BANQUE D'INVESTISSEMENT ET DE DÉVELOPPEMENT DE LA CEDEAO (BIDC)

ECOWAS BANK FOR INVESTMENT AND DEVELOPMENT (EBID)

TERMES DE RÉFÉRENCE

RECRUTEMENT D'UN CONSULTANT CHARGE DE REALISER UNE ETUDE ET D'ELABORER UNE POLITIQUE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL AU PROFIT DE LA BIDC.

Référence : EBID/ToR/PDPP/2026

Date de publication : AOÜT 2026

Siège : Lomé, Togo

Table des matières

1. CONTEXTE

La Banque d'investissement et de développement de la CEDEAO (BIDC), dont le siège est situé à Lomé, au Togo, est l'institution financière de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), créée pour contribuer au développement économique de l'Afrique de l'Ouest par le financement de projets dans les secteurs public et privé au sein de ses quinze (15) États membres.

Dans le cadre de ses activités, la BIDC traite des volumes importants de données à caractère personnel relatives à son personnel, à ses consultants, à ses clients, aux bénéficiaires de ses projets, à ses sous-traitants, à ses fournisseurs, à ses actionnaires et à d'autres parties prenantes. Ces activités de traitement de données mettent en jeu d'importantes responsabilités juridiques, réglementaires, en matière de réputation et opérationnelles pour la protection des données à caractère personnel et des droits à la vie privée des personnes concernées.

La BIDC a récemment chargé un cabinet d'audit indépendant d'évaluer son dispositif de protection des données. Les résultats de cet audit se sont révélés satisfaisants et conformes au pilier n° 9 de l'Union européenne. Selon les conclusions finales de l'audit, les huit (8) recommandations d'ordre non critique formulées ne remettent pas en cause la conformité au pilier n° 9.

Toutefois, l'audit a mis en évidence certaines lacunes entre les dispositifs existants de protection des données de la BIDC et les meilleures pratiques internationales reconnues, notamment le règlement général sur la protection des données de l'Union européenne (règlement (UE) 2016/679 – « RGPD »), l'acte additionnel A/SA.1/01/10 de la CEDEAO relatif à la protection des données à caractère personnel au sein de la CEDEAO, ainsi que les législations nationales applicables sur la protection des données dans les États membres de la BIDC.

Dans le souci de combler les lacunes identifiées par l'audit et d'aligner ses pratiques sur les normes internationales, la BIDC envisage de faire appel aux services d'un consultant qualifié (cabinet ou particulier) afin de mener une étude diagnostique exhaustive et d'élaborer une politique de protection des données à caractère personnel solide et conforme au RGPD, ainsi que le cadre, les procédures, les outils et les modèles nécessaires à son application effective.

Les présents termes de référence (TdR) définissent le contexte, les objectifs, la portée, les livrables, les qualifications requises et les modalités contractuelles applicables à la mission.

2. JUSTIFICATION ET FONDEMENT

En tant qu'institution financière multilatérale opérant dans plusieurs juridictions, la BIDC doit se conformer aux normes les plus strictes de gouvernance, d'intégrité et de responsabilité dans le traitement des données à caractère personnel. La Banque s'expose à divers risques du fait de

l'inexistence d'un cadre de protection des données à caractère personnel intégral, fonctionnel et pleinement conforme au RGPD, notamment :

- Risques juridiques et réglementaires découlant de divergences entre les règles internes de la BIDC et la législation applicable en matière de protection des données dans les juridictions où elle exerce ses activités ou interagit.
- Risques de réputation liés à d'éventuelles violations de données à caractère personnel, à des constats de non-conformité ou à des plaintes émanant des personnes concernées.
- Risques opérationnels liés à l'absence de procédures documentées, de tests d'équilibre, de registres des activités de traitement et de vérifications de conformité programmées à l'avance.
- Risques contractuels découlant des relations de traitement des données avec les prestataires informatiques, les banques correspondantes, les partenaires et les contreparties.
- Risques stratégiques liés à la confiance des actionnaires, partenaires, donateurs, clients et autres parties prenantes de la BIDC.

L'élaboration et l'application d'une politique globale de protection des données à caractère personnel, conforme au RGPD et aux instruments régionaux et nationaux applicables, permettront à la BIDC d'atténuer ces risques, de formaliser ses engagements, de démontrer sa transparence et de renforcer son cadre de gouvernance global.

3. CONCLUSIONS DE L'AUDIT À TRAITER

Le consultant devra tenir dûment compte des conclusions et des recommandations formulées par le cabinet d'audit indépendant. Le tableau ci-dessous résume les principales conclusions et les recommandations correspondantes auxquelles le consultant devra donner suite dans la politique de protection des données à caractère personnel et le cadre qui l'accompagne, qu'il devra élaborer :

N°	CONCLUSIONS DE L'AUDIT	RECOMMANDATION À TRAITER
1	Bases juridiques distinctes de traitement des données à caractère personnel par rapport au RGPD, et risque que le RGPD interdise l'agrégation des consentements.	Modifier l'Acte additionnel et la politique générale de protection des données à caractère personnel afin d'aligner formellement les bases juridiques applicables au traitement sur le libellé de l'article 6 du RGPD. Évaluer l'utilisation des

N°	CONCLUSIONS DE L'AUDIT	RECOMMANDATION À TRAITER
		formulaires de consentement conformément aux exigences des articles 6 et 7 du RGPD et abandonner les pratiques conduisant à l'association du consentement à d'autres bases juridiques ou à une confusion quant à la base juridique effective de chaque opération de traitement.
2	Non-conformité aux exigences du RGPD concernant le traitement fondé sur l'intérêt légitime de la BIDC.	Élaborer un modèle de critères d'évaluation du test d'équilibre des intérêts légitimes équivalent aux exigences du RGPD ; réaliser et consigner ces évaluations avant tout traitement fondé sur un intérêt légitime. Comparer le modèle à ceux publiés par les autorités de contrôle de la protection des données de l'UE. S'abstenir de procéder au traitement lorsque les résultats de l'évaluation montrent que les droits et intérêts des personnes concernées prévalent sur les intérêts de la BIDC.
3	Absence de documentation systématique équivalente à la tenue de registres des activités de traitement en tant que responsable du traitement au sens de l'article 30 du RGPD.	Rédiger et tenir à jour un document équivalent aux registres des activités de traitement requis en vertu de l'article 30 du RGPD. Pour ce faire, il faudra mettre à jour le document Excel existant intitulé « Cartographie des flux de données à caractère personnel de la BIDC », qui contient déjà certaines des informations requises.
4	Absence d'un calendrier annuel complet pour les questions relatives à la protection des données.	Établir une liste claire des mesures à prendre pour mettre en place des contrôles et des activités complets et planifiés à l'avance en matière de protection des données, à effectuer à des intervalles précis (un « calendrier annuel ») indépendamment des problèmes liés à la cybersécurité et à l'informatique. Prévoir la

N°	CONCLUSIONS DE L'AUDIT	RECOMMANDATION À TRAITER
		vérification des registres des activités de traitement, des durées de conservation des données et des modalités de traitement, ainsi que des contrôles réguliers du respect de la protection des données par les prestataires informatiques (sous-traitants).
5	Absence de justification des procédures retenues en matière de tests d'intrusion et d'analyse des vulnérabilités.	Étendre les tests d'intrusion et les évaluations de vulnérabilité périodiques à l'ensemble des systèmes informatiques opérationnels, en prévoyant des fréquences plus espacées pour les systèmes non critiques. Documenter la justification des fréquences retenues, en expliquant notamment pourquoi des tests annuels sont jugés suffisants pour les systèmes informatiques critiques dans le contexte actuel des cybermenaces.
6	Projet de politique de cybersécurité et d'atténuation des risques non encore approuvé ; mise en place d'un centre d'opérations de sécurité (SOC) fonctionnant 24 h/24 et 7 j/7, ainsi que de tests d'intrusion récurrents et de détection des vulnérabilités, non encore effective.	Finaliser l'approbation de la politique de cybersécurité et d'atténuation des risques. Mettre en place un centre d'opérations de sécurité (SOC) fonctionnant 24 h/24 et 7 j/7, et rendre opérationnels les tests d'intrusion récurrents et la détection des vulnérabilités. Aligner la politique de cybersécurité sur le cadre de protection des données à caractère personnel en cours d'élaboration.
7	Lacunes dans la procédure de réalisation des analyses d'impact relatives à la protection des données (AIPD) pour les activités de traitement prévues.	Élaborer une méthodologie et un modèle complets pour l'analyse d'impact relative à la protection des données (AIPD), conformes à l'article 35 du RGPD, comprenant notamment les critères permettant de déterminer quand une AIPD est requise, la méthodologie à suivre pour la réaliser, les exigences en matière de documentation, ainsi que le processus de

N°	CONCLUSIONS DE L'AUDIT	RECOMMANDATION À TRAITER
		validation impliquant le responsable de la protection des données (RPD).
8	Absence de justification claire pour les pratiques retenues en matière de formation sur la protection des données.	Réévaluer la fréquence des formations sur la protection des données, en envisageant des formations plus intensives pour l'ensemble du personnel (par exemple, au moins une fois tous les six mois), étant donné que le sujet est nouveau pour le personnel et que la formation porte sur le RGPD, qui n'est pas directement applicable à la BIDC mais auquel la Banque cherche à se conformer. Documenter la justification de la fréquence et de la structure des formations adoptées.

La liste ci-dessus n'est pas exhaustive. Le consultant devra également recenser toute lacune supplémentaire mise en évidence lors de la phase de diagnostic de la mission et proposer des mesures correctives appropriées.

4. OBJETIF DE LA MISSION

4.1 Objectif général

L'objectif général de cette mission est d'appuyer la BIDC dans l'élaboration d'une politique globale de protection des données à caractère personnel, conforme au RGPD, ainsi que du cadre de mise en œuvre correspondant, afin de combler les lacunes identifiées par l'audit indépendant et d'aligner les pratiques de la BIDC en matière de protection des données sur les meilleures pratiques internationales.

4.2 Objectif spécifique

Les objectifs spécifiques de la mission sont les suivants :

1. Réaliser un diagnostic complet des dispositifs actuels de protection des données à caractère personnel de la BIDC, y compris son acte additionnel, ses politiques existantes, ses procédures, ses formulaires de consentement, ses registres, ses programmes de formation et son cadre de sécurité informatique, et les évaluer à l'aune du RGPD et des autres instruments applicables.

2. Élaborer une politique de protection des données à caractère personnel formellement conforme aux articles 6 et 7 du RGPD, notamment en ce qui concerne les bases juridiques du traitement et les exigences applicables au consentement.
3. Élaborer un modèle de test d'équilibre des intérêts légitimes (LIA) équivalent aux exigences du RGPD, en s'inspirant des modèles publiés par les autorités de contrôle de la protection des données de l'UE.
4. Élaborer un cadre de registre des activités de traitement (RoPA) équivalent aux exigences de l'article 30 du RGPD, en s'appuyant sur la « cartographie des flux de données à caractère personnel » existante de la BIDC et en l'améliorant.
5. Élaborer un « calendrier annuel de protection des données » définissant les contrôles de conformité, les examens et les activités préprogrammés à effectuer à des intervalles définis.
6. Élaborer une méthodologie et un modèle d'analyse d'impact relative à la protection des données conformes à l'article 35 du RGPD.
7. Élaborer un plan de formation à la protection des données, accompagné d'une justification documentée concernant la fréquence, le contenu et le public cible de la formation.
8. Élaborer les procédures, modèles et outils supplémentaires nécessaires à l'application efficace de la politique de protection des données à caractère personnel (par exemple : procédure relative aux droits des personnes concernées, procédure de notification des violations de données, liste de contrôle de diligence raisonnable pour les sous-traitants, durée de conservation).
9. Appuyer la BIDC dans l'identification des interfaces entre la politique de protection des données à caractère personnel et le projet de politique en matière de cybersécurité de l'information et d'atténuation des risques, y compris la justification des tests d'intrusion et des évaluations de vulnérabilité récurrente.
10. Renforcer les capacités du personnel de la BIDC, en particulier celles du responsable de la protection des données (ou de la fonction équivalente), du département juridique, du département de la gestion des risques et de la conformité, des ressources humaines, du département informatique et de l'audit interne, en ce qui concerne la nouvelle politique et son application.

5. PORTÉE DE LA MISSION

La mission couvre l'ensemble des activités de traitement des données à caractère personnel menées par la BIDC à son siège de Lomé et, le cas échéant, dans ses représentations ou bureaux situés dans les États membres de la CEDEAO. La mission portera notamment, sans s'y limiter, sur :

- Les données à caractère personnel des membres du personnel de la BIDC (personnel permanent, contractuel, consultants, stagiaires) et des anciens membres du personnel.
- Les données à caractère personnel des membres du Conseil d'administration, du Conseil des gouverneurs, des comités et des représentants des actionnaires.
- Les données à caractère personnel des clients, des emprunteurs, des bénéficiaires de projets et des intermédiaires.
- Les données à caractère personnel des sous-traitants, des fournisseurs, des prestataires de services et des contreparties.
- Les données à caractère personnel des visiteurs et des personnes qui accèdent aux locaux de la BIDC (y compris les données issues de la vidéosurveillance et du contrôle d'accès).
- Les données à caractère personnel collectées par le biais des sites web, des applications et des canaux numériques de la BIDC.
- Les données à caractère personnel traitées par des tiers agissant en tant que sous-traitants pour le compte de la BIDC.

Le cadre juridique applicable à prendre en considération comprend, sans s'y limiter :

- L'Accord de siège et le statut juridique de la BIDC en tant qu'organisation internationale.
- Les statuts et l'acte additionnel de la BIDC.
- L'acte additionnel de la CEDEAO A/SA.1/01/10 relatif à la protection des données à caractère personnel au sein de la CEDEAO.
- Le règlement général sur la protection des données de l'Union européenne (règlement (UE) 2016/679 – RGPD) constitue la référence en matière de bonnes pratiques internationales.
- La législation nationale pertinente en matière de protection des données des États membres de la BIDC, en particulier la loi togolaise relative à la protection des données à caractère personnel.
- Les obligations sectorielles spécifiques applicables au secteur bancaire et financier, notamment en matière de lutte contre le blanchiment d'argent et le financement du terrorisme (LBC/FT), de connaissance du client (KYC) et de déclaration prudentielle.
- Les lignes directrices pertinentes émises par le Comité européen de la protection des données (CEPD) et les autorités nationales de contrôle.

6. TÂCHES ET ACTIVITÉS SPÉCIFIQUES

Le consultant devra mener à bien les tâches suivantes, organisées en cinq (5) phases :

Phase 1 – Lancement et diagnostic

- Tenir une réunion de lancement avec l'équipe de projet de la BIDC afin d'affiner la méthodologie, le plan de travail et le calendrier.
- Examiner l'ensemble de la documentation pertinente de la BIDC (acte additionnel, politiques existantes, formulaires de consentement, contrats, la cartographie actuelle des flux de données à caractère personnel, le projet de politique de cybersécurité de l'information et d'atténuation des risques, le rapport d'audit, les supports de formation, etc.).
- Mener des entretiens avec les principales parties prenantes (responsable de la protection des données, département juridique, conformité, gestion des risques, ressources humaines, informatique, audit interne, opérations, communication).
- Cartographier l'ensemble des activités actuelles de traitement des données à caractère personnel.
- Réaliser une analyse des écarts par rapport au RGPD, à l'Acte additionnel de la CEDEAO, aux législations nationales applicables et aux conclusions de l'audit.
- Soumettre un rapport de lancement comprenant un plan de travail détaillé, la méthodologie, la liste des parties prenantes, la liste des documents examinés et une analyse préliminaire des écarts.

Phase 2 – Élaboration de la politique de protection des données à caractère personnel

- Élaborer une politique de protection des données à caractère personnel exhaustive, conforme aux articles 5 à 7 du RGPD (principes, licéité du traitement, conditions du consentement).
- Veiller à ce que la politique couvre l'ensemble des droits des personnes concernées (articles 12 à 22 du RGPD) : droit à l'information, à l'accès, à la rectification, à l'effacement, à la limitation du traitement, à la portabilité, à l'opposition, ainsi que les droits liés à la prise de décision automatisée.
- Définir les rôles et responsabilités de gouvernance, notamment ceux du responsable de la protection des données (RPD), des propriétaires de données, des gestionnaires de données, du responsable de la sécurité des systèmes d'information et du rôle de la Haute Direction.
- Définir le cycle de vie des données (collecte, utilisation, stockage, communication, conservation, destruction) et le principe de minimisation des données.
- Définir les règles relatives aux transferts internationaux de données, notamment au regard des activités multi-juridictionnelles de la BIDC.

- Définir le régime applicable aux sous-traitants et aux sous-traitants, y compris les exigences contractuelles (accords de traitement des données, diligence raisonnable, droits d'audit) ; et
- Définir le régime de notification et de gestion des violations de données à caractère personnel.

Phase 3 - Élaboration d'outils et de procédures d'accompagnement

- Élaborer le modèle et le canevas d'évaluation de l'intérêt légitime (LIA – Legitimate Interest Assessment).
- Mettre à jour et améliorer la cartographie des flux de données à caractère personnel existante afin qu'elle fasse office de registre complet des activités de traitement (RoPA – Record of Processing Activities) au sens de l'article 30 du RGPD, en incluant les registres du responsable du traitement et du sous-traitant, le cas échéant.
- Élaborer le calendrier annuel de protection des données, avec un planning clair des activités, des responsables et des fréquences de révision.
- Élaborer la méthodologie, l'arbre de décision, le modèle et le processus de validation de l'AIPD (Analyse d'Impact relative à la Protection des Données).
- Élaborer des formulaires de consentement révisés conformes aux articles 6 et 7 du RGPD (Règlement Général sur la Protection des Données), en veillant à distinguer clairement le consentement des autres bases juridiques applicables.
- Élaborer la procédure de gestion des droits des personnes concernées, comprenant un registre des demandes, des modèles de réponse et des délais de traitement.
- Élaborer la procédure de notification des violations de données à caractère personnel, en précisant les mécanismes d'escalade interne, les exigences de documentation ainsi que les modalités de notification aux autorités de contrôle et aux personnes concernées, le cas échéant.
- Élaborer le calendrier de conservation des données à caractère personnel applicable à l'ensemble des unités opérationnelles de la Banque.
- Élaborer une liste de contrôle relative à la diligence raisonnable et à la gestion contractuelle des tiers et sous-traitants.
- Élaborer la justification et la documentation nécessaires pour déterminer les fréquences retenues en matière de tests d'intrusion et d'évaluations de vulnérabilité, en distinguant les systèmes informatiques critiques des systèmes non critiques.

Phase 4 – Formation et renforcement des capacités

- Élaborer un plan de formation à la protection des données, assorti d'une justification claire de la fréquence retenue (en proposant, le cas échéant, une fréquence minimale d'une session tous les six (6) mois pour l'ensemble du personnel au cours des deux (2) premières années suivant l'adoption de la politique).
- Concevoir des supports de formation destinés (i) à l'ensemble du personnel dans une perspective de sensibilisation générale, (ii) aux responsables et gestionnaires de données dans une perspective opérationnelle, et (iii) à la Haute direction ainsi qu'au Conseil d'administration dans une perspective de gouvernance.
- Organiser une première session de formation des formateurs (ToT) à l'intention du délégué à la protection des données (DPD) et des relais identifiés ; et
- Organiser au moins une (1) session de sensibilisation générale ainsi qu'une (1) session d'information à l'intention des titulaires des postes statutaires.

Phase 5 – Finalisation et transfert des livrables

- Présenter le projet de politique et le cadre d'accompagnement aux comités compétents de la BIDC.
- Intégrer les commentaires et observations de la BIDC.
- Soumettre les versions finales de l'ensemble des livrables en anglais et en français.
- Fournir une feuille de route de mise en œuvre couvrant une période minimale de 24 mois, comprenant des mesures prioritaires à effet rapide ainsi que des actions de plus long terme.
- Produire un rapport de clôture récapitulant les travaux réalisés, les lacunes comblées, les risques résiduels et les recommandations en vue d'une amélioration continue.

7. LIVRABLES ATTENDUS

Le consultant produira les livrables ci-après. Il les soumettra en anglais et en français, sous forme électronique modifiable (Microsoft Word, Excel, PowerPoint selon le cas) ainsi qu'au format PDF :

N°	LIVRABLES	PHASE	ÉCHÉANCE INDICATIVE
D1	Rapport de démarrage (méthodologie, plan de travail, cartographie des parties prenantes, analyse préliminaire des écarts).	Phase 1	1re semaine après le lancement

N°	LIVRABLES	PHASE	ÉCHÉANCE INDICATIVE
D2	Rapport de diagnostic et d'analyse des écarts.	Phase 1	3e semaine
D3	Projet de politique de protection des données à caractère personnel.	Phase 2	5e semaine
D4	Outils et procédures d'appui : modèle LIA, RoPA, « Annual Clock » (calendrier annuel), méthodologie et modèle d'AIPD, formulaires de consentement révisés, procédure relative aux droits des personnes concernées, procédure de notification des violations de données à caractère personnel, calendrier de conservation et liste de contrôle de diligence raisonnable applicable aux sous-traitants.	Phase 3	8e semaine
D5	Document justifiant la fréquence des tests d'intrusion et des évaluations de vulnérabilité.	Phase 3	9e semaine
D6	Plan de formation à la protection des données et supports de formation.	Phase 4	10e semaine
D7	Organisation de sessions de formation des formateurs, de sensibilisation générale et d'information à l'intention des titulaires des postes statutaires.	Phase 4	11e semaine
D8	Version finale de la Politique de protection des données à caractère personnel, ensemble complet d'outils et de procédures consolidés, feuille de route de mise en œuvre (24 mois) et rapport de clôture.	Phase 5	12e semaine

La BIDC examinera chaque livrable et son point focal désigné devra l'approuver avant toute acceptation définitive. La Banque communiquera ses observations dans un délai de dix (10) jours ouvrables à compter de la réception de chaque livrable.

8. DURÉE ET CALENDRIER DE LA MISSION

La durée totale de la mission est estimée à douze (12) semaines calendaires, soit environ trois (3) mois , à compter de la date de signature du contrat. Cette durée inclut le temps nécessaire à la BIDC pour examiner chaque livrable et formuler ses observations.

Le consultant proposera dans le rapport de démarrage un plan de travail détaillé précisant notamment la répartition proposée des jours-consultant par phase et par profil d'expert. Le calendrier proposé devra demeurer réaliste et refléter la complexité de la mission.

9. MÉTHODOLOGIE ET APPROCHE

Le consultant adoptera une méthodologie participative, fondée sur des données factuelles et axée sur les risques. Cette méthodologie comprendra au minimum les éléments suivants :

- examen documentaire de l'ensemble des documents pertinents de la BIDC ainsi que des instruments juridiques applicables,
- conduite d'entretiens structurés et d'ateliers avec les parties prenantes de la BIDC,
- réalisation d'une analyse comparative fondée sur les bonnes pratiques en vigueur dans des banques multilatérales de développement et des institutions financières internationales comparables,
- utilisation de documents de référence conformes au RGPD, en particulier les directives publiées par le Comité européen de la protection des données (EDPB) et les autorités de contrôle compétentes,
- validation progressive des projets de documents avec l'équipe de projet de la BIDC et les départements concernés,
- mise en œuvre d'un dispositif d'assurance qualité, y compris la revue par les pairs des livrables au sein de l'équipe du consultant.

Le Consultant réalisera l'ensemble des travaux en étroite collaboration avec le point focal désigné par la BIDC, qui constituera son principal interlocuteur pendant toute la durée de la mission. Le consultant devra effectuer au moins deux (2) missions sur site au siège de la BIDC à Lomé au cours de la mission (réunion de lancement et atelier de validation). Les autres activités pourront se dérouler à distance ou sur site selon les modalités convenues entre les parties.

10. COMPÉTENCES ET EXPÉRIENCE DU CONSULTANT

La mission pourra être exécutée par un cabinet de conseil, un cabinet juridique spécialisé dans la protection des données ou un consortium réunissant de telles entités. Le Consultant mobilisera une équipe pluridisciplinaire comprenant au minimum les profils d'experts clés ci-après :

10.1 Chef d'équipe / Expert senior en protection des données

- Être titulaire d'un diplôme de niveau Master (ou équivalent) en droit, avec une spécialisation en protection des données, en droit de la vie privée ou en droit des technologies de l'information.
- Justifier d'au moins douze (12) années d'expérience professionnelle dans le conseil en matière de protection des données et de respect de la vie privée.
- Détenir une certification reconnue en protection des données (CIPP/E, CIPM, CIPT ou équivalent).
- Justifier d'une expérience avérée dans l'élaboration de politiques de protection des données pour au moins trois (3) organisations internationales, institutions financières ou grandes entreprises.
- Maîtriser parfaitement le RGPD, l'Acte additionnel de la CEDEAO relatif à la protection des données à caractère personnel ainsi qu'au moins un (1) régime national de protection des données en vigueur dans l'espace CEDEAO.
- Posséder d'excellentes capacités rédactionnelles et de présentation en anglais ainsi qu'une connaissance pratique du français, ou inversement.

10.2 Expert juridique –Législations nationales / de la CEDEAO en matière de protection des données

- Être titulaire d'un diplôme de niveau Master (ou équivalent) en droit.
- Justifier d'au moins huit (8) années d'expérience professionnelle, dont une expérience significative dans l'application des législations relatives à la protection des données au sein des États membres de la CEDEAO.
- Posséder une solide compréhension du statut juridique et des immunités dont bénéficient les organisations internationales.
- Maîtriser l'anglais et le français constituera un atout majeur.

10.3 Expert en sécurité informatique et en AIPD

- Être titulaire d'un diplôme en informatique, en sécurité de l'information, en ingénierie ou dans une discipline connexe.
- Justifier d'au moins huit (8) années d'expérience professionnelle en sécurité de l'information et en gestion des risques, notamment dans la conduite de l'AIPD, la supervision des tests d'intrusion et la gestion des vulnérabilités.
- Détenir une certification reconnue (CISSP, CISM, auditeur principal / responsable de la mise en œuvre ISO 27001, CDPSE).

- Justifier d'une expérience de conseil auprès d'institutions financières sur les interactions entre sécurité de l'information et protection des données à caractère personnel.

10.4 Expert en formation et en gestion du changement

- Être titulaire d'un diplôme dans une discipline pertinente (éducation, communication, ressources humaines, droit ou domaine connexe).
- Justifier d'au moins six (6) années d'expérience dans la conception et l'animation de formations relatives à la conformité et/ou à la protection des données.
- Démontrer une expérience avérée en matière d'andragogie et de dispositifs de formation des formateurs.

10.5 Exigences applicables au cabinet

- Le Consultant (cabinet) devra être une entité légalement constituée depuis au moins dix (10) ans.
- Il devra avoir réalisé au moins cinq (5) missions similaires au cours des sept (7) dernières années, dont au moins une (1) au profit d'une banque multilatérale de développement, d'une organisation internationale ou d'une institution financière régionale.
- Il devra démontrer sa capacité à exécuter des missions en anglais et en français.
- Il ne doit présenter aucun conflit d'intérêts avec la BIDC, ses actionnaires ou ses principales contreparties.

11. RAPPORTS ET SUPERVISION

Le consultant rendra compte au point focal désigné par la BIDC (ci-après dénommé « le promoteur du projet »), qui bénéficiera de l'appui d'un comité de pilotage composé de représentants du département juridique, du département des risques et de la conformité, de la division des ressources humaines, du département informatique, du département de l'audit interne et de la fonction de délégué à la protection des données.

Le comité de pilotage se réunira au minimum aux étapes clés suivantes :

- Réunion de lancement (semaine 1).
- Validation du rapport de démarrage (semaine 1).
- Validation du rapport de diagnostic et d'analyse des écarts (semaine 3).
- Validation du projet de politique (semaine 5).
- Validation des outils d'appui (semaine 8).
- Clôture du projet (semaine 12).

Le consultant transmettra au promoteur du projet des notes d'avancement bimensuelles, résumant les activités menées, les livrables en cours d'élaboration, les risques et les difficultés rencontrés ainsi que les décisions ou contribution attendues de la BIDC.

12. CONFIDENTIALITÉ ET PROTECTION DES DONNÉES

Le Consultant traitera comme strictement confidentielle toute information mise à sa disposition dans le cadre de la mission. Avant le démarrage des travaux, le Consultant ainsi que chacun des membres de son équipe signeront un Accord de Confidentialité.

Le Consultant ne pourra divulguer, publier, reproduire ou utiliser aucune information confidentielle obtenue auprès de la BIDC à d'autres fins que l'exécution de la mission, sauf autorisation écrite préalable de la Banque. Cette obligation de confidentialité demeurera en vigueur après l'expiration ou la résiliation du contrat.

Lorsque l'exécution de la mission nécessitera l'accès à des données à caractère personnel, le Consultant agira en qualité de sous-traitant pour le compte de la BIDC. À ce titre, il respectera l'ensemble des instructions raisonnables de la Banque, les principes du Règlement Général sur la Protection des Données (RGPD), les dispositions de l'Acte additionnel de la CEDEAO relatif à la protection des données à caractère personnel ainsi que les mesures techniques et organisationnelles appropriées.

13. DROITS DE PROPRIÉTÉ INTELLECTUELLE

Dès le paiement des honoraires correspondants, l'ensemble des livrables, rapports, outils, modèles, supports de formation et autres documents élaborés par le Consultant dans le cadre de la mission deviendront la propriété exclusive de la BIDC. La Banque disposera d'un droit illimité d'utilisation, de modification, de reproduction et de diffusion de ces livrables pour ses propres besoins, notamment en vue de leur adaptation à de futures versions ou de leur utilisation par ses filiales et entités affiliées.

Le Consultant garantit que les livrables fournis ne portent atteinte à aucun droit de propriété intellectuelle appartenant à des tiers. Il indemnisera la BIDC contre toute réclamation, action ou procédure résultant d'une telle violation.

14. CRITÈRES DE SÉLECTION ET ÉVALUATION

La BIDC procédera à la sélection du Consultant conformément à ses règles et procédures de passation des marchés. L'évaluation reposera sur une analyse combinée des offres technique et financière, selon les pondérations indicatives ci-après :

CRITÈRES D'ÉVALUATION	NOTE MAXIMALE	PONDÉRATION
Offre technique	100 points	80%
a) Expérience générale du cabinet dans des missions similaires	15	
b) Expérience spécifique en matière de protection des données et de conformité au RGPD dans le cadre de missions auprès d'organisations internationales ou d'institutions financières	20	
c) Pertinence et qualité de la méthodologie et du plan de travail proposés	25	
d) Qualifications et compétences des experts clés proposés	30	
e) Compétences linguistiques et connaissance du contexte régional (anglais/français, expérience au sein de la CEDEAO)	10	
Offre financière	100 points	20%
TOTAL		**100%**

Pour qu'une offre soit jugée techniquement conforme, elle devra obtenir une note minimale de 80 points sur cent (100). La BIDC écartera toute offre obtenant une note inférieure à ce seuil. Dans ce cas, elle n'ouvrira pas l'offre financière correspondante.

15. SOUMISSION DES OFFRES

Les consultants intéressés transmettront leurs propositions par voie électronique à l'adresse suivante :

Courriel : ichabimougnan@bidc-ebid.org au plus tard le **31 août 2026 à 23H59 minutes.**

La BIDC se réserve le droit de demander des éclaircissements, d'inviter les candidats présélectionnés à un entretien ou à une présentation, de rejeter tout ou partie des offres reçues, ou encore d'annuler la procédure de passation de marché à tout moment, sans encourir aucune responsabilité à l'égard des candidats.

16. CONTRAT ET MODALITÉS DE PAIEMENT

Le consultant retenu conclura avec la BIDC un contrat à prix forfaitaire. Le contrat comprendra, entre autres, des dispositions habituelles relatives aux livrables, à la propriété intellectuelle, à la confidentialité, à la protection des données, à la responsabilité, à la force majeure, à la suspension et à la résiliation du contrat, au droit applicable ainsi qu'au règlement des litiges.

La BIDC effectuera les paiements par tranches, en fonction de la validation des livrables, selon le calendrier indicatif suivant :

- cinquante pour cent (50 %) à la signature du contrat et à la remise du rapport de démarrage (D1),
- zéro (0 %) à la validation du rapport de diagnostic et d'analyse des écarts (D2),
- zéro (0 %) à la validation du projet de politique de protection des données à caractère personnel (D3),
- vingt-cinq pour cent (25 %) à la validation des outils et procédures d'appui (D4 et D5),
- zéro pour cent (0 %) après validation du plan de formation, des supports pédagogiques et de la réalisation des sessions de formation (D6 et D7),
- vingt-cinq pour cent (25 %) après validation des livrables finaux, de la feuille de route de mise en œuvre et du rapport de clôture (D8).

La BIDC effectuera chaque paiement dans un délai de trente (30) jours calendaires à compter de la validation des livrables concernés et de la réception de la facture correspondante.

17. ANNEXES

Après la signature de l'Accord de Confidentialité et avant le démarrage de la mission, la BIDC mettra les documents suivants à la disposition du Consultant retenu :

- annexe 1 : Rapport d'audit – Conclusions et recommandations relatives à la protection des données,
- annexe 2 : Acte additionnel de la BIDC et Politique de protection des données actuellement en vigueur,
- annexe 3 : Cartographie des flux de données à caractère personnel de la BIDC (format Excel),
- annexe 4 : Projet de politique en matière de cybersécurité de l'information et d'atténuation des risques,
- annexe 5 : Formulaires de consentement actuellement utilisés,
- annexe 6 : Supports de formation actuellement utilisés en matière de protection des données,

- annexe 7 : Organigramme de la BIDC et liste des départements concernés,
- annexe 8 : Règles de passation des marchés de la BIDC et modèle de contrat type,
- annexe 9 : Modèle d'accord de confidentialité.

— FIN DES TERMES DE RÉFÉRENCE —