



BANQUE D'INVESTISSEMENT ET DE DEVELOPPEMENT DE LA CEDEAO  
ECOWAS BANK FOR INVESTMENT AND DEVELOPMENT  
BANCO DE INVESTIMENTO E DE DESENVOLVIMENTO DA CEDEAO

**ORIGINAL : FRENCH**

**N°RES.12/07/24/BIDC/EBID/CA/BD/88**

# **GENERAL POLICY ON PERSONAL DATA PROTECTION IN EBID**

-----  
General policy on personal data protection in EBID

## TABLE OF CONTENTS

<b>LIST OF ABBREVIATIONS .....</b>	<b>3</b>
<b>DEFINITIONS.....</b>	<b>4</b>
<b>1. PREAMBLE .....</b>	<b>6</b>
<b>1.1. Scope of application.....</b>	<b>6</b>
<b>1.2. Entry into Force .....</b>	<b>6</b>
<b>2. INTRODUCTION.....</b>	<b>6</b>
<b>3. LEGAL MEASURES .....</b>	<b>7</b>
<b>3.1. Legal Framework – Applicable law .....</b>	<b>7</b>
<b>3.2. Data Protection Authority .....</b>	<b>7</b>
<b>3.3. Data Protection Officer .....</b>	<b>7</b>
<b>4. TECHNICAL MEASURES .....</b>	<b>8</b>
<b>4.1. Data Storage and Organisation .....</b>	<b>8</b>
<b>4.2. CBS, HRIS and other software .....</b>	<b>8</b>
<b>4.3. Electronic Management of Documents (DEM) .....</b>	<b>8</b>
<b>4.4. Limitation of storage time .....</b>	<b>9</b>
<b>4.5. Safety .....</b>	<b>9</b>
<b>5. ORGANIZATIONAL MEASURES .....</b>	<b>9</b>
<b>5.1. Information gathering .....</b>	<b>9</b>
<b>5.2. Legitimate, equitable and transparent processing .....</b>	<b>9</b>
<b>5.3. Limitation of objectives and data minimisation .....</b>	<b>10</b>
<b>5.4. Data accuracy .....</b>	<b>10</b>
<b>5.5. Data transfer .....</b>	<b>10</b>
<b>5.6. Rights of the person concerned .....</b>	<b>10</b>
<b>5.7. Data violations .....</b>	<b>11</b>
<b>6. RESPONSIBILITIES .....</b>	<b>11</b>
<b>6.1. Roles and Responsibilities.....</b>	<b>11</b>
<b>7.ANNEXES.....</b>	<b>12</b>

## List of abbreviations

<b>DPIA</b>	Data Protection Impact Analysis
<b>EBID</b>	ECOWAS Bank for Investment and Development
<b>BOD</b>	Board of Directors
<b>CBS</b>	Core Banking System. That is the computer-based system which the bank chose for the management of its activities
<b>DPO</b>	Data Protection Officer
<b>GED</b>	Document Electronic Management

## Definitions

**Data protection authority:** Independent national administrative authority saddled with ensuring that personal data processing be carried out in line with the provisions of the existing regulations (Supplementary Act).

**Code of conduct:** Utilization charters prepared by the Data Processing Officer to establish a correct usage of computer-based resources, Internet, and electronic communication in EBID.

**Consent of the person concerned:** Any demonstration of express, unambiguous, free, specific and informed willingness by which the person concerned, or his legal, judicial or conventional representative accepts that his personal data be processed manually or electronically.

**Data Protection Officer: Data Protection Officer (DPO):** Person in charge of protection of personal data at the EBID. He will be the privileged contact person for all issues relating to personal data, be it within from sub-contractors or from a person concerned by a transaction carried by the bank. The DPO will also be the privileged contact person of the Data Protection Authority.

**Data of personal nature or Personal Data:** Any information relating to an identified physical person or person identifiable directly or indirectly through reference to an identification number or one or several aspects typical of his physical, physiological, genetical, psychical, cultural, social, or economic identity.

**Document Electronic Management (DEM):** EBID is using the Microsoft software for its routine management (Office 365 and Point among others).

**HRIS:** Human Resources Information System.

**Partner:** Any physical or moral, private, or public entity, any other organization or association with which EBID is collaborating for the purpose of achieving the end result of a processing.

**Person Concerned:** Any physical person whose personal data are being processed.

**Processing Officer:** EBID, individual or jointly with other, takes the decision to collect and process personal data and determine its end objectives.

**Sub-contractors:** Any physical or moral person, public or private; any other organization or association that processes data on behalf of the processing officer (EBID).

**Processing of personal data:** Any operation or set of operations carried out or not with the aid of automated process and applied to data such as collection, utilization, recording, organization, conservation, adaptation, amendment, extraction, back up, copying, consultation, extraction, using, communication via transmission, broadcast or any other form of making information available, reproachment or interconnection as well as locking up, encryption, erasing or destruction of personal data.

## **1. Preamble**

As part of its efforts to strengthen its management and governance systems, the Bank decided to define a set of rules applicable to the protection of personal data. Accordingly, it opted to draw from the body of existing legislation.

The purpose of this new set of rules is to establish the general policy to guarantee a high level of personal data protection in transactions between the Bank and its partners.

EBID is putting in place some legal, technical, and organizational parameters capable of guaranteeing legal, equitable and transparent personal data processing. These measures are brought together in the current “General Policy on Personal Data Protection” hereafter referred to as “the policy”.

### **1.1. Scope of application**

The policy shall apply to all personal data processing carried out to fulfil the purposes of the bank in line with the chosen legal framework. Except in case of exemptions, (for example safety files or processing relating to penal cases which are governed by Member States).

In practical terms, the regulation shall be applicable each time that a partner of EBID, whatever may be his nationality, is targeted by a data processing including through internet or connected devices.

### **1.2. Entry into force**

## **2. Introduction**

The personal data protection policy shall stipulate the manner in which personal data are collected as well as the way in which they are processed, divulged and eventually transferred to the third parties the policy also describes the manner in which the rights of the person concerned are managed.

The policy has been crafted to comprise 3 criteria:

- Legal measures,
- Technical measures,

- Organisational measures.

### **3. Legal measures**

#### **3.1. Legal framework – Applicable law**

EBID has endowed itself with a harmonized framework for securing personal data thereby strengthening the rights of the persons, the obligations of the bank, its sub-contractors and partners. This framework is based on the following documents:

- Supplementary Act on the protection of personal data in ECOWAS (A/SA. 1/01/10)

In case of any doubt, shortcoming or imprecision, the bank will have recourse to:

- General Regulations on Data Protection (RGPD) (UE 2016/679)

#### **3.2. Data Protection Authority**

EBID being an international organization, the supervisory body in terms of data protection will therefore be the ECOWAS Court of Justice.

#### **3.3. Data Protection Officer**

The officer in charge of personal data protection is EBID represented by its President. The officer determines the purposes and means to be implemented.

The sub-contractor shall process the personal data solely on account of the processing officer. The sub-contractor is generally a third party from outside the Bank.

The duties of the sub-contractor towards the officer in charge of data processing (EBID) must be clearly spelt out in a contract or in another legal act. The data sub-contractor may not recruit another joint sub-contractor to carry out part of the job except if he receives a prior written permission from the processing officer.

## **4. Technical Measures**

### **4.1. Data storage and organisation**

Personal data protection policy calls for a rational organization of files. This structuring of information will be done by means of the computer-based tools used by the Bank: the CBS, HRIS, REFINITV Office 365, other software used and to be used by the Bank as well as Electronic Document Management (EDM) software.

### **4.2. CBS, HRIS and other software**

Software that processes personal data must be compliant in terms of personal data protection. They must particularly comply with the following points:

- The consent of the individual before the collection and processing of the data.
- The right to access one's own data, correct them and delete same.
- The obligation for EBID to take appropriate safety measures to protect its data.
- Confidentiality by design: data protection is mainstreamed into the designing of the software and not added later.
- In case of violation of data, EBID will maintain the record of observed violations.

In conclusion, if a software is used to collect, store or process personal data, it must be designed and maintained in such a way as to comply with existing data protection laws and regulations.

The software used by EBID provides the necessary guarantees to comply with the GDPR.

### **4.3. Electronic Management of Documents (DEM)**

DEM organises documents and associated data. It allows for the optimisation of their management, safety and utilisation through specialized and effective electronic devices.

The automatic nature of DEM makes personal data, their management, access, utilization more reliable and enables the users to devote more attention to their jobs with some

degree of value addition by reducing the risk of forgetfulness and error.

#### **4.4. Limitation of storage time**

Personal data shall not be kept in a form that allows for the identification of persons more than as long as needed for the attainment of objectives for which they were collected or for a later processing compatible with this policy.

The storage time for personal data is fixed in accordance with the storage periods stipulated in the 'Policy and Procedures of the Documentation and Archives Centre of the ECOWAS Bank for Investment and Development (EBID)'.

#### **4.5. Safety**

Personal data shall be protected by appropriate legal, technical, and organizational guarantees against unauthorized, loss, destruction or accidental damages.

### **5. Organizational measures**

#### **5.1. Information gathering**

Personal data collection consists in gathering personal information by some means be it (manual forms or online, recovery on a data base, ...), whatever may be the purposes.

EBID shall take necessary measures to crosscheck that the said personal data are relevant, accurate, complete and up to date and that they tally with the purposes for which they are to be used. No personal data will be collected if it does not meet up with the purposes defined by the processing officer.

EBID shall collect personal data in a legitimate, equitable and transparent manner.

#### **5.2. Legitimate, equitable and transparent processing**

Personal data shall be processed for legitimate, equitable and transparent purposes in line with this policy.

These purposes of processing shall be:

- a) carried out with the consent of the person concerned;
- b) carried out in the interest of the person concerned;
- c) necessary for the implementation of a contract or honouring an obligation or a binding commitment; or
- d) compatible with, or reasonably necessary to enable the Bank fulfil very perfectly its mission, mandate or objective as an international organization.

### **5.3. Limitation of objectives and data minimization**

Personal data shall be collected for one or several specific and legitimate purposes and shall not be processed thereafter in a manner that is incompatible with the initial purpose(s) for which they were collected; the later processing for the purpose of keeping them in the archives, research or statistics shall not be considered as incompatible with the initial purpose. The quantity and nature of the collected personal data must be necessary and proportionate to the legitimate purposes for which they are processed.

### **5.4. Data accuracy**

Personal data shall be recorded as precisely as possible and, where necessary, update so as to guarantee that they meet up with the legitimate purposes for which they are processed.

### **5.5. Data transfer**

Personal data shall not be transferable to third parties than for the legitimate purposes and in furtherance of the policy governing personal data protection.

### **5.6. Rights of the person concerned.**

The person concerned must have the right to access personal data which have been collected concerning him. He must be able to exercise this right easily and at a reasonable interval so as to take due cognizance of the processing and verify its legality.

## 5.7. Data violations

EBID shall implement an effective process for the notification of eventual data violation.

The DPO will follow strictly the policies and procedures concerning the management of such a violation. The staff of EBID, its partners and sub-contractors are required to immediately report any data violation be it voluntary or otherwise, to the DPO. On his own part, the DPO will inform the processing officer of the violation and keep him informed about measures taken.

## 6. Responsibilities

The Bank shall adopt necessary procedures to:

- a) Supervise compliance with this policy and as such, have a Data Protection Officer (DPO). The description of the function of the DPO is furthermore presented.
- b) Furnish the person concerned with a method subject to common use, to:
  - i. ask for information on persona data processed by the bank and
  - ii. ask for the correction or deletion if the person concerned has reasons to believe that his personal data have been processed in violation of this policy.
- c) Train his staff on personal data protection by defining the guidelines, purposes of the bank.

### 6.1. Roles and Responsibilities

**The President:** as the officer in charge of processing, he shall report to the Board of Directors (BoD). He shall be responsible for the effective formulation, deployment and management of personal data protection policy. He shall provide leadership and training for members of the Top Management by determining the orientations and the purposes of the Bank.

**The DPO:** He shall be in charge of personal data protection at the EBID. He shall be the privileged contact person on all issues relating to personal data, be they internal from the sub-contractors or emanating from a person concerned by a processing carried out by the Bank. The DPO will also be the privileged contact person of the Data Protection Authority.

**Staff of each department:** In all the departments, a person will be responsible for informing the DPO of all incidents (collection of new information, changes in the processing, voluntary violation or otherwise, ...) on personal data protection.

## **7. Annexes**

**A** - Procedure for managing and notifying personal data breaches.

**B** - Procedure for managing the rights of the person concerned.

**C** - Data protection charter for EBID partners

**D** - Data protection charter for subcontractors

**E** - Data protection charter for staff

## **ANNEX A**

**EBID GENERAL POLICY ON PERSONAL DATA  
PROTECTION:**

# **GUIDELINES FOR THE MANAGEMENT AND NOTIFICATION OF PERSONAL DATA BREACHES**

## CONTENTS

<b>1. PREAMBLE.....</b>	<b>15</b>
<b>2. INTRODUCTION.....</b>	<b>15</b>
<b>2.1. Applicable rules on data breach notification .....</b>	<b>15</b>
<b>2.2. Purpose of the guidelines.....</b>	<b>16</b>
<b>3. GUIDELINES.....</b>	<b>16</b>
<b>3.1. What is a personal data breach .....</b>	<b>16</b>
<b>3.2. Guidelines for the management of personal data breaches .....</b>	<b>17</b>

## **1. Preamble**

EBID has adopted ‘Guidelines for the Management and Notification of Personal Data Breaches’.

As part of the implementation of its personal data protection policy, EBID is taking legal, technical and organisational measures to ensure that personal data is processed lawfully, fairly and transparently. One of the organisational measures concerns the voluntary or involuntary personal data breach.

## **2. Introduction**

### **2.1. Applicable rules on data breach notification**

As the Supplementary Act (A/SA. 1/01/10) only briefly touches on the management of breaches in Article 43, EBID will therefore be relying on the provisions of the General Data Protection Regulation, known as the GDPR (EU 2016/679).

The purpose of the rules applicable to the protection of personal data is not only to strengthen the rights of individuals about Processing but also to prevent any personal data breach (unauthorised access, leakage, etc.) and therefore prevent any damage to both the data controller and the data subjects. The controller will therefore be obliged to guarantee an appropriate level of security for personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.

Notification must therefore be an integral part of the breach management process.

EBID acts as the data controller for the processing of the personal data of its employees and for the personal data of its partners and subcontractors

As such, the EBID institutes measures to prevent personal data breaches and implements measures to enable it to react quickly in the event of an incident.

At EBID, the DPO is the focal point for notification personal data breaches. The DPO must identify the report's relevance and to whom it should be sent.

## **2.2. Purposes of the guidelines**

The purpose of these guidelines are to :

- Define personal data breaches;
- Describe the guidelines in the event of the detection of a personal data breach;
- Describe the guidelines for notification a personal data breach and;
- Present the documents that should be kept up to date to justify that notifications of breaches have been noted.

The DPO will decide which persons or entities to report to. Namely:

- The data subject,
- The ECOWAS Court of Justice,
- The supervisory authority of the country concerned,
- Any other authorities they deem useful to inform.

## **3. Guidelines**

Breaches can be " breach of confidentiality ", where there is unauthorised or accidental disclosure or access to personal data, " breach of availability ", where there is accidental or unauthorised loss of access to or destruction of personal data, and " breach of integrity ", where there is accidental or unintentional tampering with personal data.

### **3.1. What is a personal data breach?**

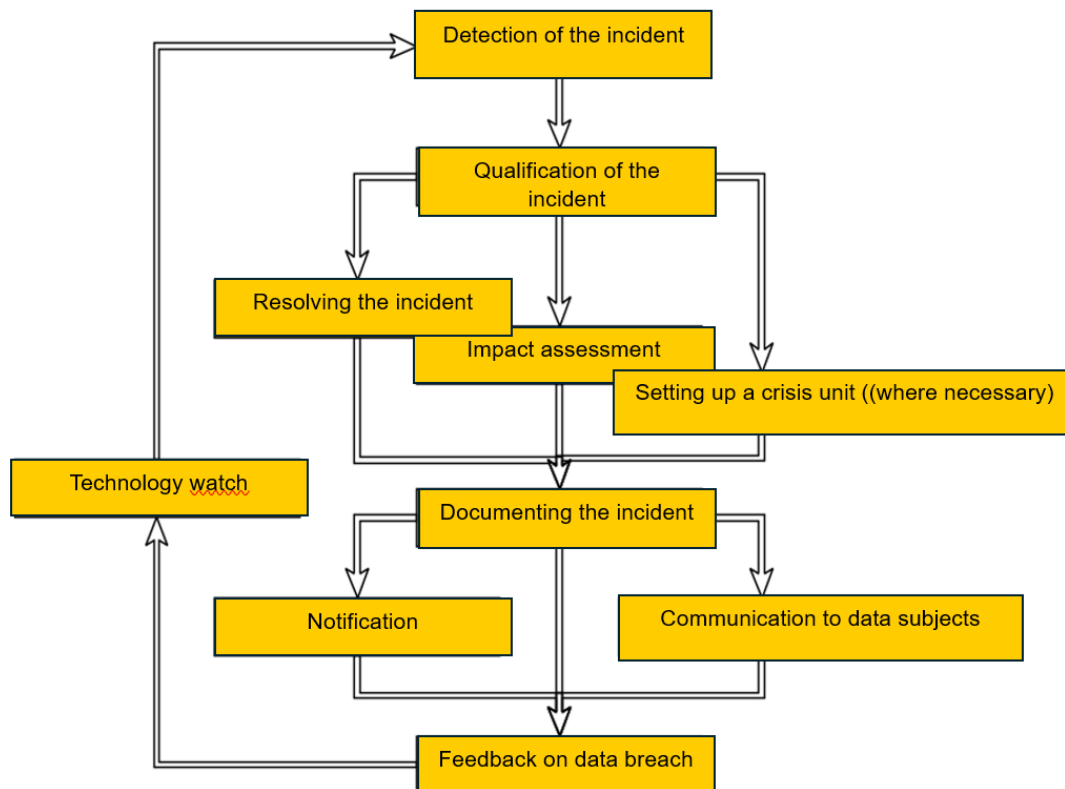
A data breach occurs when data for which EBID is responsible suffers a security incident that results in a breach of confidentiality, availability or integrity. In this case, and if the breach is likely to cause a risk to the rights and freedoms of an individual, EBID notifies the supervisory authority as soon as possible.

If the data breach creates a high risk for the affected individuals, then the latter should also be notified unless effective technical and organisational protection measures or other measures that ensure that the risk is no longer likely to materialise have been instituted

It is vital that EBID institutes appropriate technical and organisational measures to prevent potential data breaches.

### 3.2. Guidelines for management of personal data breaches

The Data Protection Regulation requires data controllers to take appropriate measures to resolve the breach, ensure that the breach does not recur, if necessary, notify the competent supervisory authority and warn interested parties where the risk is high.



To manage a data breach as effectively as possible, EBID must organise itself upstream. An internal procedure for assigning tasks should therefore be put in place, including a RACI (R: Responsible, A: Authority, C: Consulted, I: Informed).

Tasks	Dpt Inf.Tech & Org of Meth	RSSI	DPO	Dpt & Champions	Legal Dept.	Comm & Ext. Rel Dept	Office of the President
<b>Monitoring threats</b>	C	R	C	R	I		
<b>Detection of the incident</b>	I	I	I	R			
<b>Qualification of the incident</b>	I	A	I	R	I		
<b>Resolving the incident</b>	I	R	I	I	I		
<b>Impact assessment</b>		I	I	R	I		
<b>Setting up a crisis unit (where necessary)</b>	C	R	C	C	C		A
<b>Documenting the incident</b>	C	C	R	C	C		
<b>Notification of the incident (where necessary)</b>	I	I	R		I	I	I
<b>Communication to data subjects</b>		I	R	I			
<b>Feedback on data breach</b>	C	A	R	I	I	I	I

❖ **Step 1 : Detection of the incident (personal data breach)**

EBID can be said to be aware of the breach as soon as it attains a reasonable level of certainty that a security incident has occurred and that this incident has compromised Personal Data.

In some cases, it will be quite clear from the outset that a breach has occurred, while in other cases it may take some time to ascertain whether the data has actually been compromised.

Immediate action is required to investigate the incident and determine whether Personal Data has been violated and, if so, to take corrective action.

## ❖ Step 2 : Qualification of the incident

After being informed of a potential breach or when it has itself detected a security incident, the controller may undertake a brief period of investigation in order to establish whether a breach has in fact occurred.

EBID must therefore introduce internal processes to detect and deal with a breach. The controller must also have agreements in place with its subcontractors, who are also required to inform EBID in the event of a breach.

During the very brief qualification period, the EBID may be unaware of the actual existence of the breach. This brief period allows for investigation, evidence gathering and risk assessment.

The criteria for deciding whether the risk is significant are the following::

- type of breach affecting the integrity, confidentiality or availability of the data, sensitivity and volume of the personal data concerned,
- ease of identifying those affected by the breach,
- possible consequences of the breach for individuals, characteristics of these individuals (children, vulnerable individuals, etc.),
- the tasks of the data controller.

## ❖ Stage 3, a and b: Resolution, Impact assessment and the crisis unit

As soon as EBID confirms with a reasonable degree of certainty that a breach has occurred, it must inform its DPO. The DPO will decide whether to notify the ECOWAS Court of Justice and/or the relevant Supervisory Authority.

**Loss or theft of computer hardware:** Loss or theft of computer hardware or any data medium is reported to the head of the department concerned, who assesses the likelihood of a breach and, where appropriate, informs the DPO.

Note: unused IT hardware is systematically reset and therefore no longer contains personal data.

**Loss or theft of paper documents, files or other documents, hereinafter referred to as "paper documents":** Loss or theft of paper documents is reported to the head of the

department concerned, who assesses the likelihood of a breach and, if necessary, informs the DPO.

Note: unarchived and unused paper documents are systematically destroyed and therefore no longer contain personal data.

**Breach of personal data:** Any security incident, whether malicious or not and whether intentional or not, which has the effect of compromising the integrity, confidentiality or availability of personal data, regardless of how it is detected, will be notified by the competent head of department, the DPO and the Information Systems Security Manager.

In assessing the risks, the following principles shall be taken into account to determine whether notification is necessary:

- the data disclosed has already been made public ;
- the deletion of backed-up data has been immediately restored;
- the loss of data protected by an encryption algorithm, the encryption key is not compromised and a copy of the data remains available.

Disclosure of personal data on social networks or chatbots: The massive collection of personal data from social networks, like all data processing, must comply with the rules in force. The fact that data available on social networks is "public" or possibly "freely accessible" does not mean that it loses its status as personal data.

Chatbots are software applications that enable users to talk to a programme designed to provide them with information. They are used to provide answers to the most frequently asked questions, while delivering this information in a targeted, relevant and interactive manner. To do this, personal data is often processed, for example to keep a record of the conversation, even if the service is available without creating an account or directly identifiable information.

The processing of such data (consultation, extraction, recording, enrichment, etc.) must therefore be fair and lawful.

**❖ Stage 4 : Documenting the incident (Record of data breaches), notification and communication to the data subject concerned**

The documentation must record the facts of the personal data breach, its effects and the measures taken to remedy it.

The DPO updates the record of breaches and is responsible for deciding whether or not to inform the supervisory authority and the data subject.

**❖ Stage 5 : Feedback on data breach**

Data protection has always been a matter of technology. It was the advent of computers in the world of business and public administration that led to the development of data protection laws and principles. The development of IT tools has made it necessary to keep up to date with the management of personal data.

The aim of providing feedback and maintaining a technology intelligence is to:

- Draw up and update a map of requirements in terms of personal data protection;
- Define the key steps to resolve incidents quickly and, more generally, keep guidelines for compliance with the personal data protection up to date.

## **ANNEX B**

EBID GENERAL POLICY ON PERSONAL DATA  
PROTECTION:

### **GUIDELINES FOR MANAGING THE RIGHTS OF THE DATA SUBJECT**

## CONTENTS

<b>1. PREAMBLE.....</b>	<b>24</b>
<b>2. INTRODUCTION.....</b>	<b>24</b>
<b>3. MESURES TO BE ADOPTED.....</b>	<b>24</b>
<b>4. GUIDELINES.....</b>	<b>24</b>
<b>4.1. Purpose of the guidelines.....</b>	<b>24</b>
<b>4.2. Modalities for processing requests.....</b>	<b>25</b>
<b>4.3. Processing period.....</b>	<b>28</b>

## 1. Preamble

EBID has adopted "guidelines for the management of the rights of data subject".

As part of the implementation of its personal data protection policy, EBID is instituting legal, technical and organisational measures to guarantee the lawful, fair and transparent processing of personal data. One of the organisational measures concerns the rights of the data subject.

## 2. Introduction

Individuals whose data is processed by the bank have rights over this data:

- right to **information** (a person's right to be informed of the information held by the data controller)
- right of **access** (a person's right to know the purposes of the processing)
- right to **object** (the right of an individual to object to the processing of his or her data)
- right of **rectification** and right to **deletion** (a person's right to request that their data be rectified, completed, updated or deleted).

The Bank must guarantee them the means to effectively exercise their rights and make provision for the tools that will enable their rights to be taken into account, in its IT systems.

## 3. Measures to be adopted

In order to achieve its objectives, the controller, EBID, processes personal data. Any person who works with EBID, i.e. employees, staff of subcontractors, lenders and beneficiaries, may be concerned by this processing. EBID has taken steps to show where and how individuals can exercise their rights with respect to their personal data.

In any event, the number of requests to exercise these rights is relatively limited.

## 4. Guidelines

### 4.1. Purpose of the guidelines

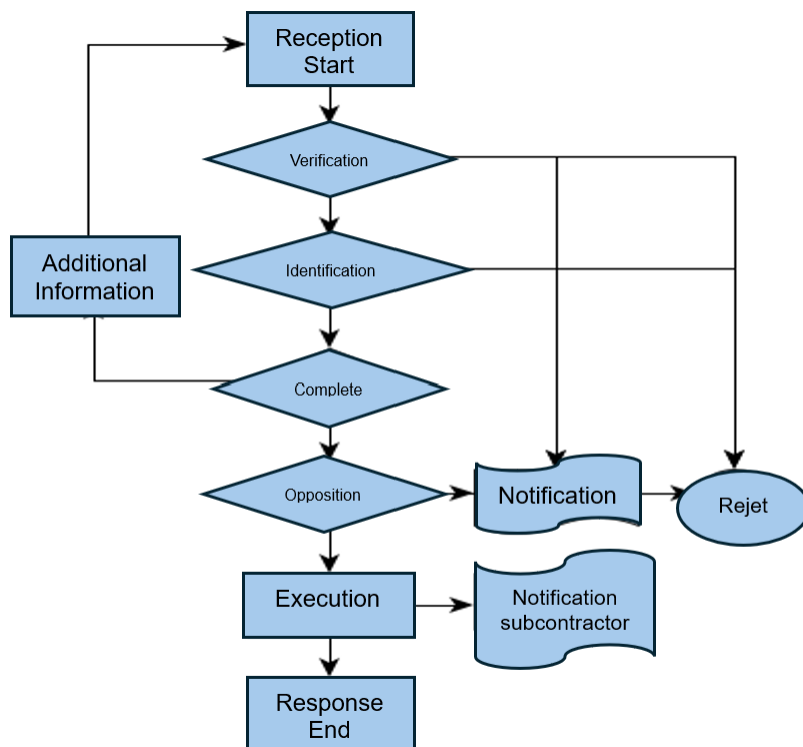
The purpose of these guidelines are to:

- describe the steps for processing requests for exercising these rights,
- keep up-to-date documentation reflecting the requests for processing

#### 4.2. Modalities for processing of requests

Requests are processed in 4 stages:

- Validation of the request
- Consideration of the request
- Executing the request
- Response and archiving the request.



*Diagram 1 : Request processing guidelines*

## ❖ Step 1 : Validation of the request

Requests are received :

- By mail to : [dpo@bidc-ebid.org](mailto:dpo@bidc-ebid.org)
- By post to the Bank's address: Data Protection Officer (DPO), ECOWAS Bank for Investment and Development (EBID), 128 Boulevard du 13 janvier, BP 2704, Lomé, Togo
- Requests to exercise rights are not accepted orally.

First of all, there is the need to ensure that the request received actually concerns the exercise of rights in respect of personal data. If the request received does not concern personal data (e.g. sending a job application), the action to be taken on the request depends on the assessment of the DPO who receives the request.

The DPO ensures that the request is valid; the email may have been sent by a robot or sent several times; the email may also have been sent by a person who is not entitled to information. In all cases, there must be a notification to the record of breaches. The validity examination phase is crucial, as the consequences of sending information to a wrong person can have serious consequences.

The DPO identifies the person making the request (name, contact details, possible link with EBID) and records the request in a file.

## ❖ Step 2 : Consideration of the request

The DPO determines the type of request (right to information, right to object, right to rectification and deletion).

If the DPO does not have all the information required to process the request, he will request the person who made the request for further information by post or e-mail. If such a step is necessary, it must also be documented.

	<b>Reason for objection</b>
Request for information or access	If the request is blatantly abusive, repetitive, or systematic
Request for objection	If there are compelling reasons overriding the rights and freedoms of Persons or as part of the dispute, exercise or defence of a right before the courts.
Request for rectification or deletion	The request may be rejected if it is clearly misleading. The data controller must always have accurate and up-to-date data. Legal or regulatory obligations requiring the data to be kept.

*Table 1: Summary table of the different reasons for objection*

In the event of an objection, the DPO must inform the person who made the request and record the request.

### **❖ Step 3 : Executing the request**

The DPO consults the register of processing operations to identify which process or application contains the personal data for which a request has been made. He then requests each department concerned to send him the personal information concerning the applicant. This includes any subcontractors. In the event of a request for deletion, each department will ensure that all data relating to the request is deleted.

The DPO will collect all the information in his possession relating to the request. He will also ensure that subcontractors have updated or deleted the information.

### **❖ Step 4 : Response and storage of the request**

Where a request is made by e-mail, the reply will be sent by e-mail. In the case of a request by post, the DPO will give preference to sending the reply by registered post with acknowledgement of receipt in order to avoid any loss.

For the purposes of proof in the event of litigation, EBID must keep the information needed to show that it has complied with requests from individuals to exercise their rights.

Requests will be kept for the current calendar year, plus five years in the archives.

At the end of these periods, the requests and associated documentation must be deleted.

#### **4.3. Processing period**

The reply must be sent within 1 month of receipt of the request.

Where the request is complex, or where EBID has received an excessive number of requests, the deadline may be extended to two months. In this case, the DPO must inform the person who made the request so that he or she is aware that it will take longer to process it.

Furthermore, in the event of doubt as to the identity of the Person who made the Request, the fact that the DPO requests additional information to identify the Person waives the 1-month period. However, a request for additional information other than the identity of the Person does not waive the processing period.

## **ANNEX C**

EBID GENERAL POLICY ON PERSONAL DATA  
PROTECTION:

### **PERSONAL DATA PROTECTION CHARTER FOR PARTNERS**

## CONTENTS

<b>1. PREAMBLE .....</b>	<b>31</b>
<b>2. INTRODUCTION.....</b>	<b>31</b>
<b>3. LENDERS OR BENEFICIARIES .....</b>	<b>31</b>
<b>4. ARTICLES TO BE INCLUDED IN THE CONTRACT WITH LENDERS OR BENEFICIARIES .....</b>	<b>32</b>
<b>4.1. Obligations of the lender or beneficiarye.....</b>	<b>32</b>
<b>4.2. No transfer of rights or subsequent subcontracting.....</b>	<b>33</b>
<b>4.3. Audit.....</b>	<b>34</b>
<b>4.4. Responsibility.....</b>	<b>34</b>
<b>4.5. Duration.....</b>	<b>35</b>
<b>4.6. Miscellaneous.....</b>	<b>35</b>
<b>4.7. Applicable law and disputes.....</b>	<b>35</b>

## 1. Preamble

EBID has adopted a "personal data protection charter for partners".

This charter contains the rules governing the protection of personal data for EBID's partners. Accordingly, it has chosen to draw from the existing legal framework.

## 2. Introduction

For the record, a Partner is any natural person or legal entity, public or private, any other body or association with which EBID works to achieve a purpose.

A partner may be a " Lender " or a " Beneficiary ".

A "**Lender**" is a natural person or legal entity, public or private, or any other body or association, be it a lender, financier, or investor, with which EBID works to achieve a purpose.

A "**Beneficiary**" is a natural person or legal entity, public or private, or any other body or association, whether borrower, debtor, beneficiary, or lender, with which EBID works.

## 3. Lenders or beneficiaries

The terms and conditions for monitoring and complying with the commitments of the lender or beneficiary of the loan.

To achieve its objectives, EBID actively works with lenders and beneficiaries of these funds. This is always done in accordance with the rules stipulated in a contract. The bank has obligations towards lenders and beneficiaries:

- **Ensuring that the lender or beneficiary complies with the personal data protection rules:** as the case may be, checking or advising the lender or beneficiary to ensure that it institutes adequate measures to comply with the criteria of the Supplementary Act (AS/A 1/01/10).
- **Drawing up a contract for the personal data processing:** This contract must above all define:
  - the purpose and duration of the processing,
  - the nature and purpose of the processing,

- the type of personal data and the categories of data subjects,
- the obligations and rights of the data controller.

The contract also lists the obligations of the lender or beneficiary (data protection, cooperation in the event of any complaints, etc.).

The contract must also include a right for EBID to audit the data protection measures implemented by the lender or beneficiary.

#### **4. Articles to be captured in a contract with lenders or beneficiaries (in case of personal data processing) EBID to audit the data protection measures instituted by the lender or beneficiary.**

##### **4.1. Obligations of the lender or beneficiaries**

4.1.1. The lender or beneficiary shall process personal data only on behalf of EBID, pursuant to this contract. Where the lender or beneficiary is unable to do so and has reason to believe that the relevant applicable laws prevent it from following the instructions of the controller and fulfilling its obligations under this agreement, it shall inform the controller before processing the data. In this case, the data controller has the right to suspend access to or communication of the data and/or terminate the contract relating to the processing of personal data.

4.1.2. The lender or beneficiary shall confirm that, taking account of the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks, which vary in probability and severity, to the rights and freedoms of natural persons, it has implemented and shall continue to implement appropriate technical and organisational security measures to guarantee a level of security commensurate with the risk. Specifically, it shall protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access as described in the Supplementary Act (A/SA 1/01/10).

4.1.3. The lender or beneficiary shall ensure that its employees are authorised to process personal data and shall undertake to comply with EBID's data protection charter.

4.1.4. The lender or beneficiary shall guarantee that it takes account of the nature of the processing and assists the data controller with appropriate technical and

organisational measures. As far as possible, the lender or beneficiary shall ensure that it fulfils its obligation to comply with requests from data subjects to exercise their rights. In this regard, the Lender or Beneficiary is required to immediately inform the EBID DPO of any request directly from a Data Subject, without complying with such request, unless otherwise agreed with EBID.

- 4.1.5. The Lender or Beneficiary shall certify that, taking account of the nature of the processing and the information at its disposal, it shall assist the controller in guaranteeing compliance with the obligations regarding the security of personal data and the data protection impact assessment provided for.
- 4.1.6. The lender or beneficiary shall guarantee that it does not transfer, make available or give access to any personal data to countries or international organisations outside ECOWAS, unless it has received instructions to do so from the controller.
- 4.1.7. The lender or beneficiary shall not store personal data for any longer than is necessary for the performance of this contract. At the end of the services relating to the processing, the lender or beneficiary shall delete the personal data or return it to the controller, at the controller's discretion.
- 4.1.8. Similarly, the lender or beneficiary shall destroy any existing copies of the personal data. At the request of the controller, the lender or beneficiary shall confirm the deletion of all copies of personal data.
- 4.1.9. The Lender or Beneficiary shall expressly confirm that it will not disclose any Personal Data or any information derived therefrom to third parties, that it will not use and/or process the Personal Data at any time for its own needs or purposes and that it will not copy the Personal Data.

## **4.2. No transfer of rights or subsequent subcontracting**

- 4.2.1. The lender or beneficiary shall not grant any right and/or impose any obligation, nor transfer same to a third party under this contract, without the prior written authorisation of EBID.
- 4.2.2. The Lender or Beneficiary shall not engage any subcontractor to perform any part of this contract without the prior written authorisation of EBID.

4.2.3. The conclusion of any subsequent sub-contract for the performance of any part of this contract shall in no way exempt the lender or beneficiary from complying with its obligations under this contract. The processing services provided by the subcontractor must be carried out in accordance with the provisions of this contract. Upon simple request, the lender or beneficiary shall immediately provide the controller with a copy of any subsequent subcontracting agreements, with the exception of financial agreements concluded between the lender or beneficiary and the subsequent subcontractor.

#### **4.3. Audit**

4.3.1. The Lender or Beneficiary expressly undertakes to submit to and cooperate with any audit, control or investigation conducted directly or indirectly by a person or organisation authorised for this purpose at the request of EBID to verify whether the Lender or Beneficiary is complying with its obligations.

4.3.2. In this case, the lender or beneficiary shall specifically provide, at the request of the controller, all information necessary to prove that it complies with the obligations related to its intervention. This includes, particularly, information relating to the personal data processing activities and the security measures implemented.

4.3.3. In this context, the lender or beneficiary also undertakes to allow the data controller access to its data processing installations/infrastructure so that it can verify compliance with this contract.

#### **4.4. Responsibility**

4.4.1. The lender or beneficiary shall comply with the existing laws and rules on personal data protection. Accordingly, the lender or beneficiary shall only be held liable for any damage caused by the processing where it fails to comply with the obligations set out in the Supplementary Act (A/SA 1/01/10), particularly Article 29 thereof.

4.4.2. The lender or beneficiary shall discharge the data controller from any legal action brought by a third party on the grounds of a breach of the rules in force and/or of this contract for which the lender or beneficiary is responsible.

4.4.3. The lender or beneficiary shall duly insure its liability. Upon request, it shall present the insurance policy to the data controller.

#### **4.5. Duration**

4.5.1. This contract shall enter into force on ..... (date) and shall remain in force until .....

4.5.2. In the event of an indefinite duration, either party may terminate this contract by sending written notification to the other party.

4.5.3. The controller may immediately terminate this agreement, without resorting to a court of law, by sending written notification of termination to the lender or beneficiary where:

- the lender or beneficiary violates this agreement, and the breach is irremediable;
- the lender or beneficiary violates this agreement, and the breach is not irremediable, but the lender or beneficiary fails to remedy the breach within ... days of receiving written notification to remedy the breach;
- the lender or beneficiary is declared bankrupt, liquidated, or dissolved.

#### **4.6. Miscellaneous**

4.6.1. This contract represents the entire agreement between the parties and does not in any way require personal data to be made available to the lender or beneficiary.

4.6.2. Where one or more provisions of this agreement are declared invalid or unenforceable, the parties undertake to replace the provision(s) in question with one or more valid and enforceable provisions that are as close as possible to the objectives of the provision(s) declared invalid or unenforceable. The other provisions of this agreement shall remain in full force and effect.

4.6.3. The mere fact that a party does not insist on strict compliance with a provision of the contract or does not apply it may not under any circumstances be interpreted as a waiver or relinquishment of that party's rights, unless confirmed in writing.

#### **4.7. Applicable law and disputes**

4.7.1. This contract shall be governed by law .....

**ANNEX D**  
EBID GENERAL POLICY ON PERSONAL DATA  
PROTECTION:  
**PERSONAL DATA PROTECTION CHARTER FOR EBID  
SUBCONTRACTORS**

## CONTENTS

<b>1. PREAMBLE .....</b>	<b>38</b>
<b>2. INTRODUCTION.....</b>	<b>38</b>
<b>3. SELECTION OF THE SUBCONTRACTOR.....</b>	<b>38</b>
<b>4. SEQUENCE.....</b>	<b>39</b>
<b>5. ITEMS TO BE INCLUDED IN THE SUBCONTRACTING AGREEMENT.....</b>	<b>39</b>
<b>5.1. Obligations of the sub-contractor.....</b>	<b>39</b>
<b>5.2. No transfer of rights or subsequent subcontracting .....</b>	<b>40</b>
<b>5.3. Audit.....</b>	<b>41</b>
<b>5.4. Responsibility.....</b>	<b>41</b>
<b>5.5. Duration.....</b>	<b>41</b>
<b>5.6. Miscellaneous .....</b>	<b>42</b>
<b>5.7. Applicable law and disputes.....</b>	<b>42</b>

## 1. Preamble

EBID has adopted a "personal data protection charter for subcontractors».

This charter contains the rules governing the protection of personal data for EBID's subcontractors. Accordingly, it has chosen to draw from the existing legal framework.

## 2. Introduction

For the record, a Subcontractor is any natural person or legal entity, public organisation or any other body that processes personal data on behalf of data controller, EBID. BIDC.

The data controller may always choose to process the data internally, or to outsource part of the processing to an external party. In the latter case, the services of a "subcontractor" are used.

## 3. Selection of the subcontractor

EBID has a database of non-approved suppliers. This database contains the list of suppliers likely to work for the Bank. It has 2 obligations vis-à-vis subcontractors:

- Selecting a suitable subcontractor: checking that the subcontractor it wishes to hire institutes sufficient measures to comply with EBID's personal data protection criteria. It is not enough to ask the subcontractor and be satisfied with a positive response. EBID will have to check the measures that the subcontractor institutes.
- Drafting sub-contracting agreement for personal data processing: This agreement must first and foremost stipulate:
  - the purpose and duration of the processing,
  - the nature and purpose of the processing,
  - the type of personal data and the categories of data subjects,
  - the obligations and rights of the data controller.

The contract shall also list the processor's obligations (data protection, cooperation in the event of any complaints, etc.). The sub-contracting contract must also include a right for EBID to audit the data protection measures implemented by the sub-contractor.

#### **4. Sequence**

The General Services and Assets Management Division will ensure that it has an up-to-date list of subcontractors authorised to work with the Bank. This list must be updated to include personal data protection.

The Bank will occasionally check to ensure that subcontractors are implementing data protection measures. It will also ensure that it has concluded a sub-contracting agreement with each supplier.

#### **5. Articles to be included in the subcontracting agreement.**

##### **5.1. Obligations of the subcontractor**

5.1.1. The subcontractor shall only process personal data on behalf of EBID, upon its instructions and based on this contract. Where the subcontractor fails to do so and has reason to believe that the applicable laws prevent it from complying with the data controller's instructions and fulfilling its obligations under this contract, it shall inform the data controller before processing the data. In this case, the data controller has the right to suspend access to or communication of the data and/or to terminate the contract.

5.1.2. The subcontractor shall confirm that, taking account of the state of the art, the costs of implementation and the nature, scope, context, and purposes of the processing as well as the risks, which vary in probability and severity, to the rights and freedoms of natural persons, it has implemented and shall continue to implement appropriate technical and organisational security measures to guarantee a level of security commensurate with the risk. Specifically, it shall protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access as described in the EBID Personal Data Protection Charter.

5.1.3. The subcontractor shall ensure that its employees are authorised to process personal data and shall undertake to comply with EBID's data protection charter.

5.1.4. The subcontractor shall guarantee that it takes account of the nature of the processing and assists the data controller with appropriate technical and organisational measures. As far as possible, the subcontractor shall ensure that it fulfils its obligation to comply with requests from data subjects for the exercise of their rights. In this regard, the subcontractor is required to immediately inform the

EBID DPO of any request directly from a Data Subject, without complying with such request, unless otherwise agreed with EBID.

- 5.1.5. The subcontractor shall certify that, taking account of the nature of the processing and the information at its disposal, it shall assist the controller in guaranteeing compliance with the obligations regarding the security of personal data and the data protection impact assessment provided for.
- 5.1.6. The subcontractor shall guarantee that it does not transfer, make available or grant access to any personal data to countries or international organisations outside ECOWAS, unless it has received instructions to do so from the controller.
- 5.1.7. The subcontractor shall not store personal data for longer than is necessary for the performance of this contract. At the end of the services relating to the processing, the subcontractor shall delete the personal data or return it to the controller, at the controller's discretion. Similarly, the contractor shall destroy any existing copies of the personal data. At the request of the controller, the subcontractor shall confirm the deletion of all copies of personal data.
- 5.1.8. The subcontractor shall expressly confirm that it will not disclose any Personal Data or any information derived therefrom to third parties, that it will not use and/or process the Personal Data at any time for its own needs or purposes and that it will not copy the Personal Data.

## **5.2. No transfer of rights or subsequent subcontracting**

- 5.2.1. The subcontractor shall not grant any right and/or impose any obligation, nor will transfer same to a third party under this contract, without the prior written authorisation of EBID.
- 5.2.2. The Subcontractor shall not engage any subcontractor to perform any part of this contract without the prior written authorisation of EBID.
- 5.2.3. The signing of any subsequent sub-contract for the performance of any part of this contract shall in no way exempt the subcontractor from complying with its obligations under this contract. The processing services provided by the subcontractor must be carried out in accordance with the provisions of this contract. Upon simple request, the Subcontractor shall immediately provide the controller

with a copy of any subsequent subcontracting agreements, except for financial agreements signed between the Subcontractor and the subsequent subcontractor.

### **5.3. Audit**

5.3.1. The Subcontractor expressly undertakes to submit to and cooperate with any audit, control or investigation conducted directly or indirectly by a person or organisation authorised for this purpose at the request of EBID to verify whether the Subcontractor is compliant with its obligations.

5.3.2. In this case, the Subcontractor shall specifically provide, at the request of the controller, all information necessary to prove that it complies with the obligations relating to its intervention. This includes, particularly, information relating to the personal data processing activities and the security measures implemented.

5.3.3. In this context, the subcontractor also undertakes to allow the data controller access to its data processing installations/infrastructure so that it can verify compliance with this contract.

### **5.4. Responsibility**

5.4.1. The subcontractor shall comply with the existing laws and rules on personal data protection. Accordingly, the subcontractor shall only be held liable for any damage caused by the processing where it fails to comply with the obligations set out in the Supplementary Act (A/SA 1/01/10), particularly Article 29 thereof.

5.4.2. The subcontractor shall discharge the data controller from any legal action brought by a third party on the grounds of a breach of the rules in force and/or of this contract for which the subcontractor is responsible.

5.4.3. The subcontractor shall duly insure its liability. Upon request, it shall present the insurance policy to the data controller.

### **5.5. Duration**

5.5.1. This contract shall enter into force on ..... (date) and shall remain in force until .....

5.5.2. In the event of an indefinite duration, either party may terminate this contract by sending written notification to the other party.

5.5.3. The controller may immediately terminate this agreement, without resorting to a court of law, by sending written notification of termination to the subcontractor where:

- the subcontractor violates this agreement, and the breach is irremediable;
- the subcontractor violates this agreement, and the breach is not irremediable, but the subcontractor fails to remedy the breach within ... days of receiving written notification to remedy the breach.
- the subcontractor is declared bankrupt, liquidated, or dissolved.

## **5.6. Miscellaneous**

5.6.1. This contract represents the entire agreement between the parties and does not in any way require personal data to be made available to the subcontractor.

5.6.2. Where one or more provisions of this agreement are declared invalid or unenforceable, the parties undertake to replace the provision(s) in question with one or more valid and enforceable provisions that are as close as possible to the objectives of the provision(s) declared invalid or unenforceable. The other provisions of this agreement shall remain in full force and effect.

5.6.3. The mere fact that a party does not insist on strict compliance with a provision of the contract or does not apply it may not under any circumstances be interpreted as a waiver or relinquishment of that party's rights, unless confirmed in writing.

## **5.7. Applicable law and disputes**

5.7.1. This contract shall be governed by law .....

**ANNEX E**

EBID GENERAL POLICY ON PERSONAL DATA  
PROTECTION:

**PERSONAL DATA PROTECTION CHARTER FOR  
EBID STAFF**

## CONTENTS

<b>1. PREAMBLE .....</b>	<b>45</b>
<b>2. OBJECTIVE OF THE CHARTER.....</b>	<b>45</b>
<b>3. PRINCIPLES AND RULES GOVERNING DATA PROTECTION.....</b>	<b>45</b>
<b>3.1. EBID'S Organisation.....</b>	<b>45</b>
<b>3.2. Records of processing activities.....</b>	<b>46</b>
<b>3.3. Data controller.....</b>	<b>46</b>
<b>3.4. Purpose of processing operations.....</b>	<b>46</b>
<b>3.5. Recipient of personal data.....</b>	<b>47</b>
<b>3.6. Data retention time .....</b>	<b>47</b>
<b>3.7. Employee rights to personal data .....</b>	<b>47</b>
<b>3.8. Exclusions.....</b>	<b>48</b>
<b>3.9. Formalities.....</b>	<b>49</b>
<b>4. COMMITMENT .....</b>	<b>49</b>

## 1. Preamble

EBID has adopted a "personal data protection charter for its staff".

This charter contains the rules on personal data protection for EBID staff. Accordingly, it decided to draw from the existing legislative framework.

Staff members are required to comply with this Charter in the same way as with the Code of Ethics. This Charter is applicable to members of the bank's staff as well as to Directors and Senior Management.

## 2. Objective of the charter

The purpose of the charter is to:

- educate each employee of his or her **rights, duties and responsibilities** with respect to personal data protection in the performance of his or her duties;
- educate each employee about personal data **processing** operations carried out by EBID and the rules to be observed when accessing and carrying out personal data operations;

All staff members shall be liable for their actions and may be held personally liable under civil or criminal law, or professionally liable, in the event of failure to honour their obligations under this Charter.

## 3. Principles and rules governing data protection.

### 3.1. EBID's Organisation

EBID has created the position of DPO responsible for issues relating to personal data protection. The DPO's main, but not exclusive, role is to:

- be actively involved in all matters relating to personal data protection, in a timely manner;
- educate and advise staff members, including Senior Management and Directors, about their obligations with respect to personal data protection;

- supervise and monitor compliance with the above-mentioned obligations, including raising awareness and training employees.
- provide advice on request, concerning, where necessary, data protection impact assessments and ensure that they are carried out;
- work closely with the supervisory authorities where necessary;
- serve as a point of contact for the supervisory authorities, where necessary, on matters relating to personal data processing;
- serve as a point of contact for data subjects on all matters relating to personal data processing and the exercise of their rights in relation to such data;
- monitor, control and supervise internal procedures and policies on personal data protection with a view to ensuring that they are effective and efficient, and update them where necessary.

The DPO will be assisted by representatives of each EBID department. All staff members are required to contact the DPO if they encounter difficulties in understanding or applying the rules concerning personal data.

Audit procedures will be implemented to ensure compliance with data protection commitments at EBID.

### **3.2. Records of processing activities**

EBID shall maintain a record of processing activities listing all personal data processing operations carried out by the data controller.

### **3.3. Data Controller**

EBID, represented by its President, is the personal data controller. It shall determine the purposes and resources to be employed.

### **3.4. Purpose of processing operations**

These processing operations are conducted mainly for but not restricted to the following

purposes:

- the administrative management of EBID staff
- the organisation of work
- recruitment management
- mobility management
- the staff health management
- management of professional development of staff.

### **3.5. Recipient of personal data**

Within the scope of their responsibilities, the recipients of employees' personal data are :

- the staff in charge of the human resources department;
- the employee's supervisors
- internal control officers
- other authorised staff of EBID;
- EBID's subcontractors;
- public and semi-public bodies, exclusively to meet legal obligations;
- representatives of the law and judicial officers within the scope of their mission of providing legal assistance and representation in court;
- certain financial organisations within the scope of their responsibilities.

### **3.6. Data retention time**

Employees' personal data shall be retained for no longer than is necessary for the purposes for which it is processed.

The length of time personal data is retained is listed in the records of processing activities.

### **3.7. Employee rights to personal data**

The employee shall have:

- the right to access, rectify and erasure personal data,
- the right to restrict processing,
- a right to object,
- a right to data portability and
- the right to define instructions for the use of their personal data after their death.

Employees shall also have the right to withdraw their consent where the processing of personal data is based on consent.

The exercise of any of these rights may be refused where the employee's request does not meet the conditions laid down by the personal data protection rules or where there is a legitimate reason on the part of EBID. In such a case, the employee will be duly informed.

These rights may be addressed to the DPO at the following email address: [dpo@bidc-ebid.org](mailto:dpo@bidc-ebid.org)

### **3.8. Exclusions**

Processing of the following personal data is prohibited, unless expressly authorised by EBID:

- processing carried out using data collected from third parties without the employee first ensuring that these third parties have the requisite rights to collect and communicate such data and guaranteeing that the data subjects have been informed and, where applicable, that their consent has been obtained;
- the re-use of personal data for purposes incompatible with the original purposes;
- the collection and processing of sensitive data, i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data, data concerning health or data concerning the sex life or sexual orientation of an individual, information relating to offences, convictions or associated security measures;
- unrestricted storage of personal data;
- the transfer of personal data to a third country without having ensured that such transfer is authorised and that the appropriate measures and safeguards have been implemented.

Where in doubt, employees should contact their supervisors or the DPO.

### **3.9. Formalities**

In accordance with the legal provisions, employees and persons with access to the workplace or premises where employees are hired have been made aware of this charter through posters.

Signing this charter implies unreserved acceptance of its provisions, which shall apply to all employees as soon as it enters into force.

### **4. Commitment.**

I, the undersigned ... .., acknowledge having read and understood the Personal Data Charter applicable to EBID staff.

Signature

Name and date :