

Data Protection, Privacy, and Information Access Policies

May 2022

Table of contents

About Cenfri.....	1
Data Protection and Privacy Policy	1
Promotion of Access to Information (PAIA) Manual	12
Annexure A	20
Annexure B	21

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

Data Protection and Privacy Policy

1. 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.

2. Policy statement

- 2.1. 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.
- 2.2. 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 we are active.

- 2.3. 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.
- 2.4. 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.

3. Scope of data considered

- 3.1. In considering the scope of data, the following categories were identified:
 - 3.1.1. In the course of performing our core business,
 - 3.1.2. 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.
 - 3.1.3. We engage with stakeholders through having data about who they are and what their interests in the markets are.
 - 3.1.4. We may engage sub-contractors to perform data collection and processing activities on our behalf.
 - 3.1.5. 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.
 - 3.1.6. We collect user behaviour data from visitors to our website through cookies.
- 3.2. 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.
- 3.3. As part of operating as a business, we may be exposed to, and/or collect and/or process:
 - 3.3.1. Personal information about our employees and prospective employees;
 - 3.3.2. Data about service providers, including individuals and the entities they represent;
 - 3.3.3. Data about entities who contract us to do work on their behalf or provide us with grants to further our objectives;

3.3.4. Data about our own business which, if accessed by unauthorised persons, may lead to financial or compliance risk to Cenfri.

4. 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 and operating procedures that 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
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 are outlined below. They can be contacted at datamanager@cenfri.org.

4.1. Data Manager

- 4.1.1. 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;
- 4.1.2. Leading and overseeing the data management team;
- 4.1.3. Liaising with the Deputy Data Manager regarding requests for information and complaints.

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

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

4.3. Information Officer (POPIA)

- 4.3.1. 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.

4.4. EU representative (GDPR)

- 4.4.1. 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".
- 4.4.2. Cenfri's data management team is confident that Cenfri thus does not need to appoint an EU representative, given:
 - 4.4.2.1. 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.
 - 4.4.2.2. 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.

- 4.4.2.3. 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 convictions 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.

5. 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.

5.1. Accountability

- 5.1.1. Cenfri is committed to ensuring that its processing of personal information is done in accordance with international best practices, thus demonstrating compliance with the other principles and conditions set out in clauses 7.2 to 7.8.
- 5.1.2. 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.
- 5.1.3. 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.

5.2. Processing limitation

- 5.2.1. 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.
- 5.2.2. Where possible, Cenfri will obtain voluntary, informed and specific consent directly from data subjects before collecting their personal information.

- 5.2.3. 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.

5.3. Purpose specification and storage limitation

- 5.3.1. Personal information will only be processed for specific, explicitly defined, and legitimate reasons relating to the functions or activities of Cenfri.
- 5.3.2. 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.
- 5.3.3. 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.
- 5.3.4. 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.

5.4. Further processing limitation

- 5.4.1. Further processing of personal information will be compatible with the purpose of collection unless the data subject has consented to such further processing.
- 5.4.2. 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.

5.5. Information quality and accuracy

- 5.5.1. 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.
- 5.5.2. Inaccurate or out-of-date information will be destroyed.
- 5.5.3. The data management team will put procedures in place to verify that records containing personal information remain relevant, accurate and up to date.

5.6. Openness

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

- 5.6.1. the information being collected and, where the information is not collected from the data subject, the source from which it is collected;
- 5.6.2. Cenfri's name and contact information;
- 5.6.3. the purpose for which the information is being collected;
- 5.6.4. whether or not the supply of the information by that data subject is voluntary or mandatory;
- 5.6.5. the consequences of failure to provide the information;
- 5.6.6. the existence of the right of access to and the right to rectify the information collected;
- 5.6.7. 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.

5.7. Security safeguard

- 5.7.1. 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.
- 5.7.2. 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.
- 5.7.3. 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.
- 5.7.4. 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.

5.8. Data subject participation

- 5.8.1. 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.
- 5.8.2. 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.

6. Data processing required by law and/or regulation

- 6.1. Cenfri commits to processing personal information fairly, lawfully and without adversely affecting the rights of the data subject.
- 6.2. 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.
- 6.3. 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:
 - 6.3.1. 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;
 - 6.3.2. 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.
 - 6.3.3. Personal information about customers, suppliers and other third parties may be
 - 6.3.4. processed for legal, administrative and management purposes and to enable Cenfri to meet its legal obligations as determined by agreement.

7. Cenfri's legitimate interests

- 7.1. 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.
- 7.2. 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.
- 7.3. We will share updates and publications with data subjects in our database 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.
- 7.4. 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.
- 7.5. We will invite data subjects in our database to events (whether in person or online) if we think that they will benefit from it.
- 7.6. Our Legitimate Interests will never override the interests or fundamental rights of data subjects.

8. 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:

- 8.1. 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.
- 8.2. Users will refer the request to the data management team.
- 8.3. The data management team will consider the request and obtain consent from the data subject before disclosing any information.
- 8.4. Where providing information to a third party, users will do so in accordance with the processing principles and conditions.

9. Monitoring and review of the policy

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

10. Definitions

10.1. 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 practices 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 practices 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.

Promotion of Access to Information (PAIA) Manual

Prepared in terms of Section 51 of the Promotion of Access to Information Act 2 of 2000 (as amended) – March 2022

Document History

Version	Issue Date	Changes <i>[Section, Page(s) and Text Revised]</i>

1. List of Acronyms and Abbreviations

- 1.1. CIO” Chief Information Officer
- 1.2. “DIO” Deputy Information Officer
- 1.3. “Minister” Minister of Justice and Correctional Services;
- 1.4. “PAIA” Promotion of Access to Information Act No. 2 of 2000 (as Amended);
- 1.5. “POPIA” Protection of Personal Information Act No.4 of 2013;
- 1.6. “Regulator” Information Regulator; and
- 1.7. “Republic” Republic of South Africa

2. Purpose of PAIA Manual

- 2.1. This PAIA Manual is for the public to-
 - 2.1.1. check the categories of records held by Cenfri which are available without a person having to submit a formal PAIA request;
 - 2.1.2. have a sufficient understanding of how to make a request for access to a record of Cenfri, by providing a description of the subjects on which the Cenfri holds records and the categories of records held on each subject;
 - 2.1.3. know the description of the records of Cenfri which are available in accordance with any other legislation;

- 2.1.4. access all the relevant contact details of the Information Officer and Deputy Information Officer who will assist the public with the records they intend to access;
- 2.1.5. know the description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it;
- 2.1.6. know if Cenfri will process personal information, the purpose of processing of personal information and the description of the categories of data subjects and of the information or categories of information relating thereto;
- 2.1.7. know the description of the categories of data subjects and of the information or categories of information relating to these;
- 2.1.8. know the recipients or categories of recipients to whom the personal information may be supplied;
- 2.1.9. know if Cenfri has planned to transfer or process personal information outside the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied; and
- 2.1.10. know whether Cenfri has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

3. Request for Access to Information

- 3.1. In the event that a person or entity requires access to information as contemplated in the Act, the requester must contact the Deputy Information Officer.
- 3.2. A person who wants access to the records held by Cenfri must complete the necessary required form, as set out in Annexure B. The completed form must then be sent to the email address of the Deputy Information Officer as set out in clause 5 of this Manual.
- 3.3. The requester must indicate which form of access is required (inspection of copy, paper copy, electronic copy, transcript, etc.) and identify the right that is sought to be exercised or protected, providing an explanation for why the requested record is required for the exercise or protection of that right. Proof of the capacity in which the requester is requesting the information must be provided.
- 3.4. You will be notified in writing whether your request has been approved or denied within 10 working days. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

4. Fees

- 4.1. A request for access to a record, other than a record containing personal information about yourself, will be processed only after a request fee has been paid.
- 4.2. The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record. The schedule of fees is set out in Annexure A.

5. Key contact details for Access to Information for Cenfri (Centre for Financial Regulation and Inclusion NPC)

5.1. Chief Information Officer

Name: Stephanie van der Westhuizen
Tel: +21 9139510
Email: Steph@cenfri.org
Fax number: +21 9139644

5.2. Access to information general contacts

Email: info@cenfri.org

5.3. Head Office

Postal Address: P O Box 5966, Tygervalley, 7535
Physical Address: Building A, Farm 1, Vineyard Office Park, 99 Jip de Jager Drive, Bellville, 7530, Cape Town, South Africa
Telephone: 021 9139510
Email: info@cenfri.org
Website: www.cenfri.org

6. Guide on how to use PAIA and how to obtain access to the Guide

- 6.1. The Regulator has, in terms of section 10(1) of PAIA, as amended, updated and made available the revised Guide on how to use PAIA (“Guide”), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.
- 6.2. The Guide is available in each of the official languages and in braille.
- 6.3. The aforesaid Guide contains the description of-
 - 6.3.1. the objects of PAIA and POPIA;
 - 6.3.2. the postal and street address, phone and fax number and, if available, electronic mail address of-

- 6.3.2.1. the Information Officer of every public body, and
- 6.3.2.2. every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA and section 56 of POPIA;
- 6.3.3. the manner and form of a request for-
 - 6.3.3.1. access to a record of a public body contemplated in section 11; and
 - 6.3.3.2. access to a record of a private body contemplated in section 50;
- 6.3.4. the assistance available from the IO of a public body in terms of PAIA and POPIA;
- 6.3.5. the assistance available from the Regulator in terms of PAIA and POPIA;
- 6.3.6. all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging-
 - 6.3.6.1. an internal appeal;
 - 6.3.6.2. a complaint to the Regulator; and
 - 6.3.6.3. an application with a court against a decision by the information officer of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body;
- 6.3.7. the provisions of sections 14 and 51 requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;
- 6.3.8. the provisions of sections 15 and 52 providing for the voluntary disclosure of categories of records by a public body and private body, respectively;
- 6.3.9. the notices issued in terms of sections 22 and 54 regarding fees to be paid in relation to requests for access; and
- 6.3.10. the regulations made in terms of section 92.
- 6.4. Members of the public can inspect or make copies of the Guide from the offices of the public and private bodies, including the office of the Regulator, during normal working hours.
- 6.5. The Guide can also be obtained-
 - 6.5.1. upon request to the Information Officer;
 - 6.5.2. from the website of the Regulator (<https://www.justice.gov.za/inforeg/>).

6.6. A copy of the Guide is also available in the following two official languages, for public inspection during normal office hours-

6.6.1. English

6.6.2. isiXhosa

7. Categories of records of Cenfri which are available without a person having to Request Access

7.1. On a regular basis, Cenfri makes available to the public certain information on its functions and activities. This information will continue to be available without having to make a formal request under the Act. Information is also available on Cenfri's website: www.cenfri.org. Cenfri reserves the right to charge a fee in terms of the Act for requests pertaining to information that falls outside of this scope.

8. List of the records which Cenfri hold that are available in accordance with any other legislation

8.1. The following pieces of legislation require that Cenfri hold certain personal records as prescribed. The fact that we list a record type here does not necessarily mean that we will disclose such records, and all access is subject to the evaluation processes outlined herein, which will be exercised in accordance with the requirements of the Act.

8.1.1. Empowerment Act, No 53 of 2003

8.1.2. Companies Act, No 71 of 2008

8.1.3. Compensation for Occupational Injuries and Diseases Act, No 130 of 1993

8.1.4. Constitution of the Republic of South Africa Act, No 108 of 1996

8.1.5. Consumer Protection Act, No 68 of 2008 3

8.1.6. Employment Equity Act, No 55 of 1998

8.1.7. Income Tax Act, No 58 of 1962

8.1.8. Labour Relations Act, No 66 of 1995

8.1.9. Occupational Health and Safety Act, No 85 of 1993

8.1.10. Promotion of Access to Information Act, No 2 of 2000

8.1.11. Promotion of Equality & Prevention of Unfair Discrimination Amendment Act, No 52 of 2002

8.1.12. Protection of Personal Information Act, No 4 of 2013

- 8.1.13. Skills Development Act, No 97 of 1998
- 8.1.14. Skills Development Levy Act, No 9 of 1999
- 8.1.15. Unemployment Insurance Act, No 30 of 1966

9. Categories of records held by Cenfri

- 9.1. Cenfri holds the following types of records to manage our business and comply with our legal obligations:
 - 9.1.1. Client records to provide and bill for our services
 - 9.1.2. Human resources records to recruit employees, manage existing employees and pay their salaries.
 - 9.1.3. Business records to manage our business operations.
 - 9.1.4. Supplier records to manage our relationships with service providers and pay them for products and services.

10. Processing of Personal Information

- 10.1. 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.
- 10.2. 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.
- 10.3. We recognise that for the purposes of data management we are responsible both for the actions of our staff and for third parties we contract to process data on our behalf.
- 10.4. 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.
- 10.5. Description of the categories of Data Subjects and of the information or categories of information relating thereto.

Categories of Data Subjects	Personal Information that may be processed
Customers / Clients	Name, address, registration numbers or identity numbers, employment status and bank details
Service Providers	Names, registration numbers, vat numbers, addresses, trade secrets and bank details
Prospective employees	Name, address, contact number, email address, ID or passport number, qualifications, gender and race, income tax number, personal references, record of criminal records, record of credit blacklisting, Psychometric test results
Current Employees	Name, address, contact number, email address, ID or passport number, next of kin details, qualifications, gender and race, income tax number and tax payments, personal references, record of criminal records, record of credit blacklisting, Psychometric test results, Contract of employment, performance assessments, Payroll data
Former employees	Name, address, contact number, email address, ID or passport number, next of kin details, qualifications, gender and race, income tax number and tax payments, personal references, record of criminal records, record of credit blacklisting, Psychometric test results, Contract of employment, performance assessments, Payroll data

10.6. The recipients or categories of recipients to whom the personal information may be supplied

Category of personal information	Recipients or Categories of Recipients to whom the personal information may be supplied
Identity numbers and names, for criminal checks	South African Police Services
Qualifications, for qualification verifications	South African Qualifications Authority
Credit and payment history, for credit information	Credit Bureaus
Name, ID/Passport no, police clearance certificates, qualifications, credit history	Applicable government departments for the purposes of work permit applications.
Tax number	Applicable tax authorities.

10.7. General description of Information Security Measures to be implemented by the responsible party to ensure the confidentiality, integrity, and availability of the information

10.7.1. Cenfri will take all technical and organizational measures and physical measures to prevent the unauthorized or unlawful processing of personal data or/and accidental loss or destruction of data. Cenfri has security infrastructure services in place such as Firewall authentication (Access policies; Reporting; Azure AD; certificates; Sophos antivirus and Mimecast for email security. All the data is backed up to the Cloud which is stored in South Africa.

11. Updating of the Manual

11.1. Steph van der Westhuizen, Cenfri's Chief Operating Officer, will update this manual as and when required.

Issued by:

Steph van der Westhuizen

Chief Operating Officer

09 December 2021

Annexure A

	Description	Amount
1.	The request fee payable by every requester	R140
2.	Photocopy/printed black & white copy of A4-size page	R2.00 per page or part thereof
3.	Printed copy of A4-size page	R2.00 per page or part thereof
4.	For a copy in a computer-readable form on:	R40.00
	(i) Flash drive (to be provided by requester)	R40.00
	(ii) Compact disc	R60.00
	• If provided by requestor	
	• If provided to the requestor	
5.	For a transcription of visual images per A4-size page	Service to be outsourced. Will depend on quotation from service provider
6.	Copy of visual images	
7.	Transcription of an audio record, per A4-size page	R24.00
8.	Copy of an audio record on:	R40.00
	(i) Flash drive (to be provided by requester)	R40.00
	(ii) Compact disc	R60.00
	• If provided by requestor	
	• If provided to the requestor	
	To search for and prepare the record for	
9.	To search and prepare the record for disclosure for each hour or part of an hour, excluding the first hour, reasonably required for such search and preparation. To not exceed a total cost of	R435.00
10.	Deposit: If search exceeds 6 hours	One-third of the amount per request calculated in terms of items 2 to 8.
11.	Postage, e-mail or any other electronic transfer	Actual expense, if any.”.

Annexure B

REQUEST FOR ACCESS TO RECORD OF CENFRI (Section 53(1) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000))

Particulars of Cenfri (Centre for Financial Regulation and Inclusion)

Physical address:

Building A, Farm 1, Vineyard Office Park, 99 Jip de Jager Drive, Bellville, Cape Town, 7530

Postal address:

P O Box 5966

Tygervalley

7535

Telephone: 27 21 913 9510

Email: info@cenfri.org

Information Officer: Steph van der Westhuizen (Chief Operating Officer)

Deputy Information Officer: Tessa Kock (Operational Support Manager)

Particulars of person requesting access to the record

- The particulars of the person who requests access to the record must be given below.
- The address/email and/or fax number in the Republic to which the information is to be sent must be given.
- Proof of the capacity in which the request is made, if applicable must be attached.

Full names and surname:	
Identity number:	
Postal address:	
Telephone number:	
Fax number	
E-mail address:	

Capacity in which request is made, when made on behalf of another person:	
---	--

Particulars of person on whose behalf the request is made

This section must be completed ONLY if a request for information is made on behalf of another person.

Full names and surname:	
Identity number:	

Particulars of record

- Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.
- If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

Description of record or relevant part of the record

Reference number if available:

Any further particulars of record:

If you are prevented by a disability to read, view or listen to the record in the form of access provided for in 1 to 4 below, state your disability and indicate in which form the record is required.

Disability		Form in which record is required	
------------	--	----------------------------------	--

Note:

- Compliance with your request for access in the specified form may depend on the form in which the record is available.

- Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form.
- The fee payable for access to the record, if any, will be determined partly by the form in which access is requested.

Mark the appropriate box with an X

1. If the record is in written or printed form:					
	Copy of record *		Inspection of record		
2. If the record consists of visual images (this includes photographs, slides, video recordings, computer-generated images, sketches, etc.)					
	View images		Copy of the images*		Transcription of the images *
3. If the record consists of recorded words or information which can be reproduced in sound:					
	Listen to the soundtrack (Audio cassette)		Transcription of soundtrack* (written or printed document)		
4. If the record is held on a computer or in an electronic or machine-readable form:					
	Printed copy of record*		Printed copy of information derived from the record*		Copy in computer-readable form* (memory stick)

<p>“*” If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable</p>	Yes	No
--	------------	-----------

Particulars of right to be exercised or protected

If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

Indicate which right is to be exercised or protected:

Explain why the record requested is required for the exercise or protection of the aforementioned right:

Notice of decision regarding request for access

You will be notified in writing whether your request has been approved or denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

Signed at: _____ this day _____ of _____ 202_____

Signature of requester: _____