cenfri

Data Protection and Privacy Policy

July 2021

Contents

1. About Cenfri 1
2. Purpose of the policy 1
3. Policy statement 1
4. Scope of data considered 2
5. Data governance 2
6. Processing principles and conditions 4
7. Data processing required by law and/or regulation 6
8. Cenfri's legitimate Interests 7
9. Sharing information with third parties 7
10. Monitoring and review of the policy 8
11. Definitions 8

1. About Cenfri

Cenfri is Africa's leading economic impact agency, seeking to change the way in which markets work to increase the benefits from growth and economic development for people in these markets.

We achieve our objectives through:

- Deep understanding of market systems through observation, analysis and engagement of the market and the market players.
- Articulating insights and recommendations to effect positive change in these markets and making them visible to stakeholders effectively.
- Engaging with stakeholders who are influential and positioned to effect marked changes

2. Purpose of the policy

The purpose of the policy is to:

- set the operational and governance framework according to which data is managed in Cenfri;
- fulfil the compliance requirements of POPIA;
- serve as a reference point to Cenfri employees and associates for all matters related to data management and security.

3. Policy statement

3.1. During our activities, Cenfri will collect, store and process personal information and other confidential information about staff, customers, suppliers and other third parties, in electronic and other formats. We recognise the need to treat it in an appropriate and lawful manner, and we are committed to engaging with data appropriately.

3.2. We recognise that we operate globally, both in terms of the countries our work relates to and in terms of where our donors and stakeholders are domiciled, and we therefore need to take cognisance of international data protection standards and practices as they apply to the jurisdictions in which are active.

3.3. We recognise that for the purposes of data management we are responsible both for the actions of Cenfri employees and associates we contract to process data on our behalf.

3.4. We commit to educating our staff about our data privacy and security, including the fact that breaches of this policy may result in disciplinary action.

4. Scope of data considered

In considering the scope of data, the following categories were identified:

4.1. In the course of performing our core business,

- We collect data on market systems and the role players in them, which can include data in the public domain or data collected through engagements with individuals representing themselves or those representing entities, including private enterprises, government agencies or other interested parties.
- We engage with stakeholders through having data about who they are and what their interests in the markets are.
- We may engage sub-contractors to perform data collection and processing activities on our behalf.
- We develop insights based on the review and analysis of data. These insights may be considered sensitive by the parties instrumental in supplying the underlying data.
- We collect user behaviour data from visitors to our website through cookies.

4.2. As a condition of ***funding agreements*** that we enter into, we may be required to report certain data to our funders in order for them to verify the efficacy or appropriateness of the application of the funds. This data may be subject to data protection considerations, either through legal agreements (e.g. contracts or non-disclosure agreements) or through legislation.

4.3. As part of operating as a business, we may be exposed to, and/or collect and/or process:

- Personal information about our employees and prospective employees;
- Data about service providers, including individuals and the entities they represent;
- Data about entities who contract us to do work on their behalf or provide us with grants to further our objectives;
- Data about our own business which, if accessed by unauthorised persons, may lead to financial or compliance risk to Cenfri.

5. Data governance policy and roles

The data governance framework defines the policies, roles and forums for data management at Cenfri. This section provides an overview of the policies, operating procedures give effect to data management at Cenfri.

Document/Policy name	Description
Data Privacy and Protection Policy (Dat001)	Overarching policy covering Cenfri's stance on data protection, including POPIA and other confidential information
Security Compromises Policy (Dat002)	Policy describing how to deal with a confirmed or suspected breach in data security
Policy on Record Retention and Destruction (Dat003)	Policy describing the retention timeframes and destruction rules for personal and confidential information
Personal Information Sharing Policy (Dat004)	Policy describing the process of dealing with a request for personal information
Subject Access Request Policy (Dat005)	Relates to the process of considering, responding to and dealing with a request by a data subject to their data

Document/Policy name	Description
Data Protection Complaints Procedure (Dat006)	Relates to the process of dealing with a complaint that is brought against Cenfri regarding the manner in which we deal with Personal Data
Employee Declaration	Consent to the processing of Employee and prospective employee PI
Applicant consent form	Consent to the processing of Prospective Employee information
Security measures for personal information captured physically (Dat006)	Relates to how Cenfri secures personal and/or confidential information that has been captured physically and electronically
Electronic communication policy	Policy describing Cenfri's approach to the protection of personal information and privacy in relation to electronic communication
Website and Cookie policy	Policy describing how and why Cenfri's website processes personal information. Policy for the Cenfri website which obtains consent from users for cookies and explains what the cookies are doing and why, and obtaining consent from users to store cookies on their devices

These policies and operational procedures are implemented by the Data Manager at Cenfri. The roles and responsibilities of the Data Manager and Deputy Manager is outlined below. They can be contacted at datamanager@cenfri.org

5.1. Data Manager

- Taking overall ownership of Cenfri's practical implementation of this policy and upholding of its commitment to international best practices in relation to data protection and privacy;
- Leading and overseeing the data management team;
- Liaising with the Deputy Data Manager regarding requests for information and complaints.

5.2. Deputy Data Manager (who will escalate to Data Manager where necessary)

- Receiving and dealing with data subjects' requests for information, correction or deletion;
- Receiving and dealing with data subjects' complaints;
- Receiving and dealing with staff members' questions relating to compliance with this policy.

5.3. Information Officer (POPIA)

- The data manager also acts as Cenfri's Information Officer in terms of section 56 of POPIA and has the ultimate responsibility of ensuring that Cenfri complies with the Act.

5.4. EU representative (GDPR)

- Article 27(1) of the GDPR requires that institutions processing personal information of data subjects in the EU without having an office or presence in the EU, appoint an EU representative. Article 27(2) provides for an exception where "processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing".
- Cenfri's data management team is confident that Cenfri thus does not need to appoint an EU representative, given:
  - The overwhelming majority of Cenfri's work and projects take place in developing markets (i.e. outside of the EU), with a strong focus on sub-Saharan Africa.
  - The most likely engagement that Cenfri would have with data subjects in the EU would be with development partners, financial sector regulators, or financial sector stakeholders that are businesses and not individuals, thus falling outside of the scope of the GDPR.
  - If Cenfri were to process the personal information of individuals in the EU, such processing would certainly be occasional and would not include the large-scale processing of special categories of data or criminal conviction and offences and would unlikely result in any risk to the rights and freedoms of individuals – thereby satisfying the exemption as provided by article 27.

6. Processing principles and conditions

Cenfri commits to processing personal information in accordance with the following international best-practice principles and conditions for data protection and privacy: accountability, processing limitation, purpose specification and storage limitation, further processing limitation, information quality and accuracy, openness, security safeguards, and data subject participation.

6.1. Accountability

- Cenfri is committed to ensuring that its processing of personal information is done in accordance with international best practices, thus by demonstrating compliance with the other principles and conditions set out in clauses 7.2 to 7.8.
- Cenfri has appointed a data management team, led by its Data Manager and Deputy Data Manager, who are responsible for encouraging and supporting Cenfri's upholding of international best practices regarding data protection and privacy, including adherence to the applicable laws and regulations, which include inter alia POPIA and the GDPR.
- The data management team is further responsible for the drafting and maintenance (i.e. updating) of this data protection and privacy policy document, as well as conducting training and ensuring awareness by employees of this policy and Cenfri's commitments under it.

6.2. Processing limitation

- Cenfri will process personal information lawfully and reasonably, adhering to the concept of minimisation, thus the processing will be adequate, relevant, and not excessive, given the purpose for which it is processed.
- Where possible, Cenfri will obtain voluntary, informed and specific consent directly from data subjects before collecting their personal information.
- A data subject may withdraw their consent to have their personal information processed at any time, and such withdrawal of consent will be noted and acted upon.

6.3. Purpose specification and storage limitation

- Personal information will only be processed for specific, explicitly defined, and legitimate reasons relating to the functions or activities of Cenfri.
- Personal information will only be collected to the extent that it is required for the specific purpose notified to the data subject. Any personal information that is not necessary for that purpose will not be collected in the first place.
- Records of personal information will only be kept for as long as necessary for achieving the purpose for which the information was collected or subsequently processed, except for specific legal or contractual requirements.
- Personal information will therefore be destroyed or deleted in a manner that prevents its reconstruction in an intelligible form or be de-identified as soon as reasonably practicable after Cenfri is no longer authorised to retain the record.

6.4. Further processing limitation

- Further processing of personal information will be compatible with the purpose of collection, unless the data subject has consented to such further processing.
- Where personal information is transferred to a third party for further processing, the further processing will be compatible with the purpose for which it was initially collected.

6.5. Information quality and accuracy

- Cenfri will take reasonably practicable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary in light of the purpose for which such information is collected.
- Inaccurate or out-of-date information will be destroyed.
- The data management team will put procedures in place to verify that records containing personal information remain relevant, accurate and up to date.

6.6. Openness

Cenfri will take reasonably practicable steps to ensure that the data subject is aware of:

- the information being collected and, where the information is not collected from the data subject, the source from which it is collected;
- Cenfri's name and contact information;
- the purpose for which the information is being collected;
- whether or not the supply of the information by that data subject is voluntary or mandatory;
- the consequences of failure to provide the information;
- the existence of the right of access to and the right to rectify the information collected;

- the existence of the right to object to the processing of personal information; and the right to lodge a complaint to the data protection authority and the contact details of the authority.

6.7. Security safeguards

- Cenfri will keep all personal information secure against the risk of loss, unauthorised access, interference, modification, destruction, or disclosure and will conduct regular risk assessments to identify and manage all reasonably foreseeable internal and external risks to personal information under its control.
- Cenfri has implemented through its outsourced IT service provider a data security and access management system to ensure the integrity of personal and confidential information under its control.
- Third parties further processing personal information collected by Cenfri (such as psychometric assessment centres, document management warehouses, and external consultants) will not process personal information on behalf of Cenfri without prior authorisation, and there will be a written contract in place between Cenfri and the third party, which requires the third party to maintain the confidentiality, integrity and security measures of personal information processed on behalf of Cenfri.
- In the event that personal information has been compromised, or if there is a reasonable belief that a compromise has occurred, Cenfri (or a third party processing personal information on its behalf) will comply with the Dat002 Security Compromises policy.

6.8. Data subject participation

- Cenfri recognises that a data subject has the right to request Cenfri to confirm, free of charge, whether it holds personal information about the data subject and to request Cenfri to provide a record or a description of the personal information held, including information about the identity or categories of third parties who have, or have had, access to the information at a prescribed fee.
- A data subject may request Cenfri's data management team to correct or delete personal information relating to the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, misleading, or obtained unlawfully.

7. Data processing required by law and/or regulation

7.1. Cenfri commits to processing personal information fairly, lawfully and without adversely affecting the rights of the data subject.

7.2. To ensure fair and lawful processing, Cenfri commits to obtaining the consent of the data subject where the processing is not strictly necessary for Cenfri's legitimate interests.

7.3. Personal information about users may be processed for legal, personnel, administrative and management purposes and to enable Cenfri to meet its legal obligations as an employer, for example to pay users, monitor their performance, and confer benefits in connection with their employment. Examples of when special personal information of users is likely to be processed are set out below:

- information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;
- the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with employment equity legislation; and in order to comply with legal requirements and obligations to third parties.

- Personal information about customers, suppliers and other third parties may be processed for legal, administrative and management purposes and to enable Cenfri to meet its legal obligations as determined by agreement.

8. Cenfri's legitimate interests

8.1. As a not-for-profit economic impact agency, Cenfri's objective is to effect positive societal change through the work we do. It is within this context that we consider legitimate Interest as a lawful basis for processing data.

8.2. Cenfri's work is usually funded by entities that have social impact rather than commercial objectives. In the assessment of the quality and impact of our work, we need to report certain data to our funders for them to verify the efficacy or appropriateness of the application of their funds. We will always make the terms of engagement with data subjects conditional on this requirement.

8.3. We will share updates and publications with data subjects in our data base if we believe that they will be of value to that data subject in the context of the existing relationship between Cenfri and that data subject. They may opt out at any time.

8.4. We will deliberately and intentionally consider whether the electronic introduction of data subjects in our network would be beneficial to both parties and may share the business email addresses of these data subjects to link them with each other. A part of our core business is to build and develop a network of stakeholders who play a supporting role in ensuring the sustainability of the positive change in the markets in which we work.

8.5. We will invite data subjects in our data base to events (whether in person or online) if we think that they will benefit from it.

8.6. Our legitimate Interests will never override the interests or fundamental rights of data subjects.

9. Sharing information with third parties

In addition to the legitimate interest considerations stated in section 9 above, users should be extremely cautious in responding to enquiries by third parties which would lead to the disclosure of personal or confidential information:

9.1. Users will request that the third party puts their request in writing so the third party's identity and entitlement to the information may be verified.

9.2. Users will refer the request to the data management team.

9.3. The data management team will consider the request and obtain consent from the data subject before disclosing any information.

9.4. Where providing information to a third party, users will do so in accordance with the processing principles and conditions.

10. Monitoring and review of the policy

The Data Manager reviews this policy from time to time to ensure it is achieving its stated objectives.

11. Definitions

The following terms bear the meaning given to them here in this and related policies:

"Authority" means the Information Regulator responsible for the supervision of compliance with POPIA and the European Data Protection Supervisor responsible for the compliance with the GDPR.

"Confidential information" means all information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or proprietary, or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential information includes all material, non-public, business-related information made available by the disclosing party to the receiving party, directly or indirectly, through any means of communication or observation.

"Data manager" means the person responsible for Cenfri's data management and compliance with international best practice regarding data protection and privacy. The data manager also acts as Cenfri's Information Officer in terms of section 56 of POPIA and has the ultimate responsibility of ensuring that Cenfri complies with the provisions of POPIA

"Data subjects" for the purpose of this policy include all living individuals and juristic persons about whom Cenfri holds personal and/or confidential information. All data subjects have legal rights in relation to their personal and/or confidential information.

"Deputy Data Manager" means the person responsible for assisting Cenfri's Data Manager with compliance with international best practice in terms of data protection and privacy, as well as compliance with POPIA.

"GDPR" means the General Data Protection Regulation 2016/679, an EU law governing data protection and privacy, which was implemented on 25 May 2018.

"Legitimate interests" refers to a lawful basis to process personal information, where processing is not strictly required, but there is a clear benefit to it, there is little risk of the processing infringing on the data subject's privacy, and the data subject would reasonably expect the data to be used in such a way. It is tied specifically to the activities that Cenfri undertakes as part of its core business in order to achieve impact.

"PECR" means the Privacy and Electronic Communications (EC Directive) Regulations of 2003.

"Personal information" means information relating to an identifiable, living, natural person, and (where applicable) an identifiable, existing juristic person, including the name, race, gender, marital status, address and identifying number of a person, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment to the person.

"POPIA" means the Protection of Personal Information Act 4 of 2013.

“Processing” is any activity that involves use of personal information. It includes any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
- dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, degradation, erasure, or destruction of information.

“Processing principles and conditions” are the principles and conditions for the lawful processing of personal information set out in both POPIA and the GDPR.

“Special personal information” includes personal information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

“Users” include Cenfri employees and associates whose work involves using personal information. Users have a duty to protect the information they handle by always following Cenfri’s data protection and security policies.