ECOWAS BANK FOR INVESTMENT AND DEVELOPMENT (EBID)

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

TERMS OF REFERENCE

FOR THE RECRUITMENT OF A CONSULTANT TO STUDY AND DEVELOP A PERSONAL DATA PROTECTION POLICY FOR EBID

Reference: EBID/ToR/PDPP/2026

Date: **August 2026**.

2026

Headquarters: Lomé, Togo

Table of Content

1. BACKGROUND AND CONTEXT

The ECOWAS Bank for Investment and Development (EBID), headquartered in Lomé, Togo, is the financial institution of the Economic Community of West African States (ECOWAS) established to contribute to the economic development of West Africa through the financing of public and private sector projects in its fifteen (15) Member States.

In the course of its operations, EBID processes substantial volumes of personal data relating to its staff, consultants, customers, project beneficiaries, contractors, suppliers, shareholders, and other stakeholders. Such processing activities give rise to significant legal, regulatory, reputational, and operational responsibilities for protecting personal data and the privacy rights of data subjects.

EBID recently commissioned an independent audit firm to assess its data protection framework. The audit outcome was satisfactory and Pillar No. 9 EU compliant. Eight (8) recommendations issued by the consultant are non-critical and do not call into question the compliance with Pillar No. 9, as confirmed by the final conclusions of the audit.

However, the audit identified some gaps between EBID's existing data protection arrangements and recognized the best international practice, including the European Union General Data Protection Regulation (Regulation (EU) 2016/679 - "GDPR"), the ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, and the national data protection laws applicable in EBID's Member States.

In order to address the gaps identified by the audit and to align its practices with international standards, EBID intends to engage the services of a qualified Consultant (firm or individual) to conduct a comprehensive diagnostic study and to develop a robust, GDPR-aligned Personal Data Protection Policy together with the supporting framework, procedures, tools, and templates required for its effective implementation.

These Terms of Reference (ToR) define the background, objectives, scope, deliverables, qualifications required, and contractual modalities applicable to the assignment.

2. RATIONALE AND JUSTIFICATION

As a multilateral financial institution operating across multiple jurisdictions, EBID must demonstrate the highest standards of governance, integrity, and accountability in its handling of personal data. The absence of a fully GDPR-aligned, comprehensive, and operational personal data protection framework exposes the Bank to a range of risks, including:

- Legal and regulatory risks arising from divergence between EBID's internal rules and the data protection legislation applicable in the jurisdictions in which it operates or interacts.
- Reputational risks linked to potential personal data breaches, non-compliance findings, or complaints from data subjects.

- Operational risks linked to the absence of documented procedures, balancing tests, records of processing activities, and pre-scheduled compliance verifications.
- Contractual risks arising from data processing relationships with IT providers, correspondent banks, partners, and counterparties.
- Strategic risks linked to the trust of EBID's shareholders, partners, donors, customers, and other stakeholders.

Developing and implementing a comprehensive Personal Data Protection Policy aligned with the GDPR and applicable regional and national instruments will enable EBID to mitigate these risks, formalize its commitments, demonstrate accountability, and strengthen its overall governance framework.

3. AUDIT FINDINGS TO BE ADDRESSED

The Consultant shall give due consideration to the findings and recommendations issued by the independent audit firm. The table below summarizes the principal findings and the corresponding recommendations that the Consultant shall address through the Personal Data Protection Policy and accompanying framework to be developed:

N°	AUDIT FINDING	RECOMMENDATION TO BE ADDRESSED
1	Separate legal bases for processing personal data compared to the GDPR, and the potential risk of the GDPR prohibiting the aggregation of consent.	Amend the Supplementary Law and general personal data protection policy to formally align the legal bases applicable to processing with the wording of Article 6 of the GDPR. Assess the use of consent forms in accordance with the requirements of Articles 6 and 7 of the GDPR and discontinue practices leading to integration of consent with other legal bases or confusion regarding the actual legal basis for each processing activity.
2	Non-compliance with GDPR requirements regarding processing based on EBID's legitimate interest.	Draft a model for legitimate interest balancing tests equivalent to the requirements of the GDPR; conduct and document these tests before any processing based on a legitimate interest. Compare the model with those published by EU data protection supervisory

N°	AUDIT FINDING	RECOMMENDATION TO BE ADDRESSED
		authorities. Refrain from processing where the test results show EBID's interests are overridden by the rights and interests of the individuals concerned.
3	Lack of consistent documentation equivalent to processing activity records as a data controller under Article 30 of the GDPR.	Draft and maintain a document equivalent to the records of processing activities required under Article 30 of the GDPR. This can be achieved by updating the existing "EBID Personal Data Flow Map" Excel document, which already includes some of the required information.
4	Lack of a comprehensive annual clock for data protection issues.	Establish a clear list of actions for comprehensive, pre-scheduled data protection checks and activities to be performed at specific intervals (an "annual clock") outside of cybersecurity and IT issues. Include verification of records of processing activities, data retention periods, and processing details, as well as regular checks of data protection compliance by IT providers (data processors).
5	Lack of justification for the chosen procedures surrounding penetration testing and vulnerability analysis.	Extend recurring penetration testing and vulnerability assessments to all operational IT systems, with longer recurring periods for non-critical systems. Document the rationale for the chosen recurring periods, including why annual testing for critical IT systems is considered sufficient in the current cyber threat landscape.
6	Draft information cybersecurity and risk mitigation policy not yet approved, and 24/7 SOC, recurring penetration testing and vulnerability detection not yet implemented.	Finalize approval of the information cybersecurity and risk mitigation policy. Implement a 24/7 Security Operations Centre (SOC) and operationalize recurring penetration testing and vulnerability detection. Align the cybersecurity policy

N°	AUDIT FINDING	RECOMMENDATION TO BE ADDRESSED
		with the personal data protection framework being developed.
7	Gaps in the procedure for conducting data protection impact assessments (DPIAs) for planned processing activities.	Develop a comprehensive DPIA methodology and template aligned with Article 35 of the GDPR, including criteria for determining when a DPIA is required, the methodology for conducting it, documentation requirements, and approval workflow involving the Data Protection Officer (DPO).
8	Lack of clear justification for the chosen data protection training practices.	Reassess the data protection training interval, considering more intensive training for all staff (e.g., at least once every six months), given that the topic is new to staff and the training focuses on the GDPR, which is not directly applicable to EBID but which the Bank seeks to align with. Document the rationale for the training frequency and structure adopted.

The list above is not exhaustive. The Consultant shall also identify any additional gaps emerging from the diagnostic phase of the assignment and shall propose appropriate corrective measures.

4. OBJECTIVES OF THE ASSIGNMENT

4.1 General Objective

The general objective of the assignment is to support EBID in developing a comprehensive, GDPR-aligned Personal Data Protection Policy and the associated implementation framework, in order to address the gaps identified by the independent audit and to bring EBID's data protection practices in line with international best practice.

4.2 Specific Objectives

The specific objectives of the assignment are to:

1. Conduct a comprehensive diagnostic of EBID's current personal data protection arrangements, including its Supplementary Law, existing policies, procedures, consent forms, records, training practices and IT security framework, and assess them against the GDPR and other applicable instruments.
2. Develop a Personal Data Protection Policy formally aligned with Article 6 and Article 7 of the GDPR, in particular as regards the legal bases for processing and the requirements applicable to consent.
3. Develop a model for legitimate interest balancing tests (LIA) equivalent to the requirements of the GDPR, benchmarked against the models published by EU data protection supervisory authorities.
4. Develop a Record of Processing Activities (RoPA) framework equivalent to the requirements of Article 30 of the GDPR, building upon and enhancing EBID's existing "Personal Data Flow Map".
5. Develop a Data Protection Annual Clock setting out pre-scheduled compliance checks, reviews and activities to be performed at defined intervals.
6. Develop a Data Protection Impact Assessment (DPIA) methodology and template aligned with Article 35 of the GDPR.
7. Develop a Data Protection Training Plan, with documented justification for the frequency, content and target audience of the training.
8. Develop additional supporting procedures, templates and tools necessary for the effective implementation of the Personal Data Protection Policy (e.g. data subject rights procedure, data breach notification procedure, data processor due diligence checklist, retention schedule).
9. Support EBID in identifying interfaces between the Personal Data Protection Policy and the (draft) Information Cybersecurity and Risk Mitigation Policy, including the rationale for recurring penetration testing and vulnerability assessments.
10. Build the capacity of EBID staff, in particular the Data Protection Officer (or equivalent function), Legal Department, Risk and Compliance Department, Human Resources, IT Department, and Internal Audit, in respect of the new policy and its implementation.

5. SCOPE OF WORK

The scope of work covers all personal data processing activities carried out by EBID at its headquarters in Lomé and, where applicable, in its representations or offices in ECOWAS Member States. The assignment shall encompass, without being limited to:

- Personal data of EBID staff (permanent, contractual, consultants, interns) and former staff.
- Personal data of members of the Board of Directors, Board of Governors, committees, and shareholders' representatives.

- Personal data of customers, borrowers, project beneficiaries, and intermediaries.
- Personal data of contractors, suppliers, service providers, and counterparties.
- Personal data of visitors and persons accessing EBID's premises (including CCTV and access control data).
- Personal data collected through EBID's websites, applications, and digital channels
- Personal data processed by third parties acting as data processors on behalf of EBID.

The applicable legal framework to be considered includes, but is not limited to:

- The Headquarters Agreement and the legal status of EBID as an international organization.
- The Statutes and Supplementary Law of EBID.
- The ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS.
- The European Union General Data Protection Regulation (Regulation (EU) 2016/679 - GDPR) is the benchmark for international best practice.
- Relevant national data protection legislation of EBID Member States, in particular the Togolese law on personal data protection.
- Sector-specific obligations applicable to banking and finance, including AML/CFT, KYC, and prudential reporting.
- Relevant guidelines issued by the European Data Protection Board (EDPB) and national supervisory authorities.

6. SPECIFIC TASKS AND ACTIVITIES

The Consultant shall carry out the following tasks, organized in five (5) phases:

Phase 1 - Inception and Diagnostic

- Hold a kick-off meeting with EBID's project team to refine the methodology, work plan, and timeline.
- Review all relevant EBID documentation (Supplementary Law, existing policies, consent forms, contracts, the existing Personal Data Flow Map, the draft Information Cybersecurity and Risk Mitigation Policy, the audit report, training materials, etc.).
- Conduct interviews with key stakeholders (DPO function, Legal, Compliance, Risk, HR, IT, Internal Audit, Operations, Communications).
- Map all current personal data processing activities.
- Conduct a gap analysis against the GDPR, the ECOWAS Supplementary Act, applicable national laws, and the audit findings.

- Submit an Inception Report including a detailed work plan, methodology, list of stakeholders, list of documents reviewed, and a preliminary gap analysis.

Phase 2 - Drafting of the Personal Data Protection Policy

- Draft a comprehensive Personal Data Protection Policy aligned with Articles 5 to 7 of the GDPR (principles, lawfulness of processing, conditions for consent).
- Ensure the Policy addresses all data subjects' rights (Articles 12–22 GDPR): information, access, rectification, erasure, restriction, portability, objection, and rights related to automated decision-making.
- Define governance roles and responsibilities, including the Data Protection Officer (DPO), Data Owners, Data Stewards, Information Security Officer, and the role of senior management.
- Define the data lifecycle (collection, use, storage, disclosure, retention, destruction) and the principle of data minimization.
- Define rules on international data transfers, particularly in light of EBID's multi-jurisdictional operations.
- Define the regime applicable to data processors and sub-processors, including contractual requirements (data processing agreements, due diligence, audit rights); and
- Define the personal data breach notification and management regime.

Phase 3 - Development of Supporting Tools and Procedures

- Develop the Legitimate Interest Assessment (LIA) model and template.
- Update and enhance the existing Personal Data Flow Map to function as a full Record of Processing Activities (RoPA) under Article 30 of the GDPR, including both controller and processor records as relevant.
- Develop the Data Protection Annual Clock, with a clear schedule of activities, owners, and review frequencies.
- Develop the DPIA methodology, decision tree, template, and approval workflow.
- Develop revised consent forms compliant with Articles 6 and 7 of the GDPR, ensuring that consent is not aggregated with other legal bases.
- Develop the Data Subject Rights handling procedure, including request log, response templates, and timelines.
- Develop the Data Breach Notification procedure, including internal escalation, documentation, and notification to supervisory authorities and data subjects where applicable.
- Develop the Personal Data Retention Schedule applicable across all business units.
- Develop a Third-Party / Data Processor due diligence and contract management checklist.

- Develop the rationale and supporting documentation for the chosen frequencies of penetration testing and vulnerability assessments, distinguishing between critical and non-critical IT systems.

Phase 4 - Training and Capacity Building

- Develop a Data Protection Training Plan with clear justification for the chosen frequency (proposing, where appropriate, a minimum frequency of one session every six (6) months for all staff during the first two (2) years following adoption of the Policy).
- Develop training materials targeting (i) all staff (general awareness), (ii) data owners and stewards (operational), and (iii) senior management and the Board (governance).
- Deliver an initial Training-of-Trainers (ToT) session for the DPO and identified champions; and
- Deliver at least one (1) general awareness session and one (1) executive briefing session.

Phase 5 - Finalization and Handover

- Present the draft Policy and supporting framework to EBID's relevant committees.
- Integrate comments and feedback from EBID.
- Submit the final versions of all deliverables in English and French.
- Provide an implementation roadmap covering at least 24 months, with prioritized quick wins and longer-term actions.
- Deliver a closure report summarizing the work performed, the gaps closed, residual risks, and recommendations for continuous improvement.

7. EXPECTED DELIVERABLES

The Consultant shall produce the following deliverables, all of which shall be submitted in English and French, in editable electronic format (Microsoft Word, Excel, PowerPoint as appropriate) and in PDF:

N°	DELIVERABLE	PHASE	INDICATIVE DEADLINE
D1	Inception Report (methodology, work plan, stakeholder map, preliminary gap analysis).	Phase 1	Week 1 after kick-off
D2	Diagnostic and Gap Analysis Report.	Phase 1	Week 3
D3	Draft Personal Data Protection Policy.	Phase 2	Week 5

N°	DELIVERABLE	PHASE	INDICATIVE DEADLINE
D4	Supporting tools and procedures: LIA model, RoPA, Annual Clock, DPIA methodology and template, revised consent forms, Data Subject Rights procedure, Data Breach Notification procedure, Retention Schedule, and Data Processor due diligence checklist.	Phase 3	Week 8
D5	Penetration testing/vulnerability assessment frequency rationale document.	Phase 3	Week 9
D6	Data Protection Training Plan and training materials.	Phase 4	Week 10
D7	Delivery of Training-of-Trainers, general awareness, and executive briefing sessions.	Phase 4	Week 11
D8	Final Personal Data Protection Policy, full set of consolidated tools and procedures, implementation roadmap (24 months), and closure report.	Phase 5	Week 12

Each deliverable shall be reviewed by EBID and shall be subject to approval by EBID's designated focal point before being considered as accepted. EBID shall communicate its comments within ten (10) working days of receipt of each deliverable.

8. DURATION AND TIMELINE OF THE ASSIGNMENT

The total duration of the assignment is estimated at twelve (12) calendar weeks, equivalent to approximately five and a half (3) months, from the date of signature of the contract. This duration includes the time required for EBID to review and provide feedback on each deliverable.

The Consultant shall propose a detailed work plan in the Inception Report, including the proposed allocation of consultant days per phase and per expert profile. The proposed timeline shall be reasonable and consistent with the assignment's complexity.

9. METHODOLOGY AND APPROACH

The Consultant shall adopt a participatory, evidence-based, and risk-oriented methodology, including at least the following elements:

- Documentary review of all relevant EBID documents and applicable legal instruments.
- Structured interviews and workshops with EBID stakeholders.
- Benchmarking against good practice in comparable multilateral development banks and international financial institutions.
- Use of GDPR-aligned reference materials, in particular guidelines published by the European Data Protection Board (EDPB) and supervisory authorities.
- Iterative validation of drafts with EBID's project team and the relevant Departments.
- Quality assurance, including peer review of deliverables within the Consultant's team.

All work shall be conducted in close cooperation with EBID's designated focal point, who will serve as the Consultant's primary point of contact throughout the assignment. The Consultant shall be expected to carry out at least two (2) on-site missions at EBID's headquarters in Lomé during the course of the assignment (kick-off and validation), with the remainder of the work conducted remotely or on-site as agreed.

10. QUALIFICATIONS AND EXPERIENCE OF THE CONSULTANT

The assignment may be carried out by a consulting firm, a law firm with a dedicated data protection practice, or a consortium thereof. The Consultant shall mobilize a multi-disciplinary team comprising at least the following key expert profiles:

10.1 Team Leader / Senior Data Protection Expert

- A master's degree (or equivalent) in Law, with a specialization in data protection, privacy law, or information technology law.
- A minimum of twelve (12) years of professional experience in data protection and privacy advisory work.
- Recognized data protection certification (e.g. CIPP/E, CIPM, CIPT, or equivalent) is required.
- Demonstrated experience in developing data protection policies for at least three (3) international organizations, financial institutions, or large corporate clients.
- In-depth knowledge of the GDPR, the ECOWAS Supplementary Act on Personal Data Protection, and at least one (1) national data protection regime within the ECOWAS region.
- Excellent drafting and presentation skills in English and working knowledge of French (or vice versa).

10.2 Legal Expert - ECOWAS / National Data Protection Laws

- A master's degree (or equivalent) in Law.
- A minimum of eight (8) years of professional experience, including significant exposure to data protection legislation within ECOWAS Member States.
- Sound understanding of the legal status and immunities of international organizations.
- Fluency in English and French is highly desirable.

10.3 IT Security and DPIA Expert

- A degree in Computer Science, Information Security, Engineering, or a related field.
- A minimum of eight (8) years of professional experience in information security and risk management, including DPIA, penetration testing oversight, and vulnerability management.
- Recognized certification (e.g., CISSP, CISM, ISO 27001 Lead Auditor / Implementer, CDPSE) is required.
- Experience advising financial institutions on the interaction between information security and personal data protection.

10.4 Training and Change Management Expert

- A degree in a relevant discipline (Education, Communication, Human Resources, Law, or related).
- A minimum of six (6) years of experience in the design and delivery of compliance and/or data protection training.
- Demonstrated experience in adult learning methodologies and in training-of-trainers approaches.

10.5 Firm-level Requirements

- The Consultant (firm) shall be a legally registered entity with at least ten (10) years of existence.
- At least five (5) similar assignments carried out in the past seven (7) years, of which at least one (1) for a multilateral development bank, an international organization, or a regional financial institution.
- Demonstrated capacity to deliver assignments in both English and French.
- No conflict of interest with EBID, its shareholders, or its main counterparties.

11. REPORTING AND SUPERVISION

The Consultant shall report to EBID's designated focal point (hereinafter the "Project Sponsor"), who shall be supported by a Steering Committee comprising representatives of the Legal Department, the Risk and Compliance Department, Human Resources, the IT Department, the Internal Audit Department, and the Data Protection Officer function.

The Steering Committee shall meet at least at the following milestones:

- At kick-off (Week 1).
- At the validation of the Inception Report (Week 1).
- At the validation of the Diagnostic and Gap Analysis Report (Week 3).
- At the validation of the draft Policy (Week 5).
- At the validation of the supporting tools (Week 8).
- At project closure (Week 12).

The Consultant shall submit fortnightly progress notes to the Project Sponsor, summarizing activities carried out, deliverables in progress, risks and issues, and any required decisions or inputs from EBID.

12. CONFIDENTIALITY AND DATA PROTECTION

All information made available to the Consultant in the course of the assignment shall be treated as strictly confidential. The Consultant and each member of its team shall sign a Non-Disclosure Agreement (NDA) prior to the commencement of the assignment.

The Consultant shall not disclose, publish, reproduce, or use any confidential information obtained from EBID for any purpose other than the performance of the assignment, without the prior written consent of EBID. The confidentiality obligation shall survive the termination of the contract.

Where the Consultant accesses personal data in the course of the assignment, the Consultant shall act as a data processor on behalf of EBID and shall comply with all reasonable instructions of EBID, with the principles of the GDPR and the ECOWAS Supplementary Act, and with appropriate technical and organizational measures.

13. INTELLECTUAL PROPERTY RIGHTS

All deliverables, reports, tools, templates, training materials, and other documents produced by the Consultant in the performance of the assignment shall become the exclusive property of EBID upon payment of the corresponding fees. EBID shall have the unrestricted right to use, modify, reproduce, and distribute such deliverables for its own purposes, including for adaptation to subsequent versions or for use by its subsidiaries and affiliated entities.

The Consultant warrants that the deliverables do not infringe any third-party intellectual property rights and indemnifies EBID against any claim arising from such infringement.

14. SELECTION CRITERIA AND EVALUATION

The selection of the Consultant shall be carried out in accordance with Quality and Cost Base Selection. The evaluation shall be conducted on the basis of a combined technical and financial assessment, with the following indicative weightings:

EVALUATION CRITERION	MAXIMUM SCORE	WEIGHTING
Technical Proposal	100 points	80%
a) General experience of the firm in similar assignments	15	
b) Specific experience in data protection / GDPR assignments for international organizations or financial institutions	20	
c) Adequacy and quality of the proposed methodology and work plan	25	
d) Qualifications and competence of the proposed key experts	30	
e) Language and regional capability (English/French, ECOWAS experience)	10	
Financial Proposal	100 points	20%
TOTAL		**100%**

The minimum technical score required for a proposal to be considered substantially responsive is 80 points out of one hundred (100). Proposals scoring below this threshold shall not be considered further, and the financial proposal shall not be opened.

15. SUBMISSION OF PROPOSALS

Interested consultants shall submit their technical and financial proposals in electronic means (email) provided below:

Email: ichabimougnan@bidc-ebid.org/secretariatdasg@bidc-ebid.org **No later than 31 August 2026 at 11:59 p.m. (GMT).** Any bids received after this deadline will not be considered.

For any request for additional information, please send an email to the above-mentioned addresses.

EBID reserves the right to request clarifications, to invite shortlisted candidates for an interview or presentation, to reject any or all proposals, and to cancel the procurement process at any stage, without incurring any liability towards the candidates.

16. CONTRACT AND PAYMENT TERMS

The selected Consultant shall enter a lump-sum contract with EBID. The contract shall include, among others, standard provisions relating to deliverables, intellectual property, confidentiality, data protection, liability, force majeure, suspension and termination, applicable law, and dispute resolution.

Payments shall be made in installments linked to the validation of deliverables, in accordance with the following indicative schedule:

- Fifty per cent (50%) upon signature of the contract and submission of the Inception Report (D1).
- Zero (0%) upon validation of the Diagnostic and Gap Analysis Report (D2).
- Zero (0%) upon validation of the draft Personal Data Protection Policy (D3).
- Twenty-five per cent (25%) upon validation of the supporting tools and procedures (D4 and D5).
- Zero per cent (0%) upon validation of the Training Plan, materials, and delivery of training sessions (D6 and D7).
- Twenty-five per cent (25%) upon validation of the final deliverables, implementation roadmap, and closure report (D8).

Payment shall be made within thirty (30) calendar days of EBID's validation of the specified payment under deliverables and receipt of a corresponding invoice.

17. ANNEXES

The following documents shall be made available to the selected Consultant upon signature of the Non-Disclosure Agreement and prior to the start of the assignment:

- Annex 1: Audit Report - Findings and Recommendations on Data Protection.
- Annex 2: EBID Supplementary Law and existing data protection policy (current version).
- Annex 3: EBID Personal Data Flow Map (Excel).
- Annex 4: Draft Information Cybersecurity and Risk Mitigation Policy.

- Annex 5: Current consent forms in use.
- Annex 6: Current data protection training materials.
- Annex 7: EBID Organizational Chart and list of departments concerned.
- Annex 8: EBID Procurement Rules and Standard Contract Template.
- Annex 9: Non-Disclosure Agreement template.