pour 2026 et doivent être revus lors de chaque nouvelle loi de finances.

13 Fournir des paiements et des services financiers numériques

> **À retenir**
>
> - La fourniture de services de paiement est encadrée par l'instruction BCEAO n° 001-01-2024.
> - Depuis le 1er septembre 2025, seules les structures agréées peuvent fournir des services de paiement dans l'UMOA.
> - Encaisser des fonds pour des tiers n'a pas le même régime qu'encaisser le prix de ses propres ventes.

Identifier une activité réglementée

L'instruction BCEAO n° 001-01-2024 du 23 janvier 2024 fixe les conditions de fourniture des services de paiement dans l'UMOA. Le périmètre comprend notamment des opérations sur comptes, transferts, acquisition, initiation de paiement et information sur comptes. Les régimes d'agrément ou d'enregistrement doivent être qualifiés selon les services. [R26]

Une entreprise qui accepte un paiement pour ses propres ventes n'occupe pas nécessairement la même position que celle qui encaisse, conserve ou transfère des fonds pour des tiers. Une architecture dans laquelle un prestataire agréé reçoit les fonds doit être examinée à partir des contrats et flux réels, pas seulement du vocabulaire commercial utilisé.

L'instruction prévoit aussi des limites aux activités des établissements de paiement. Le lancement d'un portefeuille, d'une collecte pour compte de tiers ou d'un service d'agrégation doit donc être précédé

d'une analyse sectorielle. La réglementation de la monnaie électronique et, le cas échéant, du crédit doit être examinée séparément. [R26]

Conditions de lancement et partenariat

La BCEAO a prorogé la période de mise en conformité jusqu'au 31 août 2025 par l'avis n° 006-05-2025 du 27 mai 2025. Cet avis précise qu'à compter du 1er septembre 2025 seules les structures agréées sont autorisées à fournir des services de paiement dans l'Union. La vérification du titre et de son périmètre doit donc précéder le lancement. [R27]

Recommandation : obtenir le titre du partenaire, son périmètre de services et les éventuelles conditions d'externalisation. Répartir les responsabilités sur l'identification, les fonds, les remboursements, les fraudes, les réclamations, les incidents et les données. Une convention commerciale ne peut pas autoriser une activité qui exige un titre réglementaire absent.

Vigilance et lutte contre le blanchiment

L'ordonnance n° 2023-875 du 23 novembre 2023 constitue une référence majeure du dispositif LBC/FT/FP. Les obligations de vigilance, d'identification et de déclaration doivent être appréciées selon l'assujettissement et le rôle de l'entreprise. La CENTIF publie les textes et instruments de supervision correspondants. [R28]

Recommandation : lorsque l'entreprise est assujettie, organiser la connaissance du client, l'identification des bénéficiaires effectifs, l'analyse des opérations, la gestion des alertes et la confidentialité des déclarations. Les seuils et procédures doivent être repris des textes applicables, sans copier ceux d'une autre juridiction.

Actifs numériques, crédit et investissement

Un service fondé sur des jetons, de la crypto, du financement participatif, une promesse de rendement ou du crédit ne doit pas être assimilé à une simple plateforme informatique. La présence d'une définition d'actif virtuel dans un texte de lutte contre le blanchiment ne vaut pas autorisation commerciale générale. [R28]

Recommandation : faire examiner les flux, les droits promis, la conservation, les clients visés et les autorités compétentes avant toute commercialisation. La communication commerciale doit rester cohérente avec le statut et les autorisations effectivement obtenus.

14 Protéger les logiciels, les marques et les contenus

> **À retenir**
>
> - Logiciel, marque, nom de domaine et base de données se protègent chacun selon des règles propres (loi n° 2016-555, Accord de Bangui).
> - Le paiement d'un développement ne vaut pas cession des droits : le contrat doit la prévoir.
> - Un registre des marques, domaines et licences prévient pertes de droits et litiges.

Le cadre de propriété intellectuelle

La loi n° 2016-555 du 26 juillet 2016 relative au droit d'auteur et aux droits voisins constitue une référence nationale. L'Accord de Bangui révisé en 2015 organise notamment les marques, brevets, noms

commerciaux, droits d'auteur et concurrence déloyale dans l'espace OAPI. La protection à rechercher dépend de l'objet et des conditions de chaque droit. [R29, R30]

Un nom de domaine, une marque, un logiciel, une base de données et une idée commerciale ne se protègent pas de la même manière. Le dépôt d'un nom de domaine n'accorde pas, à lui seul, tous les droits de marque. La documentation NIC CI expose les règles de nommage et de gestion du domaine national. [R31]

Sécuriser la chaîne des droits

Recommandation : identifier les auteurs et contributeurs, les contrats de travail ou de prestation, les composants acquis et les licences. Pour un développement externe, préciser les droits transmis, les usages, le territoire, la durée, la documentation, les codes sources et les éléments exclus. Le paiement d'une facture ne doit pas être considéré comme une cession universelle et implicite.

L'entreprise doit distinguer ce qu'elle possède de ce qu'elle utilise sous licence. Les photographies, musiques, polices, cartes et modèles peuvent comporter des conditions propres. Les licences libres imposent elles aussi des obligations variables selon leur texte et les modalités de distribution.

Registre des actifs et prévention des litiges

Recommandation : tenir un registre des marques, domaines, dépôts, contrats de cession, licences et dates de renouvellement. Vérifier les droits avant de choisir un nom ou de lancer une publicité. Les accès au bureau d'enregistrement du domaine doivent appartenir à l'entreprise ou être placés sous son contrôle contractuel.

Pour les logiciels, conserver un inventaire des dépendances et des preuves de licence. Les livraisons doivent être accompagnées d'une documentation permettant de maintenir et faire évoluer l'application. Les clauses de garantie doivent prévoir le traitement d'une réclamation de tiers et la continuité d'usage lorsqu'un composant est contesté.

15 Encadrer les contrats informatiques et les achats

> **À retenir**
>
> - Un contrat informatique doit décrire des livrables et des engagements vérifiables.
> - Disponibilité, support, sécurité, sous-traitants et pays d'hébergement font partie des clauses à négocier.
> - La réversibilité se prépare dès la signature et se teste avant la fin du contrat.

Définir le résultat attendu

Un contrat de développement, d'intégration, de maintenance, d'infogérance ou de service SaaS présente des risques différents. Le contrat doit traduire l'activité, les données et les dépendances. Les obligations légales de données, de sécurité, de signature et de fiscalité s'y ajoutent selon le projet. [R01, R05, R08, R17]

Recommandation : décrire les livrables, interfaces, utilisateurs, performances, langues, documentation et critères de réception. Une promesse générale de « solution conforme » doit être remplacée par un périmètre et des engagements vérifiables. La recette doit préciser qui teste, sur quelles données et comment les réserves sont traitées.

Négocier les clauses sensibles

Recommandation : distinguer les engagements de disponibilité, les heures de support et les délais de résolution. Prévoir les maintenances, les exclusions, le calcul des indicateurs et les conséquences d'un défaut récurrent. Un avoir commercial ne couvre pas nécessairement toutes les conséquences d'une interruption.

Le contrat devrait également traiter la sécurité, les sous-traitants, les pays d'hébergement, les audits, la propriété intellectuelle, les sauvegardes, les incidents et les demandes d'autorités. Les plafonds de responsabilité doivent être appréciés selon les risques et les règles impératives. Leur formulation ne doit pas laisser penser qu'ils effacent les pouvoirs du régulateur.

Réversibilité et dépendance au prestataire

Recommandation : prévoir un plan de sortie dès le début. Il décrit les formats, l'assistance, les délais, les coûts, la restitution des comptes, les domaines, les clés, les configurations et la documentation. Tester l'export d'un échantillon avant d'accumuler plusieurs années de données.

Pour une application critique développée sur mesure, examiner l'accès au code, les droits de maintenance et les conditions d'un éventuel séquestre. L'entreprise doit pouvoir identifier les dépendances indispensables à la reprise ; disposer du code sans les bibliothèques, secrets et procédures de déploiement peut être insuffisant.

Conflits de documents et preuve

Recommandation : fixer un ordre de priorité entre contrat, cahier des charges, conditions générales, bon de commande et annexes. Les engagements publiés sur un site peuvent évoluer ; conserver les versions acceptées. Définir le droit applicable, le mode de règlement des différends et les possibilités de mesures urgentes avec un examen de leur validité.

Les procédures de modification doivent rester simples et traçables. Un changement qui affecte les données, les pays de traitement, les paiements ou le périmètre réglementé doit déclencher une revue juridique, même s'il semble mineur sur le plan technique.

16 Gérer les usages numériques des salariés

> **À retenir**
>
> - Recrutement, paie, évaluations et contrôle d'accès sont des traitements de données personnelles.
> - Les outils de surveillance des salariés doivent être justifiés et proportionnés.
> - Une charte informatique encadre accès, outils (y compris l'IA), travail à distance et départs.

Données RH et moyens de contrôle

Le recrutement, la paie, les évaluations et le contrôle d'accès relèvent de la protection des données. Le Code du travail demeure applicable aux relations professionnelles. La dématérialisation d'un outil n'écarte pas les règles sur l'emploi et la preuve. [R01, R02, R35]

Recommandation : publier une information adaptée aux salariés et candidats. Limiter les habilitations RH, séparer les informations médicales des dossiers courants et documenter les durées par catégorie. Les

fichiers conservés sur les postes individuels doivent être intégrés à la cartographie et aux règles de suppression.

Les outils de surveillance doivent être justifiés et proportionnés. L'entreprise devrait préciser les usages autorisés de la messagerie, du réseau et des équipements, ainsi que les contrôles possibles. Le contrôle d'un salarié ne doit pas devenir un accès sans limite à ses données et communications.

Charte informatique et travail à distance

Recommandation : adopter une charte lisible et l'articuler avec les règles internes applicables. Elle doit couvrir les mots de passe, les accès distants, les logiciels, les périphériques, les données confidentielles, les outils d'IA, les incidents et le départ de l'entreprise. Les modalités d'adoption et de communication doivent être examinées au regard du droit du travail.

Pour le travail à distance, préciser l'équipement, la sécurité de connexion, l'assistance, les documents papier, les conditions d'accès et la conduite à tenir en cas de perte. Les appareils personnels demandent une séparation des données et une procédure de restitution ou d'effacement compatible avec les droits du salarié.

Entrées, mobilités et départs

Recommandation : lier les habilitations à la fonction et faire valider les accès sensibles. Une mobilité doit entraîner une revue des anciens droits. Le départ doit couvrir les comptes, sessions, appareils, badges, certificats, boîtes partagées, transferts de dossiers et données détenues localement.

Un départ ne justifie pas l'effacement immédiat de toutes les traces. Les obligations de conservation et besoins de preuve doivent être distingués de l'accès opérationnel. Le Code du travail prévoit notamment des règles propres au registre d'employeur, avec possibilité de fichier électronique fiable et à jour pour certains fascicules et conservation pendant cinq ans après la dernière mention. [R35]

17 Utiliser les avantages des startups et développer de nouveaux usages

> **À retenir**
>
> - Le label startup numérique, prévu par la loi n° 2023-901, est attribué par arrêté pour une durée de cinq ans au plus.
> - L'annexe fiscale 2026 précise les exonérations ouvertes aux startups labellisées, à examiner impôt par impôt.
> - Les usages d'IA doivent être inventoriés, et une supervision humaine maintenue pour les décisions importantes.

Label startup numérique

La loi n° 2023-901 du 23 novembre 2023 pose plusieurs conditions : société de droit ivoirien, capital majoritairement national, innovation, maturité du projet, potentiel de croissance et ressources ou accompagnement adaptés. Le label est attribué par arrêté ministériel après avis du Comité. Le pré-label et le label répondent à des conditions distinctes. [R36]

La validité du label ne peut excéder cinq ans. La loi prévoit des mesures d'accompagnement et des sanctions en cas de manquement, dont suspension, retrait et remboursement de certains avantages.

L'obtention du label ne dispense pas des règles sur les données, les communications, les paiements ou la fiscalité de l'activité. [R36]

Avantages fiscaux précisés en 2026

L'article 35 de l'annexe fiscale 2026 prévoit notamment des exonérations d'impôt sur les bénéfices ou d'imposition forfaitaire selon le régime, de taxe sur les opérations bancaires et d'impôt sur le revenu des créances. La DGI vise les startups labellisées situées hors de la ZBTIC et précise les conditions et modalités de calcul des trois années d'avantages. [R24, R25]

La présentation générale renvoie au 1er janvier suivant l'année de labellisation, tandis que les commentaires DGI détaillent l'application par impôt, notamment les exercices clos après la labellisation pour les BIC et une période de paiements pour l'impôt des microentreprises et la TEE. Le dossier fiscal doit donc être établi impôt par impôt. [R25]

Recommandation : conserver l'arrêté, la date d'obtention, le régime fiscal, la localisation, les déclarations et l'analyse des périodes. Ne pas budgéter une exonération générale de TVA, de douane ou de charges sociales sur la seule base du mot « label ». Les avantages doivent être rattachés à leurs textes et conditions.

Intelligence artificielle et gouvernance des données

Le Gouvernement a présenté le 13 mars 2025 les stratégies nationales d'intelligence artificielle et de gouvernance des données. Ces orientations doivent être distinguées des obligations existantes de protection des données, de confidentialité, de consommation et de propriété intellectuelle. [R37]

Recommandation : inventorier les usages d'IA, les données envoyées, les fournisseurs, les pays de traitement et les décisions produites. Interdire les usages non autorisés de secrets ou données sensibles, vérifier les conditions du service et conserver une supervision humaine pour les décisions ayant un effet important sur une personne.

Un outil d'IA ne doit pas être utilisé comme preuve de conformité à lui seul. Pour un recrutement, une tarification ou une analyse de fraude, l'entreprise devrait documenter les critères, tester les erreurs et prévoir une contestation. Les résultats doivent être vérifiés avant publication ou engagement contractuel.

Projets sectoriels et commande publique

Les projets de santé, transport, éducation, assurance ou services publics nécessitent un complément de qualification sectorielle. Les décrets de 2021 relatifs aux projets publics numériques et à la sécurité de l'administration sont particulièrement pertinents pour un fournisseur de l'État. [R08]

Recommandation : dans un appel d'offres, identifier les exigences d'hébergement, d'interopérabilité, de sécurité, de droits intellectuels et de transfert de compétences. Une préférence ou mesure de soutien aux startups ne garantit pas l'attribution d'un marché et ne supprime pas les conditions de la consultation.

18 Piloter les risques, les contrôles et les recours

À retenir

- Un même manquement peut entraîner des conséquences administratives, fiscales, civiles et pénales.
- L'Autorité de protection peut prononcer avertissements, mises en demeure, interdictions de traitement et sanctions pécuniaires.
- Une veille régulière des sources officielles permet d'anticiper les évolutions.

Distinguer les responsabilités

Une même situation peut produire une sanction administrative, une conséquence fiscale, une responsabilité civile et une procédure pénale. L'entreprise doit distinguer le manquement, la personne concernée, le pouvoir de l'autorité et les voies de contestation. Une clause de sous-traitance ne transfère pas mécaniquement toutes les obligations légales au fournisseur.

L'Autorité de protection dispose notamment de mesures d'avertissement, de mise en demeure, d'interruption ou d'interdiction de traitement, de retrait d'autorisation et de sanctions pécuniaires, dans les conditions du cadre applicable. Les montants et règles de réitération doivent être appréciés selon le texte et la situation. [R38]

Le document institutionnel ARTCI cité en R38 rappelle un plafond de sanction pécuniaire de 10 millions de francs CFA. Pour un manquement réitéré dans les cinq ans suivant une sanction devenue définitive, il mentionne 100 millions de francs CFA ou, pour une entreprise, 5 % du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 500 millions. La gravité, les avantages tirés du manquement et les conditions procédurales doivent être pris en compte. Ce plafond ne constitue pas une amende automatique pour chaque irrégularité. [R38]

Les risques ne sont pas seulement financiers. Une suspension de service, un retrait de titre, une perte de preuve ou une impossibilité de restaurer les données peut compromettre la continuité. Le registre des risques doit donc associer conformité et fonctionnement de l'entreprise.

Préparer un contrôle

Recommandation : désigner un coordinateur, identifier le fondement et le périmètre de la demande, préserver les documents et organiser une réponse cohérente. Les pièces doivent être datées et décrites ; les explications doivent distinguer le fonctionnement passé, la situation actuelle et les corrections engagées.

Ne jamais reconstituer de preuves fictives ou antidatées. Une lacune doit être constatée, expliquée et corrigée avec une date réelle. La coopération et les droits procéduraux doivent être exercés ensemble. Les délais de réponse et de recours figurant dans les actes reçus doivent être suivis immédiatement par la fonction compétente.

Gouvernance et indicateurs

Recommandation : réunir périodiquement les responsables métiers, informatique, juridique, finance et RH. Le suivi doit porter sur des éléments concrets : formalités en attente, titres à renouveler, demandes de personnes, incidents, correctifs d'audit, factures irrégulières et contrats sans clauses essentielles.

Les indicateurs doivent mesurer une action. Le nombre de politiques rédigées ne démontre pas que les accès sont retirés lors des départs. Un taux de corrections clôturées doit être fondé sur des vérifications. Les risques acceptés et les exceptions doivent avoir une échéance de réexamen.

Veille et mise à jour

Recommandation : attribuer une fréquence de consultation aux sources officielles, avec priorité aux lois de finances, communiqués DGI, décisions ARTCI, référentiels ANSSI et textes BCEAO. Enregistrer la date, le changement et son effet sur l'entreprise. Toute évolution importante doit être traduite en tâche, responsable et preuve attendue.

Le dispositif de conformité de l'entreprise doit être revu après une réforme, un changement d'activité, une acquisition ou un incident majeur. Le périmètre des activités et les versions des textes sont aussi importants que la date du document.

19 Examiner les obligations connexes et internationales

> **À retenir**
>
> - Une réglementation étrangère, comme le RGPD, peut s'appliquer à une entreprise qui cible ou suit des personnes situées dans l'Union européenne.
> - Les équipements électroniques relèvent aussi de règles sur l'importation et le traitement des déchets.
> - Données de mineurs, de santé ou de géolocalisation appellent une analyse spécifique.

Activités transfrontalières

Une entreprise ivoirienne peut devoir examiner une réglementation étrangère en raison de ses établissements, de son offre ou du suivi des utilisateurs. L'article 3 du RGPD prévoit notamment des critères liés à l'offre de biens ou services à des personnes se trouvant dans l'Union européenne ou au suivi de leur comportement. La simple accessibilité mondiale d'un site ne suffit pas à résoudre cette qualification. [R40]

Recommandation : distinguer l'obligation légale étrangère directement applicable des engagements contractuels pris envers un client étranger. Les mécanismes de transfert demandés par ce client doivent être examinés avec les formalités ivoiriennes. Une même prestation peut nécessiter deux analyses complémentaires.

Équipements et déchets électroniques

Le numérique comporte aussi une dimension matérielle. Le décret n° 2017-217 du 5 avril 2017 organise la gestion écologiquement rationnelle des déchets d'équipements électriques et électroniques. Les Douanes rappellent le dispositif de vérification et d'éco-redevance pour des équipements importés. Le Code de l'environnement issu de la loi n° 2023-900 du 23 novembre 2023 complète le cadre à examiner selon l'activité. [R41, R42]

Recommandation : intégrer les achats, importations, réemplois et mises au rebut au cycle de gestion du parc. Vérifier les obligations du producteur ou importateur, la filière de collecte et les autorisations du prestataire. Avant toute cession de disque, téléphone ou serveur, prévoir l'effacement sécurisé ou la destruction adaptée des supports et une preuve de l'opération.

Données de mineurs et activités spécialisées

Les services destinés aux enfants, les dossiers médicaux, la géolocalisation, les assurances et les transports appellent une analyse adaptée des personnes, des finalités et des règles du secteur. Les limites d'âge ou procédures de consentement d'un autre pays ne doivent pas être utilisées automatiquement comme règle ivoirienne. Le cadre général de protection des données reste à articuler avec ces exigences. [R01, R02]

Recommandation : déclencher une revue spécialisée lorsque le produit change la manière d'identifier une personne, d'évaluer un risque, de prêter, de diagnostiquer, de diffuser un programme ou de transporter un client. Vérifier aussi les règles de concurrence, de publicité, de douane et les autorisations professionnelles pertinentes avant de stabiliser le modèle économique.

20 Accomplir les démarches numériques auprès de l'État

À retenir

- L'ordonnance n° 2017-500 ouvre la saisine électronique de l'administration, mais impose le canal dédié lorsqu'il existe.
- Principaux téléservices : 225invest, IDU, e-Impôts, FNE, e-CNPS, GUCE et SIGOMAP.
- Depuis le 1er novembre 2023, l'inscription sur SIGOMAP est nécessaire pour participer aux marchés publics.
- Pour chaque démarche, conserver la preuve de dépôt, la quittance de paiement et la décision.

Portée du cadre de l'administration électronique

La relation numérique entre une entreprise et l'État, souvent désignée par B2G, couvre notamment la création, l'identification, les déclarations, les paiements, les autorisations et les marchés publics. Il faut distinguer l'objectif de dématérialisation, les obligations fixées par les textes et le parcours effectivement ouvert sur chaque plateforme. L'existence d'un portail ne signifie pas que toutes les démarches s'effectuent intégralement en ligne.

L'ordonnance n° 2017-500 du 2 août 2017 relative aux échanges électroniques entre les usagers et les autorités administratives encadre les e-services publics, la sécurité, l'interopérabilité et la saisine électronique. Elle doit être lue avec ses modifications, notamment l'ordonnance n° 2018-641 du 1er août 2018 concernant son article 5 et l'ordonnance n° 2024-950 du 30 octobre 2024 concernant les compétences institutionnelles. [R45, R59, R07]

L'article 23 permet à l'usager identifié de saisir électroniquement une autorité dotée d'un e-service. L'article 24 prévoit le traitement d'une saisine régulière sans en exiger la répétition sous une autre forme. Toutefois, l'article 27 impose le canal dédié lorsqu'il existe et prévoit des modalités, des voies alternatives pour un motif légitime et des exclusions possibles pour certaines démarches. Le droit de saisine n'équivaut donc pas à une liberté de choisir n'importe quel canal pour toute formalité. [R45]

La reconnaissance des écrits et signatures s'articule avec la loi n° 2013-546 et les exigences du service concerné. Le document transmis doit satisfaire aux conditions d'identité, d'intégrité et de signature applicables. Une copie scannée ne devient pas automatiquement un original électronique ou un acte valablement signé du seul fait de son téléversement. [R05, R16]

Recommandation : avant une première démarche, relever le fondement, le canal, les pièces, les pouvoirs du déclarant, les frais, les modalités de signature et la preuve de réception. La fiche doit distinguer les

opérations réalisables en ligne de celles qui nécessitent encore une vérification, une présence ou un document complémentaire.

Création d'entreprise et identification unique

L'ordonnance n° 2015-181 du 24 mars 2015 et son décret d'application n° 2015-286 du 29 avril 2015 constituent des références pour l'utilisation de procédés électroniques dans la création d'entreprises. Leur intitulé et le cadre présenté par le CEPICI ne permettent pas d'en déduire une obligation générale de procéder exclusivement en ligne à toutes les opérations du cycle de vie de toute société. Les modifications, radiations et autorisations doivent être qualifiées selon leurs procédures propres. [R46]

Le portail 225invest présente les services à l'investissement et les accès liés aux démarches de l'entreprise. Les délais de traitement annoncés pour une formalité doivent être appréciés selon la forme juridique, la complétude, les pièces et les validations requises. Le délai de 48 heures annoncé pour la création en ligne d'une SARL ou d'une SA est un objectif de service ; il ne constitue pas une garantie légale applicable à tous les dossiers. [R50]

L'identifiant unique est institué par l'ordonnance n° 2015-182 du 24 mars 2015, complétée par le décret n° 2015-287 du 29 avril 2015. L'ordonnance n° 2018-644 du 1er août 2018 modifie l'article 1 ; sa ratification figure dans la loi n° 2019-873 du 14 octobre 2019. L'IDU vise une identification harmonisée des entreprises auprès des administrations. [R47, R60]

Les communications institutionnelles appellent une lecture attentive. La fiche Service Public décrit une substitution aux numéros de création, tandis que la communication de juillet 2025 sur l'annuaire IDU précise qu'il complète les références existantes, notamment NCC et CNPS. Dans tous les cas, l'identification commune ne supprime pas les obligations d'immatriculation, de déclaration ou d'autorisation propres à chaque régime. L'entreprise doit conserver ses références sectorielles et utiliser celles exigées par chaque téléservice. [R47, R49]

Le portail idu.ci présente une procédure de demande destinée aux entreprises existant avant le 1er octobre 2018, avec création d'un accès et production de pièces. L'attribution n'est donc pas automatique pour toutes les entreprises, quelle que soit leur date de création. L'IDU n'est pas davantage, à lui seul, une preuve d'activation des comptes des autres administrations. [R48]

Recommandation : tenir une fiche d'identité administrative réunissant dénomination, siège, RCCM, IDU, NCC, référence employeur CNPS et code importateur ou exportateur lorsqu'il est applicable. Après un changement de dénomination, de dirigeant ou de siège, vérifier chaque dossier concerné au lieu de présumer une propagation instantanée dans tous les systèmes.

Répertoire des principaux accès officiels

Le tableau ci-dessous indique les points d'entrée et leur usage principal. Les liens opérationnels et références sont précisés immédiatement après le tableau. Les fonctionnalités accessibles dépendent de l'activation du compte, des habilitations et des modules effectivement ouverts.

Domaine	Portail	Usage principal et vigilance
Création et investissement	225invest et CEPICI	Accéder aux services et parcours de création selon la procédure
Identification harmonisée	IDU	Demander ou suivre l'identifiant selon la catégorie d'entreprise
Fiscalité	e-Impôts Côte d'Ivoire	Télédéclarer, télépayer et retrouver les documents fiscaux

Domaine	Portail	Usage principal et vigilance
Facturation	Portail FNE de la DGI	Émettre FNE ou RNE selon le dispositif et les dispenses
Protection sociale	e-CNPS	Déclarer les salariés et les cotisations, et suivre son compte
Commerce extérieur	GUCE	Préparer et suivre les formalités des modules applicables
Dédouanement	SYDAM World et outils Douanes	Traiter les opérations douanières selon le rôle de l'utilisateur
Information administrative	Service Public	Identifier une démarche et le téléservice lorsqu'il existe
Marchés publics	SIGOMAP	S'inscrire, consulter les avis et suivre le parcours de candidature

Création et identification : www.225invest.ci ; www.idu.ci. L'activation de ces accès ne remplace pas une validation sectorielle. [R48, R50]

Fiscalité : www.e-impots.gouv.ci ; www.fne.dgi.gouv.ci. Il convient de vérifier l'adresse du portail ivoirien, distinct des sites homonymes d'autres administrations fiscales. La FNE dispose de son portail et de modalités d'accès ou d'interfaçage propres. [R51, R17, R20]

Protection sociale et information administrative : e.cnps.ci ; servicepublic.gouv.ci. Le portail Service Public fournit des fiches d'information et, pour les procédures dématérialisées, une orientation vers le service disponible. Une fiche informative ne prouve pas que l'intégralité du parcours est réalisable en ligne. [R52]

Commerce extérieur : guce.gouv.ci, avec les outils et procédures indiqués par les Douanes. Le GUCE centralise des échanges et modules ; SYDAM World couvre notamment déclaration douanière, liquidation et recouvrement. L'entreprise doit identifier les interventions du commissionnaire agréé et les autres contrôles ou plateformes nécessaires. [R53, R54]

Marchés publics : sigomap.gouv.ci. La DGMP indique que l'inscription est nécessaire depuis le 1er novembre 2023 pour participer aux opérations de marchés publics. Il faut suivre les conditions de la consultation, le canal de dépôt et les instructions en vigueur, puis conserver la preuve de soumission. La création d'un compte ne vaut ni recevabilité d'une offre ni attribution. [R58]

Déclarations, paiements et preuve de dépôt

Le compte e-Impôts permet la télédéclaration, le télépaiement et l'accès aux documents du dossier fiscal. La déclaration validée et le paiement exécuté sont des événements distincts. La référence bancaire, l'accusé de réception fiscal et la quittance doivent être rapprochés pour vérifier l'imputation à la bonne période et à la bonne obligation. [R51]

Le portail e-CNPS permet notamment les déclarations des salariés et cotisations et la consultation de l'historique du compte. La dématérialisation ne supprime pas l'obligation d'exactitude des données sociales et de mise à jour des mouvements du personnel. Le processus interne doit rester cohérent avec la paie et les règles sociales applicables. [R52, R35]

Recommandation : distinguer un brouillon, un dépôt, un accusé technique, une validation métier et une décision définitive. Télécharger les justificatifs avec leur référence et leur date. Pour une autorisation, vérifier le titre délivré et ses conditions plutôt que conclure à un accord à partir du seul message « demande enregistrée ».

Le décret n° 2024-272 du 8 mai 2024 porte généralisation de TrésorPay TrésorMoney et modalités de gestion. Ce développement du paiement électronique n'emporte ni la disparition de tous les timbres physiques, ni l'acceptation de tous les moyens de paiement pour chaque recette : le rapport du Trésor sur les collectivités, publié en 2026 au titre de 2024, traite encore des timbres municipaux sécurisés. [R56, R57]

Recommandation : utiliser le canal indiqué pour la recette, vérifier le bénéficiaire et conserver la quittance reconnue par le service. Un débit Mobile Money ou bancaire ne prouve pas à lui seul que la formalité a été validée. Les frais officiels doivent être séparés des honoraires d'un intermédiaire.

Interopérabilité et échanges avec les systèmes publics

Le référentiel ivoirien pertinent est adopté par le décret n° 2021-913 du 22 décembre 2021. Les articles 19 à 21 de l'ordonnance n° 2017-500 organisent les standards et la connexion des autorités administratives à la plateforme d'interopérabilité. Ce cadre régit les échanges avec les systèmes publics ; il ne constitue pas une obligation identique pour toute application privée. [R55, R45]

Pour un fournisseur ou partenaire qui se connecte à un système de l'État, le périmètre applicable découle du projet, du texte pertinent, du cahier des charges, de la convention et des exigences de sécurité. La qualification de fintech ne donne pas automatiquement un droit d'accès aux bases publiques ou aux interfaces de l'administration.

Recommandation : avant toute interconnexion, convenir des données autorisées, des finalités, des responsabilités, de l'authentification, des formats, des journaux, du traitement des incidents et des modalités de retrait des accès. La compatibilité technique ne remplace pas la licéité du partage de données ni les formalités de protection des données.

Les articles 25 et 26 organisent, dans les conditions qu'ils prévoient, l'absence de nouvelle production de certaines informations déjà détenues ou directement accessibles par des systèmes conformes. Leur application doit être vérifiée pour le service utilisé ; elle ne justifie pas de refuser indistinctement toute pièce demandée par une administration. [R45]

Contrôles internes recommandés pour les démarches B2G

L'entreprise devrait conserver un inventaire des comptes administratifs, avec le titulaire, les délégations, le responsable de validation et les moyens de récupération. Les comptes attachés à un prestataire ou à une adresse personnelle doivent être réexaminés pour garantir la continuité au changement d'interlocuteur.

Recommandation : faire vérifier les déclarations et paiements sensibles par une deuxième personne, rapprocher les pièces avec la comptabilité ou la paie, puis archiver le dossier complet. La traçabilité renforce le contrôle des frais et des décisions ; elle ne garantit pas à elle seule l'absence d'erreur, de fraude ou de corruption.

En cas d'indisponibilité, documenter l'heure, le service, le message, les tentatives et le ticket d'assistance. Rechercher la procédure de secours admise par l'autorité. Une panne ne suspend pas automatiquement un délai légal et une relance informelle ne remplace pas un recours ou une déclaration dans les formes exigées.

Recommandation : tester les accès avant une échéance importante, notamment une soumission à un marché public. À la clôture de la démarche, vérifier la décision, les éventuelles réserves, sa date d'effet et les obligations de renouvellement. Réintégrer ces informations dans le registre général de conformité de l'annexe C.

Annexe A Questionnaire de qualification

Questions à traiter avant un lancement

Ce questionnaire est un outil de travail recommandé. Toute réponse positive doit déclencher l'examen du chapitre correspondant et l'ouverture d'une action documentée. Une réponse négative doit être cohérente avec les contrats et le fonctionnement technique.

Question	Analyse à engager	Chapitre
Collectons-nous des données sur des clients, des salariés ou des visiteurs ?	Responsable du traitement, finalité et formalités	3
Utilisons-nous des empreintes, une reconnaissance faciale ou des données médicales ?	Autorisation et proportionnalité	3 et 4
Des personnes situées à l'étranger accèdent-elles aux données ?	Transferts et sous-traitance	4
Vendons-nous à distance à des consommateurs ?	Information, contrat, garanties et réclamations	7
Envoyons-nous des publicités par courriel, SMS ou messagerie ?	Consentement, exception et opposition	8
Permettons-nous à des tiers de publier ou de vendre ?	Plateforme, contenus et responsabilités	10 et 11
Recevons-nous des fonds pour des tiers ?	Services de paiement et flux financiers	13
Émettons-nous des factures ou des tickets ?	FNE, RNE, dispense et archivage	12
Exploitons-nous un réseau ou utilisons-nous des fréquences ?	Titre sectoriel et ressources	10
Faisons-nous signer des contrats électroniquement ?	Pouvoir, identité, intégrité et preuve	9
Développons-nous ou achetons-nous un logiciel ?	Droits intellectuels, recette et réversibilité	14 et 15
Utilisons-nous l'IA pour une décision sur une personne ?	Données, critères, contrôle et contestation	17
Avons-nous un audit réglementaire à jour ?	PASSI, périmètre et correction	5
Intervenons-nous pour un client public ou un secteur réglementé ?	Exigences sectorielles et contractuelles	17
Accomplissons-nous des démarches en ligne auprès de l'État ?	Comptes, délégations et preuves de dépôt	20
Nos équipes utilisent-elles des outils d'IA ?	Outils autorisés, données admissibles et supervision	17 et annexe J

Fiche de validation du projet

Recommandation : consigner le nom du projet, l'entité juridique, le propriétaire métier, la version, la date prévue de lancement, les activités réglementées, les traitements, les flux financiers et les dépendances. Joindre les avis, titres, contrats et résultats de tests nécessaires.

La décision devrait identifier les points bloquants, les actions restant ouvertes et les responsables. Une réserve interne ne peut pas autoriser le lancement d'une activité pour laquelle un titre préalable légalement requis manque.

Annexe B Plan de conformité sur 90 jours

Une organisation indicative

Le calendrier ci-dessous est une recommandation de conduite de projet. Il ne reporte aucune échéance légale déjà applicable. Les activités dépourvues d'un titre préalable requis doivent être traitées en priorité avec les responsables compétents.

Période	Travaux prioritaires	Résultat vérifiable
Jours 1 à 15	Désigner un pilote ; cartographier les activités, les données, les paiements et les prestataires	Périmètre validé, registre des risques et urgences
Jours 16 à 30	Qualifier les formalités (données et plateformes) ; contrôler la FNE et les titres financiers	Dossiers de formalités ouverts et anomalies fiscales traitées
Jours 31 à 45	Corriger les notices, les conditions de vente, les contrats fournisseurs et les habilitations	Versions publiées, preuves d'acceptation et accès revus
Jours 46 à 60	Préparer ou engager l'audit réglementaire ; sécuriser les sauvegardes et les accès sensibles	Commande conforme et tests de restauration documentés
Jours 61 à 75	Tester les droits des personnes, la gestion d'incident, la fraude et la sortie d'un fournisseur	Comptes rendus et actions correctives attribuées
Jours 76 à 90	Vérifier les preuves, clôturer les écarts prioritaires et organiser la veille	Revue de direction et programme annuel approuvés

Responsabilités proposées

La direction arbitre et finance. Le juridique qualifie les obligations, les titres et les contrats. Le correspondant données suit les traitements et droits. L'informatique et la sécurité mettent en œuvre les mesures techniques. Les finances contrôlent les flux, la FNE et les déclarations. Les métiers décrivent les usages et appliquent les procédures.

Recommandation : pour chaque action, retenir un responsable unique, même lorsque plusieurs services contribuent. La clôture doit reposer sur une preuve, pas seulement sur une déclaration d'avancement. Les écarts non résolus doivent rester visibles avec leur impact et leur date de décision.

Annexe C Registre des obligations et preuves

Structure du registre

Le registre ci-dessous est un modèle de pilotage recommandé. Il peut être tenu dans un outil partagé à accès contrôlé. Les lignes doivent être adaptées aux activités et aux textes applicables ; aucune liste générique ne dispense d’une qualification.

Obligation à qualifier	Responsable proposé	Preuve attendue
Formalités données personnelles	Juridique et correspondant	Déclaration, autorisation ou dispense documentée
Information des personnes	Métier et correspondant	Notice datée et preuve de diffusion
Demandes de droits	Correspondant et métier	Journal des demandes et réponses
Transfert international	Juridique et achats	Analyse et titre applicable avec contrat
Déclaration de plateforme	Juridique et direction	Récépissé et périmètre du service
Audit réglementaire	Direction et sécurité	Agrément du PASSI, rapport et plan de correction
Gestion des incidents	Sécurité et juridique	Chronologie, décisions et notifications requises
Vente électronique	Commercial et juridique	CGV versionnées et dossier de commande
Prospection	Marketing et correspondant	Source des contacts, choix et oppositions
Facturation	Finance	FNE, RNE ou justification de dispense
Service de paiement	Conformité financière	Titre partenaire et carte des flux
Propriété intellectuelle	Juridique et produit	Licences, cessions et dépôts
Réversibilité	Informatique et achats	Plan de sortie et test d’export
Label startup	Direction et finance	Arrêté et calcul des avantages par impôt

Ajouter pour chaque ligne : source, article, date de vérification, entité, système, échéance, niveau de risque, statut, emplacement de la preuve et date de prochaine revue. Lorsqu’un texte est modifié, conserver l’ancienne analyse et documenter le passage au nouveau régime.

Annexe D Inventaire des traitements et transferts

Champs recommandés

Chaque traitement devrait disposer d’une fiche comprenant les informations suivantes :

- Nom du traitement, entité responsable, propriétaire métier et contact du correspondant.
- Finalités précises, personnes concernées, catégories de données et justification de la licéité.
- Sources, destinataires, sous-traitants, systèmes et interconnexions.
- Formalité applicable, numéro, date et conditions du titre ou justification de dispense.
- Durées par catégorie, événement de départ, effacement et gestion des contentieux.
- Mesures de sécurité, habilitations, information et exercice des droits.

- Pays d’hébergement, de sauvegarde et d’accès distant, et analyse des transferts.
- Date de revue et changements depuis la version précédente.

Exemple de fiche pour une gestion de clients

Finalité proposée : gérer les commandes, la livraison, le service après-vente et les obligations de facturation. Les campagnes de prospection doivent être identifiées et examinées séparément lorsque leur finalité et leurs conditions diffèrent.

Données à décrire : identité et contacts nécessaires, commandes, factures, paiements référencés et réclamations. Le stockage des données sensibles de paiement doit être limité selon l’architecture retenue et les exigences applicables ; un commerçant peut privilégier un prestataire spécialisé plutôt que conserver lui-même ces éléments.

Destinataires à vérifier : service commercial, comptabilité, livraison, hébergeur, maintenance et prestataire de paiement. La fiche doit préciser les accès réels. La durée ne doit pas être une valeur uniforme recopiée pour les prospects, factures, tickets de support et comptes inactifs.

Ce modèle est une recommandation d’organisation. Les informations à déclarer et les formalités restent celles prévues par les textes et demandées par l’Autorité.

Annexe E Grille de conservation

Des durées liées à une catégorie et à un fondement

La grille doit articuler obligation de conservation, protection des données et besoin de preuve. Un litige ou une injonction peut suspendre une destruction habituelle. Les durées légales et les durées internes recommandées doivent apparaître dans des colonnes distinctes.

Catégorie	Repère juridique	Application pratique
Documents électroniques relevant de l’article 40	Dix ans, sous réserve des dispositions légales prévoyant un délai plus court	Vérifier la catégorie, l’intégrité et le point de départ
Livres et pièces comptables	Dix ans selon le cadre comptable OHADA	Préserver la lisibilité, l’ordre et les justificatifs
Données d’identification des contributeurs visées par l’article 53	Trois ans pour les prestataires concernés	Limiter au périmètre légalement visé
Données relatives aux abonnés visées par l’article 72	Dix ans pour les fournisseurs concernés	Distinguer abonnés, trafic et contenu
Registre d’employeur	Cinq ans après la dernière mention selon le Code du travail	Appliquer au registre et aux fascicules concernés
Prospects, candidatures, images et comptes clients	Durée à déterminer selon finalité et règles applicables	Justifier, documenter, purger et réexaminer
Données visées par une conservation judiciaire	Selon la mesure et les besoins de la procédure	Geler la destruction sur un périmètre défini

Références : [R04, R05, R14, R35]. Ces repères ne constituent pas une autorisation de conserver toutes les données personnelles pendant dix ans.

Procédure de destruction recommandée

Définir la liste des données arrivées à échéance, vérifier les gels contentieux, obtenir une validation, exécuter la suppression et conserver une trace minimale de l'opération. Le traitement des copies, exports et sauvegardes doit être documenté. Une donnée masquée dans l'interface peut rester accessible dans la base ou les exports.

Annexe F Grille de revue des contrats numériques

Clause	Question de contrôle	Pièce utile
Objet et périmètre	Les fonctionnalités et exclusions sont-elles vérifiables ?	Cahier des charges et inventaire
Recette	Les tests, réserves et conditions d'acceptation sont-ils définis ?	Plan et procès-verbal de recette
Disponibilité	Le calcul, les maintenances et les conséquences sont-ils précis ?	Annexe de niveaux de service
Données	Les rôles, instructions, destinataires et pays sont-ils connus ?	Annexe de traitement et transferts
Sécurité	Les mesures, audits et responsabilités sont-ils attribués ?	Annexe de sécurité et rapports
Incident	L'alerte permet-elle de respecter les obligations applicables ?	Procédure et contacts à jour
Propriété intellectuelle	L'entreprise peut-elle exploiter, maintenir et faire évoluer la solution ?	Cession, licence et liste des composants
Facturation	Prix, taxes, avoirs et justificatifs sont-ils cohérents ?	Annexe financière et FNE
Responsabilité	Plafonds, exclusions et assurances couvrent-ils les risques ?	Contrat et attestations
Réversibilité	Les données et accès peuvent-ils être récupérés utilement ?	Plan de sortie et test d'export
Résiliation	Les motifs, délais et effets sont-ils compréhensibles ?	Conditions de fin et assistance
Différends	Droit applicable, règlement et urgence sont-ils examinés ?	Clause validée juridiquement

Cette grille est une recommandation de négociation. Une clause doit être adaptée au type de contrat, aux parties, au secteur et aux règles impératives.

Annexe G Cas pratiques

PME de distribution avec boutique en ligne

L'entreprise possède une boutique physique, un site marchand et un fichier clients. Elle utilise une agence marketing, un hébergeur étranger et un prestataire de paiement. Le chantier doit couvrir les données, les

transferts, le contrat consommateur, la prospection, les factures, les contrats fournisseurs et la qualification éventuelle de plateforme.

Recommandation : commencer par une commande test complète. Vérifier l’offre, le prix, la confirmation, l’acceptation, la facture, la livraison, la réclamation et la suppression du compte. Comparer ce parcours aux documents publiés. Cet exercice révèle souvent des différences entre les conditions écrites et les opérations.

Entreprise de services avec pointage biométrique

Le pointage par empreinte nécessite une analyse et une autorisation préalable. Le fournisseur doit expliquer les données conservées, les accès, les transferts et les modalités de suppression. L’information des salariés et l’articulation avec le droit du travail doivent être préparées.

Recommandation : évaluer une solution de badge, limiter les données, séparer le pointage du dossier médical et prévoir le départ du salarié. Le responsable RH doit pouvoir expliquer le besoin et produire le dossier de formalité, pas seulement la fiche technique du matériel.

Place de marché encaissant pour ses vendeurs

La plateforme met en relation des vendeurs et acheteurs et retient une commission avant reversement. La déclaration de plateforme, les conditions vendeurs et clients, les données, la modération et les flux de paiement doivent être examinés ensemble. La conservation de fonds pour des tiers peut soulever une question de réglementation financière.

Recommandation : produire un schéma des flux où chaque compte et chaque titulaire sont identifiés. Faire qualifier l’activité avant le lancement et s’appuyer sur un partenaire autorisé dans un cadre réellement conforme. Éviter que les conditions commerciales présentent la plateforme comme simple intermédiaire alors qu’elle agit autrement.

Startup fournissant un outil d’intelligence artificielle

La société développe un outil de traitement de dossiers clients. Elle doit examiner les données utilisées, les droits sur les documents, les contrats du fournisseur de modèle, les transferts, la sécurité et les erreurs possibles. Le label startup est un dossier distinct de la conformité du produit.

Recommandation : séparer données de démonstration et données réelles, définir les usages autorisés, contrôler les sorties et permettre une correction humaine. L’analyse fiscale du label doit préciser les impôts et périodes concernés, tandis que le contrat client répartit les responsabilités et décrit les limites du service.

Annexe H Glossaire

Terme	Signification utile
ANSSI	Agence Nationale de la Sécurité des Systèmes d’Information
ARTCI	Autorité de Régulation des Télécommunications et des TIC de Côte d’Ivoire
BCEAO	Banque Centrale des États de l’Afrique de l’Ouest
CENTIF	Cellule nationale de traitement des informations financières
CEPICI	Centre de Promotion des Investissements en Côte d’Ivoire

Terme	Signification utile
CNPS	Caisse Nationale de Prévoyance Sociale
DGI	Direction générale des Impôts
FNE	Facture normalisée électronique
GUCE	Guichet unique du commerce extérieur
HACA	Haute Autorité de la Communication Audiovisuelle
IDU	Identifiant unique des entreprises
LBC/FT/FP	Lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération
NCC	Numéro de compte contribuable
OAPI	Organisation Africaine de la Propriété Intellectuelle
OHADA	Organisation pour l'Harmonisation en Afrique du Droit des Affaires
PASSI	Prestataire d'audit de sécurité des systèmes d'information agréé pour le périmètre concerné
PND	Plan national de développement
PPIC	Plan de protection des infrastructures critiques
RCCM	Registre du commerce et du crédit mobilier
Responsable du traitement	Entité qui détermine les finalités et moyens du traitement
Réversibilité	Organisation de la reprise des données et services à la fin d'une prestation
RGPD	Règlement général sur la protection des données de l'Union européenne
RGSSI	Référentiel général de sécurité des systèmes d'information
RNE	Reçu normalisé électronique
SIGOMAP	Système intégré de gestion des opérations des marchés publics
Sous-traitant de données	Entité traitant des données pour le compte du responsable selon ses instructions
TERNE	Terminal d'émission de reçus normalisés électroniques
UEMOA	Union économique et monétaire ouest-africaine
UMOA	Union monétaire ouest-africaine
ZBTIC	Zone franche de la biotechnologie et des technologies de l'information et de la communication

Annexe I Maturité numérique et contexte économique

Utiliser les études sans confondre leurs indicateurs

Les études sur les usages numériques éclairent les besoins des entreprises et les choix de transformation. Elles ne créent pas d'obligations juridiques. Un taux de connexion, une mesure de maturité des organisations, le chiffre d'affaires des prestataires et une enveloppe de projets publics décrivent des

réalités différentes. Une entreprise doit conserver cette distinction lorsqu'elle présente son marché, justifie un investissement ou sollicite un financement.

Au 30 octobre 2026, aucune mesure homogène et récente ne couvre l'ensemble des entreprises ivoiriennes. Les chiffres disponibles proviennent de sources de nature différente : articles de presse, enquêtes multipays, études sectorielles ou documents de programmation. Ils doivent donc être cités avec leur source, leur périmètre et leur date.

Chiffre examiné	Source et périmètre	Précaution d'usage
28 % de maturité	Article de CIO Mag du 16 mai 2025, citant des agences onusiennes et Smart Africa	Estimation rapportée, dont la méthode n'est pas publiée ; à ne pas confondre avec un taux national d'adoption
Productivité × 2,8 et ventes × 6	SFI et Banque mondiale, 3 325 microentreprises dans sept pays africains	Corrélations observées dans une enquête qui ne couvre pas la Côte d'Ivoire
Coût 35 % et compétences 34 %	Réponses des non-utilisateurs dans la même enquête	Freins déclarés dans cet échantillon, non transposables tels quels aux PME ivoiriennes
CA de 172,1 milliards FCFA, dont 61,6 % pour les dix premiers acteurs	Présentation StatsAfrica de juillet 2026, 113 entreprises, exercices 2023 et 2024	Valeurs du périmètre recensé, et non mesure exhaustive du secteur
2 836 milliards FCFA et 19 projets	Fiche officielle du Groupe consultatif pour le financement du PND 2026-2030	Programmation présentée aux partenaires ; les opportunités se concrétisent avec la publication des projets

Références du tableau : [R61, R62, R63, R64]. Le périmètre de chaque publication est précisé ci-dessous.

L'estimation de maturité de 28 %

L'article de CIO Mag consacré au B2B Digital Day 2025 rapporte une estimation de 28 %, attribuée à des agences onusiennes et à Smart Africa. Le rapport d'origine, l'échantillon, la date de mesure et le mode de calcul n'étant pas précisés, ce chiffre est à utiliser comme un ordre de grandeur rapporté et non comme une statistique nationale. Il ne permet pas, à lui seul, de décrire une tendance depuis 2022. [R61]

La CGECI conduit un travail de baromètre destiné à cartographier les besoins numériques des entreprises. Ses publications mettent notamment en avant la connaissance des outils et la conduite du changement organisationnel. La publication des résultats détaillés permettra de hiérarchiser ces freins par rapport au coût, à la connectivité ou à la sécurité. [R66]

Recommandation : pour citer un taux de maturité, joindre la définition de l'indicateur, l'année d'enquête, la population couverte, le nombre de répondants et les pondérations. Pour comparer plusieurs années ou pays, vérifier que les questionnaires et les méthodes restent compatibles.

Les résultats africains sur les microentreprises

La SFI présente en 2023 une analyse menée avec la Banque mondiale sur 3 325 microentreprises au Ghana, au Kenya, au Mozambique, au Nigeria, au Sénégal, en Afrique du Sud et en Tanzanie. La Côte d'Ivoire ne figure pas dans cet échantillon. L'entreprise médiane est une activité individuelle sans salarié à temps plein. [R62]

Les utilisateurs de smartphones et d'ordinateurs déclarent une productivité 2,8 fois et des ventes 6 fois plus élevées que les non utilisateurs. Ces écarts sont des associations observées ; ils ne prouvent pas que l'achat d'un équipement produit, à lui seul, ces gains. Parmi les non utilisateurs, 35 % citent un coût excessif et 34 % une difficulté d'utilisation. Ces résultats éclairent des obstacles possibles, sans mesurer leur fréquence parmi les PME ivoiriennes ni garantir le rendement d'un projet local. [R62]

Le périmètre de l'étude sur les prestataires numériques

La présentation publique de l'étude StatsAfrica publiée le 15 juillet 2026 annonce une base consolidée de 113 entreprises rapprochées par numéro de compte contribuable, sur les exercices 2023 et 2024. Elle indique 172,1 milliards FCFA de chiffre d'affaires recensé et 61,6 % du chiffre d'affaires pour les dix premiers acteurs. Le périmètre comprend plusieurs métiers et distingue la distribution de matériel et de logiciels. [R63]

Ces chiffres relèvent de la responsabilité de leur éditeur et décrivent le périmètre recensé ; ils ne constituent pas une statistique publique exhaustive du marché. L'étude souligne une forte concentration des acteurs et une rentabilité inégale selon les métiers. [R63]

Recommandation : avant d'utiliser cette étude dans un plan d'affaires, obtenir les règles d'inclusion, le traitement des comptes manquants et des groupes, la distinction entre prestations et revente, les années comparées et la méthode de calcul de la concentration.

Les investissements publics et les programmes d'accompagnement

La fiche d'opportunité officielle consacrée à la numérisation des services publics, préparée pour le Groupe consultatif des 8 et 9 juillet 2026, mentionne 2 836 milliards FCFA et 19 projets numériques majeurs dans le PND 2026 à 2030. Ce montant correspond à une programmation présentée aux partenaires financiers. Pour une entreprise, les opportunités se concrétisent au fur et à mesure de la publication des projets et des procédures de passation : c'est à ce stade qu'il convient de les suivre. [R64]

Le Gouvernement confirme le lancement, le 29 juillet 2026, d'Ivoire Tech Next 15 pour les startups et d'Ivoire Tech Scale Up pour les PME numériques. L'annonce prévoit l'accompagnement de 30 entreprises pendant vingt-quatre mois, réparties entre les deux programmes. Elle décrit une sélection avec des conditions propres à chaque public. Au 30 octobre 2026, la date de candidature de septembre figurant dans l'annonce est passée ; il faut consulter les avis officiels pour connaître les résultats, une éventuelle réouverture ou une nouvelle cohorte. [R65, R67]

L'admission à un programme d'accompagnement doit être distinguée du label prévu par la loi n° 2023-901 et des conditions fiscales exposées au chapitre 17. Une annonce d'accès au financement ou à la commande publique ne constitue pas une garantie de crédit, une attribution de marché ou une exonération automatique. Les décisions d'admission, les conventions et les textes applicables doivent être conservés dans le dossier de l'entreprise. [R36, R24, R25, R65]

Relier le diagnostic de maturité à la conformité

Recommandation : commencer par les processus dont les erreurs ont un coût mesurable, comme la facturation, le suivi des stocks, la paie et les déclarations. Évaluer le coût total, y compris les abonnements, la formation, l'assistance, la sécurité et la sortie du contrat. Les indicateurs utiles sont notamment le temps de traitement, les erreurs, l'utilisation réelle du service et la capacité à restituer les données.

Pour chaque projet retenu, reprendre le questionnaire de l'annexe A et le registre de l'annexe C. Un besoin de cloud appelle l'examen des transferts et du contrat ; une solution de vente implique

l'information du client et la preuve de commande ; un service de paiement nécessite une qualification réglementaire. Le niveau de maturité économique ne dispense pas des formalités exigibles avant le lancement.

Pour un prestataire, les besoins possibles de formation, d'intégration, de sécurité ou d'archivage constituent des hypothèses commerciales à tester auprès des clients. Les entretiens et appels d'offres doivent préciser le problème, le budget, les exigences de conformité et les critères de réception. Une tendance continentale ou une enveloppe publique ne remplace pas cette validation.

Annexe J Gouverner les usages de l'IA et la cybersécurité

La mobilisation du secteur privé en 2026

La CGECI Academy 2026, programmée les 29 et 30 octobre, retient le thème « Capital humain, levier stratégique pour l'Afrique ». Le programme publié comprend une table ronde sur les effets de l'intelligence artificielle sur le capital humain et des échanges sur la connaissance et les compétences. [R68, R69]

La deuxième CGECI Data Day, organisée le 10 septembre 2026 selon le compte rendu du patronat, traite de la stratégie de données et de l'usage de l'IA dans la décision des dirigeants. La CGECI documente également, avec le soutien du FDFP, un projet de formation à l'IA et au Big Data ayant formé 276 auditeurs de 44 entreprises. Le projet visait 62 entreprises ; le bilan publié fait état de 44 entreprises représentées. [R70, R71]

Ces initiatives témoignent d'une mobilisation sur les compétences et la gouvernance des données. Elles ne mesurent pas, en revanche, le taux national d'adoption de l'IA ni le rendement moyen des projets. Les recommandations qui suivent sont donc à adapter au diagnostic de chaque entreprise.

La portée de la stratégie nationale de l'IA

La Stratégie nationale de l'intelligence artificielle à l'horizon 2030 s'organise autour de l'investissement, de l'inclusion et de la gouvernance. Elle propose notamment des actions sur les compétences, les infrastructures, la qualité des données et le cadre juridique. Elle envisage un cloud souverain et l'élaboration d'un dispositif spécifique à l'IA. Les actions proposées doivent être distinguées des mesures effectivement adoptées et des services disponibles. [R72]

Ni la stratégie nationale ni les initiatives citées ne créent, pour les entreprises privées, d'obligation générale de migrer vers un cloud local ou d'acquérir une solution de cybersécurité fondée sur l'IA. L'entreprise doit examiner ses obligations de sécurité, les traitements et transferts de données, les règles de son secteur et les exigences contractuelles. Un hébergement local peut répondre à un besoin précis ; sa localisation ne suffit pas à démontrer la conformité du service. [R01, R43, R72]

Recommandation : vérifier le texte applicable à chaque exigence annoncée par un fournisseur. Une certification commerciale, une orientation nationale ou une participation à un événement ne remplace pas une autorisation de traitement, un agrément sectoriel ou une preuve de sécurité.

Qualifier les risques et protéger les données

Les usages d'IA non approuvés, parfois désignés par « Shadow AI », doivent être recherchés dans l'inventaire des outils et des flux. Leur ampleur dans les entreprises ivoiriennes n'est pas mesurée à ce jour. Leur risque doit être évalué à partir des usages réels : documents transmis, catégories de personnes, conservation, réutilisation par le fournisseur et accès des sous-traitants.

La loi n° 2013-450 reste pertinente dès qu'un outil d'IA traite des données personnelles. Le projet doit être rattaché à une finalité, à une justification de licéité, aux formalités applicables et aux mesures de sécurité. L'analyse inclut l'information des personnes, leurs droits, la durée de conservation et les transferts éventuels. Un outil déjà utilisé pour une tâche ne peut être étendu sans examen à un autre objectif, comme la notation des salariés. [R01, R02]

Le profil de gestion des risques de l'IA générative du NIST, publié en juillet 2024, décrit notamment les erreurs produites avec assurance, les atteintes à la vie privée, les risques de sécurité et les dépendances aux composants et fournisseurs. Il constitue une référence technique volontaire, sans créer à lui seul une obligation ivoirienne. [R75]

Recommandation : autoriser une liste d'outils et de cas d'usage, définir les données admissibles et vérifier les paramètres de conservation et d'entraînement. Exiger une validation avant de connecter un assistant à la messagerie, aux fichiers partagés ou aux logiciels métiers. Pour un agent capable d'agir, limiter les droits et les opérations, tester les résultats et maintenir une possibilité d'arrêt et de reprise humaine. Les secrets professionnels et données sensibles demandent un examen spécifique avant toute transmission.

Choisir et tester des cas d'usage

Les cas ci-dessous sont des exemples à évaluer. Ils ne constituent ni une mesure de la demande nationale ni une promesse de gains.

Usage envisagé	Vérification avant le pilote	Preuve à conserver
Assistant documentaire interne	Droits sur les documents et accès selon le métier	Liste des sources autorisées et tests de restitution
Réponses au service client	Exactitude des réponses et recours à un interlocuteur humain	Scénarios de test et validation des messages
Détection d'anomalies ou de fraude	Qualité des données et conséquences des faux positifs	Mesures de performance et décisions de revue humaine
Aide à la gestion des ressources humaines	Pertinence des critères et effets sur les personnes	Analyse juridique et procédure de contestation
Agent de traitement de tâches	Permissions et opérations nécessitant une approbation	Journal des actions et test de retour au fonctionnement antérieur

Recommandation : définir avant le pilote une situation de référence, le gain attendu et les critères d'arrêt. Mesurer le temps réellement économisé après contrôle humain, le taux d'erreur et le coût total, y compris l'intégration, les abonnements et la maintenance. Un résultat de démonstration doit être confirmé sur des cas représentatifs avant une extension.

Interpréter les chiffres de cybercriminalité

Une communication gouvernementale du 15 juillet 2025, rapportant les données présentées par l'ANSSI, indique 12 100 dossiers enregistrés en 2024, contre 8 132 en 2023 et 6 579 en 2022. La hausse sur deux ans est d'environ 84 %. Le chiffre concerne des dossiers couvrant plusieurs catégories de victimes et d'infractions ; il ne correspond ni à 12 100 entreprises attaquées, ni à des incidents causés par l'IA. [R73]

L'ANSSI cite notamment le hameçonnage, les rançongiciels, les compromissions de comptes et les fuites de données dans son panorama des menaces. Ces risques justifient une préparation adaptée à l'activité.

Les dossiers enregistrés reflètent aussi les signalements et ne constituent pas, à eux seuls, une mesure exhaustive de la fréquence des attaques. [R74]

Organiser la sécurité et les responsabilités

Recommandation : traiter d'abord les accès, l'authentification, les mises à jour, les sauvegardes testées et les procédures de réaction. Les alertes automatisées doivent parvenir à une personne ou à un prestataire identifié, avec une capacité d'intervention définie. Une surveillance continue peut être pertinente selon la criticité, mais l'achat d'un outil présenté comme intelligent ne démontre pas l'existence d'un service opérationnel.

Pour les systèmes soumis au RGSSI ou à l'audit réglementaire, les mesures et preuves doivent être rattachées au périmètre et aux exigences applicables, comme indiqué aux chapitres 5 et 6. Le recours à l'IA ne remplace ni les audits requis ni le traitement des incidents. Les journaux de sécurité contenant des données personnelles doivent eux-mêmes être encadrés. [R01, R43, R44]

Recommandation : faire approuver les usages importants par la direction avec le métier, l'informatique et le juridique. Former les utilisateurs à vérifier les réponses et à signaler les erreurs, les envois de données non autorisés et les messages suspects. La charte doit décrire les outils permis, les restrictions et le circuit d'assistance dans un langage accessible.

Le dossier du projet devrait réunir la décision de lancement, la description des flux, les formalités, le contrat fournisseur, les tests, les habilitations et le plan de réaction. Prévoir une réévaluation lorsqu'un modèle, une fonction, un fournisseur ou une catégorie de données change. Les annexes B et C peuvent servir au suivi des actions et des preuves.

Répertoire des textes et sources

Les références ci-dessous permettent de retrouver les textes et publications utilisés. Les pages institutionnelles et commentaires administratifs complètent la lecture des textes ; ils doivent être interprétés selon leur nature. Les références à des articles sont indiquées dans les chapitres lorsqu'elles fondent un point précis. Consultation au 30 octobre 2026.

R01 Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel

Texte de la loi publié par l'Autorité de protection. Articles 5 à 9 pour les formalités et dispositions sur les principes, droits et responsabilités.

Consulter la source

R02 Autorité de protection des données personnelles

FAQ institutionnelle sur les traitements, la biométrie, les droits, la sécurité et le correspondant.

Consulter la source

R03 Décret n° 2015-79 du 4 février 2015

Modalités de dépôt des déclarations, demandes, octroi et retrait des autorisations. Répertoire officiel ARTCI.

Consulter la source

R04 Loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité

Texte du Journal officiel conservé par l'UNIDIR. Articles 47 et suivants sur les prestataires, 53 et 72 sur la conservation, 73 et suivants sur les enquêtes. Lire avec R06.

Consulter la source

R05 Loi n° 2013-546 du 30 juillet 2013 relative aux transactions électroniques

Publication du Trésor. Articles 5 et 6, 14 et 15, 21 à 23 et 40. L'article 50 a été abrogé par l'ordonnance citée en R07.

Consulter la source

R06 Loi n° 2023-593 du 7 juin 2023

Modification des articles 17, 33, 58, 60, 62 et 66 de la loi sur la cybercriminalité. Répertoire ANSSI.

Consulter la source

R07 Ordonnance n° 2024-950 du 30 octobre 2024

Modification des articles 3 et 17 de l'ordonnance n° 2017-500 et abrogation de l'article 50 de la loi n° 2013-546. Texte publié par l'ANSSI.

Consulter la source

R08 Décrets de sécurité et de gouvernance numérique

Répertoire ANSSI comprenant les décrets de 2021 sur les projets publics, la PSSI, le RGSSI, le PPIC et l'audit, ainsi que le décret n° 2024-958 créant l'ANSSI.

Consulter la source

R09 ANSSI et agrément des PASSI

FAQ sur les prestataires agréés et les audits réglementaires. Voir également le rappel opérationnel du cycle triennal sur le site ANSSI.

Consulter la source

R10 Loi n° 2024-352 du 6 juin 2024 relative aux communications électroniques

Texte officiel publié par le ministère. Régimes de licence, autorisation, déclaration et régime libre.

Consulter la source

R11 ARTCI communiqué du 4 avril 2025 sur les plateformes de services numériques

Récépissé préalable de déclaration et rappel de l'échéance de régularisation du 30 avril 2025.

Consulter la source

R12 Loi n° 2017-803 du 7 décembre 2017 d'orientation de la société de l'information

Répertoire officiel de l'ARTCI.

Consulter la source

R13 OHADA Acte uniforme portant sur le droit commercial général du 15 décembre 2010

Présentation et accès au texte par l'OHADA. Vie commerciale, RCCM et procédures électroniques.

Consulter la source

R14 OHADA Acte uniforme du 26 janvier 2017 relatif au droit comptable et à l'information financière

Répertoire des Actes uniformes de l'OHADA. Voir notamment l'article 24 pour la conservation des livres et pièces pendant dix ans.

Consulter la source

R15 Loi n° 2016-412 du 15 juin 2016 relative à la consommation

Texte publié sur le portail institutionnel de l'économie ivoirienne. À articuler avec le contrat et le type de consommateur.

Consulter la source

R16 Décrets n° 2014-106 du 12 mars 2014 et n° 2016-851 du 19 octobre 2016

Écrit et signature électroniques, puis archivage électronique. Répertoire officiel ARTCI.

Consulter la source

R17 DGI textes réglementaires de la FNE

Article de l'annexe fiscale 2025 et arrêté n° 0337 du 9 mai 2025 sur la mise en œuvre.

Consulter la source

R18 DGI FAQ officielle de la FNE

FNE, RNE, procédures, article 145 du LPF, dispenses et cas pratiques. Les précisions opérationnelles doivent être vérifiées à la date d'utilisation.

Consulter la source

R19 DGI communiqués de la FNE

Répertoire comprenant la fin du papier et l'inscription de janvier 2026, les contrôles d'août 2026 et la conformité API de septembre 2026.

Consulter la source

R20 DGI procédure d'interfaçage de la FNE

Présentation du contexte légal, de la génération, de la certification et de la numérotation.

Consulter la source

R21 Contribution de la Côte d'Ivoire au groupe intergouvernemental de la CNUCED en 2026

Présentation officielle ivoirienne de la TVA sur les services numériques et de l'immatriculation des non résidents. Document hébergé par la CNUCED.

Consulter la source

R22 DGI Bulletin officiel 2026 analyse de l'article 33

Champ des plateformes étrangères et seuil. Consulter les pages 50 à 52 du lecteur.

Consulter la source

R23 DGI Bulletin officiel 2026 calcul des BIC des plateformes étrangères

Page 53 du lecteur. Base forfaitaire de 10 %, taux de 30 % et imputation des retenues prévues.

Consulter la source

R24 DGI Bulletin officiel 2026 article 35 sur les startups labellisées

Page 156 du lecteur. Présentation des exonérations et des régimes concernés.

Consulter la source

R25 DGI Bulletin officiel 2026 conditions et durée des avantages startup

Page 157 du lecteur. Localisation hors ZBTIC, arrêté de label et modalités de décompte selon les impôts.

Consulter la source

R26 BCEAO instruction n° 001-01-2024 du 23 janvier 2024

Cadre des services de paiement dans l'UMOA. Texte et téléchargement officiels.

Consulter la source

R27 BCEAO avis n° 006-05-2025 du 27 mai 2025

Prorogation jusqu'au 31 août 2025 et rappel de l'exigence d'agrément à compter du 1er septembre 2025.

Consulter la source

R28 CENTIF cadre de lutte contre le blanchiment

Répertoire officiel comprenant l'ordonnance n° 2023-875 du 23 novembre 2023, les décisions UMOA et le cadre des sanctions administratives.

Consulter la source

R29 OAPI Accord de Bangui révisé le 14 décembre 2015

Présentation officielle et accès aux versions. Annexes sur les titres et droits de propriété intellectuelle.

Consulter la source

R30 OMPI WIPO Lex législation ivoirienne de droit d'auteur

Répertoire comprenant la loi n° 2016-555 du 26 juillet 2016 relative au droit d'auteur et aux droits voisins.

Consulter la source

R31 NIC CI documentation officielle

Règles de nommage, gestion du domaine national et résolution des litiges.

Consulter la source

R32 HACA textes juridiques de la communication audiovisuelle

Répertoire officiel comprenant la loi n° 2017-868 et sa modification par la loi n° 2022-979.

Consulter la source

R33 HACA présentation de la Charte des réseaux sociaux du 26 octobre 2023

Principes de responsabilité et d'éthique ; à distinguer des obligations issues des textes contraignants.

Consulter la source

R34 Union africaine état de la Convention de Malabo au 2 février 2026

Liste officielle des signatures, adhésions ou ratifications et dépôts. Ligne Côte d'Ivoire.

Consulter la source

R35 Loi n° 2015-532 du 20 juillet 2015 portant Code du travail

Version consolidée publiée par CivLII (Laws.Africa). Article 92.3 sur le registre d'employeur, son fichier électronique et sa conservation.

Consulter la source

R36 Loi n° 2023-901 du 23 novembre 2023 portant promotion des startups numériques

Texte publié par l'Université virtuelle de Côte d'Ivoire. Articles 5 à 7 sur le label, 9 sur l'accompagnement et 11 à 12 sur les obligations et sanctions.

Consulter la source

R37 Gouvernement présentation des stratégies IA et gouvernance des données du 13 mars 2025

Publication officielle sur les orientations nationales.

Consulter la source

R38 ARTCI décision n° 2021-0676 du Conseil de régulation

Document institutionnel reprenant notamment les mesures de contrôle et sanctions en protection des données, articles 17 à 19.

Consulter la source

R39 DGI communiqué de janvier 2026 sur la fin de la facture normalisée physique

Justification des charges, déduction de TVA, RNE, inscription et attestation de régularité fiscale, à lire avec les dispenses du LPF.

Consulter la source

R40 Union européenne règlement 2016 679 du 27 avril 2016

Article 3 du RGPD sur le champ territorial. Référence complémentaire pour les activités internationales, sans application générale à toute entreprise ivoirienne.

Consulter la source

R41 Douanes ivoiriennes textes sur les équipements électriques et électroniques

Répertoire rappelant le décret n° 2017-217 et les avis relatifs à la vérification et à l'éco-redevance.

Consulter la source

R42 Loi n° 2023-900 du 23 novembre 2023 portant Code de l'environnement

Texte publié par le ministère chargé de l'environnement.

Consulter la source

R43 ANSSI Référentiel général de sécurité des systèmes d'information révisé

Version publiée par l'ANSSI. Page 13 sur les niveaux N1 N2 N3 ; section B14 pages 48 à 50 sur les incidents.

Consulter la source

R44 Décret n° 2021-917 du 22 décembre 2021

Texte publié par l'ANSSI. Articles 3 et 4 sur le champ et les cycles ; 11 et 13 sur le rapport et son rejet ; 15 sur les corrections.

Consulter la source

R45 Ordonnance n° 2017-500 du 2 août 2017 sur les échanges administratifs électroniques

Texte original publié par l'ANSSI. Articles 19 à 27 sur l'interopérabilité et la saisine. Lire avec les modifications de 2018 et 2024.

Consulter la source

R46 Ordonnance n° 2015-181 et décret n° 2015-286 sur les procédés électroniques de création

Texte du décret n° 2015-286 sur la plateforme électronique de création d'entreprises, version publiée par CivLII (Laws.Africa).

Consulter la source

R47 Service Public certificat d'immatriculation unique d'entreprise

Présentation de l'ordonnance n° 2015-182 et du décret n° 2015-287, de l'IDU et des pièces. La présentation de la substitution doit être lue avec R49.

Consulter la source

R48 IDU portail d'identification des entreprises

Présentation et étapes pour les entreprises existant avant le 1er octobre 2018.

Consulter la source

R49 District autonome d’Abidjan lancement de l’annuaire IDU en juillet 2025

Communication institutionnelle sur l’identification harmonisée et le maintien des autres références administratives.

Consulter la source

R50 225invest portail unique des services à l’investissement

Point d’entrée des services à l’investissement et des parcours destinés aux entreprises.

Consulter la source

R51 DGI portail e-Impôts Côte d’Ivoire

Télédéclaration, télépaiement, comptes, documents et guides officiels.

Consulter la source

R52 Gouvernement répertoire des services numériques

Présentation d’e-CNPS et du portail Service Public, avec les usages et accès institutionnels.

Consulter la source

R53 GUCE brochure officielle utilisateur

Présentation du guichet du commerce extérieur et des conditions d’obtention d’un compte selon le rôle.

Consulter la source

R54 Douanes ivoiriennes présentation de SYDAM World

Fonctions de dédouanement, recouvrement, transit et profils d’utilisateurs.

Consulter la source

R55 Décret n° 2021-913 du 22 décembre 2021

Référentiel général d’interopérabilité des systèmes d’information. Texte publié par l’ANSSI.

Consulter la source

R56 Décret n° 2024-272 du 8 mai 2024 sur TrésorPay TrésorMoney

Référence au Journal officiel n° 2024-065 sur la généralisation et les modalités de gestion de la plateforme.

Consulter la source

R57 Trésor rapport annuel sur les collectivités décentralisées au titre de 2024

Publication de 2026. Recommandations page 63 sur les timbres municipaux sécurisés et TrésorPay TrésorMoney.

Consulter la source

R58 DGMP avis aux opérateurs économiques sur SIGOMAP

Rappel de l’inscription nécessaire depuis le 1er novembre 2023 et de l’accès sigomap.gouv.ci.

Consulter la source

R59 Assemblée nationale ratification de l’ordonnance n° 2018-641

Document institutionnel identifiant la modification de l’article 5 de l’ordonnance n° 2017-500.

Consulter la source

R60 Loi n° 2019-873 du 14 octobre 2019

Journal officiel du 2 décembre 2019, page 1322, reproduit par CivLII (Laws.Africa). Ratification de l’ordonnance n° 2018-644 modifiant l’article 1 du cadre IDU.

Consulter la source

R61 CIO Mag compte rendu du B2B Digital Day du 16 mai 2025

Source du chiffre rapporté de 28 %. Le protocole et le rapport d’origine ne sont pas identifiés dans cet article.

Consulter la source

R62 SFI analyse des usages numériques des microentreprises publiée en 2023

Enquête sur 3 325 microentreprises dans sept pays ne comprenant pas la Côte d'Ivoire. Écarts observés et freins déclarés.

Consulter la source

R63 StatsAfrica présentation de l'étude sectorielle ESN édition 2026

Page de l'éditeur publiée le 15 juillet 2026. Base annoncée de 113 entreprises sur 2023 et 2024. Rapport intégral non examiné.

Consulter la source

R64 Groupe consultatif PND 2026 à 2030 fiche sur la numérisation des services publics

Fiche OP 5.03-036 pour les 8 et 9 juillet 2026. Page 3 du lecteur sur les 2 836 milliards FCFA et les 19 projets annoncés. Document de promotion de l'investissement et non texte créateur de droits fiscaux.

Consulter la source

R65 Gouvernement lancement des programmes Ivoire Tech Next 15 et Ivoire Tech Scale Up

Communication du 30 juillet 2026 sur le lancement du 29 juillet. Objectifs d'accompagnement et calendrier initial de sélection.

Consulter la source

R66 CGECI présentation des travaux sur la maturité numérique des entreprises

Entretien avec la présidente de la Commission économie numérique et entreprise digitale sur le baromètre et les besoins des PME.

Consulter la source

R67 Ivoire Tech Next 15 portail de présentation du programme

Offre et calendrier initial affichés lors de la consultation. Vérifier les avis actualisés avant une démarche de candidature.

Consulter la source

R68 CGECI Academy présentation de l'édition 2026

Thème officiel relatif au capital humain. Communication de l'organisateur.

Consulter la source

R69 CGECI Academy programme des 29 et 30 octobre 2026

Programme publié des sessions sur le capital humain, l'IA et la connaissance. Ne constitue pas des actes définitifs des débats.

Consulter la source

R70 CGECI compte rendu de la deuxième Data Day

Rencontre du 10 septembre 2026 consacrée notamment à la stratégie de données et à l'usage de l'IA par les dirigeants.

Consulter la source

R71 CGECI bilan du projet de formation à l'IA et au Big Data

Publication sur le projet soutenu par le FDFP. Bilan annoncé de 276 auditeurs issus de 44 entreprises.

Consulter la source

R72 Ministère Stratégie nationale de l'intelligence artificielle à l'horizon 2030

Document stratégique de 71 pages. Piliers et actions proposées sur les infrastructures, les compétences et la gouvernance. À distinguer des textes effectivement adoptés.

Consulter la source

R73 Gouvernement bilan des dossiers de cybercriminalité présenté en juillet 2025

Communication du 15 juillet 2025 avec les chiffres 2024, 2023 et 2022 et la ventilation des victimes.

Consulter la source

R74 ANSSI panorama des menaces

Présentation des menaces fréquentes et de leur périmètre national.

Consulter la source

R75 NIST AI 600-1 profil de gestion des risques de l’IA générative

Publication technique de juillet 2024. Référence volontaire sur les risques et les mesures de gestion, sans valeur de loi ivoirienne.

Consulter la source