ACEECA

African Centre For Environment, Energy and Climate Advocacy

Advocating for a Just, Resilient and Sustainable Kenya

DATA PROTECTION POLICY

Safeguarding Personal Data.
Building Trust. Enabling Impact.

- Protecting Privacy. Upholding Rights.
- Secure Data. Strong Systems.
- Accountable Governance. Shared Responsibility.
- For People. For Planet. For Future Generations.

Website: www.aceeca.org

CONTENT

1.0 PREAMBLE

The ***African Centre for Environment, Energy and Climate Advocacy (ACEECA)*** recognizes that the protection of personal data is fundamental to the respect of human dignity, privacy, and trust in the digital age. In carrying out its mandate on environmental conservation, climate advocacy, clean energy transition, and community empowerment, ACEECA collects, processes, stores, and uses various categories of personal data belonging to staff, partners, beneficiaries, communities, donors, and stakeholders.

In doing so, ACEECA is guided by internationally recognized principles of data protection, including those articulated under the United Nations system, as well as applicable national legislation, particularly the Kenya Data Protection Act, 2019, and globally accepted frameworks such as the General Data Protection Regulation (GDPR).

This Policy establishes a clear framework for lawful, fair, transparent, and accountable data handling practices across all ACEECA operations.

2.0 PURPOSE OF THIS POLICY

The purpose of this Data Protection Policy is to establish a clear, principled, and enforceable framework that governs how personal data is collected, processed, stored, shared, and protected within the Africa Centre for Environment, Energy and Climate Advocacy (ACEECA).

In an increasingly data-driven operational environment, ACEECA recognizes that the handling of personal data is not merely a technical function, but a matter of ethical responsibility, institutional integrity, and human rights protection. This Policy therefore serves as a foundational instrument for ensuring that all data-related activities are aligned with both legal obligations and internationally recognized best practices.

Specifically, the Policy seeks to:

2.1 Ensure lawful, fair, and transparent processing of personal data

ACEECA commits to processing personal data in strict accordance with applicable legal frameworks and ethical standards. This includes ensuring that individuals are fully informed, in clear and accessible language, about the nature, purpose, and scope of data being collected from them.

Fairness requires that data is not used in ways that are misleading, unexpected, or detrimental to the rights of individuals. Transparency further demands openness in organizational practices, allowing data subjects to understand how and why their information is being used.

2.2 Safeguard the rights and freedoms of individuals

This Policy is grounded in the principle that personal data protection is intrinsically linked to the protection of human dignity, privacy, and individual autonomy.

ACEECA is committed to ensuring that all data subjects—whether community members, staff, partners, or beneficiaries—retain meaningful control over their personal information. This includes safeguarding their rights to access, correct, restrict, or object to the processing of their data, as well as ensuring that no individual is subjected to harm, discrimination, or exploitation arising from misuse of their information.

2.3 Establish institutional responsibility and accountability

Effective data protection requires clearly defined roles, responsibilities, and accountability mechanisms across the organization.

This Policy therefore establishes a governance structure that ensures that data protection is not treated as an isolated function, but as an integrated organizational responsibility. All units within ACEECA, including leadership,

programme teams, and field operations, are collectively responsible for ensuring compliance.

Accountability also extends to documentation, monitoring, and auditability of data processing activities to ensure institutional transparency and oversight.

2.4 Prevent unauthorized access, misuse, loss, or disclosure of data

ACEECA recognizes that personal data is vulnerable to risks including unauthorized access, cyber threats, human error, and physical loss.

This Policy therefore establishes preventive and corrective safeguards designed to protect data integrity and confidentiality. These include technical measures (such as encryption and secure systems), organizational controls (such as access restrictions and staff training), and procedural safeguards (such as data handling protocols and incident response mechanisms).

The objective is to ensure that personal data remains protected throughout its lifecycle—from collection to eventual disposal.

2.5 Strengthen trust with stakeholders

Trust is a critical enabler of ACEECA's work in communities, particularly in environmental conservation, climate resilience, and sustainable development programmes.

By ensuring responsible data management practices, ACEECA seeks to strengthen the confidence of communities, government institutions, development partners, donors, and other stakeholders. This trust is essential for effective collaboration, data sharing, and long-term programmatic impact.

A strong data protection framework also enhances ACEECA's credibility as a professional and accountable organization operating in alignment with international standards.

2.6 Ensure compliance with applicable legal and international frameworks

This Policy is designed to ensure full compliance with relevant data protection legislation, including national laws such as the Kenya Data Protection Act, 2019, as well as internationally recognized frameworks such as the General Data Protection Regulation (GDPR) and principles promoted by the United Nations system.

Compliance is not limited to legal conformity but extends to adherence to best practices in governance, ethics, and institutional accountability.

3.0 SCOPE OF APPLICATION

This Policy applies comprehensively across all operational, administrative, and programmatic dimensions of ACEECA's work. It establishes a uniform standard for data protection that is binding across the entire organization and its extended operational ecosystem.

3.1 Applicability to all personnel

The Policy applies to all individuals engaged by ACEECA, regardless of contractual arrangement or duration of engagement. This includes:

- Full-time employees
- Part-time staff
- Interns and volunteers
- Consultants and temporary experts

All such individuals are required to comply with this Policy in the course of performing their duties. Compliance is mandatory and forms part of professional responsibility and contractual obligation.

3.2 Coverage of all programmes and activities

This Policy applies to all ACEECA programmes, projects, and field-based interventions, whether implemented independently or in partnership with other organizations.

This includes activities related to environmental protection, climate action, clean energy initiatives, community engagement, research, advocacy, and capacity-building programmes.

No programme or activity is exempt from the provisions of this Policy, regardless of funding source, geographic location, or implementing modality.

3.3 Coverage of all forms of data

The Policy governs the processing of all personal data handled by ACEECA, regardless of format or medium. This includes:

- Digital data stored in databases, cloud systems, and electronic devices
- Physical records such as printed forms, registers, and field notes
- Audio, visual, and multimedia recordings where individuals can be identified
- Any derived or aggregated datasets containing personal identifiers

This comprehensive scope ensures that data protection principles are consistently applied across both modern digital systems and traditional paper-based operations.

3.4 Third-party and partner compliance

ACEECA recognizes that data processing may involve external actors, including service providers, implementing partners, and contractors.

Accordingly, this Policy extends to all third parties that process data on behalf of ACEECA. Such entities are required to uphold equivalent standards of data protection through formal agreements and contractual obligations.

ACEECA retains ultimate accountability for ensuring that all partners comply with applicable data protection principles.

3.5 Geographic scope of application

This Policy applies to all ACEECA operations regardless of geographic location. This includes:

- National-level operations within Kenya
- County-level field engagements across ACEECA operational regions
- Cross-border collaborations and regional partnerships
- Digital or remote engagements conducted through online platforms

The Policy ensures consistency in data protection standards irrespective of jurisdictional differences, while remaining compliant with applicable local and international laws.

4.0 DEFINITIONS

For the purpose of this Policy:

- **Personal Data** refers to any information relating to an identified or identifiable natural person.
- **Data Subject** refers to the individual whose personal data is collected or processed.
- **Processing** includes collection, storage, use, transmission, analysis, sharing, and deletion of data.
- **Data Controller** refers to ACEECA, which determines the purposes and means of processing personal data.
- **Data Processor** refers to any entity processing data on behalf of ACEECA.
- **Sensitive Personal Data** includes information such as health status, biometric data, financial information, or any data that may expose an individual to harm if disclosed.
- **Consent** means a freely given, specific, informed, and unambiguous indication of a data subject's agreement to the processing of their data.

5.0 GUIDING PRINCIPLES OF DATA PROTECTION

ACEECA's data protection framework is anchored in universally recognized principles of privacy, accountability, and ethical data governance. These principles are not merely aspirational; they constitute binding operational standards that guide all data-related activities across the organization.

They ensure that personal data is handled in a manner that respects human dignity, strengthens institutional trust, and aligns with international best practices as promoted by global governance frameworks.

5.1 Lawfulness, Fairness, and Transparency

ACEECA shall ensure that all personal data is processed in strict accordance with applicable legal frameworks, institutional policies, and ethical norms.

Lawfulness requires that every data processing activity has a valid legal basis and is not conducted outside the scope of established regulations or consent frameworks.

Fairness ensures that data is not used in ways that are misleading, discriminatory, or detrimental to the interests or rights of individuals. Data subjects shall not be subjected to unexpected or unjustified uses of their information.

Transparency requires that individuals are clearly and adequately informed, at the point of data collection or prior to processing, about:

- The identity of the data controller (ACEECA)
- The specific purpose for which their data is being collected
- The categories of data being processed
- The rights available to them under this Policy

This principle reinforces trust and ensures informed participation by all stakeholders.

5.2 Purpose Limitation

Personal data shall be collected only for clearly defined, explicit, and legitimate purposes that are directly related to ACEECA's mandate.

Once collected, data shall not be further processed in a manner that is incompatible with the original purpose unless:

- The data subject has provided additional consent; or
- Such processing is required or authorized by law; or
- It is necessary for public interest or humanitarian purposes consistent with ACEECA's mandate.

This principle prevents function creep, where data is repurposed beyond its original intent, thereby protecting individuals from unintended or unethical use of their information.

5.3 Data Minimization

ACEECA shall adhere to the principle that data collection must be limited to what is strictly necessary for achieving a defined purpose.

This means that:

- Excessive or irrelevant data shall not be collected
- Data collection instruments (forms, surveys, digital tools) shall be regularly reviewed to eliminate unnecessary fields
- Staff shall be trained to assess necessity before collecting personal information

The principle ensures operational efficiency while reducing risks associated with over-collection of sensitive information.

5.4 Accuracy

ACEECA shall take all reasonable and proportionate steps to ensure that personal data remains accurate, complete, and up to date.

This includes:

- Verification of data at the point of collection
- Periodic review and updating of datasets
- Providing mechanisms for data subjects to correct inaccurate information
- Ensuring that outdated or misleading data is either corrected or securely removed

Accurate data is essential not only for compliance but also for the integrity of programme delivery, reporting, and decision-making processes.

5.5 Storage Limitation

Personal data shall be retained only for as long as it is necessary to fulfil the specific purpose for which it was collected, or as required by applicable legal, regulatory, or donor obligations.

ACEECA shall establish clear retention schedules that define:

- Retention periods for different categories of data
- Conditions under which data may be archived
- Procedures for secure deletion or anonymization

This principle ensures that unnecessary accumulation of data is avoided, thereby reducing security risks and storage inefficiencies.

5.6 Integrity and Confidentiality

ACEECA shall implement appropriate technical, administrative, and physical safeguards to ensure the confidentiality, integrity, and security of personal data.

These measures include:

- Controlled access to data systems based on roles and responsibilities
- Encryption of sensitive data during storage and transmission
- Secure storage environments for both physical and digital records
- Regular cybersecurity assessments and system audits
- Confidentiality obligations binding all personnel and third parties

The objective is to protect data against unauthorized access, accidental loss, alteration, destruction, or disclosure.

5.7 Accountability

ACEECA shall remain fully accountable for compliance with this Policy and all applicable data protection obligations.

Accountability shall be demonstrated through:

- Documentation of all data processing activities
- Internal monitoring and compliance audits
- Assignment of clear institutional responsibilities
- Maintenance of records demonstrating adherence to data protection principles
- Prompt corrective action in the event of non-compliance

Accountability ensures that data protection is not theoretical but actively embedded in institutional practice.

6.0 LEGAL BASIS FOR DATA PROCESSING

ACEECA shall only process personal data where a valid and recognized legal basis exists. This ensures that all data activities are justified, proportionate, and compliant with applicable legal frameworks.

The following legal bases shall guide all data processing operations:

6.1 Consent of the Data Subject

Where applicable, ACEECA shall obtain explicit, informed, and freely given consent from individuals before collecting or processing their personal data.

Consent shall:

- Be specific to the intended purpose
- Be obtained without coercion or undue influence
- Be revocable at any time by the data subject

Consent shall be properly documented and stored as part of ACEECA's compliance records.

6.2 Compliance with Legal Obligations

ACEECA may process personal data where such processing is necessary to comply with statutory, regulatory, or judicial obligations.

This may include obligations related to:

- Financial reporting and auditing
- Regulatory compliance requirements
- Court orders or lawful requests from competent authorities

In such cases, processing shall be limited strictly to what is legally required.

6.3 Performance of Contractual Obligations

Data processing may be necessary for the performance of contracts between ACEECA and:

- Employees and consultants
- Partners and service providers
- Donor agencies and implementing stakeholders

This ensures that contractual obligations are fulfilled efficiently and transparently.

6.4 Legitimate Interests

ACEECA may process personal data where it is necessary for legitimate organizational interests, provided such interests do not override the fundamental rights and freedoms of the data subject.

Legitimate interests may include:

- Programme management and monitoring
- Organizational security and fraud prevention
- Institutional reporting and evaluation

A balancing test shall always be conducted to assess proportionality and necessity.

6.5 Public Interest and Humanitarian Necessity

In alignment with its mandate in environmental protection, climate action, and community resilience, ACEECA may process data where necessary for public interest or humanitarian objectives.

This may include:

- Climate vulnerability assessments
- Emergency response interventions
- Environmental and community research

Such processing shall always be guided by ethical safeguards and respect for individual rights.

7.0 DATA COLLECTION AND USE DATA

ACEECA shall ensure that all personal data collection activities are purposeful, justified, and aligned with its institutional mandate.

7.1 Methods of Data Collection

Personal data may be collected through various channels, including:

- Structured project registration systems and beneficiary enrolment forms
- Community consultations, surveys, and participatory assessments
- Digital platforms, websites, and mobile-based applications

- Donor reporting tools and partner data systems
- Human resource and recruitment processes
- Monitoring, evaluation, and research activities

All collection methods shall be designed to ensure clarity, accessibility, and informed participation.

7.2 Principles Governing Data Use

Collected data shall be used strictly in accordance with predefined purposes and shall not be repurposed without proper justification or consent.

ACEECA shall ensure that data use is:

- Relevant to organizational objectives
- Proportionate to the intended outcome
- Respectful of individual privacy and dignity
- Consistent with donor, legal, and ethical requirements

7.3 Permitted Uses of Data

Personal data collected by ACEECA may be used for the following legitimate purposes:

Programme Implementation and Evaluation

To support planning, execution, monitoring, and evaluation of environmental, energy, and climate-related interventions.

Reporting and Accountability

To fulfil reporting obligations to donors, government agencies, and regulatory authorities, ensuring transparency and accountability in programme delivery.

Communication and Stakeholder Engagement

To facilitate communication with beneficiaries, partners, and stakeholders, including dissemination of relevant information and updates.

Capacity Building, Research, and Learning

To support evidence-based research, knowledge generation, and institutional learning aimed at improving programme effectiveness and policy advocacy.

Organizational Administration and Compliance

To manage internal operations such as human resources, finance, logistics, and compliance functions efficiently and responsibly.

8.0 DATA SUBJECT RIGHTS

ACEECA recognizes that individuals whose personal data is collected and processed by the organization retain fundamental rights over their information. These rights are central to the principles of dignity, autonomy, and informed participation, and shall be respected in all data processing activities undertaken by the organization.

Accordingly, ACEECA commits to ensuring that all data subjects are able to exercise their rights in a simple, accessible, and non-discriminatory manner, without fear of retaliation or disadvantage.

8.1 Right to be informed

Data subjects shall have the right to be clearly and adequately informed about:

- The identity and contact details of ACEECA as the data controller
- The specific purpose(s) for which their data is being collected
- The legal basis for processing their data
- The categories of personal data being collected
- Any third parties with whom their data may be shared
- The duration for which their data will be retained

This information shall be provided in a concise, transparent, and easily understandable format at the point of data collection or prior to processing.

8.2 Right of access

Data subjects have the right to request and obtain confirmation as to whether ACEECA holds personal data relating to them.

Where such data exists, individuals may request:

- A copy of their personal data
- Information on how their data is being processed
- The purposes of processing and categories of data involved

ACEECA shall respond to such requests within reasonable and legally defined timelines, ensuring that access is not unduly delayed or restricted.

8.3 Right to rectification

Data subjects may request the correction or updating of personal data that is inaccurate, incomplete, or outdated.

ACEECA shall take reasonable steps to:

- Verify the accuracy of the requested correction
- Update records promptly where inaccuracies are confirmed
- Communicate corrections to any third parties where applicable

This ensures that organizational decisions are based on accurate and reliable information.

8.4 Right to erasure (right to be forgotten)

Data subjects may request the deletion of their personal data where:

- The data is no longer necessary for the original purpose
- Consent has been withdrawn and no other legal basis exists
- The data has been unlawfully processed
- Deletion is required to comply with legal obligations

However, this right shall be subject to legal, regulatory, and operational limitations, including donor reporting requirements and statutory retention obligations.

8.5 Right to restrict or object to processing

Data subjects may request the restriction of processing in situations where:

- The accuracy of the data is contested
- Processing is unlawful but deletion is not requested
- ACEECA no longer needs the data but retention is required for legal claims

Additionally, individuals may object to processing based on legitimate interests or public interest grounds. ACEECA shall assess such objections carefully and cease processing unless compelling legitimate grounds override the objection.

8.6 Right to data portability

Where technically feasible and legally applicable, data subjects may request that their personal data be transferred in a structured, commonly used, and machine-readable format.

This right applies particularly where:

- Data processing is based on consent or contract
- Processing is carried out by automated means

This ensures greater individual control and interoperability of personal data.

8.7 Right to withdraw consent

Where processing is based on consent, data subjects shall have the right to withdraw such consent at any time.

Withdrawal of consent shall:

- Not affect the lawfulness of processing conducted prior to withdrawal
- Be as easy to execute as the original consent process
- Be promptly reflected in ACEECA systems and processes

8.8 Response to requests

All requests relating to data subject rights shall be:

- Acknowledged promptly upon receipt
- Processed within reasonable and legally established timelines
- Addressed in a clear, transparent, and accessible manner

ACEECA shall ensure that appropriate internal mechanisms are in place to facilitate timely and efficient handling of all requests.

9.0 DATA SECURITY MEASURES

ACEECA shall implement comprehensive technical, organizational, and administrative safeguards to ensure the confidentiality, integrity, and availability of personal data throughout its lifecycle.

These measures are designed to prevent unauthorized access, accidental loss, alteration, disclosure, or destruction of personal data.

9.1 Secure digital storage systems

ACEECA shall ensure that all digital data is stored in secure environments that include:

- Role-based access control systems limiting access to authorized personnel only
- Secure servers and cloud infrastructure compliant with recognized security standards
- Regular system updates and patch management
- Controlled user authentication mechanisms

These systems shall be regularly reviewed to ensure continued effectiveness and resilience against emerging threats.

9.2 Encryption of data

Sensitive personal data shall be protected through encryption during:

- Transmission across networks (data in transit)
- Storage in databases or devices (data at rest)

Encryption ensures that even in the event of unauthorized access, data remains unintelligible and unusable to unauthorized parties.

9.3 Access control and authentication

ACEECA shall implement strict access control mechanisms, including:

- Unique user identification credentials for all system users
- Password protection policies aligned with best practice standards
- Multi-factor authentication for sensitive systems and databases
- Regular review and revocation of access rights when no longer required

Access shall be granted strictly on a “need-to-know” basis.

9.4 Security monitoring and audits

The organization shall conduct regular security assessments, including:

- Internal audits of data protection compliance
- Vulnerability testing of digital systems
- Monitoring of system access logs and unusual activity
- Periodic external security reviews where necessary

These processes ensure early identification and mitigation of risks.

9.5 Physical security of records

Where personal data exists in physical form, ACEECA shall ensure:

- Secure storage in locked and access-controlled facilities
- Restricted access to authorized personnel only

- Protection from environmental risks such as fire, water damage, or theft

9.6 Confidentiality obligations

All staff, consultants, partners, and contractors shall be bound by strict confidentiality obligations.

These obligations shall remain in force during and after the termination of engagement with ACEECA and shall prohibit unauthorized disclosure of personal data under any circumstances.

10.0 DATA RETENTION AND DISPOSAL

ACEECA shall adopt a structured and responsible approach to data retention and disposal, ensuring that personal data is not kept longer than necessary and is securely destroyed when no longer required.

10.1 Retention principles

Personal data shall be retained only for as long as necessary to:

- Fulfil the specific purpose for which it was collected
- Comply with legal, regulatory, or contractual obligations
- Support audit, reporting, or accountability requirements

Retention periods shall be defined through internal retention schedules aligned with operational needs and donor requirements.

10.2 Secure storage during retention period

During the retention period, all personal data shall be:

- Stored securely in controlled systems or environments
- Protected against unauthorized access or alteration
- Regularly reviewed to ensure continued relevance and accuracy

10.3 Data disposal procedures

Upon expiry of the retention period, ACEECA shall ensure secure and irreversible disposal of personal data.

Digital data disposal

Digital records shall be:

- Permanently deleted using secure deletion methods
- Anonymized where deletion is not feasible but continued analytical use is required
- Removed from all backups in accordance with system capabilities and retention policies

Physical data disposal

Hard-copy records shall be:

- Shredded using cross-cut or industrial shredding methods
- Incinerated or destroyed in a manner that prevents reconstruction
- Handled under supervision to ensure secure destruction

10.4 Documentation and accountability

All data disposal activities shall be properly documented, including:

- Type of data disposed
- Date and method of disposal
- Responsible personnel
- Confirmation of secure destruction

This ensures traceability and accountability in accordance with good governance standards.

10.5 Ethical disposal considerations

Beyond technical compliance, ACEECA shall ensure that data disposal practices respect:

- The dignity and privacy of individuals
- The sensitivity of community-based and field-collected data

- The reputational and ethical responsibilities of the organization

11.0 DATA SHARING AND DISCLOSURE

ACEECA recognizes that data sharing is an essential component of effective programme delivery, partnership coordination, reporting, and compliance. However, such sharing carries inherent risks and must therefore be governed by strict safeguards that ensure personal data is protected at all times and is disclosed only under clearly defined and justified conditions.

Accordingly, ACEECA shall adopt a restrictive and controlled approach to data sharing, guided by the principles of necessity, proportionality, transparency, and accountability.

11.1 Conditions for data sharing

Personal data may only be shared by ACEECA under the following strictly defined circumstances:

a) With the consent of the data subject

Where sharing is based on consent, such consent must be:

- Freely given without coercion or undue influence
- Specific to the intended recipient and purpose of sharing
- Fully informed, with clear explanation of potential implications
- Documented and verifiable

Data subjects shall retain the right to withdraw consent at any time, subject to legal and operational constraints.

b) With donors, partners, or regulatory authorities

ACEECA may share personal data with legitimate institutional stakeholders, including donors, implementing partners, and government regulators, where such sharing is:

- Required under funding agreements or reporting obligations
- Necessary for programme monitoring, evaluation, or accountability
- Aligned with agreed project implementation frameworks

In all such cases, data sharing shall be limited to the minimum necessary information required to fulfil the stated purpose.

c) With service providers under confidentiality obligations

Where ACEECA engages third-party service providers (including IT providers, consultants, evaluators, or cloud service vendors), personal data may be shared only where:

- A formal contractual relationship exists
- The service provider is bound by enforceable confidentiality and data protection obligations
- The provider demonstrates adequate technical and organizational safeguards

Such providers shall act strictly on behalf of ACEECA and shall not process data for independent purposes.

d) Where required by law or court order

ACEECA may disclose personal data where such disclosure is:

- Mandated by applicable law or regulation
- Required under a valid court order or lawful directive from competent authorities

In such cases, ACEECA shall, where legally permissible, seek to limit the scope of disclosure and ensure that only the minimum required data is shared.

11.2 Data Sharing Agreements (DSAs)

All third-party data sharing arrangements shall be governed by formal Data Sharing Agreements.

These agreements shall define:

- The purpose and scope of data sharing
- Categories of data to be shared
- Roles and responsibilities of each party
- Security and confidentiality obligations
- Data retention and deletion requirements
- Breach notification procedures

No personal data shall be shared with external entities in the absence of such a legally binding agreement.

11.3 Oversight and accountability

ACEECA shall maintain oversight of all data sharing activities through:

- Internal approval mechanisms prior to disclosure
- Documentation of all data sharing transactions
- Periodic review of partner compliance with data protection obligations

This ensures that data sharing remains controlled, justified, and aligned with organizational values and legal obligations.

12.0 CROSS-BORDER DATA TRANSFERS

ACEECA acknowledges that in the context of global partnerships, digital systems, and international development cooperation, personal data may at times be transferred beyond the territorial boundaries of Kenya.

Such transfers present additional risks due to varying levels of data protection standards across jurisdictions. Accordingly, ACEECA shall ensure that all cross-border data transfers are subject to strict safeguards and prior assessment.

12.1 Principle of adequacy

Personal data shall only be transferred to countries or jurisdictions that ensure an adequate level of data protection.

Adequacy shall be assessed based on:

- Existence of robust data protection laws in the receiving jurisdiction
- Availability of enforceable rights for data subjects
- Existence of independent supervisory authorities
- Effective legal remedies in case of misuse or breach

Where adequacy cannot be demonstrated, additional safeguards shall be required.

12.2 Binding contractual safeguards

In cases where data is transferred to jurisdictions without equivalent protection standards, ACEECA shall ensure that legally binding contractual safeguards are in place.

Such safeguards may include:

- Standard contractual clauses aligned with international best practice
- Explicit obligations on data security and confidentiality
- Restrictions on onward transfer of data
- Audit and compliance rights for ACEECA
- Breach notification obligations

These mechanisms ensure that transferred data remains protected regardless of jurisdictional differences.

12.3 Compliance with international standards

All cross-border data transfers shall comply with applicable international data protection principles, including those derived from:

- The United Nations data protection and privacy principles
- The General Data Protection Regulation (GDPR) where applicable
- Regional and national data protection frameworks

ACEECA shall adopt a precautionary approach, ensuring that cross-border transfers do not undermine the rights and freedoms of data subjects.

12.4 Risk-based assessment

Prior to any cross-border transfer, ACEECA shall conduct a risk-based assessment to determine:

- The sensitivity of the data involved
- The purpose and necessity of the transfer
- Potential risks to data subjects
- Mitigation measures required

Transfers shall only proceed where risks are adequately mitigated and justified.

13.0 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

ACEECA shall adopt a proactive and preventive approach to data protection through the systematic use of Data Protection Impact Assessments (DPIAs) for high-risk processing activities.

A DPIA is a structured process designed to identify, assess, and mitigate risks to the rights and freedoms of individuals arising from data processing activities.

13.1 Purpose of DPIAs

The primary objective of a DPIA is to ensure that data protection risks are identified and addressed at the earliest possible stage of programme or system design.

It enables ACEECA to:

- Embed privacy and data protection into project planning ("privacy by design")
- Avoid or minimize potential harm to individuals
- Demonstrate accountability and regulatory compliance
- Strengthen stakeholder trust and institutional credibility

13.2 Identification of risks to data subjects

ACEECA shall conduct DPIAs where processing activities are likely to result in high risk, including but not limited to:

- Large-scale collection of personal or sensitive data
- Use of new technologies or digital platforms
- Processing involving vulnerable populations or communities
- Data sharing across multiple institutions or jurisdictions

Risk identification shall consider potential impacts such as:

- Loss of privacy or confidentiality
- Discrimination or exclusion
- Identity theft or misuse of personal information
- Reputational or social harm to individuals or communities

13.3 Assessment of necessity and proportionality

Each DPIA shall evaluate whether:

- The proposed data processing is strictly necessary to achieve its intended purpose
- Less intrusive alternatives exist
- The scope of data collection is proportionate to the expected outcomes

This ensures that data processing is not excessive or unjustified in relation to programme objectives.

13.4 Mitigation and risk management measures

Where risks are identified, ACEECA shall implement appropriate mitigation measures prior to project implementation.

These may include:

- Strengthening data security controls
- Limiting data access to authorized personnel
- Anonymizing or pseudonymizing personal data
- Revising data collection tools to reduce sensitivity
- Enhancing consent and transparency mechanisms

No high-risk processing activity shall proceed without adequate mitigation measures in place.

13.5 Documentation and review

All DPIAs shall be:

- Documented in a standardized format
- Reviewed and approved by designated institutional authorities
- Periodically updated where project conditions or risks change

This ensures that DPIAs remain living instruments of accountability rather than one-time exercises.

14.0 ROLES AND RESPONSIBILITIES

Effective data protection within ACEECA is dependent on clearly defined roles, institutional accountability, and coordinated responsibility across all levels of the organization. Data protection is not the sole responsibility of a single unit, but a shared institutional obligation embedded in governance, programme delivery, and operational systems.

14.1 Executive Leadership

The Executive Leadership of ACEECA bears ultimate responsibility for ensuring strategic oversight and institutional accountability for data protection compliance.

In particular, Executive Leadership shall:

- Provide overall direction and leadership on data governance and privacy protection
- Ensure that adequate financial, technical, and human resources are allocated for data protection implementation
- Approve institutional policies, procedures, and frameworks related to data protection
- Foster a culture of compliance, accountability, and ethical data management across all departments
- Ensure that data protection considerations are integrated into strategic planning and decision-making processes

Executive Leadership shall be accountable for ensuring that data protection is treated as a core governance and risk management priority within the organization.

14.2 Data Protection Officer (DPO)

The Data Protection Officer (DPO) shall serve as the central technical and advisory authority on data protection matters within ACEECA.

The DPO shall be responsible for:

- Monitoring and ensuring compliance with this Policy and applicable legal frameworks
- Advising management, staff, and partners on data protection obligations and best practices
- Conducting periodic audits, assessments, and reviews of data processing activities
- Serving as the primary point of contact for data subjects regarding their rights and concerns
- Liaising with national regulatory authorities and external oversight bodies where required

- Supporting the development of training programmes and awareness initiatives
- Reviewing high-risk processing activities, including DPIAs and data sharing arrangements

The DPO shall operate with a high degree of independence to ensure objectivity, integrity, and impartial oversight.

14.3 Programme and Field Staff

Programme and Field Staff are at the frontline of data collection and engagement with communities, beneficiaries, and stakeholders. As such, they play a critical role in ensuring that data protection principles are applied in practice.

Their responsibilities include:

- Ensuring that personal data is collected in accordance with this Policy and approved tools
- Obtaining informed consent from data subjects where required
- Collecting only data that is necessary, relevant, and proportionate to programme objectives
- Safeguarding data during field collection, transport, and storage
- Reporting any suspected data breaches or irregularities immediately
- Ensuring confidentiality in all interactions involving personal data

Programme and Field Staff shall be expected to exercise professional judgment and ethical responsibility when handling personal data in community settings.

14.4 IT and Systems Personnel

IT and Systems Personnel shall be responsible for the technical protection of digital infrastructure and information systems used by ACEECA.

Their responsibilities include:

- Designing and maintaining secure digital systems for data storage and processing
- Implementing cybersecurity measures, including firewalls, encryption, and access controls
- Monitoring systems for vulnerabilities, breaches, or unauthorized access attempts
- Ensuring regular system updates, backups, and disaster recovery mechanisms
- Supporting secure integration of third-party platforms and applications
- Advising the organization on emerging technological risks and mitigation strategies

IT personnel shall ensure that all systems are aligned with recognized cybersecurity standards and best practices.

14.5 Partners and Contractors

All partners, consultants, vendors, and contractors engaged by ACEECA shall be required to comply fully with this Data Protection Policy.

Their responsibilities include:

- Processing personal data strictly in accordance with contractual instructions from ACEECA
- Maintaining confidentiality and security of all data accessed or processed
- Implementing adequate technical and organizational safeguards
- Ensuring that data is not used for any unauthorized or independent purpose
- Promptly reporting any data breach or security incident involving ACEECA data

Compliance shall be enforced through binding Data Sharing or Data Processing Agreements, and failure to comply may result in termination of contractual relationships.

15.0 TRAINING AND AWARENESS

ACEECA recognizes that effective data protection is dependent not only on policies and systems, but also on the knowledge, awareness, and behavior of its personnel and partners.

Accordingly, the organization shall implement continuous capacity-building and awareness initiatives to ensure that all stakeholders understand their roles and responsibilities in safeguarding personal data.

15.1 Regular staff training

ACEECA shall provide periodic training sessions on data protection principles and practices, including:

- Legal and ethical obligations related to data handling
- Safe data collection, storage, and transmission practices
- Identification and reporting of data breaches
- Use of secure systems and tools

Training shall be tailored to different staff categories based on their level of data access and responsibility.

15.2 Induction programmes

All new employees, interns, volunteers, and consultants shall undergo mandatory induction training on data protection as part of their onboarding process.

This induction shall ensure that:

- New personnel are familiar with ACEECA's data protection obligations from the outset
- Clear expectations are established regarding confidentiality and responsible data handling
- Awareness of reporting mechanisms and escalation procedures is reinforced

15.3 Awareness campaigns

ACEECA shall conduct ongoing awareness initiatives across all operational units to reinforce a culture of data protection.

These may include:

- Internal communication campaigns and newsletters
- Posters and visual reminders in offices and field offices
- Thematic sessions during staff meetings and retreats

The aim is to embed data protection awareness as part of everyday organizational practice.

15.4 Continuous capacity building

Given the evolving nature of digital technologies and cyber risks, ACEECA shall ensure continuous professional development on emerging data protection issues, including:

- Cybersecurity threats and mitigation techniques
- Evolving legal and regulatory frameworks
- Best practices in digital governance and ethical data use

This ensures that the organization remains adaptive, informed, and resilient in its data protection approach.

16.0 DATA BREACH MANAGEMENT

ACEECA shall adopt a structured and proactive approach to the identification, management, and mitigation of data breaches, recognizing that timely response is critical to minimizing harm to data subjects and the organization.

A data breach refers to any incident that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

16.1 Immediate containment measures

Upon discovery of a suspected or confirmed data breach, ACEECA shall take immediate steps to:

- Contain and limit the scope of the breach
- Prevent further unauthorized access or data loss
- Secure affected systems, devices, or records
- Preserve evidence for investigation purposes

Rapid containment is essential to minimize potential harm and prevent escalation.

16.2 Reporting to the Data Protection Officer

All suspected or confirmed breaches shall be reported without delay to the Data Protection Officer.

The DPO shall:

- Assess the nature, severity, and scope of the breach
- Coordinate internal response actions
- Determine whether external reporting is required
- Provide guidance on mitigation and recovery measures

Timely escalation ensures coordinated institutional response and compliance with legal obligations.

16.3 Notification of affected individuals

Where a data breach is likely to result in a high risk to the rights and freedoms of individuals, ACEECA shall notify affected data subjects without undue delay.

Such notification shall include:

- A description of the nature of the breach
- The categories of personal data affected
- Potential consequences of the breach
- Measures taken or proposed to address the breach
- Guidance on steps individuals may take to protect themselves

The objective is to ensure transparency and enable affected individuals to take appropriate protective action.

16.4 Corrective and preventive measures

Following containment, ACEECA shall implement corrective and preventive actions, including:

- Strengthening system security controls
- Revising internal processes and protocols
- Providing additional staff training where necessary
- Reviewing third-party compliance and contractual safeguards

These measures shall aim to prevent recurrence and strengthen institutional resilience.

16.5 Documentation and review

All data breach incidents shall be fully documented, including:

- Timeline and description of the incident
- Root cause analysis
- Response actions taken
- Impact assessment
- Lessons learned and recommendations

Incident reports shall be reviewed by management and used to improve ACEECA's overall data protection framework.

17.0 COMPLAINTS AND REDRESS MECHANISM

ACEECA is committed to ensuring that all data subjects and stakeholders have access to an effective, transparent, and accessible mechanism for raising concerns, lodging complaints, and seeking redress regarding the handling of their personal data.

The organization recognizes that accountability in data protection is strengthened when individuals are empowered to challenge perceived misuse, seek clarification, and obtain timely remedies.

17.1 Right to lodge complaints

Any data subject who believes that their personal data has been:

- Misused or processed unlawfully
- Collected without proper consent or legal basis
- Disclosed without authorization
- Inaccurately recorded or improperly managed

shall have the right to lodge a formal complaint with ACEECA.

Complaints may be submitted through designated communication channels, including email, written submissions, or in-person reporting through programme offices.

17.2 Acknowledgement and handling of complaints

All complaints shall be:

- Acknowledged promptly upon receipt
- Registered in an internal complaint tracking system
- Assigned to a responsible officer for review and investigation

ACEECA shall ensure that complaints are handled in a fair, impartial, and confidential manner, with due respect for the rights of all parties involved.

17.3 Investigation and resolution

Each complaint shall be subject to a structured review process, which may include:

- Verification of facts and supporting documentation
- Consultation with relevant departments or personnel
- Assessment of compliance with this Policy and applicable laws
- Determination of corrective or remedial action

Where necessary, corrective actions shall be implemented promptly to address identified breaches or weaknesses.

17.4 Communication of outcomes

Upon completion of the review process, ACEECA shall communicate the outcome to the complainant in a clear and transparent manner, including:

- Findings of the investigation
- Actions taken or proposed
- Guidance on further recourse, where applicable

Where complaints are not substantiated, clear explanations shall be provided to ensure understanding and maintain trust.

17.5 External escalation

Where complainants are not satisfied with the internal resolution process, they may escalate their concerns to the relevant national data protection authority or other competent regulatory bodies, in accordance with applicable legal frameworks.

18.0 COMPLIANCE AND MONITORING

ACEECA is committed to ensuring continuous compliance with this Data Protection Policy, applicable national legislation, and internationally recognized data protection standards.

Compliance is regarded as a core governance function and an integral component of institutional accountability, risk management, and ethical practice.

18.1 Internal compliance monitoring

ACEECA shall establish internal mechanisms to monitor adherence to this Policy, including:

- Regular compliance reviews across all departments
- Periodic audits of data processing activities
- Evaluation of adherence to data protection principles in programmes and operations
- Review of partner and third-party compliance

These mechanisms shall ensure that data protection is consistently implemented in practice and not limited to policy documentation.

18.2 Risk management and oversight

Data protection risks shall be integrated into ACEECA's broader institutional risk management framework.

This shall include:

- Identification of emerging risks in data processing activities
- Assessment of vulnerabilities in systems and processes
- Implementation of mitigation and corrective measures
- Continuous monitoring of high-risk operations

18.3 Reporting and accountability

Regular compliance reports shall be submitted to ACEECA's leadership structures, detailing:

- Status of data protection implementation
- Identified gaps or incidents
- Corrective actions taken
- Recommendations for improvement

This ensures that leadership remains informed and able to provide strategic oversight.

18.4 Consequences of non-compliance

Failure to comply with this Policy may result in:

- Disciplinary action for staff and affiliated personnel
- Suspension or termination of contracts for partners or service providers
- Legal or regulatory consequences where applicable

ACEECA shall apply enforcement measures consistently and fairly, in accordance with internal procedures and applicable law.

19.0 REVIEW OF THE POLICY

This Data Protection Policy is a living document and shall be subject to periodic review to ensure continued relevance, effectiveness, and alignment with evolving legal, technological, and operational contexts.

19.1 Periodic review cycle

The Policy shall be formally reviewed at least once every two (2) years. However, earlier review may be initiated where necessary, particularly in cases of:

- Changes in applicable data protection laws or regulations
- Introduction of new technologies or digital systems
- Emergence of new operational risks or vulnerabilities
- Organizational restructuring or expansion of operations

19.2 Review process

The review process shall involve:

- Assessment of implementation effectiveness
- Consultation with internal stakeholders and technical experts

- Consideration of audit findings and incident reports
- Benchmarking against international best practices

19.3 Approval and adoption of revisions

Any amendments to this Policy shall be:

- Reviewed by relevant technical and governance structures
- Endorsed by senior management
- Formally approved by the appropriate governing authority within ACEECA

Revised versions shall be communicated to all staff and stakeholders to ensure awareness and compliance.

20.0 STATEMENT OF COMMITMENT TO DATA PROTECTION

The Africa Centre for Environment, Energy and Climate Advocacy (ACEECA) affirms its unwavering commitment to the highest standards of data protection, privacy, and information governance in all aspects of its work.

In fulfilling its mandate to advance environmental sustainability, climate action, clean energy transitions, and community resilience, ACEECA recognizes that the responsible handling of personal data is fundamental to maintaining trust, integrity, and accountability in its engagements with communities, partners, donors, and stakeholders.

ACEECA commits to ensuring that all personal data collected, processed, stored, shared, or disposed of in the course of its operations shall be handled in strict accordance with applicable national legislation, particularly the Kenya Data Protection Act, 2019, as well as internationally recognized principles of data protection and privacy, including those promoted by the United Nations system and other global governance frameworks.

The organization undertakes to uphold the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability in all data processing activities. These principles shall guide institutional decision-making, programme implementation, and stakeholder engagement across all levels of operation.

ACEECA further commits to safeguarding the rights and freedoms of all data subjects, ensuring that individuals have meaningful control over their personal data, including the right to be informed, access, correct, restrict, object to processing, and withdraw consent where applicable.

The organization shall continuously strengthen its technical, administrative, and organizational safeguards to protect personal data against unauthorized access, loss, misuse, or disclosure. This includes ongoing investment in secure systems, staff capacity building, risk management frameworks, and compliance monitoring mechanisms.

ACEECA recognizes that data protection is a shared institutional responsibility. As such, all staff, consultants, partners, and service providers are expected to adhere strictly to this Policy and to demonstrate the highest standards of professionalism, confidentiality, and ethical conduct in the handling of personal data.

Through this commitment, ACEECA reaffirms its dedication to building trust with the communities it serves, strengthening accountability to its partners and donors, and advancing a data governance culture that is aligned with global best practices and sustainable development principles.

This Statement of Commitment is hereby adopted as a guiding expression of ACEECA's values and institutional responsibility in the protection of personal data.

Protecting personal data is fundamental to safeguarding human dignity, strengthening institutional accountability, and building trust with the communities we serve. Through this Policy, African Centre for Environment, Energy and Climate Advocacy (ACEECA) reaffirms its commitment to responsible data governance, ethical practice, and the highest standards of privacy and confidentiality in all its operations.

ANNEX 1: CONSENT FORM FOR PERSONAL DATA COLLECTION AND PROCESSING

African Centre for Environment, Energy and Climate Advocacy (ACEECA)

Personal Data Consent Form

1. Introduction

ACEECA collects and processes personal data in order to implement programmes related to environmental protection, climate action, clean energy, and community development. This form explains how your data will be used and seeks your informed consent.

2. Type of Data Collected

We may collect the following personal data:

- Full name
- Contact details (phone number, email, address)
- Identification details (where applicable)
- Demographic information
- Programme participation data
- Photos, audio, or video recordings (where applicable)

3. Purpose of Data Collection

Your data will be used for:

- Programme implementation and follow-up
- Monitoring and evaluation activities
- Reporting to donors and partners
- Communication and stakeholder engagement
- Research and learning purposes

4. Data Protection Assurance

ACEECA commits to:

- Keeping your data secure and confidential
- Using your data only for the stated purposes
- Not sharing your data without legal justification or consent
- Allowing you to request access, correction, or deletion of your data

5. Consent Declaration

By signing below, you confirm that:

- You have read and understood this form
- You voluntarily agree to the collection and processing of your personal data
- You understand that you may withdraw consent at any time

Name: _____

Signature: _____

Date: _____

ANNEX 2: DATA PROTECTION IMPACT ASSESSMENT (DPIA) TEMPLATE

ACEECA Data Protection Impact Assessment (DPIA)

1. Project Information

- Project Name: _____
- Department/Unit: _____
- Responsible Officer: _____
- Start Date: _____

2. Description of Processing Activity

- What data is being collected?
- Why is it being collected?
- Who are the data subjects?
- What systems will be used?

3. Necessity and Proportionality

- Is the data processing necessary for the project?
- Are there less intrusive alternatives?
- Is the data collection limited to what is required?

4. Risk Identification

Identify risks to individuals:

- Unauthorized access
- Data loss or leakage
- Misuse of personal data
- Harm to vulnerable groups
- Reputational risk

5. Risk Level Assessment

- Low □
- Medium □
- High □

Justification:

_____

6. Mitigation Measures

- Encryption of data
- Access restrictions
- Staff training
- Data minimization
- Secure storage systems

7. Residual Risk

After mitigation:

- Acceptable □
- Requires further action □

8. Approval

- Prepared by: _____
- Reviewed by DPO: _____
- Approved by Management: _____

ANNEX 3: DATA BREACH REPORT FORM

ACEECA Data Breach Incident Report

1. Incident Details

- Date of Incident: _____
- Time of Incident: _____
- Reported By: _____
- Department: _____

2. Description of Breach

Provide a clear description of what happened:

3. Type of Data Involved

- Personal identification data
- Contact details
- Financial data
- Sensitive data
- Other: _____

4. Number of Individuals Affected

- Estimated number: _____

5. Immediate Action Taken

- System isolated ☐
- Access revoked ☐
- Data secured ☐
- Other measures: _____

6. Risk Assessment

- Low ☐
- Medium ☐
- High ☐

7. Notification

- Data Protection Officer informed ☐
- Affected individuals notified ☐
- Regulators informed ☐

8. Corrective Actions

9. Report Prepared By

Name: _____
Signature: _____
Date: _____

ANNEX 4: DATA REGISTER TEMPLATE (RECORD OF PROCESSING ACTIVITIES)

ACEECA Data Processing Register

1. Department Information

- Department: _____
- Data Controller Unit: _____
- Contact Person: _____

2. Data Processing Activity

Activity Name	Purpose	Data Subjects	Data Type	Legal Basis

3. Data Categories

- Personal identification data
- Contact information
- Financial information
- Programme participation data
- Sensitive data (if any)

4. Data Sharing

Recipient	Purpose	Country	Safeguards in Place

5. Data Storage

- Storage Location: _____
- System Used: _____
- Security Measures: _____

6. Retention Period

- Duration: _____
- Justification: _____

7. Data Disposal Method

- Secure deletion ☐
- Anonymization ☐
- Physical destruction ☐

8. Responsible Officer

Name: _____
Signature: _____
Date: _____