

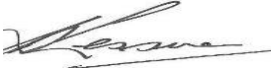


**PROTECTION OF PERSONAL INFORMATION
(POPIA)
POLICY**

Version	1
Publishing Date	June 2021
Last Review Date	N/A
Frequency of Review	Annually or as and when material changes occur
Next Review Date	June 2022
Policy Owner	Broker Solutions Group (Pty) Ltd
Responsible Person	Chris Thessner

POLICY ADOPTION

By signing this document, I authorise the policy owner's approval and adoption of the processes and procedures outlined herein.

Name & Surname	Chris Thessner
Capacity	Executive Director, KI, Rep and IO
Signature	
Date	30 June 2021

Contents

1	INTRODUCTION	2
2	DEFINITIONS	2
2.1	Personal Information	2
2.2	Data Subject	3
2.3	Responsible Party	3
2.4	Operator	3
2.5	Information Officer	3
2.6	Processing	3
3	POLICY PURPOSE	4
4	POLICY APPLICATION	5
5	RIGHTS OF DATA SUBJECTS	5
5.1	The Right to Access Personal Information	5
6	GENERAL GUIDING PRINCIPLES	6
6.1	Accountability	6
6.2	Processing Limitation	7
6.3	Purpose Specification	7
6.4	Further Processing Limitation	7
6.5	Information Quality	7
6.6	Open Communication	7

6.7	Security Safeguards	7
6.8	Data Subject Participation	8
7	INFORMATION OFFICERS	8
8	SPECIFIC DUTIES AND RESPONSIBILITIES	8
8.1	Information Officer	8
8.2	IT Manager	9
8.3	Employees and other Persons acting on behalf of BRS	9
9	REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE	11
10	POPI COMPLAINTS PROCEDURE	11

1 INTRODUCTION

The right to privacy is an integral human right recognised 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.

Through the provision of quality goods and services, BRS is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

A person’s right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

Given the importance of privacy, BRS is committed to effectively managing personal information in accordance with POPIA’s provisions.

2 DEFINITIONS

(Please note that the below definitions were extracted directly from POPIA (safe for those that had been customised, accordingly))

2.1 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, colour, 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 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.

2.2 Data Subject

This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies BRS with products or other goods.

2.3 Responsible Party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, BRS is the responsible party.

2.4 Operator

An 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. For example, a third-party service provider that has contracted with BRS to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

2.5 Information Officer

The Information Officer is responsible for ensuring BRS' compliance with POPIA.

Where no Information Officer is appointed, the head of BRS will be responsible for performing the Information Officer's duties.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

2.6 Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- the collection, receipt, recording, BRS, 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.

1.1 Record

Means any recorded information, regardless of form or medium, including:

- Writing on any material;
- 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;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph or drawing;

- 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.

1.2 Filing System

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

1.3 Unique Identifier

Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

1.4 De-Identify

This means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

1.5 Re-Identify

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

1.6 Consent

Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

1.7 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.

1.8 Biometrics

Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

3 POLICY PURPOSE

This purpose of this policy is to protect BRS from the compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality. For instance, BRS could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer choice. For instance, all data subjects should be free to choose via their broker on how and for what purpose BRS uses information relating to them.
- Reputational damage. For instance, BRS could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by BRS.

This policy demonstrates BRS' commitment to protecting the privacy rights of data subjects in the following manner:

- Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
- By cultivating an BRS' culture that recognises privacy as a valuable human right.
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
- By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of BRS.
- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of BRS and data subjects.
- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4 POLICY APPLICATION

This policy and its guiding principles applies to:

- All BRS' employees and volunteers
- All contractors, suppliers and other persons acting on behalf of BRS

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

The legal duty to comply with POPIA's provisions is activated in any situation where there is:

- A **processing** of.....
personal information
entered into a **record**
by or for a **responsible person**
who is **domiciled** in South Africa.

POPIA does not apply in situations where the processing of personal information:

- is concluded in the course of purely personal or household activities, or
- where the personal information has been de-identified.

5 RIGHTS OF DATA SUBJECTS

Where appropriate, BRS will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects.

BRS will ensure that it gives effect to the following seven rights.

5.1 The Right to Access Personal Information

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

An example of a "Personal Information Request Form" can be found under "**Annexure A**".

5.2 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 BRS is no longer authorised to retain the personal information.

5.3 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, BRS will give due consideration to the request and the requirements of POPIA. BRS 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.

A data subject who wishes to object to the processing of personal information, must submit the objection to the responsible party on **Form 1** of the Regulations to the Act. The responsible party, or a designated person, must must render such reasonable assistance as is necessary, free of charge, to enable the data subject to make an objection on **Form 1**.

5.4 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.

A responsible party who wishes to process personal information of a data subject for the purpose of direct marketing by electronic communication must submit a request for written consent to that data subject on **Form 4** of the Regulations to the Act.

5.5 The Right to Complain to the Information Regulator

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

An example of a "POPI Complaint Form", for internal use, can be found under "Annexure B".

Any person who wishes to submit a complaint contemplated in section 74(1) of the Act must submit such a complaint to the *Regulator* on **Part I of Form 5**. A responsible party or a data subject who wishes to submit a complaint contemplated in section 74(2) of the Act must submit such a complaint to the *Regulator* on **Part II of Form 5** of the Regulations to the Act.

5.6 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 BRS.

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

6 GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of BRS will at all times be subject to, and act in accordance with, the following guiding principles:

6.1 Accountability

Failing to comply with POPIA could potentially damage BRS' reputation or expose BRS to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

BRS will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, BRS 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.

6.2 Processing Limitation

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

- in a fair, lawful and non-excessive manner, and
- only for a specifically defined purpose – which can be dependent on brokers for the insurance portfolio.

BRS will under no circumstances distribute or share personal information between separate legal entities or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the data subjects consent will be provided through the broker to BRS' for further processing.

6.3 Purpose Specification

BRS will process personal information only for specific, explicitly defined and legitimate reasons. The reasons for same will be purely for administrative purposes for insurance and/or claims related.

6.4 Further Processing Limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose, such as claims as an example.

6.5 Information Quality

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

BRS will take 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.

6.6 Open Communication

BRS will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

- Enquire whether BRS holds related personal information, or
- Request access to related personal information, or
- Request BRS to update or correct related personal information (not without intervention from broker and/or reasonable expectancy that the broker should be aware), or
- Make a complaint concerning the processing of personal information.

6.7 Security Safeguards

BRS will manage the security of its filing system to ensure that personal information is adequately protected. To this end, reasonable security controls have been implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

BRS will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised 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 unauthorised disclosures of personal information for which BRS 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.

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

6.8 Data Subject Participation

A data subject may request the correction or deletion of his, her or its personal information via their broker to inform BRS. Where applicable, BRS will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7 INFORMATION OFFICERS

BRS will appoint an Information Officer and a Deputy Information Officer to assist the Information Officer. BRS' Information Officer is responsible for ensuring compliance with POPIA.

8 SPECIFIC DUTIES AND RESPONSIBILITIES

8.1 Information Officer

BRS' Information Officer is responsible for:

- Taking steps to ensure BRS' reasonable compliance with the provision of POPIA.
- In the case of a security breach, the employee who became aware of same will immediately and/or as soon as reasonably became known raise it with the Information Officer who will ensure compliance and discussion with the relevant personnel as well as Information Regulator.
- Continually analysing privacy regulations and aligning them with BRS' personal information processing procedures. This will include reviewing BRS's information protection procedures and related policies.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of BRS are fully aware of the risks associated with the processing of personal information and that they remain informed about BRS's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of BRS.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by BRS' data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

- Ensure that a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).
- Ensure that internal measures are developed together with adequate systems to process requests for information or access thereto.
- Ensure that internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.
- The information officer shall upon request by any person, provide copies of the manual to that person upon the payment of a fee to be determined by the Regulator from time to time.

The Deputy Information Officer will assist the Information Officer in performing his or her duties.

8.2 IT Manager

BRS' IT Manager is responsible for:

- Ensuring that BRS's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Ensuring that personal information being transferred electronically is encrypted.
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- Performing regular IT audits to ensure that the security of BRS' hardware and software systems are functioning properly.
- Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on BRS' behalf. For instance, cloud computing services.

8.3 Employees and other Persons acting on behalf of BRS

Employees and other persons acting on behalf of BRS 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 BRS 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 BRS may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within BRS 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 BRS 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 BRS will only process personal information where:

- 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 BRS 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.

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 via the broker/s.

Employees and other persons acting on behalf of BRS 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 BRS' central database (including Cardinal360 and Flexi) or a dedicated server.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. 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 BRS 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 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 unauthorised 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, 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 unauthorised 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 unauthorised individuals could see or copy them. For instance, close to the printer.
- 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, authorisation 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, authorisation 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.

Where an employee, or a person acting on behalf of BRS, becomes aware or suspicious of any security breach such as the unauthorised 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 or the Deputy Information Officer.

9 REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data subjects have the right to:

- Request what personal information BRS holds about them and why.
- Request access to their personal information.
- Be informed how to keep their personal information up to date.

Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form".

In addition to the aforementioned, where the data subject requests the correction, deletion or destruction of a record of personal information, the Information Officer will provide the data subject with **Form 2** to the Regulations of the Act. The responsible party, or a designated person, must render such reasonable assistance, as is necessary free of charge, to enable a data subject to complete **Form 2**.

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against BRS's PAIA Policy.

The Information Officer will process all requests within a reasonable time.

10 POPI COMPLAINTS PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. BRS takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

- POPI complaints must be submitted to BRS in writing. Where so required, the Information Officer will provide the data subject with a "POPI 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.

- 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 endeavour 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 BRS'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 unauthorised person, the Information Officer will consult with BRS'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 BRS's governing body within 7 working days of receipt of the complaint. In all instances, BRS 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,
 - 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 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.

ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer:	
Name	
Contact Number	
Email Address:	

Please be aware that we may require you to provide proof of identification prior to processing your request.
 There may also be a reasonable charge for providing copies of the information requested.

A. Particulars of Data Subject

Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	

B. Request

I request BRS to:

(a) Inform me whether it holds any of my personal information	<input type="checkbox"/>
(b) Provide me with a record or description of my personal information	<input type="checkbox"/>

C. Instructions

D. Signature Page

Signature	
Date	

ANNEXURE B: POPI COMPLAINT FORM

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:	
Name	
Contact Number	
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: Adv Pansy Tlakula
Physical Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001.
Email: complaints.IR@justice.gov.za
Website: <http://www.justice.gov.za/inforeg/index.html>

A. Particulars of Complainant

Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	

B. Details of Complaint

C. Desired Outcome

D. Signature Page

Signature:
Date

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)

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

Note:

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

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

Signed at this day of20.....

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