|  |  |
| --- | --- |
| **Document number:**  | AB/PMU/2019/0001 Data Protection Policy  |
| **Content**:  | Guidelines and Procedures on Protecting Personal Data  |
| **Department**:  | Human Resources Unit |
| **Area**:  | Group |
| **Version Number**:  |  |
| **Title**: | AB Data Protection Policy  |
| **Date of Issue**: |  |
| **Purpose:**  | To Ensure the Protection of Personal Data of Persons of Concern to AB |
| **Author/Originator and Title**: | Kwaku Owusu-Yeboah: HR Manager |
| **Description of Amendments**: | Protocol for Policy Formulation |
| **Approved By**: | Afrobarometer Board  |
| **Review Date**: |  |
| **Responsibility Of**: | Human Resources Unit |
| **Training Required**:  | YES – Periodic trainings shall be organized for all stakeholders |
| **Name of Trainer/s:** |  |

**Article 1 – Aim of the Data Protection Policy**

AFROBAROMETER (hereafter referred to as “AB”) acknowledges that information technology is a very useful tool and, in its use, shall not violate human identity, human rights, privacy, or individual or public liberties.

AB is committed to international compliance with data protection laws. This Data Protection Policy applies worldwide to AB and is based on globally accepted, basic principles on data protection. Ensuring data protection is the foundation of trustworthy relationships and the reputation of AB as a credible institution.

The Data Protection Policy ensures the adequate level of data protection as prescribed by relevant legal frameworks, including in countries that do not yet have adequate data protection laws.

AB’s Data Protection Policy is meant to be a practical and easy-to-understand document to which all AB departments, stakeholders, and partners can refer.

**Article 2 – Scope of the Data Protection Policy**

This Data Protection Policy applies to all entities of AB, including partners and network offices in all countries of operation.

1. The policy applies to all AB staff, volunteers, affiliates, associates, interns, project partners, and governance members.
2. The provisions of this policy may also be applied to any person employed by an entity that carries out missions for AB.
3. In particular, this policy applies to implementing partners, suppliers, sub-grantees, stakeholders, and other associated entities.

AB’s Data Protection Policy applies to all personal data that AB holds relating to identifiable individuals, meaning any information relating to an identified or identifiable individual.

**Article 3 – AB’s Sets of Data and Definitions**

1. AB’s Data Protection Policy applies to all sets of personal data, currently stored, maintained, and handled by AB, and more specifically to the following identified sets of personal data:
2. AB’s personnel, including national and international staff, volunteers, affiliates, associates, and interns
3. AB’s direct and indirect beneficiaries, including interviewees
4. AB’s individual donors and sympathizers
5. AB’s contractors, suppliers, consultants, and implementing partners currently under contract with AB.
6. Personal data herein referred to means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity. This can include in particular:
7. Names of individuals
8. Postal or living addresses
9. Email addresses
10. Telephone numbers
11. Identity card and passport
12. Date and place of birth
13. Identification of relatives
14. Fingerprints
15. Business reference
16. Geo-referencing
17. Processing of personal data means any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organization, retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion, or destruction.

**Article 4 - Application of National Laws and Sources of Authority**

1. AB is headquartered in Ghana and observes the principles of Ghana’s Data Protection Act, 2012 (Act 843)and the 1990 United Nations General Assembly’s Guidelines for the Regulation of Computerized Personal Data File (*UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, as adopted by Resolution A/Res/45/95 of 14 December 1990, available at:* [*http://www.refworld.org/docid/3ddcafaac.html*](http://www.refworld.org/docid/3ddcafaac.html)). AB partner and network operations observe the laws of their country.
2. This Data Protection Policy comprises internationally accepted data privacy principles without replacing existing national laws. It supplements national data privacy laws. The relevant national law will take precedence in the event that it conflicts with this Data Protection Policy or has stricter requirements than this Policy. The content of this Data Protection Policy must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed. Each entity of AB, including partners and network offices, is responsible for compliance with this Data Protection Policy and all legal obligations.
3. At the same time, AB has rules and standards that seek to create a consistent approach and that, in some cases, may be stricter than national or local laws. This Policy must, therefore, be followed in addition to the relevant national and local laws on data protection.
4. In the event of conflicts between national legislation and the Data Protection Policy, AB will work with the relevant country offices to find a practical solution that meets the purpose of the Data Protection Policy.
5. This policy is aimed at guiding AB staff and must be considered together with:
6. AB’s Code of Conduct and policies that are annexed to it, and
7. AB’s operational manuals and guidelines.

**Article 5 - Principles for Processing Personal Data**

1. Fairness and Lawfulness
2. When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.
3. Collected data shall be adequate, relevant, and not excessive in relation to the purposes for which they are obtained and their further processing.
4. Individual data can be processed upon voluntary consent of the person concerned.
5. Restriction to a Specific Purpose
6. Personal data can be processed only for the purpose that was defined before the data was collected. Personal data shall be obtained for specified, explicit, and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes. Subsequent changes to the purpose are only possible to a limited extent and require justification.
7. However, further data processing for statistical, scientific, and historical purposes shall be considered compatible with the initial purposes of the data collection, if it is not used to take decisions with respect to the data subjects.
8. Transparency
9. The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be made aware of or informed of:
10. The purpose of data processing
11. Categories of third parties to whom the data might be transmitted
12. Processing of personal data must have received the consent of the data subject or must meet one of the following conditions: compliance with any legal obligation to which AB is subject; the protection of the data subject’s life; the performance of a public service mission entrusted to AB.
13. Confidentiality and Data Security

Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification, or destruction.

1. Deletion

Personal data shall be retained in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which it is obtained and processed. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or AB’s archive has evaluated the data to determine whether it must be retained for historical purposes.

1. Factual Accuracy and Up-to-Datedness of Data

Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data is deleted, corrected, supplemented, or updated.

**Article 6 – Data Processing**

1. Consent for Data ProcessingPersonal data shall not be processed without the prior consent of the data subject unless the purpose for which the personal data is processed is:
2. necessary for the purpose of a contract to which the data subject is a party;
3. authorized or required by law;
4. to protect a legitimate interest of the data subject;
5. necessary for the proper performance of a statutory duty; or
6. necessary to pursue the legitimate interest of the data controller or a third party to whom the data is supplied.
7. Collection of Personal Data
8. AB may collect personal data directly from the data subject.
9. Despite subsection (i), personal data may be collected indirectly where:
10. the data is contained in a public record;
11. the data subject has deliberately made the data public;
12. the data subject has consented to the collection of the information from another source;
13. the collection of the data from another source is not likely to prejudice a legitimate interest of the data subject;
14. compliance would prejudice a lawful purpose for the collection; or
15. compliance is not reasonably practicable.
16. Notification of a Personal Data Breach
17. AB personnel are required to notify the COO as soon as possible upon becoming aware of a personal data breach and to properly record the breach.
18. If a personal data breach is likely to result in personal injury or harm to a data subject, the COO 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.
19. The notification should describe:
20. The nature of the personal data breach, including the categories and number of data subjects and data records concerned;
21. The known and foreseeable adverse consequences of the personal data breach; and
22. The measures taken or proposed to be taken to mitigate and address the possible adverse impacts of the personal data breach.

**Article 7 – Rights of Data Subject**

1. When collecting personal data from a data subject, AB 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:
2. The specific purpose(s) for which the personal data or categories of personal data will be processed;
3. Whether such data will be transferred to partner(s) or third parties or, where the data is being collected by a partner or Network on behalf of AB, that the data subject is informed of this fact;
4. The importance of the data subject providing accurate and complete information;
5. The data subject’s duty to keep AB, and/or, as appropriate, partners, informed of changes to their personal situation;
6. Any consequences for refusing or failing to provide the requested personal data;
7. The data subject’s right to request access to their personal data, or correction or deletion of it;
8. The data subject’s right to object to the collection of personal data.
9. Modalities of Requests

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 orally or in writing to the AB office in the country where the data is being processed.

Before complying with any request or objection, AB should satisfy itself of the identity of the person making the request or objection. The individual is required to identify himself 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.

1. Recording and Response by AB

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

AB 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.

1. Restrictions

Based on consultations, AB may refuse to provide a response or limit or restrict its response to a request or objection under Article 7 where;

1. It would constitute a necessary and proportionate measure to safeguard or ensure one or more of the following:
2. The safety and security of AB, its personnel, or the personnel of implementing partners; or
3. The overriding operational needs and priorities of AB in pursuing its mandate.
4. There are grounds for believing that the request is manifestly abusive, fraudulent, or obstructive to the purpose of processing.

**Article 8 – Data Processing by Implementing Partners**

1. General Condition

Where the collection and processing of personal data is one of the responsibilities of partners, the personal data is being collected and processed on behalf of AB. For these reasons, 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 AB intends to transfer personal data to partners or partners collect personal data in order to carry out agreed activities.

1. Verification

Irrespective of a partnership agreement, AB needs to verify, prior to transferring personal data to a partner or to engaging a partner in the collection and processing of personal data, that the processing of personal data by the partner satisfies the standards and basic principles of this Policy. Such verification may form part of a Data Protection Impact Assessment.

1. Partnership Agreements

AB is to require partners to comply with this Policy through an undertaking as part of the signing of partnership agreements. Such agreements also need to specify the specific purpose(s) for the processing of personal data and the legitimate basis for processing.

1. Capacity of the Partner

AB may need to assist partners in building or enhancing their capacity in order to comply with the data protection standards and principles contained in this Policy. Such assistance may relate to the establishment or adjustment of policies, the delivery of training or putting in place technical and organizational measures.

1. Partnership Termination

After termination of a partnership, all personal data collected in the performance of the partnership should be returned to AB. Partnership agreements may provide for exceptions, in particular where there are legitimate reasons to do so, namely consent of the data subjects.

**Article 9 – Transfer of Personal Data to Third Parties**

1. General Condition

AB may transfer personal data to third parties on condition that the third party affords a level of data protection equal or comparable to this Policy.

Given the potential data protection risks involved in transfers to third parties, AB needs to pay particular attention to the following basic principles of this Policy:

1. Transfer is based on one or more legitimate bases;
2. Transfer is for one or more specific and legitimate purpose(s);
3. The personal data to be transferred is adequate, relevant, necessary, and not excessive in relation to the purpose(s) for which it is being transferred;
4. The data subject has been informed, either at the time of collection in accordance with Articles 6 and 7, or subsequently, about the transfer of his/her personal data, unless one or more of the restrictions in Article 6 apply;
5. The third party respects the confidentiality of personal data transferred to them by AB. Whether or not a data transfer agreement has been signed between AB and the third party, AB must seek written agreement from the third party that the personal data will be kept confidential at all times. In order to ensure and respect confidentiality, personal data must be filed and stored in a way that is accessible only to authorized personnel and transferred only through the use of protected means of communication;
6. The third party maintains a high level of data security that protects personal data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to it.

In addition, AB needs to ensure that transferring personal data does not negatively impact:

1. the safety and security of AB personnel and/or personnel of partners; and/or
2. the effective functioning of an AB’s operation or compromise AB’s mandate, for example due to the loss of the climate of trust and confidence between AB and persons of concern or the loss of the perception of AB as a pan-African, independent, non-partisan research network.

Before agreeing to transfer personal data to a third party, AB needs to assess the level of data protection afforded by the third party. As part of this assessment, the COO should assess, *inter alia*, the applicable laws and regulations, internal statutes and policies of the third party, specific contractual obligations or undertakings to respect specific data protection frameworks, their effective implementation as well as the technical and organizational means of data security put in place.

1. Data Transfer Agreements
2. Unless there are satisfactory reasons not to do so, prior to transferring personal data to a third party, the COO should seek to sign a data transfer agreement, or, as appropriate, incorporate data protection clauses within broader agreements, particularly where transfers of personal data are likely to be large, repeated, or structural, i.e. where the same type(s) of data is shared with the same third party for the same purpose over a certain period of time.
3. Data transfer agreements should, *inter alia*:
4. address the purpose(s) for data transfer, specific data elements to be transferred as well as data protection and data security measures to be put in place;
5. require the third party to undertake that its data protection and data security measures are in compliance with this Policy; and
6. stipulate consultation, supervision, accountability, and review mechanisms for the oversight of the transfer for the life of the agreement.
7. Transfer to National Law Enforcement Agencies and Courts
8. In appropriate circumstances, AB 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 AB’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.

In addition to the general conditions for transferring personal data to third party, AB may only cooperate with such a request and transfer personal data to a national law enforcement agency or national court if the following conditions are met:

1. 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;
2. The requesting law enforcement agency or court is competent in relation to the detection, prevention, investigation, or prosecution of the offence in question;
3. The transfer will substantially assist the law enforcement agency or court in the pursuit of these purposes and the personal data cannot otherwise be obtained from other sources;
4. The transfer does not disproportionately interfere with a data subject’s or another person of concern’s right to privacy or other human rights.

**Article 10 - Data Protection Control**

Compliance with the Data Protection Policy and the applicable data protection laws is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of AB’s Central Management Team or appointed representative. The results of the data protection controls performed by appointed representative must be reported to the Central Management Team.

**Article 11 - Violation, Sanction, and Reporting**

1. Any failure to comply with the current Policy or any attempt to deliberately violate the rules set forth in the Policy will result in the launching of an appropriate investigation by AB.
2. Depending on the gravity of the suspicion or accusations, AB may suspend staff or relations with other stakeholder during the investigation. This will not be subject to challenge.
3. Depending on the outcome of the independent investigation, if it comes to light that anyone associated with AB has deliberately violated the rules set forth in the Policy for personal profit or any other usage of personal data, or has systematically and deliberately contravened the principles and standards contained in this document, AB will take immediate disciplinary action and any other action that may be appropriate to the circumstances. This may mean, for example, for:
4. Employees - disciplinary action/dismissal;
5. Trustees, volunteers, associates, and interns - ending the relationship with the organization or individual;
6. Partners - withdrawal of funding/support;
7. Contractors and consultants - termination of contract.
8. Depending on the nature, circumstances, and location of the case and violation, AB will also consider involving authorities to ensure the protection of personal data and victims. The reporting of suspected or actual violations of this Policy is a professional and legal obligation of all staff and partners. Failure to report information can lead to disciplinary action. AB encourages its staff and stakeholders to report suspected cases that involve any AB staff, consultants, board members, guests, or staff of AB’s partner organizations, their board members, staff, and/or suppliers.
9. AB encourages its staff and stakeholders to report suspected cases through the following means:
10. Staff and interns can report through standard lines of hierarchy (contained in the HR Policy) and/or the Human Resources Manager.
11. Suppliers and contractors can use the confidential email address transparency@afrobarometer.org.
12. Donors and sympathizers can refer to the confidential email address transparency@afrobarometer.org.
13. All reports will be treated as confidential in line with AB’s Code of Conduct and AB’s human resources guidelines.
14. AB will not tolerate false accusations that are designed to damage a member of staff’s or a partners’ reputation. Anyone found making false accusations will be subject to investigation and disciplinary action.

**Article 12 - Responsibilities**

AB’s Central Management Team is responsible for ensuring that legal requirements and requirements contained in this Data Protection Policy for data protection are met (e.g. national reporting duties). The Senior Advisory Team is responsible for ensuring that organizational, human resources, and technical measures are in place so that any data processing is carried out in accordance with data protection. The managers must ensure that their employees are sufficiently trained in data protection. Compliance with these requirements is the responsibility of the relevant employees.