



Protection of Personal Information Act, 2013

Introduction to POPIA

ELDO Group Holdings (K2019/559363/07) hereinafter referred to as The Responsible Party.

Table of Contents

1. Introduction	3
2. Purpose of POPIA.....	3
3. POPIA References	3
4. Information Protection Principles.....	5
5. Cross-border Information Flows.....	7
6. Application of POPIA.....	8
7. Exclusions.....	8
8. The Responsible Party's Obligations when Processing Personal Information.....	9
9. Direct Marketing.....	9
10. Information Officer	10
11. Effective Date of POPIA	11
12. Investigation and Compliance Order.....	11
13. Damages in the Civil Courts.....	12
14. POPIA Offences and Penalties.....	12
15. Punishable Offences in terms of POPIA.....	13
16. Compliance with POPIA.....	13
17. Information Regulator.....	14
18. POPIA Regulations.....	14

1. Introduction

The Protection of Personal Information Act has significant implications for both the citizens and legal entities of South Africa whose Personal Information is processed by any private person, company and/or public body, as well as for the private persons, companies and public bodies that process this Personal Information, (ELDO Group Holdings 2019/559363/07). POPIA is a dedicated law aimed at protecting Personal Information from abuse and misuse.

2. Purpose of POPIA

POPIA aims to regulate the collection and processing of Personal Information by natural persons, as well as both private and public bodies, including the State. POPIA seeks to protect and prevent the abuse and misuse of Personal Information, owned by individuals and companies in South Africa, whose information is collected, processed, and used by the Responsible Party. POPIA, however, must not be seen as a law that disrupts the operations of the Responsible Party's business. POPIA seeks to create a careful balance between a person's Constitutional right to privacy and the needs and interests of commerce, government and business in the private and public sectors.

3. POPIA References

POPIA makes use of certain references, as explained below.

- "Responsible Party"* the Responsible Party or public body, that collects and uses any individual or legal entities' Personal Information, is herein also referred to as *ELDO Group Holdings*. Responsible Party is defined as a public or private body or any other person which, alone or in conjunction with others, determines the purpose of -and means for processing Personal Information.
- "Data Subject"* the individual or legal entity whose Personal Information is being collected, used and processed, is referred to as the Data Subject;
- "Personal Information"* which may be processed, collected, and used of a Data Subject by a Responsible Party will include any information related to a private or public entity and/or natural living individual including his/her or its:

- > Name, address and ID number;
- > Blood type and fingerprints;
- > Educational, medical, criminal or employment history, as well as information in respect of financial transactions;
- > Views or opinions;
- > Information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.

"Processing"

when a Responsible Party attempts to collect Personal Information, which has been defined as any operation or activity or any set of operations, whether by automatic means or not, in respect of Personal Information, including—

- > the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- > dissemination by means of transmission, distribution or making available in any other form;
- > merging, linking, as well as restriction, degradation, erasure or destruction -of information.

"Record"

means any recorded information—

- > regardless of form or medium, including any of the following:
 - 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 to be capable, with or without the aid of some other equipment, of being reproduced;
- > in the possession or under the control of a Responsible Party;
- > whether or not it was created by a Responsible Party; and
- > regardless of when it came into existence.

4. Information Protection Principles

POPIA has adopted eight core international principles / conditions which apply to the processing of Personal Information. Once one understands these principles, the provisions of POPIA will make sense.

Condition 1: Processing Limitation

Personal Information must be collected directly from the Data Subject and may only be processed with the consent of the Data Subject or, in the absence of consent, where it is necessary to comply with a legal obligation, public law duty, or a contractual obligation.

Condition 2: Specific Purpose

Personal Information must be collected for a specific, explicitly defined and legitimate purpose. The Data Subject should be made aware of the purpose for which the Personal Information is collected, as well as who the likely recipients of the Personal Information will be.

Condition 3: Further Processing Limitation

Personal Information may not be processed further in a way that is incompatible with the purpose for which the information was collected initially. Thus, if Personal Information was processed for the purpose for which it was collected, it may only be processed further if it can be shown that the purpose for the further processing is compatible with the original purpose. POPIA provides guidelines to assist with such an assessment.

Condition 4: Information Quality

The person or institution in its capacity as the Responsible Party that processes Personal Information, should ensure that the Personal Information is complete, not misleading, up to date and accurate.

Condition 5: Openness

Where Personal Information of a Data Subject is collected, the Responsible Party must ensure that the Data Subject is made aware of—

- > the fact that the information is being collected;
- > the name and address of the person or institution collecting the information;
- > whether or not the supply of the information by that Data Subject is voluntary or mandatory;
- > the consequences of failure to provide the Personal Information; and
- > where the collection of Personal Information is authorised or required under any law, such law to which the collection is subject.

Condition 6: Security Safeguards

POPIA requires the implementation of technical and organisational measures to secure the integrity of Personal Information, and to guard against the risk of loss, damage or destruction to or of such Personal Information. Any person holding Personal Information must protect that Personal Information against any unauthorised or unlawful access or processing.

Condition 7: Individual Participation

A Data Subject is entitled to the details of his/her/its Personal Information held by any institution or person, as well as to the identity of any person that had access to his/her/its Personal Information. The Data Subject is also entitled to request the correction of any incorrect Personal Information held by another party.

Condition 8: Accountability

The Responsible Party must give effect to the principles/conditions for the protection of Personal Information, as set out under POPIA. Despite the conditions set out above, the Regulator may exempt the Responsible Party from compliance with some of the conditions of processing, and authorise the processing of the identified Personal Information where the processing will be in the public interest, or where there is a clear benefit for the people concerned.

The “public interest” includes:

- > The interests of State security;
- > The prevention, detection and prosecution of criminal offences;
- > Important economic and financial interests of the State and other public bodies; or

- > Scientific research and government statistics.

5. Cross-border Information Flows

It is interesting to note that POPIA not only regulates Personal Information held in South Africa. It also regulates the transfer of Personal Information to parties outside of South Africa. The Responsible Party may therefore not transfer Personal Information cross-border, unless—

- > the recipient is subject to a law, binding corporate rules, binding agreement or memorandum of understanding, which provide an adequate level of protection that is substantially like the conditions for the processing of Personal Information, as set out in POPIA; or
- > the Data Subject has consented to the transfer; or
- > the transfer is necessary for the performance of a contract; or
- > the transfer is for the benefit of the Data Subject and it was not reasonably practicable to get their consent.

6. Application of POPIA

POPIA regulates the processing of Personal Information within South Africa, including the processing of Personal Information, that is entered in a record, by the Responsible Party, where it is domiciled in South Africa, or where it uses a Responsible Party, Operator or other entity, which is domiciled elsewhere, by using an automated or non-automated manner of collection situated in South Africa. POPIA therefore must be complied with by every employee of the Responsible Party, where they collect and process another's Personal Information.

7. Exclusions

POPIA does not affect the processing of Personal Information—

- > during a purely personal or household activity;
- > that has been deleted to the extent that it cannot be recovered;
- > by or for the State, if it involves national security, defense, public safety, or the prevention of crime;

- > for exclusively journalistic purposes, by media companies that are subject to a code of ethics that has safeguards for the protection of Personal Information;
- > by Cabinet, Provincial Executive Councils and Municipal Councils;
- > if it relates to the exercise of judicial functions;
- > if it has been specifically exempted from POPIA and the conditions of processing by the Regulator;
- > in cases where other legislation regulates the processing of that information in a manner that is more beneficial to the Data Subject.

8. The Responsible Party's obligations when it processes Personal Information of its Employees and Third Parties

The processing of Personal Information by the Responsible Party must strictly comply with the eight core processing conditions set out in POPIA. Of these eight core conditions, the following five provisions should always be complied with by the Responsible Party:

- > The Responsible Party must obtain approval to process Personal Information directly from the Data Subject, prior to such processing;
- > The Personal Information must be obtained directly from the Data Subject;
- > The Responsible Party must ensure that the Personal Information obtained is accurate and, on a regular basis, give the Data Subject an opportunity to rectify any inaccuracies;
- > The Responsible Party must safeguard the Personal Information and ensure that it does not fall into the wrong hands;
- > The Personal Information may only be used for as long as the purpose for which it was collected exists. Once this purpose expires, the Responsible Party must ensure that the Personal Information is permanently destroyed.

9. Direct Marketing

In line with a person's right to privacy, POPIA strictly controls how one can engage in direct marketing activities. POPIA provides that the Responsible Party cannot process Personal Information for the purposes of using it in direct marketing, unless—

- > the Data Subject is a customer or client of the Responsible Party, and the direct marketing is in respect of any related products or services which the Responsible Party had previously sold to the Data Subject, and the Data Subject had given the Responsible Party

express permission to use his or her Personal Information, for the purposes of such direct marketing; or

- > where not a customer or client of the Responsible Party, such Data Subject has given the Responsible Party express permission to use his or her Personal Information for the purposes of direct marketing; and
- > in both cases, the Data Subject is always given the option to opt out of such communication.

All such communications sent to the Data Subject must include the Responsible Party's identity, contact details and an opportunity to "opt out."

10. Information Officer

The Responsible Party should appoint an Information Officer, and one or more Deputy Information Officer, where required, to oversee compliance with POPIA.

An information officer must ensure that—

- > a compliance framework is developed, implemented and monitored;
- > adequate measures and standards exist to comply with the conditions for the lawful processing of Personal Information;
- > preliminary assessments are conducted;
- > a manual in compliance with the Promotion of Access to Information Act, 2000 and POPIA is developed, detailing—
 - the purpose of the processing;
 - a description of the categories of Data Subjects and of the information or categories of information relating thereto;
 - the recipients or categories of recipients to whom the Personal Information may be supplied;
 - the planned trans-border or cross-border flows of Personal Information;
 - a general description allowing preliminary assessment of the suitability of information security measures to be implemented and monitored by the Responsible Party;
- the manual referred to above is available—
 - on the website, of the Responsible Party; and
 - at the office or offices of the Responsible Party for public inspection during normal business hours of that Responsible Party.

- > internal measures are developed together with adequate systems to process requests for information or access thereto; and
- > ongoing awareness sessions are conducted regarding the provisions of POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Regulator.

The Information Officer, or a person designated by him or her, can upon request of any person, provide copies of the manual to that person upon payment of a fee determined by the Responsible Party, which may not be more than R 3.50 per page.

11. Effective Date of POPIA

There is a 12-month phase-in period from 1 July 2020 during which Responsible Parties will be required to develop systems and align their business processes and practices to comply with POPIA. The Responsible Party and its employees should take note of the various provisions and related obligations included in POPIA, and initiate the implementation of said provisions, where applicable, into its business processes, sooner rather than later. The Responsible Party and its employees should also take note of the consequences of any non-compliance with POPIA.

12. Investigation and Compliance Order

Any person who is affected by non-compliance of any of the provisions of POPIA, is referred to as the complainant.

The complainant may submit a complaint to the Regulator in writing, detailing the acts of non-compliance in respect of the information processing principles. If the Regulator finds the complaint to be valid, an investigation will be conducted.

There are certain instances in which the Regulator may decide not to take action. Some of these instances are listed below:

- > If the subject matter of the complaint is insignificant;
- > If a lengthy period has passed;
- > If a complaint is not serious, frustrating or is not made in good faith, or
- > If the person making the complaint has failed to use a complaints procedure under a code.

The Regulator may attempt to reach a settlement between the parties, or it can conduct a hearing, at which it can summon witnesses and receive evidence. The Regulator can also request a judge or magistrate for a warrant to enter and search premises. If the Regulator grants an order in favour of the complainant, it may serve a Responsible Party with an enforcement notice, requiring it to take certain steps.

13. Damages in the Civil Courts

A Data Subject, or the Regulator at the request of a Data Subject, may institute a civil action for damages against a Responsible Party for a breach of any provision of POPIA, relating to interference with the protection of Personal Information of a Data Subject. It does not matter whether there was intent or negligence on the part of the Responsible Party, or not.

14. POPIA Offences and Penalties

POPIA regulates how anyone who processes Personal Information must handle, keep and secure that information. If an individual or a Responsible Party processes Personal Information relating to a person, that individual or Responsible Party must comply with POPIA. Failure to comply with POPIA may lead to the imposition of certain penalties under POPIA.

15. Punishable Offences in terms of POPIA

The following offences are, if committed, punishable with either a fine (not exceeding R10 million), or imprisonment (for a period not exceeding 10 years), or both:

- > Obstruction of the Regulator;
- > Failure to comply with enforcement or information notices;
- > Offences by witnesses - Giving false evidence before the Regulator;
- > Unlawful acts by a Responsible Party in connection with information/usage;
- > Unlawful acts by third parties in connection with information/usage;
- > Any person who sells/offers to sell information obtained illegally;

- > Failure to notify the Regulator that processing is subject to prior authorisation;
- > Breach of confidentiality;
- > Obstruction of the execution of a warrant.

16. Compliance with POPIA

To ensure compliance with the provisions of POPIA, the Responsible Party and its employees should ensure that the following controls are implemented within the Responsible Party environment:

- > POPIA training and awareness sessions;
- > All employees must ensure that all processing is done in accordance with the provisions of POPIA and the eight core conditions of processing;
- > All Personal Information must only be used for the purpose that it has been collected for;
- > The Data Subject must be provided with the standard Responsible Party's POPIA Section 18 Consent document (Document 12 included in your CelaPOPI Toolkit);
- > All direct marketing activities must provide for an "opt in" procedure before engaged in;
- > The Responsible Party must ensure that where Personal Information is sent cross-border, adequate personal data protection measures, equivalent to those measures determined in POPIA, are in place in such countries, where the Data Subject has not given consent to such processing and transfer.

17. Information Regulator

POPIA creates an "Information Regulator," which is a supervisory body that consists of a chairperson and four other members. The Regulator, who is independent and subject only to the Constitution, is responsible for, amongst other things, promoting, monitoring and enforcing compliance with the provisions of POPIA on a national level.

The Regulator also has the power to investigate complaints, and to draft or approve category-specific or industry-specific codes of conduct.

Once a code of conduct has been created, it will regulate the Processing of Information within that category or industry. Failure to comply with a code will be considered a breach of the conditions for the lawful processing of Personal Information.

18. POPIA Regulations

The POPIA Regulations contain various prescribed forms that should be used. These include forms which may be used by the Data Subject to lodge an objection to processing of his/her/its Personal Information to the Responsible Party, who kept the Personal Information, to correct or delete such Personal Information and to submit a complaint to the applicable Regulator.

There is also a prescribed form setting out an application for the consent of a Data Subject for the Processing of Personal Information for direct marketing.

The Regulations also stipulate the obligations of the Information Officer, which include inter alia the following—

- > Ensuring a compliance framework and adequate measures at the Responsible Party, to comply with the conditions for the lawful Processing of Personal Information, and
- > Updating the Responsible Party's PAIA Manual, published in terms of the Promotion of Access to Information Act, to address various aspects of processing in terms of POPIA.

A private or public body which represents a class of bodies, industry, profession or occupation, may apply to the Regulator for codes of conduct to be issued, which stipulate a standard for POPIA compliance within that specific class, industry or profession.

The Regulations also set out the powers of the Regulator when conducting a pre-investigation and handling an investigation, in relation to allegations of interference with the protection of the Personal Information of a Data Subject.