



**UMZIMVUBU**  
LOCAL MUNICIPALITY

**PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023**

---

**PROTECTION OF PERSONAL INFORMATION  
ACT POLICY (POPIA)**

**2023**

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

Table of Contents	Page
1. <i>Definitions</i> .....	3-7
2. <i>Introduction</i> .....	8
3. <i>Objectives, Scope, and Key Risks</i> .....	8-10
4. <i>Current Control Measures</i> .....	11-12
5. <i>Rights of Data Subjects and Guiding Principles</i> .....	12-18
6. <i>Data Subjects Participation</i> .....	19-22
7. <i>Data Cloud Providers</i> .....	22-23
8. <i>POPIA Compliance Roadmap</i> .....	23-24
9. <i>POPIA Complaints Procedure</i> .....	24-26
10. <i>Rights of Data Subjects</i> .....	26-27
11. <i>Employees and Other persons acting on behalf of ULM</i> .....	27-31
12. <i>Disciplinary Action</i> .....	31
13. <i>Exemptions from Conditions of POPIA</i> .....	32
14. <i>Policy Review</i> .....	32
15. <i>Authorization</i> .....	33
16. <i>ANNEXURES: Forms and Clauses</i> .....	34-42



## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

1. DEFINITIONS:	
<b>“consent”</b>	<ul style="list-style-type: none"><li>• means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.</li></ul>
<b>“data subject”</b>	means the person to whom personal information relates.
<b>“de-identify”</b>	<ul style="list-style-type: none"><li>• means, in relation to personal information of a data subject, to delete any information that:</li><li>• identifies the data subject;</li><li>• can be used or manipulated by a reasonably foreseeable method to identify the data subject; or</li><li>• can be linked by a reasonably foreseeable method to other information that identifies the data subject; and</li><li>• “de-identified” has a corresponding meaning.</li></ul>
<b>“direct marketing”</b>	<ul style="list-style-type: none"><li>• means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:</li><li>• promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or</li><li>• requesting the data subject to make a donation of any kind for any reason.</li></ul>
<b>“electronic communication”</b>	<ul style="list-style-type: none"><li>• means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient’s terminal equipment until it is collected by the recipient.</li></ul>
<b>“operator”</b>	<ul style="list-style-type: none"><li>• means a natural or juristic person.</li></ul>



## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

<b>“personal information”</b>	means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to: • information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; • information relating to the education or the medical, financial, criminal or employment history of the person; • any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; • the biometric information of the person; • the personal opinions, views or preferences of the person; • 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; • the views or opinions of another individual about the person; and • 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.
<b>“private body”</b>	• means: • a natural person who carries or has carried on any trade, business or profession,



## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

	but only in such capacity; • a partnership which carries or has carried on any trade, business or profession; or • any former or existing juristic person but excludes a public body.
<b>“processing”</b>	means 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.
<b>“public body”</b>	means: • any department of state or administration in the national or provincial sphere of government; or • any other functionary of institution when: - exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or - exercising a public power or performing a public function in terms of any legislation.
<b>“public record”</b>	• means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body
<b>“record”</b>	means any recorded information: ∞ regardless of form or medium, including any of the



## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

	<p>following:</p> <ul style="list-style-type: none"><li>• writing on any material;</li><li>• information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;</li><li>• label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;</li><li>• book, map, plan, graph or drawing;</li><li>• photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;</li><li>• in the possession or under the control of the responsible party;</li><li>• whether or not it was created by the responsible party; and</li><li>• regardless of when it came into existence.</li></ul>
<b>“Regulator”</b>	<p>means the Information Regulator established in terms of the Protection of Personal Information Act.</p>
<b>“re-identify”</b>	<ul style="list-style-type: none"><li>• means, in relation to personal information of a data subject, to resurrect any information that has been de-identified, that:<ul style="list-style-type: none"><li>• identifies the data subject;</li><li>• can be used or manipulated by a reasonably foreseeable method to identify the data subject; or</li><li>• can be linked by a reasonably foreseeable method to other information that identifies the data subject;</li></ul></li></ul>



## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

	and “re-identified” has a corresponding meaning.
<b>“Responsible party”</b>	• means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.
<b>“Special personal information”</b>	means personal information relating to: • the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of the 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.
<b>“Unique identifiers”</b>	• means any identifier that is assigned to a data subject and is used by the responsible party for the purposes of the operations of the responsible party and that uniquely identifies that data subject in relation to the responsible party.

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

### 2. INTRODUCTION

The right to privacy is an integral human right recognized and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 (“POPIA”). POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the **processing of personal information** in a context-sensitive manner. A person’s right to privacy entails having control over his or her personal information and being able to conduct their affairs relatively free from unwanted intrusions.

Given the importance of privacy, Umzimvubu Local Municipality (ULM) is committed to effectively managing personal information in accordance with the provisions of POPIA.

### 3. Objectives, Scope, Policy Statement and Key Risks

#### 3.1. Objectives of policy

The objective of this policy is to ensure compliance with the Protection of Personal Information Act 4 of 2013 by setting out ULM’s strategy to uphold the rights to privacy and confidentiality of personal information of its employees, and third parties

The purpose of this policy is to enable ULM to:

- Comply with the law in respect of the data it holds about individuals.
- Follow industry best practices with regards to protection of personal information.
- Protect ULM Councillors, staff and third parties.
- Protect ULM from the consequences of non-compliance i.e. Litigations.

#### 3.2. Scope

This policy applies to the business of ULM wherever it is conducted. This Policy applies to:

- ULM’s Council.
- All departments, units, and divisions of the organization.



## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

- All employees and volunteers.
- All contractors, suppliers and other persons acting on behalf of the organization.

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the organization's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

### 3.3. Policy Statement

ULM will:

- Comply with both the law and best practice.
- Respect individuals' rights.
- Be open and honest with individuals whose data is held.

Provide training and support for staff who handle personal data, so that they can act confidently and consistently.

ULM recognizes that a priority under the POPI Act is to avoid causing harm to individuals either directly or through inaction.

In the main this means:

- Retaining personal data and information securely
- Retention of good quality personal information.

The Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are considered. ULM will comply with the Act in this respect. In addition to being open and transparent, ULM will seek to give individuals as much choice as is reasonably possible over what data is retained, for how long, and how it is used by ULM.

### 3.4. Key risks

ULM has identified the following potential key risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately) and accordingly non-compliance with the Act.

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

- Insufficient clarity about the range of data usage leading to Data Subjects being insufficiently informed.
- Breach of security by allowing unauthorized access.
- Harm to individuals if personal data is not up to date.
- Data Operator contracts failing to meet the minimum standards set out by the Act.

### **3.5. Current Controls Measures and Strategies Supporting POPIA Compliance**



Policy	Recommended amendment to improve compliance with POPIA
<b>ICT Accounts &amp; Password Man Policy</b>	Recommend amendment to incorporate POPIA compliance with regards to confidentiality declaration to accessing and processing of personal information and Data Subjects Consent where necessary.
<b>Employment Policy</b>	Recommend amendment to comply with POPIA requirements with regards to accessing and processing personal information of Employees, Applicants, Interns/Trainees and Third Parties (i.e. Labour Brokers and Recruitment Agencies).  To incorporate POPIA Compliance Procedure Manual and Consent Form.
<b>Expenditure Internal Controls</b>	Recommend amendment to POPIA compliance with regards to confidentiality declaration to accessing and processing of personal information and Consent where necessary.
<b>Records Management Policy</b>	Recommend amendment to incorporate Promotion of Access to Information Act (PAIA) Policy and POPIA Compliance Procedure Manual (SOP).
<b>Records Management Procedure Manual</b>	Recommend amendment to incorporate Promotion of Access to Information Act (PAIA) Policy and POPIA Consent of Data Subjects where necessary.
<b>ICT Internet Usage Policy</b>	No recommended amendment to this policy
<b>ICT Security Policy</b>	Recommend amendment to POPIA compliance with regards to confidentiality declaration to accessing and processing of personal information and Data Subjects Consent where necessary.
<b>Payroll Procedure Manual</b>	No recommended amendment to this policy.
<b>Subsistence and Travelling Policy</b>	Recommend amendment to comply with POPIA requirements of consent with regards to accessing and processing personal information for travelling purposes including sending the information to third parties (i.e. travel agents).
<b>Supply Chain Management Policy</b>	Recommend amendment to Incorporate a POPIA and PAIA procedure manual (SOP) SCM Employees and confidentiality form to be signed by SCM Bid Committee members for lawful processing of personal information.  The municipality and Suppliers/Contractors to POPIA Agreement and Consent Declaration.

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

<b>Disaster Recovery Plan Policy</b>	Recommend amendment to Incorporate a POPIA procedure manual (SOP) with regards to informing the Information Regulator and affected Data Subjects in the case of data loss/hacking/destruction.
<b>Promotion of Access to Information Act (PAIA) Policy</b>	Recommend this policy and manual to be developed to regulate the personal information flows – This policy does not exist.

#### 4. OVERVIEW OF DEFINITIONS, RIGHTS OF DATA SUBJECTS AND GENERAL GUIDING PRINCIPLES

##### Definition of Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

- Race, gender, sex, pregnancy, marital status, national or ethnic origin, color, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person.
- Information relating to the education or the medical, financial, criminal or employment history of the person.
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person.
- The biometric information of the person.
- The personal opinions, views or preferences of the person.
- 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

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

correspondence.

- The views or opinions of another individual about the person.
- 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 Lawful Conditions of Processing Personal Information – Set by the Act**

#### **4.1. Accountability**

Failing to comply with POPIA could potentially damage ULM's reputation or expose ULM to a civil claim for damages or sanction from the industry regulators.

The protection of personal information is therefore everybody responsibility.

ULM to ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of a compliance culture within the organization.

ULM will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

#### **4.2. Processing Limitation**

ULM will ensure that personal information under its control is processed:

- In a fair, lawful, and non-excessive manner.
- Only with the informed consent of the data subject.
- Only for a specifically defined purpose.

ULM will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.

Alternatively, where services or transactions are concluded over the telephone or electronic video feed, ULM will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

consent.

ULM will under no circumstances distribute or share personal information between separate legal entities, associated organizations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of ULM's business and be provided with the reasons for doing so.

### **4.3. Purpose specification**

All ULM's business units and operations must be informed by the principle of transparency.

ULM will process personal information only for specific, explicitly defined and legitimate reasons.

ULM will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

### **4.4. Further Processing Limitation**

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

Therefore, where ULM seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, ULM will first obtain additional consent from the data subject.

### **4.5. Information Quality**

ULM will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

The more important it is that the personal information be accurate the greater the effort ULM will put into ensuring its accuracy.

Where personal information is collected or received from third parties, ULM will take

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

### **4.6. Open Communication**

ULM will take reasonable steps to ensure that data subjects are notified (are always aware) that their personal information is being collected including the purpose for which it is being collected and processed.

ULM will ensure that it establishes and maintains a “contact us” facility, for instance via its website or through a monitored email address, for data subjects who want to:

- Enquire whether the organization holds related personal information; or
- Request access to related personal information; or
- Request the organization to update or correct related personal information; or
- Make a complaint concerning the processing of personal

information.

### **4.7. Security Safeguards**

ULM deploys up to date technology to safeguard confidentiality and ensure integrity of Personal Information under its control. ULM information security measures includes:

(i) Firewalls;

(ii) Encryptions;

(iii) Logical access control;

(iv) Oath of secrecy for employees, services providers and third parties ULM may share information with;

(v) Physical access control;

(vi) Secure hardware and software;

(vii) Confidentiality and data privacy clauses in agreements concluded with employees, suppliers and service providers.

## **PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023**

---

ULM will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on ULM's IT network.

ULM will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorized individuals.

All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorized disclosures of personal information for which ULM is responsible.

All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

ULM's operators and third-party service providers will be required to enter into service level agreements with ULM where both parties pledge their mutual commitment to POPIA compliance and the lawful processing of any personal information pursuant to the agreement.

### **4.8. Data Subject Participation**

Data subjects may request whether their personal information is held, as well as the correction and/or deletion of any personal information held about them. Data Subjects may request information from you on whether you are holding their personal information.

The Data Subject has the right to correct the personal information that you hold. They also have the right to withdraw consent at any time.



## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

### **4.9. Appointment of an Information Officer**

#### **Duties and Responsibilities**

The Information Officer is responsible for ensuring compliance with POPIA.

Developing, publishing and maintaining a POPI Policy which addresses all relevant provisions of the POPI Act, including but not limited to the following:

Reviewing the POPI Act and periodic updates as published; Ensuring that POPI Act induction training takes place for all staff;

Ensuring that periodic communication awareness on POPI Act responsibilities takes place; and

Ensuring that Privacy Notices for internal and external purposes are developed and published.

Handling data subject access requests.

Approving unusual or controversial disclosures of personal data.

Ensuring that appropriate policies and controls are in place for ensuring the Information Quality of personal information.

Ensuring that appropriate Security Safeguards in line with POPI Act for personal information are in place.

Handling all aspects of relationship with the Regulator as foreseen in the POPI Act.

Provide direction to any Deputy Information Officer when appointed.

### **4.10. Electronic Storage**

The internal procedure requires that electronic storage of important documents and information must be referred to and is discussed with line management who will arrange for the indexing, storage and retrieval thereof.

This will be done in conjunction with the departments concerned.

Scanned documents: If documents are scanned, the hard copy must be retained for as long as the information is used and be disposed in terms of records management procedures.

### **4.11. Processing Limitation Definition**

The act of processing information includes any activity or any set of operations, whether by automatic means, concerning personal information and includes:

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

- The collection, receipt, recording, organization, 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 any restriction, degradation, erasure or destruction of information.

ULM undertakes to comply with the POPI Act, Conditions 2 in terms of processing limitation, Sections 9 to 12.

### **4.12. Accuracy**

ULM will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held in as few places as necessary, and all staff will be discouraged from establishing unnecessary additional data sets.
- Effective procedures will be in place so that all relevant systems are updated when information about any individual changes.

Staff who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.

### **4.13. Openness**

In line with Conditions 6 and 8 of the Act, ULM is committed to ensuring that in principle Data Subjects are aware that their data is being processed:

- For what purpose it is being processed.
- What types of disclosure are likely.

How to exercise their rights in relation to the data held by ULM.

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

### 5. Procedure to Inform Data Subjects

Data Subjects will generally be informed in the following ways:

- Staff: through the processes and procedures set out in this policy.
- Customers and other interested parties: through the Privacy Notice
- Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

### 6. Specific Risks

ULM has identified the following additional risks:

- Staff with access to personal information could misuse it.
- Staff may be tricked into giving away information, either about customers / members or colleagues, especially over the phone or email.

### 7. Data Subjects Participation

#### 7.1. Procedure for making a requests

Subject access requests must be in writing. All staff are required to pass on anything which might be a subject access request to the POPI Act Information Officer without delay.

Where the individual making an access request is not personally known to the POPI Act Information Officer their identity will be verified before handing over any information.

Requests for access to personal information will be handled in compliance with the POPI Act and in compliance with the Promotion of Access to Information Act (PAIA), as defined in the ULM PAIA Manual.

#### 7.2. Consent from Data Subjects

Consent can be obtained in written form in a prescribed form which includes any appropriate electronic medium that is accurately and readily reducible to printed form.

## **PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023**

---

Alternatively, the organization will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject.

### **7.3. Processing of Special Personal Information**

ULM has a duty of adhering POPIA to the process of Special Personal Information which relates to 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.

Special personal information includes criminal behavior relating to alleged offences or proceedings dealing with alleged offences.

Unless a general authorization, alternatively a specific authorization relating to the different types of special personal information applies, a responsible party is prohibited from processing special personal information.

### **7.4. Processing of Personal Information of Children**

ULM has the policy of adhering to the process of Special Personal Information of children. This applies to under-18 individuals, so an age check is required for all personal information records. General authorization concerning personal information of children only applies where under-18's are involved.

ULM has engaged in an extensive internal due diligence process to identify all instances of personal

information held by it and the safeguards in place to protect such data and to identify any records held which contain Personal Information of children.

### **7.5. Direct Marketing, Directories and Automated Decision Making**

Direct Marketing is defined in the POPIA as marketing aimed at an individual with the direct or indirect purpose of selling goods or services or to solicit a donation of some

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

sort from the data subject.

Section 69 of the Act outlaws direct marketing by means of any form of electronic communication unless the data subject has given their consent. Such an electronic communication obviously includes emails, SMSs and automatic calling machines. A subject can only be approached once to obtain such a consent.

ULM undertakes to comply with the POPI Act Chapter 8, Sections 69 to 71 of the Act. ULM through appropriate management of its business partners and counterparty relationships shall hold its partners accountable in respect of any direct marketing undertaken on ULM's behalf.

### 7.6. Trans-Boarder Information Flows

Section 72 of POPIA sets out the requirements for the export of data while ensuring that the data is subject to adequate legal protection. In particular, section 72 states that a responsible party may only transfer personal information to a third party that is in a foreign country if certain protections are in place.

To provide personal information abroad, one of the following protections must be present:

- **Adequate legal protection:** The cross-border recipient of the personal information is subject to a law, corporate rules or an agreement that provides an adequate level of protection that effectively upholds the principles for reasonable processing. The law, corporate rules or agreement should include provisions that are:
  - (i) substantially similar to the conditions for the lawful processing of personal information in South Africa, and
  - (ii) substantially similar to section 72 of POPIA, relating to the further transfer of personal information from the recipient to third parties that are in a foreign country.
- **Consent:** The data subject consents to the transfer of personal information.
- **Necessary for the performance of a contract:** The transfer of personal information is necessary for the performance of a contract between the data

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

subject and the responsible party, or to implement pre-contractual measures taken in response to a data subject's request.

- **Interests of the data subject:** The transfer of personal information is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party.
- **Benefit of the data subject:** The transfer of personal information is for the benefit of the data subject in circumstances where:
  - (i) it is not reasonably practicable to obtain the consent of the data subject for the transfer, and
  - (ii) if it were reasonably practicable, the data subject would be likely to give consent.

ULM will ensure that the POPI Act Chapter 9, section 72 is fully complied with.

ULM has reviewed its processes to identify Trans border flows which contain personal Information.

Compliance with section 72 will be achieved through the use of the necessary contractual commitments from the relevant third parties outside South Africa.

### **8. How POPIA will impact data cloud providers**

#### *Cloud providers and the POPI Act*

Even though cloud providers and third parties (such as managed service providers) are obligated to protect any personal data they handle, process or store, when it comes to ensuring the safety of their information, the onus is on the municipality that contracted them.

Primarily, cloud providers need to ensure that data is stored within South Africa's borders. In fact, should any data be stored outside the country, they should seek legal advice and get full consent from the data owners to make sure that any affected individuals are aware of this.

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

In addition, anyone who is storing data outside South Africa should make sure it is being stored in a territory that has either similar or stronger regulation in place than the POPIA. The data responsibility ultimately lies with the municipality to make sure their data is safe and secure. They need to understand where their data is being stored and if they haven't been contacted by their cloud provider yet, they should take the initiative and contact them.

As with any other business, cloud providers themselves need to comply with the POPIA. They need to understand their processes, such as how they are storing data, and ensure they are not processing any data that they shouldn't.

Any cloud providers that are hosting data need to ensure that the data is being stored securely, and that it can't easily be breached by an attacker.

Referring to sections 21(1) and (2) of the Act, it specifies: "A responsible party must, in terms of a written contract between the responsible party and the operator, ensure the operator, which processes personal information for the responsible party, establishes and maintains the security measures referred to in Section 19. The operator must notify the responsible party immediately where there are reasonable grounds to believe the personal information of a data subject has been accessed or acquired by any unauthorised person."

The cloud provider is responsible for making sure data is stored correctly, that only the authorised people have access to it, that data is fully backed up, and that service is uninterrupted.

### 9. POPIA Compliance Road map

- Appointment of an **Information Officer** and ensure that he/she is aware of his roles and responsibilities.
- Make decision makers and key personnel in your organization aware that the law has changed in accordance with the POPI Act and the severe consequences of non-compliance.

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

- Conduct a current status risk assessment / information audit to establish data protection compliance level.
- Document what Personal Information you currently hold, where it comes from, how it is to be used and who you share it with.
- Produce a POPI Act policies and procedures manual and ensure that everyone who deals with Personal Information is aware of the legal implications of this Act. This manual is to include your organizations privacy policy with regard to:
  - Data collection (type of data, purpose, consent, legal aspects, minimality, and transparency) Data access and accuracy (correct, complete, reliable and process of updating information)
  - Data usage and restrictions (purpose, relevance, restrictions, legality, permission, limitations)
  - Data storage (physical, off-site, electronic, back-up, cloud storage)
  - Data security safeguards (physical, electronic, network, password control, disaster recovery. Disclosure (legality, consent, data subject awareness, data request handling)
  - Responsibilities (All directors, top management, Information Officer, personnel dealing with Personal Information, vendors, contractors, suppliers)
  - Complaints (process, handling, legalities, transparency)
  - Retention (retention schedule) Destruction (destruction schedule) Implement staff awareness training (all current staff, new appointees and regular refresher training).
  - Put procedures in place to monitor and enforce compliance.

### 10. POPIA Complaints Procedure

POPI complaints must be submitted to ULM in writing. Where so required, the Information Officer will provide the data subject with a “**POPIA Complaint Form**”.

- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.



## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
- The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavor to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on ULM's data subjects.
- Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorized person, the Information Officer will consult with ULM's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.
- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to ULM's governing body within 7 working days of receipt of the complaint.  
In all instances, ULM will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
- The Information Officer's response to the data subject may comprise any of the following:
  - A suggested remedy for the complaint;
  - A dismissal of the complaint and the reasons as to why it was dismissed;
  - and
  - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- Where the data subject is not satisfied with the Information Officer's suggested remedies, the
- data subject has the right to complain to the Information Regulator.
- The Information Officer will review the complaints process to assess the effectiveness of the

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

procedure on a periodic basis and to improve the procedure where it is found wanting. The reason

- for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

### 11. RIGHTS OF DATA SUBJECTS

#### 11.1. The Right to Access Personal Information

ULM recognizes that a data subject has the right to establish whether ULM holds personal information related to him, her or it is including the right to request access to that personal information.

#### 11.2. The Right to have Personal Information Corrected or Deleted

. The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where ULM is no longer authorized to retain the personal information.

#### 11.3. The Right to Object to the Processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information. In such circumstances, ULM will give due consideration to the request and the requirements of POPIA. ULM may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

#### 11.4. The right to object to direct marketing

The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

#### 11.5. The Right to Complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator

## **PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023**

---

regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

### **11.6. The Right to be Informed**

The data subject has the right to be notified that his, her or its personal information is being collected by ULM.

The data subject also has the right to be notified in any situation where ULM has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorized person.

## **12. Employees and Other persons acting on behalf of ULM**

Employees and other persons acting on behalf of ULM will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

Employees and other persons acting on behalf of the municipality are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of the municipality may not directly or indirectly, utilize, disclose or make public in any manner to any person or third party, either within the organization or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of the municipality must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of the municipality will only process personal information where:

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

- The data subject, or a competent person where the data subject is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interests of the organization or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

- Clearly understands why and for what purpose his, her or its personal information is being collected; and
- Has granted the municipality with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of the municipality will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the organization will keep a *voice recording* of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- the personal information has been made public, or
- where valid consent has been given to a third party, or

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

- the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of the municipality will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the municipality's central database or a dedicated server.
- Share personal information informally. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
- Transfer personal information outside of South Africa without the express permission from the Information Officer.

Employees and other persons acting on behalf of the municipality are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. IT Manager will assist employees and where required, other persons acting on behalf of the municipality, with the sending or sharing of personal information to or with authorized external persons.

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorized persons.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information is stored on removable storage medias such as external drives, USB's, CDs or DVDs that these are kept locked away securely when not being used.
- Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorized people cannot access it. For instance, in a locked drawer of a filing cabinet.
- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorized individuals could see or copy them.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorization must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorization must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPI Awareness training from time to time.

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

Where an employee, or a person acting on behalf of the municipality, becomes aware or suspicious of any security breach such as the unauthorized access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer.

### 12. Disciplinary Action

- Where a POPI complaint or a POPI infringement investigation has been finalized, ULM may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.
- In the case of ignorance or minor negligence, ULM will undertake to provide further awareness training to the employee.
- Any gross negligence or the willful mismanagement of personal information, will be considered.
- a serious form of misconduct for which ULM may summarily dismiss the employee.
- Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.
- Examples of immediate actions that may be taken subsequent to an investigation include:
  - A recommendation to commence with disciplinary action;
  - A referral to appropriate law enforcement agencies for criminal investigation;
  - Recovery of funds and assets in order to limit any prejudice or damages caused.

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

### 13. Exemptions from the conditions of POPIA

The Information Regulator may exempt a responsible party from having to comply with POPIA (or part of it) if:

1. the public interest outweighs the interference of privacy, or
2. the benefit to the data subject (or third party) outweighs the interference of privacy. (section 37 of the Act)

For example, if a Pension Fund wants to find people who have not claimed their pension, but they can't because of POPIA, the Information Regulator would probably grant them an exemption.

#### 13.1. Exemption of Bodies that protects the Public

If complying with POPIA means that a body (or person) that protects the public cannot perform their function (section 38 of the Act), they are exempt from having to:

- give the data subject the right to object to them processing (section 11(3) and (4)),
- collect personal information directly from the data subject (section 12),
- restrict further processing (section 15),
- notify the data subject about their processing (section 18).

A good example is the public protector. Remember that they must comply with the rest of POPIA. A body wishing to rely on this partial exemption must document the reasons it relies on so that it can provide them to the Information Regulator if asked.

### 14. Policy Review

The ULM Information Officer is responsible for an annual review to be completed prior to the policy anniversary date.



## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

### 14. Authorisation

This Policy Document was approved by the Council of Umzimvubu Local Municipality on this day.....of.....20.....and signed by the Mayor and Municipal Manager on behalf of the Council.

<b>Municipal Manager Signature</b>	
<b>Date</b>	
<b>Executive Mayor Signature</b>	
<b>Date</b>	

Version Control		
POPI Policy	Version No	Approval Date
3-yearly	Version 2	



## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

### Annexure A: Forms

#### 1. CONSENT FORM: CONSENT TO PROCESS PERSONAL INFORMATION IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT, NO. 4 OF 2013 (POPIA)

By signing this form, you consent to your personal information to be processed by the Umzimvubu Local Municipality (ULM) and consent is effective immediately and will remain effective until such consent is withdrawn.

1. I ..... A natural person "herein referred to as the Data Subject" with ID No..... hereby give my consent to the ULM to collect, process and distribute my personal information where the ULM is legally required to do so.
2. I understand my right to privacy and the right to have my personal information processed in accordance with the conditions for the lawful processing of personal information.
3. I understand the purposes for which my personal information is required and for which it will be used and consent to accessing my personal information.
4. I declare that all my personal information supplied to the ULM is accurate, up to date, not misleading and will be held and/ or stored securely for the purpose for which it was collected and that I will immediately advise the ULM of any changes to my Personal Information should any of these details change.
5. I also understand that I have the right to request that my personal information be corrected or deleted, if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully or that the personal information or record be destroyed or deleted if the ULM is no longer authorized to retain it.

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

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

.....  
Name/Surname/Dept of ULM

.....  
Signature

.....  
Date

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

### 2. POPI 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:**

**Address to:** The Information Officer

**Email Address:**

Where we are unable to resolve your complaint, to your satisfaction you have the right to complain to the Information Regulator.

**The Information Regulator**

**Address:** 33 Hoof Street Forum III, 3rdFloor, Braampark, Johannesburg **Email:** inforreg@justice.gov.za

#### A. Particulars of Complainant

Name & Surname

Identity Number:

Postal Address:

Contact Number:

Email Address:

**B. Details of Complaint (Attach a detailed annexure where necessary):**

**C. Desired Outcome (Attach a detailed annexure where necessary):**

**D. Signature of the Complainant:**

**Date:**

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

### Form 3: Objection to processing of personal information

#### (Form 1 of the Regulations)

#### FORM 1

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

#### [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.

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) <i>(Please provide detailed reasons for the objection)</i>

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

.....

*Signature of data subject/designated person*

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

**Form 4: Request for correction or deletion of personal information  
(Form 2 of the Regulations)**

**FORM 2**

**REQUEST FOR CORRECTION OR DELETION OF PERSONAL 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:*

1. *Affidavits or other documentary evidence as applicable in support of the request 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.*

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:	



## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

C	INFORMATION TO BE CORRECTED/DELETED/ DESTROYED/ DESTROYED
<b>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 PERSONALINFORMATION 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)</b>	

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

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

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

### ANNEXURE B: Employee and SLA Clauses

#### 1. Employee Consent and Confidentiality Clause

The employer undertakes to process the personal information of the employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the employer's relevant policy available to the employee on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an employer and within the framework of the employment relationship and as required by South African law.

The employee acknowledges that the collection of his/her personal information is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the employer. The employee therefore irrevocably and unconditionally agrees:

That he/she is notified of the purpose and reason for the collection and processing of his or her personal information insofar as it relates to the employer's discharge of its obligations and to perform its functions as an employer.

That he/she **consents** and **authorizes** the **employer** to undertake the collection, processing and further processing of the employee's personal information by the employer for the purposes of securing and further facilitating the employee's employment with the employer.

Without derogating from the generality of the foretasted, the employee consents to the employer's collection and processing of personal information pursuant to any of the employer's Internet, Email and Interception policies in place insofar as personal information of the employee is contained in relevant electronic communications.

To make available to the employer all necessary personal information required by the employer for the purpose of securing and further facilitating the employee's employment with the employer.

To absolve the employer from any liability in terms of POPIA for failing to obtain the employee's consent or to notify the employee of the reason for the processing of any of the employee's personal information.

To the **disclosure** of his/her personal information by the employer to any **third party**, where the **employer** has a **legal or contractual duty** to disclose such personal information.

The employee further agrees to the disclosure of his/her personal information for any reason enabling the employer to carry out or to comply with any business obligation the employer may have or to pursue a legitimate interest of the employer in order for the employer to perform its business on a day-to-day basis.

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

The employee authorizes the employer to transfer his/her personal information outside of the Republic of South Africa for any legitimate business purpose of the employer within the international community. The employer undertakes not to transfer or disclose his/her personal information unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.

The **employee acknowledges** that **during the course** of the **performance** of his/her **services**, he/she **may gain access to and become acquainted** with the personal information of certain clients, suppliers and other employees. The employee will **treat** personal information as a **confidential business asset** and agrees to respect the privacy of clients, suppliers, and other employees.

To the extent that he/she is exposed to or insofar as personal information of other employees or third parties are disclosed to him/her, the employee hereby agree to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the personal information of third parties or employees.

Employees may not directly or indirectly, utilize, disclose or make public in any manner to any person or third party, either within the organization or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties on behalf of the employer.



## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

### 2. SLA Confidentiality Clause

The parties acknowledge that for the purposes of this agreement that the parties may come into contact with or have access to personal information and other information that may be classified, or deemed as private or confidential and for which the other party is responsible. Such personal information may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the personal information and that the information may have value.

The parties agree that they will at all times comply with POPIA's Regulations and Codes of Conduct and that it shall only collect, use and process personal information it comes into contact with pursuant to this agreement in a lawful manner, and only to the extent required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.

The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of personal information that it, or its employees, its contractors or other authorized individuals comes into contact with pursuant to this agreement.

Unless so required by law, the parties agree that it shall not disclose any personal information as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any personal information out of the Republic of South Africa.

## PROTECTION OF PERSONAL INFORMATION ACT POLICY 2023

---

### ANNEXURE C:

#### WEBSITE DISCLAIMER – PROTECTION OF PERSONAL INFORMATION ACT

*Umzimvubu Local Municipality (ULM) would like to welcome you to its website.*

*By viewing this website you hereby acknowledge that you have read and accepted the following **Protection of Personal Information (POPI)** disclaimer.*

*You understand and agree that all information provided, whether personal or otherwise, may be used and processed by the “owner” of this website, and such use may include placing such information in the public domain.*

*Further by continuing to access this website you specifically agree that the municipality will use such information provided by you, irrespective of the nature of such information.*

*(ULM) shall take all reasonable measures to protect the personal information of users and for the purpose of this disclaimer “personal information” shall be defined as detailed in the Promotion of Access to Information Act, Act 2 of 2000 (“PAIA”) and the **Protection of Personal Information Act, Act 4 of 2013 (“POPI”)**.*

*The PAIA and POPI Acts are available online at [www.gov.za/documents/acts](http://www.gov.za/documents/acts).*

*As per the POPI Act personal information refers to information that identifies or relates specifically to you as a person or data subject, for example, your name, age, gender, identity number and your email address. A definition of personal information can be found in the (ULM)’s POPI policy.*

#### Annexure D: Information Regulator Details

In the event that any of the Group’s Data Subjects has any queries or concerns that cannot be addressed by the Information Officer, the Data Subject has the right to contact the Information Regulator. The Information Regulator’s details are as follows:

---

**Physical address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001**

**Postal address: PO Box 31533, Braamfontein, Johannesburg, 2017**

**Email address: [complaints.IR@justice.gov.za](mailto:complaints.IR@justice.gov.za) and [inforeg@justice.gov.za](mailto:inforeg@justice.gov.za)**

---