human settlements

Department:
Human Settlements
REPUBLIC OF SOUTH AFRICA

DATA PROTECTION AND PRIVACY POLICY

of the

NATIONAL DEPARTMENT OF HUMAN SETTLEMENTS
("DHS")

TABLE OF CONTENTS

ANNEXURES

DEFINITIONS AND ABBREVIATIONS		
NO.	**TERM/ ABBREVIATION**	**DEFINITION**
1.	**"Data Subject"**	means the person to whom Personal Information relates. Examples of Data Subjects include, employees, applicants for housing benefits and juristic persons such as service providers of the DHS;
2. 2	"**Deputy Information Officer**"	means the person(s) designated by the Director-General as such;
3.	"**Information Officer**"	means the Director-General of the DHS;
4.	"**Operator**"	means a person who Processes Personal Information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that party. Examples of Operators include IT service providers, vendors and other suppliers that Process Personal Information on the DHS's behalf;
5.	"**PAIA Manual**"	means a manual prepared in accordance with section 14 of PAIA;
6.	"**PAIA**"	means the Promotion of Access to Information Act, 2 of 2000;

DEFINITIONS AND ABBREVIATIONS		
NO.	**TERM/ ABBREVIATION**	**DEFINITION**
7.	"**Personal Information**"	means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person. Categories of Personal Information include an identifier such as a name, an identification number, contact details and financial information of entities;
8.	"**Personal Information of Children**"	means Personal Information concerning a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person (parent of guardian), to take any action or decision in respect of any matter concerning him or herself;
9.	"**Policy**"	means policy on Data Privacy and Protection policy
10.	"**POPIA**"	means the Protection of Personal Information Act, 4 of 2013;

DEFINITIONS AND ABBREVIATIONS		
NO.	**TERM/ ABBREVIATION**	**DEFINITION**
11.	"**Process/Processing**"	means any operation or activity or any set of operations whether or not by automatic means, concerning Personal Information, including: • dissemination by means of transmission, distribution or making available in any other form; and • merging, linking, as well as restriction, degradation, erasure, or destruction of information; • the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
12.	"**Regulator**"	means the Information Regulator of South Africa;
13.	"**Responsible Party**"	means any 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. The DHS is a Responsible Party;
14.	"**Special Personal Information**"	means Personal Information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a Data Subject, or the criminal behaviour of a Data Subject; and

DEFINITIONS AND ABBREVIATIONS		
NO.	**TERM/ ABBREVIATION**	**DEFINITION**
15.	"**Users**"	means DHS's officials, whether permanent, on probation, contract (internship) or consultancy basis, service providers, and other stakeholders who are in possession of, or have been granted access to Personal Information for which the DHS is either a Responsible Party or an Operator.

1. Introduction

POPIA is South Africa's comprehensive data privacy and protection legislation which gives effect to both natural and juristic persons' right to privacy as enshrined in section 14 of the Constitution of the Republic of South Africa, 1996. Non-compliance with POPIA has serious consequences. The DHS may be liable for a fine up to R10 million, individuals may be subject to imprisonment of a term of up to 10 years or both a fine and imprisonment.

Consequently, it is important that this Policy is carefully read and understood so that all officials comply with its contents. All officials are required to comply with this Policy and all other policies it refers to. The use of Personal Information contrary to this Policy may give rise to disciplinary action and/or civil and criminal proceedings.

The DHS is obliged to respond to requests from Data Subjects in relation to their Personal Information.

Requests to exercise these rights must be identified and analysed carefully to ensure they are handled and documented correctly. Any delays in attending to requests from Data Subjects may be a breach of POPIA.

2. Legislative Mandate

POPIA requires that all Responsible Parties ensure compliance with the conditions of Processing and implement measures to give effect to POPIA's provisions of section 8 of POPI Act.

The Act affords rights to Data Subjects thereby placing an obligation on Responsible Parties to ensure that such rights are upheld.

The Information Officer must ensure that internal measures are developed together with adequate systems to process requests for information or access thereto.

3. Aims and Objectives

This policy establishes the DHS's approach to the protection and management of Personal Information.

This policy establishes data privacy principles as contained in POPIA and expands on the

Compliance Framework of how the DHS collects, retains, disseminates or share and uses Personal Information.

It further gives effect to Data Subject Rights under POPIA and regulates implemention procedures to ensure that Data Subject's rights can be exercised.

4. Scope

The policy applies to all Personal Information that the DHS or its Operators Processes on its behalf.

5. Mandatory Compliance

The policy is applicable to all the DHS officials, whether permanent, on probation, contract (internship) or consultancy basis, service providers, and other stakeholders who are in possession of, or have been granted access to, Personal Information for which the DHS is either a Responsible Party or an Operator.

6. References

This Policy must be read in conjunction with the following policies/procedures:

- POPIA Compliance Framework;
- DHS Data Inventory;
- Consent Management Procedure;
- Departmental Security Policy.
- ICT Security Policy and
- The DHS's PAIA Manual.

7. POPIA's Eight Processing Conditions

Special Personal Information and Personal Information of Children are categories of Personal Information that are especially sensitive. If it is misused, it could significantly impact the rights of Data Subjects and potentially cause great harm. It is for this reason that POPIA

introduces additional safeguards when Processing this kind of information.

POPIA sets out principles that each Responsible Party must follow when using Personal Information. It is important that all the conditions are adhered to when Personal Information is handled. The conditions are further detailed below.

7.1. Condition 1 – Accountability

The accountability condition requires that the DHS ensure that the conditions set out in POPIA, and all the measures that give effect to such conditions, are complied with at the time of determining the purpose and means of Processing Personal Information, as well as during the Processing itself.

Accountability is a broad condition. In order to demonstrate accountability, there are a number of measures which the DHS has implemented.

7.1.1. POPIA Compliance Framework, Policies and Procedures

The DHS has developed and implemented a compliance framework that ensures that all eight conditions in POPIA are adhered to. The POPIA Compliance Framework is a tool used to ensure and track compliance with POPIA. The DHS will ensure that the compliance framework is monitored and maintained regularly.

The DHS has standards and procedures which enable and maintain POPIA compliance. All officials are required to adhere to the policies, standards and procedures.

7.1.2. Personal Information Impact Assessments

The DHS will conduct Personal Information impact assessment every 5 years to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful Processing of Personal Information.

If a DHS User carries out a new activity and/or undertakes a new activity which gives rise to Processing Personal Information, such User must complete the form attached as **Annexure "A",** with the information about the Processing activity and send it to the PAIA and POPIA Unit using the following email address popia@dhs.gov.za

The PAIA and POPIA Unit shall assess whether it is necessary to perform a Personal Information impact assessment

A Personal Information impact assessment shall also be done with reference to any change or update of existing activities leading to a change in quantity or type of Processed Personal

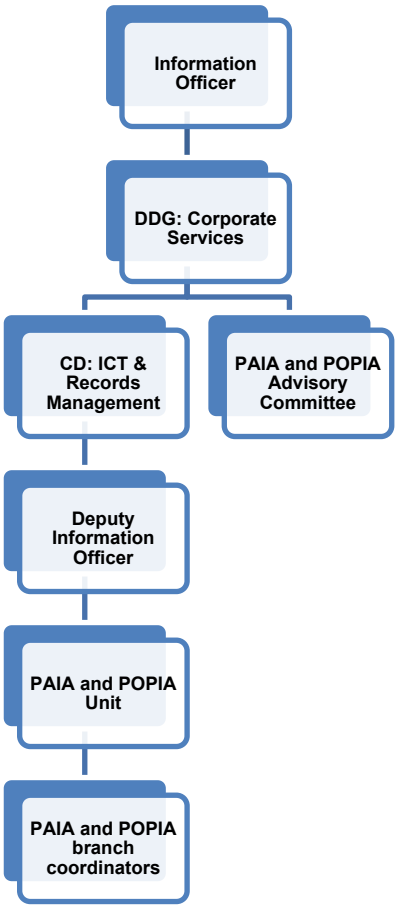
Information or to the procedure of Processing of Personal Information.

7.1.3. Designating Responsible Persons

The Information Officer is ultimately responsible for POPIA compliance. The Information Officer has appointed a Deputy Information Officer to assist with POPIA compliance.

There are other individuals who have also been appointed to assist with POPIA compliance. The PAIA and POPIA Unit has been established to ensure compliance with POPIA as well as PAIA. However, compliance with data privacy and protection laws is the responsibility of anyone who handles Personal Information in the DHS.

The following structure sets out the persons responsible for POPIA compliance.



7.1.4. Training and Awareness

POPIA requires that internal awareness sessions are conducted regarding its provisions, regulations and codes of conduct or information obtained from the Regulator.[1]

The DHS will provide POPIA awareness sessions to employees setting out their obligations

[1] Regulation 4(e) of the POPIA Regulations 2018.

under POPIA, this Policy and related policies. The purpose of the awareness sessions is to ensure that all employees understand their privacy-related obligations. At least on an annual basis, each employee should attend an awareness session. Further awareness sessions might be arranged for specific Directorates at the discretion of the Deputy Information Officer. All new employees are expected to attend awareness sessions as part of their induction process.

7.2. Condition 2 – Processing Limitation

7.2.1. Lawfulness of Processing

The DHS must Process Personal Information lawfully and in a reasonable manner that does not infringe the Data Subject's privacy.

7.2.2. Minimality

Personal Information will only be Processed if, given the purpose for which it is Processed, it is adequate, relevant, and not excessive. If a User does not have a valid reason for collecting Personal Information, it should not be collected. The DHS will only lawfully collect that amount of Personal Information that is necessary for its purposes. If there is any doubt whether Personal Information may be Processed lawfully, please contact the PAIA and POPIA Unit at popia@dhs.gov.za

7.2.3. Grounds of Justification

DHS will rely on the following grounds to process Personal Information.

- if it has obtained consent from the Data Subject;
- to ensure completion of a contract with a Data Subject (e.g service providers or employees);
- if another law obliges the DHS to do so (e.g the finance Directorate is obliged by the Income Tax Act, 58 of 1962 to submit payroll information to SARS);
- if it protects the Data Subject's legitimate interest (e.g Processing beneficiaries' Personal Information for the purposes of paying an employee death benefit);
- if it is the DHS' or a third party's legitimate interest (e.g using Personal Information of an employee to defend an unfair dismissal claim); or
- to fulfil a public law duty (e.g providing emergency housing after a natural disaster).
- Where Personal Information is Processed on the basis of consent, a Data Subject may withdraw consent at any time and such withdrawal should be noted.

- A Data Subject may also object at any time, on reasonable grounds, to the Processing of their Personal Information, save if other legislation provides for such Processing. The DHS may then no longer Process the Personal Information, unless it has another lawful justification for doing so.
- Where consent is relied on to Process Personal Information, Consent Management Procedure should be followed to ensure that a valid consent is implemented.

7.2.4. **Collection Directly from the Data Subject**

Generally, Personal Information must be collected from the Data Subject directly except in certain circumstances. This may include where the Data Subject has made Personal Information public or consents to the collection from another source.

When undertaking a new Processing activity that requires collecting Personal Information from a source other than the Data Subject, for example obtaining information from a verification database, processing limitations should be taken into account.

7.2.5. **Sharing personal information**

The general rule is that Personal Information must be kept confidential and safe from unjustified disclosures. Sharing personal information with an external party is an exception to the confidentiality rule and must be done in a lawful manner. In addition, before sharing Personal Information, the DHS must ensure that:

- there is a legitimate ground for the sharing to take place;
- the Data Subjects must be sufficiently informed about the sharing in the privacy notice and in the DHS PAIA Manual;
- consideration should be given as to how to share the minimum amount of Personal Information;
- consideration should be given as to the length of the sharing arrangement and what will happen at the end of it; the details should clearly be stated in the data sharing agreement.
- consideration must be given as to how to share the Personal Information securely; and
- the sharing must be sufficiently documented in the DHS Data Inventory.
- The sharing of Personal Information includes two different cases:
    - sharing with a Responsible Party where **two Responsible Parties** share Personal

Information between them; and

- sharing with an **Operator** where the DHS, as the Responsible Party, shares data with another party that Processes Personal Information on our behalf.

- Understanding the responsibilities for Personal Information that is shared is essential in ensuring the DHS complies with POPIA. The DHS's obligations under POPIA vary depending on whether it is a Responsible Party, joint Responsible Party or Operator.

*7.2.5.1. **Sharing with a Responsible Party***

The following illustrate a range of data sharing types with another Responsible Party:

- a one-way or reciprocal exchange of Personal Information between departments;
- the DHS providing another organisation with access to Personal Information on its IT system for a purpose;
- several organisations pooling information and making it available to each other or to a third party or parties;
- Personal Information sharing on a routine basis for an established purpose;
- once-off, exceptional, or ad hoc Personal Information sharing; and
- once-off Personal Information sharing in an urgent or emergency situation.

An example of where the DHS may share Personal Information with another Responsible Party is where details of a fraudulent transaction is exchanged with the South African Police Service.

When Personal Information is shared with another Responsible Party, data sharing agreement must be in place.

Data sharing agreements set out the purpose of the data sharing, cover what happens to the data at each stage, set standards and help all the parties involved in sharing to be clear about their roles and responsibilities.

The data sharing agreement should address the following:

- the purpose, or purposes, of the sharing;
- the potential recipients or types of recipients and the circumstances in which they will have

access;

- the data to be shared;
- the quality, accuracy, relevancy, and usability of the Personal Information;
- data security;
- retention of shared data;
- Data Subject rights – procedures for dealing with access requests, queries and complaints;
- review of effectiveness/termination of the sharing agreement; and
- sanctions for failure to comply with the agreement or breaches by staff.

Data sharing agreements in place should be reviewed annually by the relevant business unit in consultation with PAIA/POPIA Unit and Contract Management. Any request to share data that contains Personal Information with a party with whom the DHS has no data sharing agreement in place, must be approved by the Information Officer upon the applicable Directorate providing motivation as to why the Personal Information should be shared with the requesting party. If there is no data sharing agreement in place, the third party must provide sufficient guarantees in relation to security and confidentiality requirements, for example they can provide a Data Privacy and Protection Policy which sets out how they Process Personal Information in compliance with POPIA.

7.2.5.2. ***Sharing Information Processed by Operator or Person Acting Under Authority***

An Operator or anyone Processing Personal Information on behalf of a Responsible Party or an Operator, must:

- Process such information only with the knowledge or authorisation of the Responsible Party; and
- Treat Personal Information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.
- Every time an Operator or any third party has access to Personal Information Processed by the DHS, it shall be verified that such third party is suitable to Process Personal Information on behalf of the DHS in compliance with POPIA by facilitating signing of Operator Agreement at onboarding stage to demonstrate Security Safeguards in terms of Section 19 and Section 21 of POPIA.
- Supply Chain Directorate and Legal Services should ensure that the successful bidders

completes the Operator Checklist (**Annexure D**) during contracting . The completed Operator Checklist shall be sent to PAIA and POPIA Unit for evaluation.

7.3. Condition 3 – Purpose Specification

7.3.1. Collection for a Specific Purpose

The DHS should not collect Personal Information unless it is for a specific and lawful purpose and related to its activities. All DHS officials collecting Personal Information must ensure that the Data Subject knows why the DHS is collecting information, unless the law excuses the DHS from notifying the Data Subject (e.g it may defeat the objective of a criminal investigation). The purpose for collection of Personal Information should always be recorded in the DHS Data Inventory which is managed by PAIA and POPIA unit. So business units must always check if collection of personal information is in line with what is recorded in the DHS Data inventory, if not, update when necessary with PAIA and POPIA unit.

7.3.2. Retention and Restriction of Records

Records of Personal Information should only be kept for as long as necessary for achieving the purpose for which the information was collected or subsequently Processed, unless:

- retention of the record is required or authorised by law;
- the DHS reasonably requires the record for lawful purposes related to its functions or activities;
- retention of the record is required by a contract between the parties thereto; or
- the Data Subject or a competent person, where the Data Subject is a child, has consented to the retention of the record.

The DHS manages records as per the directives of the National Archives and Record Service of South Africa Act, 43 of 1996. Personal Information should also be assigned a retention period in the DHS Data Inventory.

The DHS will ensure that it keeps records of any Personal Information used to make a decision about a Data Subject, for any period required by law, or for a period that will give the Data Subject a reasonable opportunity to request the information.

As soon as there is no reason to keep a record of Personal Information, it must be disposed of. Personal Information must be destroyed or deleted in a manner that prevents its reconstruction in an intelligible form or be de-identified as soon as reasonably practicable

after the DHS is no longer authorised to retain the record. The destruction of records of Personal Information must be done in line with the Records Management Policy on destruction of records.

7.4. Condition 4 – Further Processing Limitation

Further Processing of Personal Information must be compatible with the original purpose of collection. To assess whether further Processing is compatible with the original purpose of collection, the official must take account of:

- the relationship between the purpose of the intended further Processing and the purpose for which the information has been collected;
- the nature of the information concerned;
- the consequences of the intended further Processing for the Data Subject;
- the manner in which the information has been collected; and
- any contractual rights and obligations between the parties.

Where Personal Information is transferred to a third party for further Processing, the further Processing must be compatible with the purpose for which it was initially collected, unless the Data Subject has consented to such further Processing or it is permitted in terms of POPIA.

If Personal Information is to be used for any other purpose, further consent of the Data Subject may need to be obtained.

7.5. Condition 5 – Information Quality

Each business unit must take reasonably practicable steps to ensure that Personal Information in their possession is complete, accurate, not misleading and updated where necessary in light of the purpose for which such information is collected.

Information which is incorrect, or misleading is not accurate. Regular steps must therefore be taken to check the accuracy of any Personal Information at the point of collection and at regular intervals afterwards. Out-of-date information must be destroyed in line with the Records Management policy.

All DHS officials should follow the following guidance when collecting Personal Information:

- Personal Information should be dated when received;
- a record should be kept of where the Personal Information was obtained;
- any updates or changes to Personal Information records should be dated; and

if Personal Information is not necessary, it should be deleted or destroyed destroyed in line with the Records Management policy.

In general, reasonably practicable steps should be taken to ensure that the Special Personal Information and Personal Information of Children held by the DHS is complete, not misleading, accurate and up to date.

When Special Personal Information or Personal Information of Children is being transferred or shared ensure that it is complete, accurate and updated where possible.

7.6. Condition 6 – Openness

Documentation: As part of demonstrating openness, the DHS has a PAIA Manual which broadly lists the categories of Personal Information that it Processes.

Notification to Data Subject when Collecting Personal Information. Officials must ensure that Data Subjects are always told in a clear and comprehensive way how their Personal Information will be used. The following information must be communicated to the Data Subjects prior to collection:

- what Personal Information is collected;
- the purpose of collection;
- the DHS's name, address and contact details;
- whether the supply of their information is voluntary or mandatory;
- the consequences of failing to provide the information;
- the relevant and applicable laws that authorise or require the collection of the information;
- whether the DHS intends transferring the information to a recipient in a foreign country;
- information about a Data Subject's rights in respect of their Personal Information (including the rights to access and correct information, to object to the Processing of their information and to lodge complaints); and
- the recipients or categories of recipients of their Personal Information.

This information must be provided before the DHS collects the Personal Information from the Data Subject or, if not possible to do so at the point of collection, as soon as possible after that. Notification shall be provided at the time of the collection of the Personal Information unless the person is already aware of the information contained in the notification.

Where the DHS obtains a Data Subject's Personal Information from a source other than the Data Subject, for example, a third party, the DHS will disclose the source from which the information is collected to the Data Subject when their Personal Information is first recorded or, if it is to be disclosed to a third party, no later than the time when the Personal Information is first disclosed.

The DHS must ensure that Data Subjects are aware of certain information. The information is provided at the point of collection of Personal Information. The information will be provided to Data Subjects by implementing DHS privacy notices.

The DHS may receive an information request on how a Data Subject's Personal Information is being Processed. For example, a Data Subject may ask the DHS with whom their Personal Information is shared. It is imperative that officials are aware that this information is set out in the DHS's privacy notice and are able to direct or provide the Data Subject with the applicable privacy notice. In addition, the DHS Data Inventory contains information that can be referred to if Data Subjects have any questions relating a specific Processing activity.

7.7. Condition 7 – Security Safeguards

The DHS is required to implement appropriate technical and organisational measures to protect Personal Information against accidental or unlawful destruction, being lost or damaged, and from unauthorised disclosure or access.

In assessing the appropriate level of security, the risks that are presented by Processing should be taken into account.

In light of the above, all officials must comply with the procedures described, among others, in the following policies:

- ICT Security Policy;
- Minimum Information Security Standards;
- Disaster Recovery Plan;
- Records Management Policy; and

- Departmental Security Policy.

The security and integrity of Special Personal Information and Personal Information of Children should be maintained using appropriate, reasonable technical and organisational measures to prevent loss, damage or unlawful access to the Special Personal Information or Personal Information of Children.

Security measures also need to be applied in a context-sensitive manner. Greater security is required for Special Personal Information and Personal Information of Children given the fact that it is of a sensitive nature. For example, special care should be taken with regard to access control.

Third party service providers who Process Special Personal Information or Personal Information of Children on behalf of the DHS are required to maintain security measures referred to in the DHS's information security policies.

7.7.1. **Information Processed by Operator or Person Acting Under Authority**

Every time an Operator or any third party has access to Personal Information Processed by the DHS, it shall be verified that such third party is suitable to Process Personal Information on behalf of the DHS in compliance with POPIA.

The DHS terms of reference where the required services include access to Personal Infmation by the Service Provider should include the following POPIA clause:

" In addition to the requirements listed above, the service provider will be processing personal information on behalf of the DHS, as a result in terms of Section 21of POPIA Act the service provider will be expected to sign the operator agreement to demonstrate that it is it compliant with Security Safeguards in terms Section 19 Protection of Personal Information Act, 4 of 2013 ("POPIA").

The service provider must complete the Operator Checklist and provide all necessary information, which will then be assessed the DHS."

Supply Chain Management and Legal Services should ensure that the successful bidder completes the Operator Checklist. The completed Operator Checklist shall be sent to PAIA and POPIA Unit for evaluation.

If, following such checks, it is found that the Operator is unable to provide sufficient guarantees from a technical and organisational viewpoint with reference to the Processing of Personal Information in compliance with POPIA, the Operator should therefore put Security Safeguards in terms of Section 19 of POPIA.

On an annual basis, the Operator shall complete a new checklist in order to assess the continued suitability of the Operator to Process Personal Information in accordance with POPIA. Such documents should then be analysed by PAIA and POPIA Unit who will assess the appropriate remedial actions, if the inadequate methods of Processing of Personal Information are identified by the Operator.

An Operator or anyone Processing Personal Information on behalf of DHS as a Responsible Party, must:

- process such information only with the knowledge or authorisation of the Responsible Party; and
- treat Personal Information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.

7.7.2. **Notification of Incidents**

In the case of a security compromise, a breach of POPIA and/or of this Policy or other data privacy related policies or a breach for any other reason, Officials must immediately report the event by sending an email to popia@dhs.gov.za. The Deputy Information Officer must notify the data subject and the Information Regulator in terms of Section 22 of POPIA.

Examples of a security compromise include:

- loss or theft of documents containing Personal Information or of devices (e.g mobile devices, computers, tablets, etc.) provided by the DHS or other device containing Personal Information collected in the context of the activities of the DHS;
- unauthorised internal or external access to the DHS's network (e.g hacking) or any other violation of IT systems which could cause loss, compromise, access to or disclosure of Personal Information or information;
- any installation of malware or viruses downloaded onto DHS devices;
- any suspicious emails or telephone calls asking officials to provide information;
- any information in paper or electronic format sent outside of the DHS which does not reach

the intended recipient or is sent to an undesired recipient;

- any breach of security checks on information which could lead to the loss or compromise of information; and
- any unsecure communication of information classified as internal, confidential or secret.

7.8. Condition 8 – Data Subject Participation

Data Subjects are afforded various rights as outlined in paragraph 7 and DHS has an obligation to adhere to requests by Data Subjects in exercising their right:

7.8.1. **Right of Access by the Data Subject**

- The DHS is obliged to respond to requests from Data Subjects in relation to their Personal Information. Requests to exercise these rights must be identified and analysed carefully to ensure they are handled and documented correctly. Any delays in attending to requests from Data Subjects may be a breach of POPIA
- Data Subjects, having provided adequate proof of identity, have the right to obtain confirmation, free of charge, as to whether or not Personal Information the DHS hold Personal Information about them. Data Subjects may also request the record or a description of the Personal Information held by the Responsible Party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information.
- A request for a record may be subject to a prescribed fee and must be provided to the Data Subject in a reasonable manner and format and in a form that is generally understandable. If a Data Subject has requested a record of their Personal Information, the DHS must advise them of their right to correction.
- All requests for access to information must be completed in the manner as set out in the DHS PAIA Manual.
- Data Subjects, having provided adequate proof of identity, have the right to obtain confirmation, free of charge, as to whether or not the DHS holds Personal Information about them.
- Data Subjects may also request a record, or a description of the Personal Information held by the DHS, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information.

- A request for access to a record may be subject to a prescribed fee. The record of Personal Information must be provided to the Data Subject in a reasonable manner and format and in a form that is generally understandable. The DHS must also advise the Data Subject of their right to correction of Personal Information once they have been provided with the record.
- An access request can be received via email, post or telephone.
- The Data Subject must be advised that they are required to make this request on Form 2 to the PAIA Regulations attached as **Annexure "B".** The Deputy Information Officer should provide assistance to any person, at no charge, to complete the form.
- Once the Data Subject has submitted the form, the Deputy Information Officer must handle the request as per the PAIA procedure in the DHS PAIA Manual.
- All valid access requests in terms of PAIA received by the DHS must be dealt with within 30 (thirty) days of receipt of a request, or within 30 (thirty) days of receipt of any further information the DHS may ask the Data Subject to provide to enable it to comply with a request, whichever is the latest.

7.8.2. **Right to Correction, Deletion or Destruction of Personal Information**

- Data Subjects have the right to request correction or deletion of Personal Information that is inaccurate, irrelevant, excessive, misleading or obtained unlawfully or request deletion or destruction of a record of Personal Information that the DHS is no longer authorised to retain.
- All requests of correction or deletion must be completed in the manner as set out in the DHS PAIA Manual.
- A Data Subject may request the DHS to correct or delete Personal Information in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.
- A Data Subject may also request the DHS to destroy or delete a record of Personal Information about the Data Subject that the Responsible Party is no longer authorised to retain in terms of section 14 of POPIA.
- A Data Subject who wishes to request the correction or deletion of Personal Information or deletion of a record of Personal Information in terms of POPIA must submit such request by completing the form attached as **Annexure "C".**
- The procedure to correct, delete or destroy a Data Subject's Personal Information coupled with any reasonable assistance that the DHS may provide to the Data Subject must be free of charge.

- When a request for correction, deletion or destruction of a Data Subject's Personal Information is received, the Deputy Information Officer must assess the validity of such request and decide whether to abide by the request. The DHS must as soon as reasonably possible:
    - correct the Personal Information;
    - destroy or delete the Personal Information;
    - notify the relevant third parties who have the Personal Information of the Data Subject to either correct, destroy, or delete the Personal Information;
    - provide the Data Subject, to his or her satisfaction, with credible evidence in support of the correction or deletion; or
    - where agreement cannot be reached between the DHS and the Data Subject, and if the Data Subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.
- If the DHS has taken steps that result in a change of information and the changed information has an impact on decisions that have been or will be taken in respect of the Data Subject in question, the DHS must, if reasonably practicable, inform each person or body or Responsible Party to whom the Personal Information has been disclosed of those steps.

7.8.3. **Right to Restriction of Processing**

Data Subjects may request the DHS to restrict Processing of their Personal Information where:

- the Data Subject contests the accuracy of the Personal Information, but only for the period necessary for enabling the DHS to verify the accuracy of such data;
- the DHS no longer needs the Personal information for achieving the purpose for which the information was collected or subsequently Processed, but it has to be maintained for purposes of proof;
- the Processing is unlawful and the Data Subject opposes its destruction or deletion and requests the restriction of its use instead; or
- the Data Subject requests to transmit the Personal Information into another automated Processing system.

If any of the above conditions apply, the DHS will only store and will not otherwise Process the Personal Information of the Data Subject according to procedures defined in this Policy.

The DHS must restrict Processing of Personal Information if:

- the Data Subject contest its accuracy but only for a period enabling the DHS to verify the accuracy of the information;
- the DHS no longer needs the Personal Information for achieving the purpose for which the information was collected or subsequently Processed, but it has to be maintained for purposes of proof;
- the Processing is unlawful and the Data Subject opposes its destruction or deletion and requests the restriction of its use instead; or
- the Data Subject requests to transmit the Personal Information into another automated processing system.

Where the Processing is restricted as set out above, the DHS must inform the Data Subject before lifting the restriction on Processing.

7.8.4. **Right to Object**

Data Subjects have the right to object to the Processing of Personal Information concerning themselves in the case where the data is, amongst others:

- Processed in the legitimate interest of the DHS acting as a Responsible Party or of third parties;
- Processing is necessary for the proper performance of a public law duty by a public body;
- Processed for purposes protecting a legitimate interest of the Data Subject.

All objections must be completed in the manner as set out in the DHS PAIA Manual.

Data Subjects have the right to object to the Processing of their Personal Information where the DHS Processes Personal Information of a Data Subject on the basis that:

- it protects a legitimate interest of a Data Subject;
- processing is necessary for the proper performance of a public law duty by a public body; or
- processing is necessary for pursuing the legitimate interest of the DHS or a third party to whom the information is supplied to.

The objection must be made on reasonable grounds relating to the Data Subject's situation unless a specific piece of legislation provides for the Processing.

In addition, a Data Subject may object at any time to the Processing of Personal Information for the purpose of direct marketing other than direct marketing by means of unsolicited electronic communications.

Where a Data Subject wishes to object to the Processing of their Personal Information, they may do so on the form attached as **Annexure "D".**

When an objection is received, the DHS's Information Officer must assess the validity of the Data Subject's objection and, if satisfied, must within 30 (thirty) days cease Processing the Data Subject's Personal Information. The Deputy Information Officer must render proof to the Data Subject that it has stopped Processing the Personal Information. In the event that an objection is manifestly unfounded, excessive and/or does not accord with the dictates of POPIA, the DHS may refuse the objection, and provide notification of this decision to the Data Subject.

7.8.5. Processing of Special Personal Information

The DHS will assess whether Special Personal Information is required for the proposed use and if it is absolutely necessary in the context of its activities.

The DHS will only use Special Personal Information where the Data Subject's express consent has been obtained, unless the DHS has an alternative legitimate basis for doing so, consistent with POPIA.

If you are unsure, whether you can collect or use Special Personal Information please contact the PAIA and POPIA Unit.

7.8.6. Processing of Personal Information of Children

The DHS will only Process Personal Information of Children if it is necessary to use it.

The DHS will assess whether Personal Information of Children is required for the proposed use and when it is necessary in the context of its operations. The DHS will ensure that the Personal Information of Children is Processed in accordance with the Conditions contained in this Policy and POPIA.

The DHS will only use Personal Information of Children where the expressed consent of a competent person has been obtained, unless the DHS has an alternative legitimate basis for doing so, consistent with POPIA.

If you are unsure, whether you can collect or use Personal Information of Children please contact the PAIA and POPIA Unit.

7.8.7. **General Authorisation Concerning Special Personal Information**

The general rule is that the DHS may not Process Special Personal Information unless one of the following general authorisations below are met:

- the Data Subject's consent is obtained before Processing;
- it is necessary for the establishment, exercise or defence of a right or obligation in law; or
- it is necessary to comply with an obligation of international public law; or
- it is for historical, statistical or research purposes (subject to certain requirements) ; or
- information has deliberately been made public by the Data Subject.

7.8.8. **Special Authorisations Concerning Special Personal Information**

POPIA allows the DHS to Process certain categories of Special Personal Information based on a special authorisation. Set out below is some special authorisations that apply to the activities of the DHS:

- the DHS may Process information concerning a person's race or ethnic origin if it is for carried out to comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination. This is the case where the DHS collects information relating to the race of employees to comply with Broad Based Black Economic Empowerment laws; and
- the DHS may Process criminal behaviour or biometric information of employees in accordance with the rules established in compliance with labour legislation.

7.8.9. **Using the Personal Information of Children**

Children need particular protection when you are collecting and Processing their Personal Information because they may be less aware of the risks involved.

A child is anyone under the age of 18 years old.

The general rule is that the DHS may not Process Personal Information of Children unless one of the following conditions are met below:

- prior consent of a competent person (any person who is legally competent to consent to any action or decision regarding the child) has been obtained;
- where it is necessary for the establishment, exercise or defence of a right or obligation in

law;

- where it is necessary to comply with an obligation under international public law;
- where it is required for historical, statistical or research purposes (subject to certain requirements) and sufficient guarantees are provided to ensure that the Processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
- where the Personal Information has been deliberately made public by the child with the consent of a competent person

7.8.10. Data retention of Special Personal Information and Personal Information of Children

The DHS and third parties who Process Personal Information of Children and Special Personal Information on behalf of the DHS should retain Personal Information only for as long as is necessary to achieve the purpose for which it is collected. Retention periods should be kept to a minimum.

Destruction of Special Personal Information and Personal Information of Children should be done in accordance with the DHS's Records Management Policy.

7.8.11. **Information Sharing and Transfer of Special Personal Information and Personal Information of Children**

The DHS may not transfer or share Special Personal Information or Personal Information of Children, except under the following circumstances:

- to the relevant authorities as required by applicable law;
- to external audit authorities;
- to third party service providers, who contract under a signed written agreement, subject to the provisions set out in this policy.
- where the DHS has prior permission from the Data Subject to do so.

The DHS may not transfer Special Personal Information or Personal Information of Children to a third party who is in a foreign country unless a transborder data Processing agreement has been entered into between the DHS and the foreign third party.

The transborder data Processing agreement must provide for an adequate level of protection and stipulate that the foreign organisation effectively upholds principles for reasonable Processing of the information that are substantially similar to the conditions for the lawful Processing of Personal Information relating to a data subject who is a natural person and,

where applicable, a juristic person.

7.8.12. **Transborder Flows of Personal Information outside the Republic of South Africa**

All Directorates must document all transborder flows of Personal Information in the DHS Data Inventory.

All Directorates must ensure that when it transfers Personal Information outside of South Africa, that it does so in compliance with the mechanisms set out in POPIA.

The DHS may only transfer Personal Information outside the Republic of South Africa in limited instances.

Before any transfer of Personal Information outside the Republic of South Africa is done, it must be approved by the PAIA and POPIA Unit if it is not recorded in the DHS Data Inventory.

The DHS and the foreign recipient must enter into a transborder data Processing agreement unless an exception is applicable under POPIA.

This transborder data Processing agreement must provide for an adequate level of protection and stipulate that the foreign recipient effectively upholds principles for reasonable Processing of the information. These principles must be substantially similar to the conditions for the lawful Processing of Personal Information relating to a Data Subject who is a natural person and, where applicable, a juristic person.

The transborder data Processing agreement must further include provisions relating to the further transfer of Personal Information from the recipient to third parties who are in a foreign country.

The above process does not need to be applied where:

- the Data Subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the Data Subject and the Responsible Party, or for the implementation of pre-contractual measures taken in response to the Data Subject's request;
- the transfer 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; or
- the transfer is for the benefit of the Data Subject, and
- it is not reasonably practicable to obtain the consent of the Data Subject to that transfer; and
- if it were reasonably practicable to obtain such consent, the Data Subject would be likely to

give it.

Should Personal Information be transferred outside of South Africa without a data transfer agreement in place, the Information Officer must provide prior approval.

7.8.13. **Direct Marketing**

Direct Marketing by use of unsolicited electronic communications (including by way of automated calling machines, SMSs, fax machines or e-mails) falls under the ambit of POPIA.

Direct Marketing means to approach a Data Subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- promoting or offering to supply, in the ordinary course of business, any goods or services to the Data Subject; or
- requesting the Data Subject to make a donation of any kind for any reason;

Although the DHS does not generally engage in direct marketing, officials must be aware of what constitutes direct marketing and contact the PAIA and POPIA Unit if they intend to engage in activity that may be regarded as direct marketing. An example of direct marketing is where the DHS promotes a Social Housing Scheme by way of sending SMSs to a database of qualified applicants.

8. Security of Information at DHS

DHS as a Responsible Party is required to properly safeguard personal information in its possession. Processing includes automated and non-automated means. DHS is further required by law to take appropriate measures to prevent:

a) Loss of, damage to or unauthorised destruction of personal information, and

b) Unlawful access to or processing of personal information.

Personal information may get lost, damaged or unlawfully accessed in a variety of ways, including:

a) Theft of documents or electronic records,

b) Computer viruses,

c) Computer crashes,

d) Hacking of databases,

e) Accidental damage caused by employees or contractors, or

f) Natural disasters.

DHS is taking comprehensive approach to prevent the loss, damage, and unauthorised personal information access through the above processes. Physical Security Policy provisions should be always adhered to by all departmental officials. It is the responsibility of every departmental official to safeguard personal information held by the department.

8.1. ICT Security

DHS has put in place an effective IT systems and infrastructure in place to safeguard the personal information in its custody namely; Anti-Virus software and Firewall Protection which are regularly updated; Password Protection, Access Control Protocols, Backups, device encryption, Information Security Awareness and ICT Security Policy that governs ICT environment in relation to security of DHS ICT infrastructure.

In ensuring safeguarding computer hardware and the personal information stored on the hardware and departmental network, all DHS officials are mandated to comply with ICT Security Policy and should read this policy in conjunction with ICT Security Policy.

9. Dealing with Complaints

Data Subjects have the right to complain to the Regulator if they are of the view that their rights are not respected or if the DHS has violated POPIA.

The DHS should make every effort to resolve a Data Subject complaint internally before the Data Subject lodges a complaint with the Regulator.

It is therefore important that all complaints are submitted to the Deputy Information Officer as soon as possible. The Deputy Information Officer should acknowledge receipt of the complaint and provide the Data Subject with a timeline on when it can expect feedback

regarding the complaint.

Data Subject should be notified and provided with proof once it is resolved.

10. Monitoring, Evaluation and Reporting

The PAIA and POPIA Unit is responsible for facilitating approval of the Policy and ensuring compliance with the Policy.

All officials are responsible for monitoring their compliance with the principles or procedures detailed in this Policy. The Directorate responsible for monitoring compliance with legislation in the department must monitor compliance on a regular basis.

The Information Officer must approve any deviations or exceptions.

This Policy will be subject to a review every five years or as deemed necessary by the Information Officer.

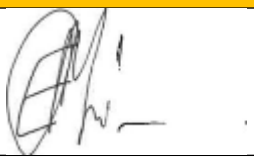
11. Implementation Date

This Policy shall commence on the date of approval by the Information Officer.

12. Consequences of Non-Compliance

It is essential that officials comply with all relevant parts of this Policy. Any failure to comply with this Policy could have serious consequences for the DHS. Failure to comply may lead to disciplinary action, civil or criminal proceedings; and/or personal liability for those responsible.

Approved by:

Name:	Designation	Signature	Date
A Moemi	Director-General		**16/07/2024**

Annexure A – Personal Information Processing Form

1.	Name of Employee:	
2.	Directorate and Sub-Directorate:	
3.	Please provide a clear description of the new Processing activity that is being undertaken.	
4.	Please explain why you are collecting the Personal Information, why it is required, and how it will be collected:	
5.	Please list who the categories of Data Subjects are. For example, who will the Personal Information relate to, for example: employees, housing applicants or supplier:	
4.	Please provide a description of the categories of Personal Information that will be collected. See below for a definition of what constitutes Personal Information. If you need guidance on what is or is not Personal Information,	

	please contact the PAIA and POPIA Unit:	
5.	Does the activity contemplate the processing of Special Personal Information or Personal Information of Children? See below for a definition of what constitutes Special Personal Information:	
6.	Please provide a list of people (internal and external) that will have access to the Personal Information:	
7.	Does the activity contemplate the transfer of Personal Information across the borders of South Africa? If so, please provide a list of countries:	
8.	Will the Personal Information be collected in a paper or electronic format? Please provide details on how the information will be stored, e.g., local server, computer hard drive, cloud, or filing cabinet	

	etc.	
9.	If the information is hosted, where is it hosted?	
10.	Please list the security measures that should be implemented or are in place to protect the Personal Information:	
11.	How long will the Personal Information need to be kept for and are there any considerations in terms of how it needs to be disposed of once no longer required:	

Annexure B– Request for Access

FORM 2

REQUEST FOR ACCESS TO RECORD

[Regulation 7]

NOTE:

1. *Proof of identity must be attached by the requester.*
2. *If requests made on behalf of another person, proof of such authorisation, must be attached to this form.*

TO: The Information Officer

_____
_____
_____
_____

(Address)

E-mail address: _____

Fax number: _____

*Mark with an **"X"***

☐ Request is made in my own name ☐ Request is made on behalf of another person.

PERSONAL INFORMATION				
Full Names				
Identity Number				
Capacity in which request is made *(when made on behalf of another person)*				
Postal Address				
Street Address				
E-mail Address				
Contact Numbers	Tel. (B):		Facsimile:	
	Cellular:			
Full names of person on whose behalf request is made *(if applicable):*				
Identity Number				
Postal Address				

Street Address				
E-mail Address				
Contact Numbers	Tel. (B)		Facsimile	
	Cellular			

PARTICULARS OF RECORD REQUESTED

Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located. (If the provided space is inadequate, please continue on a separate page and attach it to this form. All additional pages must be signed.)

Description of record or relevant part of the record:	
Reference number, if available	
Any further particulars of record	

TYPE OF RECORD
*(Mark the applicable box with an "**X**")*

Record is in written or printed form	
Record comprises virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Record consists of recorded words or information which can be reproduced in sound	
Record is held on a computer or in an electronic, or machine-readable form	

FORM OF ACCESS *(Mark the applicable box with an "**X**")*	
Printed copy of record *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)*	
Written or printed transcription of virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Transcription of soundtrack *(written or printed document)*	
Copy of record on flash drive *(including virtual images and soundtracks)*	
Copy of record on compact disc drive*(including virtual images and soundtracks)*	
Copy of record saved on cloud storage server	

MANNER OF ACCESS *(Mark the applicable box with an "**X**")*	
Personal inspection of record at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)*	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format *(including transcriptions)*	
E-mail of information *(including soundtracks if possible)*	
Cloud share/file transfer	
Preferred language *(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)*	

PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED *If the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.*	
Indicate which right is to be exercised or protected	

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

FEES	
a) A request fee must be paid before the request will be considered. *b) You will be notified of the amount of the access fee to be paid.* *c) The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.* *d) If you qualify for exemption of the payment of any fee, please state the reason for exemption*	
Reason	

You will be notified in writing whether your request has been approved or denied and if approved the

costs relating to your request, if any. Please indicate your preferred manner of correspondence:

Postal address	Facsimile	Electronic communication *(Please specify)*

_____

Signed at _____ this _____ day of _____ 20 _____

Signature of Requester / person on whose behalf request is made

FOR OFFICIAL USE

Reference number:	
Request received by: (State Rank, Name And Surname of Information Officer)	
Date received:	
~~Access fees:~~	
Deposit (if any):	

Signature of Information Officer

Annexure C: Request for Correction of Deletion

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, 2017

[Regulation 3(2)]

Note:

1. *Affidavits or other documentary evidence in support of the request must be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to thisForm and sign each page.*

Reference Number….

Mark the appropriate box with an "x".

3. 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 isin possession or under the control of the responsible party and who is no longer authorisedto retain the record of information.

1. A	**2. DETAILS OF THE DATA SUBJECT**
3. Surname:	
4. Full names:	
5. Identity number:	
6. Residential, postal orbusiness address:	
7. Contact number(s):	
8. Fax number:	
9. E-mail address:	
10. DETAILS OF RESPONSIBLE PARTY	
11.Name and surname of responsible party*(if the responsible party is a natural person)*:	

12. Residential, postal orbusiness address:	
	Code ( )
11. Contact number(s):	
12. Fax number:	
13. E-mail address:	

14. ame of public or private body *(if the responsible party is not anatural person)*:	
38. Business address:	
	Code ( )
39. Contact number(s):	
40. Fax number:	
41. E-mail address:	

42.	**REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT/*DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATIONABOUT THE DATA SUBJECT WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY.** *(Please provide detailed reasons for the request)*

Delete whichever is not applicable.

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

.....
Signature of Data subject

Annexure D: Objection to the Processing of Personal Information

FORM 1

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

REGULATIONS RELATING TO THE PROTECTION OF PERSONALINFORMATION, 2017

[Regulation 2(1)]

Note:

1. *Affidavits or other documentary evidence in support of the objection must be attached.*
2. *If the space provided for in this Form is inadequate, submit information as anAnnexure to thisForm and sign each page.*

Reference Number….

A	**DETAILS OF DATA SUBJECT**
Name and surname ofdata subject:	
Residential, postal orbusiness address:	
	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name and surname of responsible party*(if theresponsible party is a natural)*:	
Residential, postal orbusiness address:	
	Code ( )
Contact number(s):	

Fax number:	
E-mail address:	

Name of public or private body*(if the responsible party is not anatural person)*:		
Business address:		
	Code ( )	
Contact number(s):		
Fax number:		
E-mail address:		
C	**REASONS FOR OBJECTION** *(Please provide detailed reasons for the objection)*	

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

.....

Signature of data subject (applicant)

Annexure E: Operator checklist

human settlements

Department:
Human Settlements
REPUBLIC OF SOUTH AFRICA

OPERATOR COMPLIANCE CHECKLIST

Company Name:			
Registration Number:			
Nature of Services:			
No	**Question**	**Answer**	**Additional Information**
1	Have you registered your Information Officer and, where relevant, your Deputy Information Officer with the Regulator?		If yes, please specify the Information Officer and Deputy Information Officer:
2	In the event that you have delegated the role of Information Officer or the Deputy information Officer, is there a formal authorisation or delegation in place?		
3	Have you implemented any formal data privacy and protection policies or procedures within your organisation?		If yes, please specify the policies and procedures:
4	Have you conducted a POPIA Gap Assessment/Analysis/Personal Information Impact Assesment?		If in progress, please advise when it is expected to be completed by:
5	Do you have any Operators that provide key parts of the service to us?		If yes, please specify the company and the service:
6	Have you reviewed and compiled a list of all of your Operators?		
7	Have you entered into an Operator agreement with all your Operators?		
8	Have you implemented a ROPA (Record of Processing Activities)?		
9	Have you considered whether you are required to implement a PAIA Manual and if so, has it been implemented?		
10	Is there a process in place to identify all reasonably foreseeable		

	internal and external risks to Personal Information?		
11	Is there a process in place to establish and maintain appropriate security safeguards against the risks identified?		If yes, please specify the security safeguards in place:
12	Is there a process in place to regularly verify that the safeguards are effectively implemented, for example, have you employed someone to conduct a security assessment?		
13	Is there a process in place to ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards?		
14	Do you have physical access control measures to secure access to the premises where Personal Information is stored?		
15	Do you restrict access to Personal Information to trained and authorised staff members?		
16	Have you implemented a procedure to be followed in the event of a security compromise / data breach?		
17	Have you ensured that you have appropriate privacy notices in place and that they are displayed?		
18	Have you implemented a Data Subject Rights Procedure?		
19	If you are established outside the Republic of South Africa, have you appointed a representative in South Africa for the purposes of POPIA implementation?		
20	Have you developed appropriate procedures to ensure that Personal Information is accurate and up to date?		
21	Have you reviewed your direct marketing practices and amended it in line with POPIA?		
22	Have you trained your employees on POPIA and all policies and procedures that have been implemented as part of your compliance framework?		

23	Do you have a data retention policy or procedure in place that advises you how and when to retain and destroy data?		
24	Are there any transfers of Personal Information outside the Republic of South Africa?		If yes, please specify the countries and list the safeguards taken to protect data, e.g. Data Processing Agreement etc.:
25	Are cloud services used for the services you provide?		If yes, please specify where the servers for the Personal Information are located: