BERGRIVIER MUNICIPALITY

DRAFT PRIVACY POLICY: PROTECTION OF PERSONAL INFORMATION (POPIA) ACT (4 OF 2013)

DATE APPROVED	:	BKN047/04/2022 26/04/2022
COMMITTEE	:	EXECUTIVE MAYORAL
DIRECTORATE	:	CORPORATE SERVICES

BERGRIVIER MUNISIPALITEIT

ITEM VIR DIE KORPORATIEWE DIENSTE KOMITEE

"PRIVACY POLICY: PROTECTION OF PERSONAL INFORMATION ACT (4 of 2013), AS AMENDED"

DEUR DIE DIREKTEUR: KORPORATIEWE DIENSTE

(opgestel deur: S Lesch)

1. REDE VIR DIE VERSLAG

Die rede vir die verslag is om die Privaatheidsbeleid aan die Burgemeesterskomitee voor te lê vir oorweging.

2. AGTERGROND

Tydens die Formele Direksievergadering, gehou op Maandag 16 Augustus 2021, is besluit dat 'n POPIA-Voldoeningskomitee saamgestel word en op 30 Augustus 2021 is besluit dat maandeliks terugvoer aan die Formele Direksie gegee sal word.

Die Privaatheidsbeleid is tydens die POPIA-Voldoeningskomiteewerkswinkel in diepte bespreek en die insette is verwerk deur die Bestuurder: Administrasie (wnd.) (sien *Aanhangsel A*). Die Beleid was tydens die Direksievergadering van 22 November 2021 bespreek en is alle insette bygewerk.

3. FINANSIËLE IMPLIKASIES

Geen

4. WETLIKE IMPLIKASIES

"Protection of Personal Information Act (4 of 2013) as amended Government Gazette 43461 dated 22 June 2020"

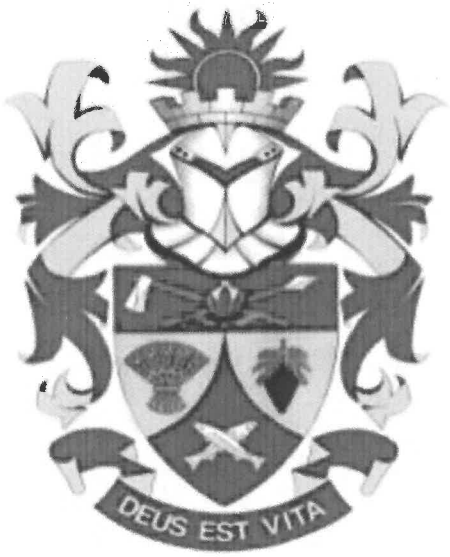
"Promotion of Access to Information Act (2 of 2000)"

5. AANBEVELINGS: VIR BESLUITNEMING DEUR DIE UITVOERENDE BURGEMEESTERSKOMITEE

5.1. Dat die Uitvoerende Burgemeesterskomitee kennis neem van die verslag rakende die POPIA-Voldoeningskomitee; en

5.2. Dat die Uitvoerende Burgemeesterskomitee die "Privacy Policy" goedkeur.

29 MAART 2022



BERGRIVIER MUNICIPALITY

DRAFT PRIVACY POLICY

Council Resolution ..... dated .....

TABLE OF CONTENTS

Contents

1. VERSION CONTROL 1
2. DEFINITIONS 1
3. INTRODUCTION 2
4. POLICY STATEMENT 2
5. SCOPE 3
6. PROVISION OF PERSONAL INFORMATION AND CONSENT 3
7. COLLECTION OF PERSONAL INFORMATION 4
8. CATEGORIES OF PERSONAL INFORMATION THE MUNICIPALITY MAY USE AND PROCESS 4
9. SENSITIVE PERSONAL INFORMATION 5
10. REASONS FOR KEEPING PERSONAL INFORMATION 5
11. SHARING PERSONAL INFORMATION 6
12. THIRD PARTY INSURANCE 6
13. SAFEGUARDING OF PERSONAL INFORMATION 6
14. DATA ACCURACY 7
15. DATA MINIMISATION 7
16. RETENTION OF PERSONAL INFORMATION 7
17. DATA SUBJECTS RIGHT TO ACCESS AND MANAGE PERSONAL INFORMATION 7
18. MUNICIPAL WEBSITE 8
19. RISKS 8
20. RESPONSIBLITIES 9
21. POPIA COORDINATING COMMITTEE 10
22. GENERAL STAFF GUIDELINES 11
23. BREACHES OF THE ACT OR POLICY 11
24. MAINTENANCE AND UPDATING OF THE PRIVACY POLICY 12
25. INFORMATION OFFICER AND CONTACT DETAILS 12

1. VERSION CONTROL

Document Name	Version / Document Number	Drafted by	Change Made/Brief Description	Date Approved	Date Implemented
Privacy Policy	*Version 0.2*	*S Lesch*	*Draft new policy*		

2. DEFINITIONS

Cookie	A cookie is a text file that is placed on the user's hard disk by a webpage server. Cookies cannot be used to run programmes or deliver viruses to the user's computer. Cookies are uniquely assigned to the user and can only be read by a web server in the domain that issued the cookie to the user.
Data subject	Means the identifiable natural/juristic person to whom personal information relates.
Events	A planned meeting, gathering, engagement or activity organised by the Municipality, whereto invitees or the public has access.
Information assets	Means the assets the organisation uses to create, store, transmit, delete and/or destroy information to support its business activities as well as the information systems with which that information is processed. It includes: • All electronic and non-electronic information created or used to support business activities regardless of form or medium, for example, paper documents, electronic files, voice communication, text messages, photographic or video content; and • All applications, devices and other systems with which the organisation processes its information, for example telephones, fax machines, printers, computers, networks, voicemail, e-mail, instant messaging, smartphones and other mobile devices ('ICT assets').
Information custodian	Means the person responsible for defining and implementing security measures and controls for Information and Communication Technology ('ICT') assets.
Information end user	Means the person that interacts with information assets and ICT assets for the purpose of performing an authorised task.
Information officer	Means the Accounting Officer/ Municipal Manager and/or delegated authority.
Information owner	Means the person responsible for, or dependent upon the business process associated with an information asset.
Regulator	Means the Information Regulator established in terms of the POPIA Act.
PAIA	Promotion of Access to Information Act (2 of 2000).

Personal information	Means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to – a) Information relating to the race, gender, marital status, nationality, age, physical or mental health, disability, belief, culture, language and birth of the person; b) Information relating to the education or the medical, financial, criminal or employment history of the person; c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; d) the biometric information of the person; e) the personal opinions, views or preferences of the person; f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; g) the views or opinions of another individual about the person; and h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
POPIA	Protection of Personal Information Act (4 of 2013) as amended Government Gazette 43461 dated 22 June 2020.
Processing	Means any operation or activity or any set of operations concerning personal information, including: a) the collection, receipt, recording, organisation, collation, storage, updating, modification, retrieval, alteration, consultation or use; b) dissemination by means of transmission, distribution or making available in any other form; or c) merging, linking, as well as restrictions, degradation, erasure or destruction of information.
Special personal information	Means personal information as referred to in section 26 of POPIA (Act 4 of 2013).

3. INTRODUCTION

(1) The Bergrivier Municipality ("Municipality") needs to gather and use certain personal information about individuals and juristic persons (collectively referred to as "data subjects"). These can include clients/customers, suppliers or service providers, business contacts, employees and other people and/or organisations that the Municipality has a relationship with or may need to contact.

(2) The policy ensures that the Municipality:
- (a) Complies with the Protection of Personal Information Act, 2013 (Act 4 of 2013) (POPIA).
- (b) Protects the rights of data subjects.
- (c) Is open about how it stores and processes personal information of data subjects.
- (d) Protects itself from the risks of security breaches in any form.

(3) The policy is available on the Municipality's website and at municipal offices in the municipal area.

4. POLICY STATEMENT

(1) The Municipality is committed to protecting the privacy of data subjects in accordance with the obligations imposed by POPIA. POPIA describes how organisations must collect, handle and store

the personal information of data subjects.

(2) These rules apply regardless of whether the information is stored electronically, on paper or on other materials.

(3) POPIA is underpinned by the following important privacy principles. These state that personal information must:

(a) be processed fairly and lawfully;
(b) be obtained only for specific, lawful purposes;
(c) be adequate, relevant and not excessive;
(d) be accurate and kept up to date;
(e) not be held for longer than necessary;
(f) processed in accordance with the rights of data subjects;
(g) be protected in appropriate ways; and
(h) not be transferred outside South Africa unless that country or territory also ensures an adequate level of protection.

5. SCOPE

(1) The Policy applies to all municipal employees, councillors, customers/clients and all external parties with whom we interact, including but not limited to our consultants, agents, individuals, representatives of organisations, visitors to our offices and visitors to our website and social media platforms.

(2) The Municipality collects personal information for various reasons in order to fulfil its mandate as government institution in terms of the Constitution of the Republic of South Africa. The residents expecting essential and other services from the Municipality are obliged to share their personal information with the Municipality as the withholding and/or refusal of personal information may impact on the Municipality`s ability to render effective and sufficient services.

(3) Employees are also obliged to share their personal information with the Municipality as it is needed for human resource management.

6. PROVISION OF PERSONAL INFORMATION AND CONSENT

The consent use on official documentation may include the rules set out in section 6.

(1) By providing the Municipality with your personal information, you:

(a) Agree to the terms and conditions set out in the Privacy Policy and authorise the Municipality to retain, process, use and disseminate such information as set out herein; and
(b) Authorise the Municipality, its staff, members, service providers and other third parties to use, disseminate and process your personal information for the purposes stated in the Policy.

(2) The Municipality will not use your personal information for any other purpose than that is set out in the Policy and will endeavour to protect your personal information that is in the Municipality's possession, from unauthorised alteration, loss, disclosure, use, dissemination or access.

(3) Please note that the Municipality may review and update the Policy from time to time. The latest version of the Policy is available on request, free of charge, at the municipal offices and available on the Municipality's website. See our contact details herein below.

(4) Special events may require that a data subject sign an in-person consent.

7. COLLECTION OF PERSONAL INFORMATION

(1) The Municipality collects information to support its service delivery mandate. We will process your personal information in the ordinary course of the Municipality's business. We will primarily use your personal information only for the purpose for which it was originally or primarily collected.

(2) The Municipality may collect or obtain personal information about you/our clients/customers:
- (a) directly from you;
- (b) in the course of our relationship with you/our customers/clients;
- (c) when you make your personal information public;
- (d) when you visit and/or interact with the municipal website at www.bergmun.org.za or Facebook social media platform;
- (e) when you register to use any of our services;
- (f) when you attend any activity and/or event of whatsoever nature at the Municipality and/or presented and/or organized by the Municipality;
- (g) Through surveillance cameras (with facial recognition technology);
- (h) License Plate Recognition cameras; and
- (i) when you visit our offices.

(3) The Municipality may also receive personal information about you from third parties (i.e., law enforcement authorities).

(4) In addition to the above, the Municipality may create personal information about you such as records of your communications and interactions with us, including, but not limited to, electronic communications, your attendance at events or at interviews in the course of applying for a job with us, subscription to our newsletters and other mailings and interactions with you.

8. CATEGORIES OF PERSONAL INFORMATION THE MUNICIPALITY MAY USE AND PROCESS

(1) Depending on the nature of the services required, the relationship between the individual and the Municipality and the reasons why certain information is required, personal information that may be obtained includes but is not limited to:
- (a) personal details: full name and surname, photographs, video material;
- (b) biographical information: date of birth, race, gender and marital status;
- (c) demographic information: gender, date of birth/age, nationality, culture, ethnicity, religion, salutation, title, and language preferences;
- (d) biometric information: fingerprinting, retinal scanning, voice recognition;
- (e) employment information: remuneration details, qualifications, medical information, declaration of interest;

(f) identifier information: passport or national identity number;
(g) contact details: correspondence address, telephone number, mobile number, email address, and details of your public social media profile(s);
(h) attendance records: details of meetings and other events organised by or on behalf of the Municipality that you may and/or may not have attended;
(i) consent records: records of any consents you may have given, together with the date and time, means of consent and any related information;
(j) payment details: billing address, payment method, bank account number or credit card number, invoice records, payment records, SWIFT details, IBAN details, payment amount, payment date, and records of cheques and EFT payments; and
(k) data relating to your visits to our Website and or social media platforms, your device type, operating system, browser type, browser settings, IP address, language settings, dates and times of connecting to a Website and/or social media platform, and other technical communications information.

9. SENSITIVE PERSONAL INFORMATION

(1) Where and when the Municipality needs to process, disseminate and/or use your sensitive personal information, we will do so in the ordinary course of the operation of the Municipality, for a legitimate purpose, and in accordance with applicable law.

(2) The Municipality does not intentionally collect or use personal information of children (persons under the age of 18 years), unless with express consent of a parent or guardian and/or if the law otherwise allows or requires us to process such personal special information.

10. REASONS FOR KEEPING PERSONAL INFORMATION

(1) The Municipality may keep and process personal information for the following reasons:
a) Employment and remuneration and other Human Resources needs;
b) Processing benefits i.e. medical aid and pension;
c) Considering bids in terms of tenders and quotations;
d) Closing of agreements and contracts;
e) Communication, sending and sharing of important information;
f) Maintaining data base for essential services, indigent support, housing;
g) Responding to inquiries, complaints and requests;
h) Addressing and understanding the needs and priorities of the community and other stakeholders;
i) Security background checks (vetting);
j) Rendering accounts;
k) Debt recovery;
l) Reports to council regarding outstanding debt;
m) Audit reports; and
n) Relevant Municipal compliance purposes.

(2) The Municipality will use your personal information for a secondary purpose only if such purpose constitutes a legitimate interest and is closely related to the original or primary purpose for which the personal information was collected.

(3) The Municipality shall not avail personal information to unaffiliated third parties for direct marketing purposes or sell, rent, distribute or otherwise make personal information commercially available to any third party.

11. SHARING PERSONAL INFORMATION

(1) On principle, the Municipality shall only share personal information if the Municipality has obtained consent from the data subject.

(2) Personal information may be shared with the indicated stakeholders and in the manner as follows:

(a) If required by law;

(b) Legal and regulatory authorities, upon request, or for the purpose of reporting any action or suspected breach of applicable law and/or regulation;

(c) Where it is necessary for the purposes of, or in connection with, actual or threatened legal proceedings or establishment, exercise or defence of legal rights;

(d) To any relevant party for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the executing of criminal penalties, including, but not limited to safeguarding against, and the prevention of threats to public security;

(e) To any relevant party for human resources purposes such as SARS, medical aid funds, pension funds, financial institutions;

(f) Business partners, vendors, or contractors to provide requested services or facilitate transactions;

(g) Where necessary to comply with judicial proceedings, court orders;

(h) To protect the rights, property, or safety of the Municipality or others, or as otherwise required by an applicable law; and

(i) Where consent in writing has been obtained from the data subject for sharing.

12. THIRD PARTY INSURANCE

Contracts and Service Level Agreements must include the following:

(1) Any service providers with whom the Municipality shares personal information are contractually required to implement suitable information protection and security measures. Third parties are not permitted to use personal information for any purpose, other than it was intended for.

13. SAFEGUARDING OF PERSONAL INFORMATION

(1) The Municipality implements appropriate technical and organisational security measures to protect our customers/clients' personal information that is in our possession against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access, in accordance with applicable law. The Municipality keeps hard copies and documentation containing personal information, under safe lock and key to which only authorized persons have access to. Electronic data is protected by regular password changes and firewalls.

(2) Where there are reasonable grounds to believe that your personal information that is in our possession has been accessed or acquired by any unauthorised person, the Municipality will notify the relevant Regulator and you, unless a public body responsible for detection, prevention or investigation of offences or the relevant regulator informs us that notifying you will impede a criminal investigation.

(3) Because the internet is an open system, the transmission of information via the internet is not completely secure. Although we will implement all reasonable measures to protect your personal information that is in our possession, we cannot guarantee the security of any information transmitted using the internet and we cannot be held liable for any loss of privacy occurring during the course of such transmission.

(4) When you are using our website or other social media platforms you could be directed to other sites that are beyond our control. We are not responsible for the content or the privacy policies of those third party websites.

(5) The Municipality have robust security controls and further threat detection solutions in place.

14. DATA ACCURACY

(1) The personal information provided to the Municipality should be accurate, complete and up-to-date. Should personal information change, the onus is on the provider of such data to notify the Municipality of the change and provide the Municipality with the accurate data.

15. DATA MINIMISATION

(1) The Municipality will restrict its processing of personal information to data which is sufficient for the fulfilment of the primary purpose and applicable legitimate purpose for which it was collected.

16. RETENTION OF PERSONAL INFORMATION

(1) The Municipality shall retain personal information for as long as it is necessary to fulfil the purposes for which it was collected and to comply with any legislative and or archive requirements whereafter it shall be deleted/disposed of. Depending on the purpose, retention periods shall vary.

(2) The following criteria will determine retention periods:
   (a) Legal or contractual, or other obligations to retain personal data;
   (b) Data necessary for or as part of an investigation or for litigation purposes;
   (c) In order to maintain accurate records, in line with relevant legislation; and
   (d) As determined by the Provincial Archives and Records Service of the Western Cape Act, 2005 (Act 3 of 2005).

17. DATA SUBJECT'S RIGHT TO ACCESS AND MANAGE PERSONAL INFORMATION

(1) The data subject may request (on the prescribe forms) the Municipality to access, correct, update, block, or delete personal information that the Municipality holds, subject to legislative requirements that make it compulsory for the Municipality to keep such personal information.

(2) The Information Officer will acknowledge receipt of any such request within three (3) days of the date of submission.

(3) Any such requests will be dealt with by the Information Officer who shall respond within a reasonable period and no later than thirty (30) days of the date of the request.

(4) The data subject may object to the processing of personal data at any time.

(5) On any suspicion that personal information has been unlawfully processed and rights relating to protection of your personal information were violated or that personal information has been compromised, the data subject shall contact the Information Officer and if not satisfied, may lodge a complaint with the Information Regulator.

(6) In the event of an information breach that the Municipality becomes aware of, the Municipality shall notify the data subject.

18. MUNICIPAL WEBSITE

By using the Bergrivier Municipal website, the user is deemed to have accepted the terms and conditions as specified on the website. Other sites can be accessed via links from the website. These sites are not monitored, maintained or controlled by the Municipality and thus the Municipality is not responsible in any way for any of their contents. It is possible that the website from time to time may contain links to other third-party websites. The Municipality is not responsible for any third-party content or privacy statements. The use of such sites and applications is thus subject to the relevant third-party's privacy policy statements.

The Bergrivier Municipal website respects any user's privacy. Some anonymous information about the user is automatically collected by the website. This information may include: the users browser type, access times, referring web site addresses and viewed pages. This information is collected to generate general aggregate statistics about the use of the Municipal website and is used to improve service delivery.

The Municipality's website may also use a "cookie" to save the users language preference. A cookie is a text file that is placed on the user's hard disk by a webpage server. Cookies cannot be used to run programmes or deliver viruses to the user's computer. Cookies are uniquely assigned to the user and can only be read by a web server in the domain that issued the cookie to the user.

The user can accept or decline cookies. Most web browsers automatically accept cookies, but the user can usually modify the browser settings to decline cookies if the user prefers. If a user chooses to decline cookies, the user's language choice will not be automatically selected each time the user returns to the website. No other cookies besides the language cookie may be used by the Municipality's website.

No other information is collected by the Municipality's website without the user's knowledge. The Municipality will not pass on any individual user details that may have been obtained, automatically or without the user's knowledge, unless with the user's prior consent. The Municipality only shares anonymous aggregate statistics about users and traffic patterns.

The Municipality is not responsible for any breach of security or for the actions of third parties.

19. RISKS

(1) The Policy helps to protect the Municipality from some very real security risks, including:

(a) Breaches of confidentiality: For instance, information being given out inappropriately;

(b) Failing to offer choices: For instance, all data subjects should be free to choose how the organisation uses information relating to them where the personal information is not collected, used or shared in terms of a law or an agreement between the data subject and the organisation;

(c) Reputational damage: For instance, the organisation could suffer if hackers successfully gained access to the personal information of data subjects.

20. RESPONSIBLITIES

(1) All municipal employees have a responsibility to ensure that the personal information of data subjects is collected, stored and handled appropriately to ensure the confidentiality, integrity and availability thereof.

(2) Each Information End User, Information Owner or Municipal Department that handles personal information must ensure that it is handled and processed in line with the Policy and the privacy principles.

(3) Below follows key positions and their areas of responsibility:

(a) The Information Officer (Municipal Manager) is ultimately responsible for ensuring that the organisation meets its legal obligations;

(b) The Deputy Information Officers are responsible for:

(i) The encouragement of compliance, by the Directorate under his/her responsibility, with the conditions for the lawful processing of personal information;

(ii) Dealing with requests made to the Municipality relating to the directorate under his/her responsibility, pursuant to the Act;

(iii) Working with the Regulator in relation to investigations conducted pursuant to Chapter 6 of the Act in relation to the directorate under his/her control; and

(iv) Otherwise ensuring compliance by the relevant directorate with the provisions of the Act or as may be prescribed in terms of the Act.

(c) Apart from the responsibilities listed in subparagraph (b) above, the Directors are responsible for:

(i) Keeping the Information Officer updated about information assets and personal information protection responsibilities, risks and relating issues;

(ii) Reviewing all personal information protection procedures and related policies, in line with an agreed schedule;

(iii) Arranging personal information protection training and advice for the people covered by the Policy; and

(iv) Checking and approving any contracts or agreements with third parties that may collect, handle or store personal information on behalf of the organisation.

(d) The Information Owner is responsible for:

(i) Ensuring all ICT assets used for processing personal information meet capable security standards;

(ii) Performing regular checks and scans to ensure security hardware and software is functioning optimally; and

(iii) Evaluating any third-party services, the organisation is considering using to process personal information. For instance, cloud computing services.

(e) The Information Owner is responsible for:

(i) Classifying personal information in line with the POPI Act and Regulations;
(ii) Maintaining internal procedures to support the effective handling and security of personal information;
(iii) Reviewing all personal information protection procedures and related policies, in line with an agreed schedule and make recommendations to the Information Officer/ Director: Corporate Services where applicable; and
(iv) Ensuring that all employees, consultants and others that report to the Information Officer/ Director: Corporate Services are made aware of and are instructed to comply with this and all other relevant policies.

(f) The Communication Officer is responsible for:
(i) Approving any personal information protection statement attached to communications such as e-mails and letters;
(ii) Addressing any personal information protection queries from journalists or media outlets;
(iii) Where necessary, working with other departments to ensure all communication initiatives abide by the privacy protection principles; and
(iv) When creating digital content and or statements made at events or in public ensuring that data subjects provide written consent.

21. POPIA COORDINATING COMMITTEE

(1) A POPIA-Coordinating Committee must be established to ensure the coordination of the POPIA compliance tasks and personal information requests. The Committee members will be formally appointed by the Information Officer.

(2) The Committee shall be multi-disciplinary and meet on a quarterly basis. The committee shall consist of the following portfolios:

Departmental Representatives:

- Human Resources
- Town Planning and Environmental Management
- Administration
- Revenue Services
- Supply Chain Management & Expenditure
- Community Services
- Protection Services
- Strategic Services
- Communication
- Budget and Reporting
- Civil Engineering Services
- Project Management and Building Control
- Electrical Engineering Services

Standing Invitees:

- Municipal Manager
- Director: Corporate Services
- Internal Audit Representative

- Director Financial Services
- Director Community Services
- Director Finance
- Director Technical Services

22. GENERAL STAFF GUIDELINES

(1) The only people able to access any personal information covered by the Policy should be those who need it to successfully complete their municipal duties.

(2) Personal information should not be shared informally and must never be shared over social media accounts such as Facebook, LinkedIn, Google Plus, etc.

(3) When access to confidential information is required, employees can request it from their line managers.

(4) The Municipality will provide training to all employees in order to facilitate the understanding of their responsibilities when handling personal information.

(5) Employees should keep all personal information secure, by taking sensible precautions and following the guidelines set out herein.

(6) In particular, strong passwords must be used and they should never be shared.

(7) Personal information should not be disclosed to unauthorised individuals, either within the Municipality or externally.

(8) Personal information must be reviewed regularly and updated if it is found to be outdated. If no longer required, it should be deleted and disposed of in line with the disposal instructions.

(9) Employees should request help from their line manager if they are unsure about any aspect of the protection of personal information.

(10) Line managers should seek the assistance of the relevant Director and/or Municipal Manager if they are unsure about any aspect of the protection of personal information.

23. BREACHES OF THE ACT OR POLICY

Breach of the Act, either by a councillor or employee, can lead to disciplinary action against the alleged perpetrator in terms of the applicable code of conduct or disciplinary procedures.

Non-compliance with the Policy by the organisation's employees will be dealt with in accordance with the Disciplinary Code of the organisation. Consequences may include disciplinary action up to termination of employment, and/or legal proceedings to recover any loss or damage to the organisation, including the recovery of any fines or administrative penalties imposed by the Information Regulator on the organisation in terms of POPIA.

Non-compliance with the policy by any other third party processing personal information on behalf of the organisation will be dealt with in accordance with the agreement entered into between the organisation and such third party. Consequences may include the recovery of any fines or administrative penalties imposed by the Information Regulator on the organisation in terms of POPIA.

24. MAINTENANCE AND UPDATING OF THE PRIVACY POLICY

The Municipality will maintain and regularly update the Privacy Policy and shall post updated and revised versions as and when necessary.

If any regulatory or business changes result in a significant addition or change to the nature or handling of personal information that may require a review of the Policy the changes will be developed by the Director: Corporate Services and approved by the Information Officer.
Any questions and requests to update the policy should be directed to the Director: Corporate Services.

25. INFORMATION OFFICER AND CONTACT DETAILS

The Municipal Manager, as assigned **Information Officer** in terms of the Act, is ultimately responsible for ensuring that the organisation meets its legal obligations.

Deputy Information Officers will be formally appointed by the Information Officer and registered with the Information Regulator as indicated in the PAIA manual.

Any questions, complaints or recommendations relating to the Privacy Policy may be directed to the Information Officer at the contact details below:

The Municipal Manager, Adv. H Linde
Email: mm@bergmun.org.za
Phone: 022 913 6000
Street Address: 13 Church Street, Piketberg, 7320
Postal Address: Private Bag X60, Piketberg, 7320

26. FORMS

The forms to be used. (See Annexures)

(Annexure A)

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN THE TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 2]

Note:
1. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

A	DETAILS OF DATA SUBJECT
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	Code ( )
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f)** *(Please provide detailed reasons for the objection)*

Signed at ..... this ..... day of .....20……..

.....
Signature of data subject/designated person

(Annexure B)

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 3]

Note:
4. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
5. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
6. *Complete as is applicable.*

Mark the appropriate box with an "x".
Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	DETAILS OF THE DATA SUBJECT
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	

Fax number/ E-mail address:	
C	**INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED**
D	**REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or** **REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN.** *(Please provide detailed reasons for the request)*

Signed at ..... this ..... day of .....20……..

.....

Signature of data subject/ designated person

(Annexure C)

FORM 3

APPLICATION FOR THE ISSUE OF A CODE OF CONDUCT IN TERMS OF SECTION 61(1)(b) OF TE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 5]

A	DETAILS OF PRIVATE OR PUBLIC BODY
Name of the body:	
Private / Public body	
List the class of body or any industry size, profession, or vocation, you represent: *(Attach proof of representation)*	
Total number of members of industry, or any class of bodies, profession or vocation:	
Proportion of representation (expressed as a percentage) in the industry, class of bodies, profession or vocation *(Attach proof of representation)*:	
Business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
B	**DETAILS OF PERSON WHO COMPLETES THIS FORM**
Name(s) and surname of person completing this form:	
Capacity in body:	

Does the person completing this Form have the authorisation of the body he/she represents to lodge this application? *(Attach authorisation)*	
Business address *(if different from body's address)*:	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**REASONS FOR APPLICATION FOR INFORMATION REGULATOR TO ISSUE A CODE OF CONDUCT** *(Please provide detailed reasons for the request and supporting documentation)*

Signed at ..... this ..... day of .....20……..

.....
Signature of the person completing the form

(Annexure D)

PERSONAL INFORMATION REQUEST

Please submit the completed form to the Information Officer:	
Name	
Contact Number	
Email Address:	
Please be aware that we may require you to provide proof of identification prior to processing your request. There may also be a reasonable charge for providing copies of the information requested.	
A. Particulars of Data Subject	
Name & Surname	
Identity Number:	
Postal Address.	
Contact Number:	
Email Address:	
B. Request	
I request the organisation to: (a) Inform me whether it holds any of my personal information (b) Provide me with a record or description of my personal information (c) Correct or update my personal information (d) Destroy or delete a record of my personal information	
C. Instructions	

D. Signature Page

Signature
Date

(Annexure E)

POPIA COMPLAINT FORM

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.	
Please submit your complaint to the Information Officer:	
Name	
Contact Number Email	
Address:	
Where we are unable to resolve your complaint, to your satisfaction you have the right to complaint to the Information Regulator. The Information Regulator: Physical Address: Email: Website:	
A. Particulars of Complainant	
Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	
B. Details of Complaint	
C. Desired Outcome	

D. Signature Page
Signature: Date

(Annexure F)

INFORMATION OFFICER APPOINTMENT FORM

I herewith and with immediate effect appoint you as the Information Officer as required by the Protection of Personal Information Act (Act 4 of 2013). This appointment may at any time be withdrawn or amended in writing.

You are entrusted with the following responsibilities:

Taking steps to ensure the organisation's reasonable compliance with the provision of POPIA.

Keeping the governing body updated about the organisation's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.

Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. This will include reviewing the organisation's information protection procedures and related policies.

Ensuring that POPIA Audits are scheduled and conducted on a regular basis,

Ensuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to the organisation, to do so. For instance, maintaining a "contact us" facility on the organisation's website.

Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of the organisation's employment contracts and other service level agreements.

Encouraging compliance with the conditions required for the lawful processing of personal information.

Ensuring that employees and other persons acting on behalf of the organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation's security controls.

Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organisation.

Addressing employees' POPIA related questions.

Addressing all POPIA related requests and complaints made by the organisation's data subjects.

Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

I hereby accept the appointment as Information Officer

Name and Surname

Signature

Date