Data Protection Policy

Stichting Clean Energy and Energy Inclusion for Africa (CEI Africa or the Foundation)

Adopted by a resolution of the Board on 29.06.2023

Approved by the Supervisory Council on 30.06.2023

Version Control

Document history		
Version No	Date	Description / amendments
1	30.06.2023	First version

1. Objective

Stichting Clean Energy and Energy Inclusion for Africa (**CEI Africa** or '**the Foundation'**) is committed to the highest standards of transparency and integrity. The application of these standards also results in the implementation and maintenance of systems to safeguard the security, integrity and confidentiality of Personal Data. This is key to maintaining confidence in the organisation and provide for successful business operations. CEI Africa processes Personal Data in its business operations, and this concerns Personal Data from Customers, other stakeholders such as Board members, business partners, and any other individuals with whom CEI Africa interacts for business purposes. It also refers to Personal Data in the context of employment. CEI Africa considers it important that processing Personal Data is done with the utmost care in order to prevent damage caused by abuse, incidents or negligence. Any incidents involving Personal Data may lead to a regulatory fine, reputational harm or loss of confidence from other stakeholders. Violations of the applicable data protection legislation, in fact, may lead to penalties and or claims for damages imposed by the Dutch Data Protection Authority (**DPA**) to CEI Africa. In order to ensure compliance with applicable requirements and clarity of internal processes, responsibilities and expectation amongst members of Staff, CEI Africa has established and implemented this Data Protection Policy (**this Policy**).

2. Scope

This Policy applies to the processing of all Personal Data by CEI Africa as Data Controller[1], by electronic means or paper-based filing system. In light of the territorial scope of the current applicable legislation[2], which applies to the processing of Personal Data from an organisation established in the European Union (**EU**), regardless of whether the processing takes place in the EU or not, the application of this Policy is mandatory for anyone worldwide who, in the performance of their role within CEI Africa, processes Personal Data. To have a consistent approach, CEI Africa has decided to apply the provisions of this Policy to all Personal Data, including Personal Data collected outside the EU by the CEI Africa partners. It therefore applies to all CEI Africa Staff, Executive Board and Supervisory Council members, as well as to any parties included in the on-boarding and on-going monitoring processes.

Corporate documents or data referring to institutions, albeit confidential and important, are out of scope of this Policy.

3. Regulatory requirements and Guidelines

This Policy is based on the:

- General Data Protection Regulation (2016/679 / EC, hereinafter GDPR) and General Data Protection Regulation Implementation Act (2018)
- Guidance from the European Data Protection Board
- DPA recommendations for a Data Protection Policy

4. Definitions and terms

Term	Definition
Anonymisation	The process of turning Personal Data into anonymous information so that an individual is not (or is no longer) identifiable.

[1] CEI Africa is the Data Controller but also the Data Processor unless the Personal Data processing is outsourced to a third party, which becomes the Data Processor.

[2] Articles 3.1 and 3.2 of the GDPR define the territorial scope of the Regulation, i.e., to an organisation established in the EU and/or to the processing of Personal Data of individuals based in the EU.

Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to them.
Criminal Data	Personal Data relating to criminal convictions and offences.
Customer	This definition refers to either a Contributor, an Investee, a Grantee, a Guarantee, or a Crowdlender, with reasonable interpretation necessary due to specific context, being applicable in relationship to CEI Africa. In the context of this definition, the following are referred to: ➢ **Contributor**: A legal person or entity making funds available to CEI Africa, either drawn or undrawn, based on a grant or contribution agreement with CEI Africa. ➢ **Investee**: Any party which CEI Africa lends money to (debt) or invests in (equity). ➢ **Grantee:** Developers of green mini-grids who have been selected by CEI Africa and that enter into a grant agreement with CEI Africa. ➢ **Guarantee**: a natural or legal person or entity benefiting from the promise by the Guarantor to fulfil contract obligations if another party fails to pay or perform. ➢ **Crowdlender**: Brokering of loans over an Internet services platform domiciled in an EU member state or EFTA member state between a customer (the borrower) and the lender.
Data Controller	The entity that determines the purposes and means of processing Personal Data. CEI Africa is the only Controller to determine the purposes and means of processing.
DPA	Dutch Data Protection Authority ('Autoriteit Persoonsgegevens').
Data Processor	The entity that is responsible for processing Personal Data on behalf of a Data Controller.
Data Subject	The identified or identifiable living individual to whom Personal Data relates.
DPIA	Data Protection Impact Assessment.
EEA	European Economic Area.
Encryption	Procedure that converts clear text into a hashed code using a key, where the information only becomes readable again by using the correct key.
Foundation Manager	The entity selected to assist in the management of CEI Africa and its assets and investments as well as the provision of technical assistance by CEI Africa and the provision of grant activities of CEI Africa in accordance with the Foundation Management Agreement.
GDPR	General Data Protection Regulation (EU) 2016/679, which took effect on 25 May 2018. In the Netherlands, the GDPR is referred to as the 'Algemene Verordening Gegevensbescherming (AVG)'.
Partner (CEI Africa Partner)	Any professional entities rendering services to CEI Africa.
PEP	Politically Exposed Person, as defined in Art. 2.1 of the Dutch Implementation Decree Wwft 2018, and described in section 6.1.4 of the Compliance Policy.
Personal Data	Information that relates to an identified or identifiable individual (e.g., who can be identified directly from such information / indirectly in

	combination with other information). Information about a deceased person does not constitute Personal Data.
Personal Data breach	Security incident that has affected the confidentiality, integrity or availability of Personal Data and that can lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to Personal Data transmitted, stored or processed.
Processing	Performing any operations on Personal Data including collection, recording, storing, consulting, restricting, disclosing, erasing and destructing.
Pseudonymisation	The process of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information.
Sensitive Data	Special categories of Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, trade union membership, biometric data, health or sexual orientation. This also includes criminal records or children's data.
Service Provider	A third party, such as an entity or an individual that provides services to CEI Africa, with the provision of the service(s) being governed by a service agreement between them.
Staff	Staff of the Foundation Manager that performs professional activities for the Foundation.
UBO	Ultimate Beneficial Owner, as defined in section 6.1.3 of the Compliance Policy.

5. Policy specifics

This Policy covers the following Personal Data processes:

Personal Data from	**Category of Personal Data processed**
Customers, donors, related individuals in their role as representatives, UBOs, Board members or senior managers, PEPs and any other associated individuals	Name; address, place of residence, gender; date of birth; nationality; images of signatures, location Contact details: address; telephone number; fax number; email address Employment details: Profession and employment; function/role Judicial data Identification number (e.g., national number, etc.) Copy passport or other ID documents Biometrical data as shown in passport Bank statements
Prospects Customers, donors, etc.	Name and address, gender, birth date, nationality; contact details; location data, email address for newsletters
Service Providers representatives/authorised persons	Name and address, birth date, nationality; contact details; location data Copy passport or other ID documents
Members of Staff (including members of the Supervisory Council, advisors and consultants)	Name and address, gender, birth date, nationality; contact details and emergency contact details; country registration numbers (BSN, ID nr); informal and generic information about absence in case of illness training and

	education; profession and employment; copy passport/ID; screening info; image material; location data

5.1. Roles and responsibilities

The **Executive Board** of CEI Africa (the **Board**) is responsible for establishing and implementing sound security mechanisms in order to maintain an effective and transparent regime for data protection. The Board is also responsible, and considered accountable, for complying with the data protection principles.

The **Compliance Officer** is responsible for the day-to-day implementation and maintenance of this Policy and for monitoring its effectiveness. The following data protection related tasks are also carried out by the Compliance Officer:

- Contact point for data protection related matters;
- Point of contact for individuals when exercising their rights, or submitting a complaint;
- Advisory role in implementing applicable requirements in relation to data protection;
- Dealing with Personal Data breaches;
- Periodic reporting to the Board of CEI Africa and the Supervisory Council in relation to data protection.

All Members of Staff, as defined in Section 4, and CEI Africa partners, are responsible for familiarizing themselves with the provisions of this Policy and for ensuring proper and safe processing of Personal Data in their daily activities for CEI Africa. They are also responsible for reporting a Personal Data breach, as defined in Section 4, to the Compliance Officer as soon as it is detected or suspected. They are expected to work together towards the facilitation and maintenance of a framework for the safe process of Personal Data during the entire data cycle, from collection to erasure.

5.2. Policy Statements & Principles

When processing Personal Data, CEI Africa is committed to handle Personal Data with care and in accordance with the applicable legal framework. CEI Africa's approach to Personal Data is about:

- Being transparent in processing the Personal Data of all stakeholders;
- Only processing Personal Data for a specific business purpose, and for the purpose for which Personal Data was originally collected;
- Only using Sensitive Data if necessary, and when it is legally allowed;
- Making sure that Personal Data is accurate, relevant and up-to-date;
- Informing all the relevant stakeholders on how CEI Africa processes Personal Data. This is achieved through the publication on the company's website of a Privacy Statement (e.g., information provision);
- Allowing stakeholders access to, and having an overview of, their Personal Data;
- Taking all reasonable steps and measures to protect Personal Data from unauthorised access, loss, alteration or disclosure.

CEI Africa does not process Personal Data that is not reasonably needed for or otherwise relevant to the legitimate purpose for which Personal Data is processed.

CEI Africa acknowledges the requirement for appointing a Data Protection Officer (art. 37 of the GDPR) but it determined that these requirements [(article 37 .1 (a), (b), (c)] do not apply to the Foundation. Nevertheless, assigning data protection related matters to the responsibilities of the Foundation Compliance Officer, is considered an appropriate and sufficient measure to ensure that data protection related matters are properly dealt with.

5.3. Business purposes

CEI Africa only uses Personal Data for legitimate business reasons and for the prevention of financial crime. It processes Personal Data in the following ways:

- When entering into a commercial relation and managing this relation (e.g., performing agreements);
- To verify the identity of certain individuals who are authorized to represent Customers or Service Providers or any other individuals as mentioned in Section 5 of this Policy;
- For the detection and prevention of any forms of financial crime, such as fraud, money laundering and terrorist financing, bribery and corruption, criminal tax evasion, and to comply with applicable legal requirements;
- To complete any requests from individuals (e.g., Subject Access requests);
- For publicity and commercial relationship management purposes;
- For archiving purposes (e.g., for legal proceedings);
- For the execution of employment contracts and employment related aspects.

If the processing of Personal Data is not based on an explicit business purpose, then getting consent from the relevant individual is required. CEI Africa acknowledges that an individual can deny or withdraw consent at any time.

6. Implementation of data protection requirements

6.1. Compliance with the Principles of Personal Data Processing

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime. When processing Personal Data, CEI Africa complies with the following principles and ensures that Personal Data is:

- Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
- Collected only for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes (Purpose Limitation);
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
- Accurate and where necessary kept up to date, and are erased or rectified if necessary (Accuracy);
- Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation);
- Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Integrity and Confidentiality).

CEI Africa is responsible for being able to demonstrate compliance with the provisions of the GDPR **(Accountability principle)**

6.2. Lawful basis for processing Personal Data

CEI Africa must have a valid lawful basis in order to process Personal Data. Processing only takes place if at least one of the following applies:

- The Data Subject has given consent to the processing of their Personal Data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- Processing is necessary for Compliance with a legal obligation to which CEI Africa is subject;
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person (i.e., essential for someone's life);

- Processing is necessary for the purposes of the legitimate interests (i.e., an interest that is consistent with the Foundation business) pursued by CEI Africa or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data.

Consent is understood as a **freely given, specific, informed and unambiguous indication** of the Data Subject's agreement to their processing of Personal Data. CEI Africa acknowledges that, if processing is based on consent and wishes to process Personal Data for a new purpose, then it needs to obtain a new consent for the new processing purpose. The original consent will never legitimise further or new purposes for processing. When necessary for processing purposes, CEI Africa keeps records of the consent obtained by the Data Subjects.

6.3. Processing special categories of Personal Data and Criminal Data

Processing special categories of Personal Data (e.g., Sensitive Data) is prohibited, unless specific legal grounds are available. This is because the sensitive nature of this data merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. In principle, CEI Africa processes no special Personal Data, namely a person's religion or philosophical beliefs, racial or ethnic origin, political preference, health, genetic data, sexual life and orientation, membership of a trade union. This definition does not include Personal Data about criminal records (e.g., allegations, proceedings or convictions).

If it becomes necessary to process special categories of Personal Data, CEI Africa ensures that the Data Subject has given explicit consent to the Processing, unless processing is necessary for carrying out specific obligations or to protect the vital interests of the data Subject.

There are exceptions, for example the use of special Personal Data in line with the due diligence process. Data relating to criminal behaviour, and records on proceedings are processed for protecting the interest of CEI Africa with respect to criminal offences that have been or can be committed against CEI Africa or its Staff.

The use of special Personal Data outside the circumstances above mentioned must be discussed with the Compliance Officer for further assessment on the lawful basis for processing.

7. Rights of Data Subjects

One of the key objectives of the GDPR is to grant Data Subjects with control of how their Personal Data is processed and, consequently, to guarantee a number of rights. CEI Africa takes active steps to facilitate the exercise of Data Subject rights, and has established appropriate procedures for handling requests from Data Subjects in the exercise of their right (including an identification process of the Data Subject, before proceeding with their request).

7.1. Transparency - information

Recital 39 of the GDPR states that the **principle of transparency** requires that any information and communication relating to the processing of Personal Data is easily accessible and easy to understand, and that clear and plain language is used. Transparency is intrinsically linked to the principle of accountability for data controllers (e.g., CEI Africa) and of the Data Subjects empowerment.

CEI Africa takes appropriate measures to provide detailed, specific information to Data Subjects on the nature of the Personal Data processing. When gathering Personal Data or establishing new data protection activities, it needs to be ensured that individuals whose data is being processed have received appropriate notice informing them how the data will be used. CEI Africa will publish a detailed Privacy Statement on its website, where the following information is always available and accessible:

- The contact details of CEI Africa acting as the controller of an individual's Personal Data;
- The purposes of the processing for which the Personal Data are intended as well as the legal basis for the processing;
- The recipients of the Personal Data;
- The Data Subject rights to request information data protection standards and international transfers of Personal Data (I.e., to third-party recipients outside the EU);
- The relevant retention periods;
- The individual's rights regarding their Personal Data, including their right to withdraw consent at any time and their right to lodge complaints with a supervisory authority.
- From which source the Personal Data originates, and if applicable, whether it came from publicly accessible sources.

This information is also provided when Personal Data is not collected directly from the Data Subject.

The Privacy Statement employs plain language, is easily available on the website, and is periodically reviewed to ensure that the information provided is accurate and up-to-date.

7.2. Requests from the Data Subject

Data Subjects have the right to obtain from CEI Africa, as the Data Controller, confirmation as to whether or not their Personal Data are being processed, and, where that is the case, access to the Personal Data. CEI Africa has established appropriate procedures to deal with the following requests.

Right to Access - Data subjects have the right to request information such as the:

- Purposes of the processing;
- Categories of Personal Data concerned;
- Whether Personal Data is being disclosed to third parties;
- Retention period;
- Possibility for the Data Subject to exercise their rights;
- Conditions for transfers to third countries.

CEI Africa ensures that the right to obtain this information does not adversely affect the rights and freedoms of others.

Rectification and erasure (e.g.*, right to be forgotten*) - Data Subjects have the right to request and obtain without undue delay the rectification of inaccurate Personal Data. Taking into account the purposes of the processing, Data Subjects have the right to have incomplete or incorrect Personal Data rectified, including by means of providing a supplementary statement.

Data Subjects also have the right to request and obtain the erasure of their Personal Data without undue delay. CEI Africa acknowledges that this right is exercisable when Personal Data is no longer necessary for the purposes for which it was collected and processed. Nevertheless, it does not apply to the extent that processing such Personal Data is necessary for compliance with a legal or regulatory obligation (e.g., prevention of financial crime or compliance with employment laws) or to grant CEI Africa the ability to defend complaints in the future.

If the incomplete or incorrect Personal Data is processed also by a Data Processor (I.e., on behalf of CEI Africa), then they are notified about the correction of the Personal Data (unless this proves impossible or requires a disproportionate amount of effort).

Restriction of processing - Data Subjects have the right to request and obtain restriction of processing of their Personal Data by CEI Africa, when one of the following circumstances applies:

- The accuracy of the Personal Data is contested by the Data Subject;
- The processing is unlawful;
- CEI Africa does no longer need the Personal Data.

When processing has been restricted, and with the exception of storage, such Personal Data is only processed with the Data Subject's consent, or for CEI Africa to exercise one of its legitimate rights.

Data portability - Data Subjects have the right to request and receive their Personal Data that has been provided to CEI Africa, in a structured, commonly used, and machine-readable format. The Data Subject has the right to transmit such data to another controller without hindrance from CEI Africa. Paper files are out of the scope of this right that only applies to automatic means. It is also important to remember that the right to portability should not adversely affect the rights and freedom of others (including trade secrets and intellectual property). Data portability does not automatically trigger the erasure of data from CEI Africa's systems and does not affect the original retention period.

Object - Data Subjects have the right to object at any time to processing of their Personal Data. CEI Africa would no longer process the Personal Data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject.

The GDPR prohibits Data Controllers from establishing barriers (legal, technical, or financial obstacles) for not processing any of the above-described requests in accordance to the Data Subject's wishes. When receiving any of these requests, it is always determined whether this can be done on legitimate grounds. Nevertheless, CEI Africa might be exempted from addressing Data Subject requests if:

- In case of large or complex requests that would involve a disproportionate effort to complete the request; or
- It would result in disproportionate costs.

Article 41 of the Dutch Implementation Act provides for certain exemptions that allow CEI Africa not to comply with Data Subject requests (e.g., national security, national defence, etc.).

Data Subject's requests are dealt with free of charge, without undue delay and at the latest within **one month**. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

7.3. Complaints

If a Data Subject has complaints relating to the processing of their Personal Data or the infringement of their rights, they can raise these in the first instance with the Compliance Officer at CEI Africa. Alternatively, the Data Subject may also raise their complaint(s) directly with the DPA.

8. Additional obligations for CEI Africa

Taking into account the nature, scope, context and purposes of processing, as well as the risks to affect the rights and freedoms of natural persons, CEI Africa implements appropriate technical and organisational measures to ensure, and to be able to demonstrate, that processing is performed in accordance with applicable requirements. These measures are to be reviewed and updated where necessary.

8.1. Data protection by design and by default

CEI Africa approaches data protection **by design** in a way that promotes data protection compliance from the determination of the means for processing. In this way, privacy risks are considered inherent to any new projects the firm undertakes and through the lifecycle of each data processing activity.

To comply with the data protection **by default** principle, CEI Africa only processes Personal Data to the extent that is needed for the intended purpose and for no longer than necessary. It also implements appropriate technical and organisational measures, such as pseudonymisation, and data minimisation, in an effective manner and to integrate the necessary safeguards into the processing. This approach results in the highest level of protection for individuals.

9. Dealing with Data Processors

For the execution of its services, CEI Africa may share Personal Data with third parties, although CEI Africa remains the Data Controller for the Personal Data. When processing is carried out on behalf of CEI Africa, only Data Processors that provide sufficient guarantees to implement appropriate technical and organisational measures to ensure data protection are employed. A binding written processor agreement, in electronic form, is always concluded between CEI Africa and the Data Processors, which includes the compulsory elements as per article 28 of the GDPR, such as the:

- Subject matter and duration of the processing;
- Nature and purpose of the processing;
- Type of Personal Data and categories of Data Subject;
- Obligations and rights of the controller.

It is important that the processor agreement ensures that the processor makes available to CEI Africa all information necessary to demonstrate compliance with the obligations laid down in the agreement itself. It also ensures that the processor allows for and contributes to audits, including inspections, conducted by CEI Africa or any other entity mandated by CEI Africa.

10. Security of processing and other control measures

When processing Personal Data, CEI Africa ensures that commercially appropriate technical, physical and organizational control measures are taken. This is to protect Personal Data from misuse or accidental, unlawful or unauthorised destruction, loss, alteration, disclosure, acquisition or access. These measures include:

- The implementation of a comprehensive Data Protection Policy;
- The adoption of written agreements with organisations that process Personal Data on CEI Africa's behalf;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Partially effective pseudonymisation and encryption measures;
- The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

- **Confidentiality**

All members of Staff are subject to confidentiality obligations. Additional confidentiality requirements are included in legal agreements with third parties.

- **Need-to-know principle**

Staff have access to Personal Data on the basis of the need-to-know principle. This means that they only have access to Personal Data if this is necessary for the performance of work tasks.

- **Training and awareness**

All Staff of CEI Africa (I.e., Staff of the Foundation Manager) periodically receives training and are invited to attend awareness initiatives in relation to the protection of personal data and how to

comply with applicable requirements. All external parties that are involved in processing Personal Data in relation to CEI Africa will be provided with a copy of this Policy.

10.1. Retention

As mentioned before, Personal Data should not be kept for longer than strictly necessary for the purpose for which the data was originally collected. CEI Africa has established a Retention Framework, which details the retention requirements based on the different type of Personal Data and on the different legal requirement. Statutory retention periods apply to the data retention for the prevention of financial crime, legal disputes and claims, tax and other employment related data. Soon after the expiration of the retention period, Personal Data is:

- Securely deleted or destroyed, or
- Anonymised

10.2. Data Protection Impact Assessment (DPIA)

Where processing operations are likely to result in a high risk to the rights and freedoms of persons, CEI Africa will carry out a DPIA to evaluate, in particular, the origin, nature, particularity and severity of that risk. A DPIA would for example be required in the case of the development, modification, or implementation of new systems, the outsourcing of processing or systems to third parties, the testing of systems or equipment, as part of risk assessments etc. In light of the nature and extent of processing of Personal Data at CEI Africa (e.g., no processing on a large scale of special categories of data, no automated processing, and no systematic monitoring of a publicly accessible area), it is not envisaged that a DPIA will be often required.

11. Transfer of Personal Data outside the European Economic Area (EEA)

Anyone within CEI Africa shall think carefully before sending Personal Data outside the organization. It is not allowed to disclose Personal Data to persons outside the EEA unless it is certain that they are authorized to receive it and have a proper purpose, and only to the extent it is necessary to fulfil the original legitimate purpose for which Personal Data is processed. The transfer of Personal Data to non-EEA countries, including group entities in non-EEA countries, is only allowed if a sufficient level of protection is guaranteed as set out below:

- The receiving party of the data is located in a country recognised by the European Commission as offering an adequate level of protection (e.g., adequacy decision);
- The receiving party has provided appropriate safeguards, and on condition that enforceable Data Subject rights and effective legal remedies for Data Subjects are available;
- The receiving party of the data has agreed to process these data in accordance with the 'Standard Contractual Clauses' for data controllers or data processors approved by the European Commission;
- Any other safeguards allowed under the GDPR.

Transfer of Personal Data to a country that cannot guarantee adequate protections can only take place if the cross-border transfer is necessary for the performance of a contract, or it is necessary in connection with legal proceedings or to comply with applicable laws and regulations. In absence of these conditions, explicit consent is required by the relevant individuals, following the provision of accurate information (e.g., such as the purpose of the transfer, details of the receiving country and entity, and the clarification that the receiving country is not considered having adequate protections in place).

12. Data Protection and Employment

Under the GDPR, CEI Africa is expected to process Personal Data of Staff in such a way to guarantee the protection and the rights and freedom of Staff (and applicants). Processing in the context of employment particularly applies for the purposes of recruitment, the performance of the employment

and after the termination of the employment relationship. CEI Africa adopts all suitable and specific measures to safeguard human dignity, legitimate interests and fundamental rights, as well as equality and diversity in the workplace, and health and safety at work. HR Policies from the Foundation Manager apply in relation to employment.

CEI Africa makes sure that members of Staff are notified in advance of their surveillance measures so that they are not considered a breach of article 8 of the European Convention of Human Rights (right to respect for privacy and family life), which would result in an intrusion into the life of the employees, and they are consented upon by members of Staff.

13. Personal Data breach

As soon as a breach is identified or detected, it must be reported to the Compliance Officer, who will immediately assess the impact and seriousness of the situation (i.e., how many individuals are involved; what could be the regulatory and reputational risk for CEI Africa, what is the nature/sensitivity/volume of the Personal Data affected) and inform the CEI Africa Board. A breach can concern confidentiality, integrity, and availability of Personal Data at the same time, as well as any combination of these. Examples of a Personal Data breach includes, amongst others:

- Access by an unauthorised third party;
- Sending Personal Data to an incorrect recipient;
- Computing devices containing Personal Data being lost or stolen;
- Alteration of Personal Data without permission; and
- Loss of availability of Personal Data.

In the event of a serious Personal Data breach, CEI Africa would without undue delay (e.g., promptly) and, where feasible, not later than 72 hours after having become aware of it[3], notify the Personal Data breach to the DPA. This is not required if the breach is unlikely to result in a risk to the rights and freedoms of the individuals involved.

The electronic notification to the DPA would:

- Describe the nature of the breach including where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;
- Communicate the name and contact details of the Compliance Officer for obtaining more information;
- Describe the likely consequences of the breach;
- Describe the measures taken or proposed to be taken by CEI Africa to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

When the breach is likely to result in a high risk to the rights and freedoms of natural persons, CEI Africa might need to communicate details of the breach also to the Data Subjects involved without undue delay.[4]

All Personal Data breaches are recorded by the Compliance Officer, with all relevant data and also a root cause analysis to help prevent similar incidents from happening in the future. Breaches are reported to the Board of CEI Africa and the Supervisory Council, whether they have been disclosed to the DPA or not.

14. The Data Protection Authority

[3] This means that CEI Africa has a reasonable degree of certainty that a security incident has occurred with Personal Data being compromised.

[4] Specific conditions are described in article 34 of the GDPR.

The DPA supervises the processing of Personal Data in the Netherlands, in order to ensure compliance with laws and regulations that regulate the use of Personal Data. The DPA:

- Exercises supervision;
- Provides advice;
- Investigates data protection breaches and related complaints;
- Imposes administrative fines and other penalties;
- Monitors compliance with data protection requirements.

15. Review of Policy

This Policy is reviewed by the Compliance Officer at least on an annual basis, or more frequently if:

- Changes have been made to relevant laws and regulations;
- Relevant applicable guidelines are published;
- Incidents or breaches happen so to request a change to this Policy;
- Otherwise deemed necessary to align CEI Africa approach to data protection to best practices in the industry.

The Compliance Officer will submit the revised version of this Policy to the CEI Africa Supervisory Council for final approval.

Annexes

None