AFRICAN UNION
INTERAFRICAN BUREAU
FOR ANIMAL RESOURCES

Personal Data Protection Policy

TABLE OF CONTENTS

1. GENERAL PROVISIONS

1.1 PURPOSE

This Policy lays down the rules and principles relating to the processing of personal data within AU-IBAR. Its purpose is to ensure that AU-IBAR processes personal data in a way that is consistent with the AUC Cyber Security and Personal Data Protection Convention ("AUC Convention") and other applicable international instruments concerning the protection of personal data and individuals' privacy.

1.2 RATIONALE

In pursuit of its mandate, AU-IBAR is required to process personal data of persons. This may also include the need to share personal data with Implementing Partners and/or third parties. In processing personal data there are inherent risks such as accidental or unauthorized loss or disclosure. The protection of personal data is important and AU-IBAR has a responsibility to process it in a way that respects data protection principles. The Policy will be complemented by AU-IBAR Standard Operating Procedures that will provide guidance on its implementation in the different business processes and functions. It complements the provisions of AUC Staff Rules and Regulations and AU-IBAR's Code of Conduct particularly those provisions that call on staff to safeguard and make responsible use of the information to which they have access. It should also be read together with the AU-IBAR Cookies Policy and Privacy Notice for web applications, AUC E-Mail Acceptable Use Policy, AUC Third Party Access Policy, AUC E-Mail Archiving and Retention Policy and AUC End-User Backup Policy.

1.3 SCOPE

This Policy applies to all personal data held by AU-IBAR. The processing of other data, e.g. aggregated or anonymized, does not fall within the scope of this Policy. This Policy applies whether processing takes place within one AU-IBAR office or by AU-IBAR staff in different locations, or whether personal data is transferred to Implementing Partners or third parties.

Compliance with this Policy is mandatory for all AU-IBAR personnel.

1.4 TERMS AND DEFINITIONS

For the purpose of this policy, the following definitions apply:

Consent: Any freely given and informed indication of an agreement by the data subject or his legal representative to the processing of his/her personal data, which may be given either by a written or oral statement or by a clear affirmative action.

Data controller: The AU-IBAR staff member, usually the Director of AU-IBAR, who has the authority to oversee the management of, and to determine the purposes for, the processing of personal data.

Data processor: Any AU-IBAR staff member or other natural person or organization, including an Implementing Partner or third party that carries out processing of personal data on behalf of the data controller.

Data subject: A natural person whose personal data is subject to processing.

Data transfer agreement: An agreement between AU-IBAR and an Implementing Partner or third party that states the terms and conditions of use of personal data, including which data components are to be shared, the mode of transfer, how the data may be used, data security measures and other related issues.

Implementing Partner: An organization established as an autonomous and independent entity from AU-IBAR that AU-IBAR engages through a project partnership agreement to undertake the implementation of programmatic activities within its mandate.

Personal data: Any information related to an individual who can be identified from that information directly or indirectly (in conjunction with other information). Personal data includes biographical data (biodata) such as name, sex, marital status, date and place of birth, country of origin, country of residence, individual registration number, occupation, religion and ethnicity, biometric data such as a photograph, fingerprint, facial or iris image, as well as any mental, economic, cultural or social identity factors and opinions held by the individual.

Personal data breach: A breach of data security leading to the accidental or unlawful/ illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transferred, stored or otherwise processed.

Processing of personal data: Any operation, or set of operations, automated or not, which is performed on personal data, including but not limited to the collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, transfer (whether in computerized, oral or written form), dissemination or otherwise making available, correction, or destruction.

Third party: Any natural or legal person other than the data subject, AU-IBAR or an Implementing Partner or their staff. Examples of third parties are national governments, international governmental or non-governmental organizations, private sector entities or individuals.

2. BASIC PRINCIPLES

2.1 BASIC PRINCIPLES OF PERSONAL DATA PROCESSING

AU-IBAR personnel need to respect and apply the following basic principles when processing personal data:

1. **Consent and legitimacy of data processing**
   Processing of personal data shall be deemed to be legitimate where the data subject has given his/her consent. It shall also be legitimate where the processing is necessary for the fulfilment of a legal obligation by the data processor, for the performance of a contract which the data subject is party to, for the protection of the interests of the data subject or for the performance of a task carried out in the public interest.

2. **Lawfulness and fairness**
   The collection, processing and storage of personal data shall be undertaken lawfully and fairly.

3. **Purpose, relevance and storage**
   Data collected and processing shall be for a specific and explicit purpose and limited to relevant information relative to the purpose of collection. Data shall not be stored for longer than is necessary for the purposes for which it was collected or processed except where the data shall be used for statistic or research purposes required by law.

4. **Accuracy**
   Data collected shall be accurate and where necessary, kept up to date. Where reasonably possible, the data collector shall rectify or erase inaccurate data.

5. **Transparency**
   The data controller shall disclose information on personal data collected or processed for a data subject including but not limited to the type of data, purpose of processing and retention period.

6. **Confidentiality and security**
   Personal data shall be processed confidentially and transferred or stored securely. If transferred to a third party, the third party will be required to give adequate measures of protection and security of the data.

These principles are described in detail in Article 13 of the AU Convention on Cyber Security and Personal Data Protection *https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection*.

2.2 RIGHTS OF THE DATA SUBJECT

The rights of a data subject are set out in detail in the AUC Convention but are summarised below.

2.2.1 Right to Information, Article 16

When collecting personal data from a data subject, AU-IBAR should inform the data subject of the following, in writing or orally, and in a manner and language that is understandable to the data subject:

i. The specific purpose(s) for which the personal data or categories of personal data will be processed;
ii. Whether such data will be transferred to Implementing Partner(s) or third parties, third countries or, where the data is being collected by an Implementing Partner on behalf of AU-IBAR, that the data subject is informed of this fact;
iii. The data subject's right to request access to their personal data, to rectify the data and capacity to request for removal of the personal data; and
iv. The period for which data will be stored.

2.2.2 Right of access, Article 17

Upon request the data subject may receive from AU-IBAR:

i. Confirmation as to whether or not data related to him or her has been, is being or will be processed; and
ii. Information on the personal data being processed, the purpose(s) for processing such data and the Implementing Partner(s) and/or third parties to whom such data has been, is being or will be transferred

2.2.3 Right to object to processing, Article 18

Subject to 2.3.2 below, a data subject may object to the processing of his or her personal data where there are legitimate grounds related to his or her specific personal situation. If the objection is justified, AU-IBAR should no longer process the personal data concerned.

2.2.4 Right to rectification or erasure of data, Article 19

i. The data subject may request the correction or deletion of personal data that is inaccurate, incomplete, unnecessary or excessive.
ii. Where a data subject requests the correction or deletion of his or her personal data, AU-IBAR is to request proof relating to the inaccuracy or incompleteness.

2.3 MODALITIES OF REQUESTS BY DATA SUBJECTS & RESPONSES FROM DATA PROCESSOR

2.3.1 Requests for information about access to, correction or deletion of personal data or an objection, may be made by the data subject or his or her authorized legal representative, or, in the case of a child, a parent or legal guardian. Requests are to be submitted in writing to the AU-IBAR office at the address provided at the end of this policy.

2.3.2 Before complying with any request or objection, AU-IBAR should satisfy itself of the identity of the person making the request or objection. The individual is required to identify him or herself in an appropriate manner. In the case of a legal representative or legal guardian, proof of such legal authority needs to be supplied. Requests and objections from parents or guardians for children should be evaluated against the best interests of the child.

2.3.3 AU-IBAR is to record the fact of having provided the data subject with the information pursuant to 2.3.1 as well as to record requests received for access, correction, deletion or objection and the response provided in relation to such requests.

2.3.4 AU-IBAR is to respond to a request or objection within a reasonable time, in writing or orally, and in a manner and language that is understandable to the data subject and/or his or her legal representative or legal guardian, as applicable.

2.4 RESTRICTIONS

Based on consultations with relevant counterparts at its headquarters, AU-IBAR may refuse to provide a response or limit or restrict its response to a request or objection where:

i. It would constitute a necessary and proportionate measure to safeguard or ensure one or more of the following:
ii. The safety and security of AU-IBAR, its personnel or the personnel of Implementing Partners; or
iii. The overriding operational needs and priorities of AU-IBAR in pursuing its mandate.
iv. There are grounds for believing that the request is manifestly abusive, fraudulent or obstructive to the purpose of processing.

3. DATA PROCESSING BY AU-IBAR

3.1 CONFIDENTIALITY OF PERSONAL DATA

3.1.1 Personal data is by definition classified as confidential. The confidentiality of personal data must be respected by AU-IBAR when processing personal data at all times.

3.1.2 In order to ensure and respect confidentiality, personal data must be filed and stored in a way that it is accessible only to authorized personnel and transferred only through the use of protected means of communication.

3.2 SECURITY OF PERSONAL DATA

3.2.1 AU-IBAR needs to ensure and implement a high level of data security that is appropriate to the risks presented by the nature and processing of personal data, the availability and quality of the necessary equipment, the cost and the operational feasibility.

3.2.2 AU-IBAR's data security measures are to protect personal data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

3.2.3 Having regard to the available technology and the cost of implementation, AU-IBAR needs to implement appropriate organizational and technical measures to ensure that the processing meets the requirements of this Policy. This includes the implementation of data protection enhancing technologies and tools to enable data processors to better protect personal data ("privacy by design and by default").

3.2.4 Organizational measures include:

i. Setting up Standard Operating Procedures;
ii. Organizing staff training on data protection and security; and

3.2.5 Technical measures include:

i. Maintaining physical security of premises, portable equipment, individual case files and records;
ii. Maintaining computer and information technology (IT) security, for example, access control (e.g. passwords, tiered access), user control, storage control, input control, communication and transport control (e.g., encryption).

3.2.6 In deteriorating security situations that pose a serious risk of personal data breaches, AU-IBAR should take all necessary and possible steps to avoid such personal data breaches, by relocating, or, as a matter of last resort, destroying individual case files, whether in paper or computerized form, that contain personal data, in order to prevent harm to data subjects.

3.3 ENSURING ACCURACY OF PERSONAL DATA

3.3.1 AU-IBAR may correct or delete personal data held on its systems that is inaccurate, incomplete, unnecessary or excessive.

3.3.2 AU-IBAR should update personal data records when necessary and periodically verify them.

3.3.3 When personal data is corrected or deleted in AU-IBAR's systems, AU-IBAR should notify, as soon as reasonably practicable, all Implementing Partners and/

or third parties to whom the relevant personal data was transferred.

3.4 NOTIFICATION OF A PERSONAL DATA BREACH

3.4.1 AU-IBAR personnel are required to notify the data controller as soon as possible upon becoming aware of a personal data breach and to properly record the breach.

3.4.2 If a personal data breach is likely to result in personal injury or harm to a data subject, the data controller should use his or her best efforts to communicate the personal data breach to the data subject and take mitigating measures as appropriate without undue delay.

3.5 RETENTION

3.5.1 Personal data that is not recorded in individual case files is not to be retained longer than necessary for the purpose(s) for which it was collected.

3. 5.2 All individual case files, whether open or closed, are considered permanent records, and must therefore be retained in accordance the effective records retention policy within AU-IBAR.

4. DATA PROCESSING BY IMPLEMENTING PARTNERS

4.1 Where the collection and processing of personal data is one of the responsibilities of Implementing Partners, the personal data is being collected and processed on behalf of AU-IBAR. For these reasons, Implementing Partners are expected to respect and implement the same or comparable standards and basic principles of personal data protection as contained in this Policy. This applies whether AU-IBAR intends to transfer personal data to Implementing Partners or Implementing Partners collect personal data in order to carry out agreed activities.

4.2 AU-IBAR shall ensure that the conditions of contract entered into with the Implementing Partner require the latter to uphold the principles of personal data protection contained in this agreement.

4.3 Where deemed necessary, AU-IBAR will provide training, establish technical and organizational measures or develop policies of implementing partners with regard to protection of personal data.

5 TRANSFER OF PERSONAL DATA TO THIRD PARTIES

5.1 GENERAL CONDITIONS

5.1.1 AU-IBAR may transfer personal data to third parties on condition that the third party affords a level of data protection the same or comparable to this Policy. The following matters need to be considered:

i. The transfer is for a specific legitimate purpose and is limited to relevant and necessary data in relation to the purpose;
ii. The data subject has been informed, either at the time of collection in accordance or subsequently, about the transfer of his/her personal data unless one or more of the restrictions in Part 2.4 apply;
iii. The third party respects the confidentiality of personal data transferred to them by AU-IBAR and limits access of it to only authorized personnel.

5.2 TRANSFER TO NATIONAL LAW ENFORCEMENT AGENCIES AND COURTS

5.2.1 In appropriate circumstances, AU-IBAR may transfer personal data to a national law enforcement agency or a national court. Such transfers may be upon request by the law enforcement agency or court, or on AU-IBAR's own initiative. Transfers may concern persons subject to an investigation for an allegedly committed crime, or in relation to the victim(s) of or witness (es) to a crime.

5.2.2 AU-IBAR may cooperate with such a request and transfer personal data to a national law enforcement agency or national court if the following conditions are met:

i. Transfer is necessary for the purposes of the detection, prevention, investigation, or prosecution of a serious criminal offence, in particular in order to avoid an immediate and substantial risk to the safety and security of an individual or the public;
ii. The requesting law enforcement agency or court is competent in relation to the detection, prevention, investigation or prosecution of the offence in question;
iii. The transfer will substantially assist the law enforcement agency or court in the pursuit of these purposes and that the personal data cannot otherwise be obtained from other sources;
iv. Transfer does not disproportionately interfere with a data subject's or another person of concern's right to privacy or other human rights; and
v. In the case of data in relation to victims and witnesses, their consent to the transfer has been obtained.

5.3 PRIVILEGES AND IMMUNITIES

The transfer of personal data is without prejudice to the AU-IBAR's privileges and immunities. Privileges and immunities of AU-IBAR and its staff members exist regardless of any cooperation agreement with the Government of a country.

6 DATA CONTROLLER AND DATA PROTECTION FOCAL POINT

6.1 The data controller is responsible for establishing and overseeing the processing of personal data under his or her area of responsibility. He or she therefore also bears the main responsibility for compliance with the Policy. To that end, the data controller may designate a data protection focal point.

6.2 The data controller, assisted by the data protection focal point, is to implement this Policy by, inter alia:

i. Determining the applicable legitimate basis for and the specific and legitimate purposes of data processing;
ii. Ensuring the implementation of organizational and security measures as well as assessing data security of third parties;
iii. Establishing internal procedures, for example in the form of Data Protection Standard Operating Procedures, covering all relevant aspects of this Policy, in particular regarding the respect for the rights of the data subject and measures aimed at ensuring data confidentiality and security;
iv. Ensuring that data protection and data security aspects are adequately included in Implementing Partner agreements;
v. Reviewing the terms of data transfer with third parties as required or appropriate.

African Union – Interafrican Bureau for Animal Resources
(AU-IBAR)
Kenindia Business Park
Museum Hill, Westlands Road
PO Box 30786
00100 Nairobi
Kenya
Tel: +254 (20) 3674 000
Fax: +254 (20) 3674 341 / 3674 342
Email: ibar.office@au-ibar.org
Website: www.au-ibar.org