DATA PROTECTION LAWS OF THE WORLD

South Africa

SOUTH AFRICA

Last modified 17 January 2024

LAW

The right to privacy is recognized as a fundamental human right in the Bill of Rights of the Constitution of the Republic of South Africa and is protected in terms of the Constitution and the common law. This right to privacy is not absolute and may be limited where it is reasonable and justifiable to do so.

The Protection of Personal Information Act 4 of 2013 (POPIA) came into effect on 1 July 2020 but was subject to a one year grace period which ended on 30 June 2021. POPIA specifically regulates the processing of personal information that is entered into a record pertaining to natural living persons as well as existing legal persons.

DEFINITIONS

Definition of personal data

"Personal information" is defined in POPIA as information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing, juristic person, including:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin; color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief; culture, language and birth of the person;
- Information relating to the education, medical, financial, criminal or employment history of the person;
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- The biometric information of the person;
- The personal opinions, views or preferences of the person;
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- The views or opinions of another individual about the person; and
- The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

POPIA applies to the processing of personal information entered in a record by or for a responsible party / data controller that is domiciled in South Africa and that makes use of automated or non-automated means to process the personal information. It would also apply if the responsible party is not domiciled in South Africa but makes use of automated or non-automated means in South Africa unless those means are used only to forward personal information through South Africa.

POPIA does not apply to the processing of personal information:

- In the course of a purely personal or household activity;

- That has been de-identified to the extent that it cannot be re-identified again;
- By or on behalf of the State with regard to national security, defense or public safety, or the prevention, investigation or proof of offenses; or for the purposes of the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information;
- For exclusively journalistic purposes by responsible parties who are subject to, by virtue of office, employment or profession, a code of ethics that provides adequate safeguards for the protection of personal information;
- Solely for the purposes of journalistic, literary or artistic expression to the extent that such exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression;
- By Cabinet and its committees, the Executive Council of a province and a Municipal Council of a municipality;
- For purposes relating to the judicial functions of a court referred to in section 166 of the Constitution; and
- Under circumstances that have been exempted from the application of the conditions for lawful processing by the Information Regulator in certain circumstances.

Definition of sensitive personal data

Special personal information is information concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information and criminal behavior (to the extent that such information relates to the alleged commission of an offense or any proceedings in respect of any offence allegedly committed, or the disposal of such proceedings).

Subject to certain prescribed exceptions, the processing of special personal information without the consent of the data subject is generally prohibited under POPIA.

NATIONAL DATA PROTECTION AUTHORITY

The Information Regulator has established an Enforcement Committee and initiates investigations into various possible violations of POPIA. There is scrutiny by the Information Regulator into security compromises including the establishment of a security compromise register. These activities are in line with the powers, duties and functions of the office of the Information Regulator which include providing education regarding the protection and processing of personal information; monitoring and enforcing compliance with the provisions of POPIA; consulting with interested parties and acting as mediator; receiving, investigating and attempting to resolve complaints; issuing enforcement notices and codes of conduct; and facilitating cross-border cooperation.

REGISTRATION

Data protection officers (referred to in POPIA as "**information officers**") must be registered with the Information Regulator.

Responsible parties are required to obtain prior authorization from the Information Regulator before processing personal information in certain circumstances prescribed in section 57 of POPIA, for example, where special personal information or personal information of children is transferred to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information and where information on criminal behavior or unlawful or objectionable conduct is processed on behalf of third parties. Prior authorization is also required when processing personal information for the purposes of credit reporting or when processing unique identifiers for a purpose other than the purpose for which it was originally collected and linking it with personal information processed by other third parties. Responsible parties are not otherwise required to register their processing of personal information.

The prior authorization requirements in POPIA came into effect on 1 February 2022. This means that all responsible parties (i.e. data controllers) that conduct processing activities that are subject to prior authorization need to submit an application for prior authorization and will need to cease such processing activities until such time as prior authorization is obtained.

DATA PROTECTION OFFICERS

Data protection officers (referred to in POPIA as "**information officers**") must be registered with the Information Regulator. The duties and responsibilities of a responsible party's information officer are set forth in POPIA and include encouraging and ensuring compliance with POPIA; dealing with any requests made to that responsible party in terms of POPIA; and working with

the Information Regulator in respect of investigations by the Information Regulator in relation to that responsible party. The Regulations to POPIA, among other things, further provide that the information officer must ensure that a compliance framework is developed, implemented, monitored and maintained, and that a personal information impact assessment is conducted to ensure that adequate measures and standards for the protection of personal information exist.

COLLECTION & PROCESSING

"Processing" of information is defined in POPIA as any operation or activity or any set of operations, whether or not by automatic means,concerning personal information, including:

- The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- Dissemination by means of transmission, distribution or making available in any other form; and
- Merging, linking, as well as blocking, degradation, erasure or destruction of information.

POPIA prescribes the following eight conditions for lawful processing of personal information:

- **Accountability**: The responsible party must comply with all the conditions for lawful processing.
- **Purpose specification**: Personal information must only be collected for a specific, explicitly defined lawful purpose related to a function or activity of the responsible party.
- **Processing limitation**: Processing must be justified on a ground recognized under POPIA (e.g. consent / legitimate interests of the data subject, responsible party or the third party to whom the information is supplied).
- **Further processing limitation**: Processing must be in accordance with or compatible with the purpose for which it was initially collected subject to limited exceptions.
- **Information quality**: Steps must be taken to ensure that the information is complete, accurate, not misleading and updated where necessary.
- **Openness**: Notification requirements must be complied with when collecting personal information.
- **Security safeguards**: Appropriate, reasonable technical and organizational measures must be implemented and maintained to prevent loss of, damage to or unauthorized destruction of or unlawful access to personal information.
- **Data subject participation**: Data subjects have the right to request details of the personal information that a responsible party holds about them and, in certain circumstances, request access to such information.

TRANSFER

POPIA caters for two scenarios relating to the transfer of personal information, namely where a responsible party in South Africa sends personal information to another country to be processed and where a responsible party in South Africa processes personal information that has been received from outside South Africa.

Receiving personal information from other countries

The requirements for the processing of personal information prescribed in POPIA will apply to any personal information processed in South Africa, irrespective of its origin.

Sending personal information to other countries for processing

A responsible party in South Africa may not transfer personal information to a third party in another country unless:

- The recipient is subject to a law, binding corporate rules or a binding agreement which:
    - Upholds principles for reasonable processing of the information that are substantially similar to the conditions contained in POPIA; and
    - Includes provisions that are substantially similar to those contained in POPIA relating to the further transfer of personal information from the recipient to third parties who are in another country;
- The data subject consents to the transfer;
- The transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject’s request; or

- The transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject’s request; or
- 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.

SECURITY

Section 19 of POPIA places an obligation on a responsible party to secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss, damage to, or unauthorised destruction of, and unlawful access to, personal information.

To comply with this obligation, the responsible party must take reasonable measures to do all of the following:

- Identify all reasonably foreseeable internal and external risks to personal information under its control;
- Establish and maintain appropriate safeguards against the risks identified;
- Regularly verify that the safeguards are effectively implemented; and
- Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

The responsible party must also have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

BREACH NOTIFICATION

In terms of section 22 of POPIA, where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorized person, the responsible party must notify the Information Regulator and the data subject, unless the identity of such data subject cannot be established.

The notification must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party’s information system.

The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offenses or the Information Regulator determines that notification will impede a criminal investigation by the public body concerned and must be in writing and communicated to the data subject in a prescribed manner.

The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including all of the following:

- A description of the possible consequences of the security compromise;
- A description of the measures that the responsible party intends to take or has taken to address the security compromise;
- A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
- If known to the responsible party, the identity of the unauthorized person who may have accessed or acquired the personal information.

The Information Regulator may direct a responsible party to publicize, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Information Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

An operator / data processor is not required to notify the Information Regulator or data subjects where there are reasonable grounds to believe that there has been a data breach. It must, however, notify the responsible party / data controller of the suspected data breach.

ENFORCEMENT

Any person may submit a complaint to the Information Regulator alleging non-compliance with POPIA. The Information Regulator may also initiate an investigation into interference with the protection of personal information.

Upon receipt of a complaint, the Information Regulator may, inter alia, conduct a pre-investigation or full investigation of the complaint, act as conciliator, refer the complaint to another regulatory body if the Information Regulator considers that the complaint falls more properly within the jurisdiction of the other regulatory body, or decide to take no further action.

The Information Regulator's powers, for purposes of investigating a complaint include the power to summons and enforce the appearance of persons before the Information Regulator to give evidence or produce records or things; enter and search the premises occupied by a responsible party; and conduct interviews and inquiries.

If the Information Regulator is satisfied that a responsible party has interfered or is interfering with the protection of the personal information of a data subject it my issue an enforcement notice prescribing action to be taken by the responsible party to remedy the situation.

A responsible party who fails to comply with an enforcement notice is guilty of an offense and is, liable, on conviction, to a fine or imprisonment (or both) for a period of no longer than ten years (in terms of section 107), or alternatively to an administrative fine (in terms of section 109). Currently, the maximum fine under sections 107 and 109 of POPIA is R10 million.

Section 99 also makes provision for a civil action for damages resulting from non-compliance with POPIA. In order to succeed in such a claim the complainant would need to prove all the elements of a delict: wrongful conduct, causation, fault (intent / negligence) and harm. The data subject would need to prove the quantum of the damages that s/he seeks.

ELECTRONIC MARKETING

Direct marketing by means of unsolicited electronic communications is regulated by POPIA whereby the opt-in regime has taken effect. Accordingly, under POPIA, the processing of a data subject's personal information for the purposes of direct marketing by means of unsolicited electronic communications is prohibited unless the data subject has given its consent, or the email recipient is an existing customer of the responsible party. A responsible party may only approach a data subject once in order for the data subject to opt in to receive marketing information. The Regulations to POPIA contain a prescribed form to be used when seeking this opt-in.

When sending emails to a data subject who is an existing customer:

a. the responsible party must have obtained the details of the data subject through a sale of a product or service;
b. the marketing should relate to its own similar products or services; and
c. the data subject must have been given a reasonable opportunity to opt out, free of charge, of the use of its personal information for marketing when such information was collected and on each occasion that marketing information is sent to the data subject, if the data subject has not initially refused the use of the personal information for electronic marketing purposes.

Direct marketing that is not by electronic communications (i.e. telephone or in-person marketing) continues to be regulated by the Consumer Protection Act, which requires the consumer to have an opportunity to opt out of receiving direct marketing.

ONLINE PRIVACY

There are no sections of POPIA that expressly regulate privacy in relation to cookies and location data. These issues may be dealt with in subsequent regulations or codes of conduct to be issued by the Information Regulator.

KEY CONTACTS

DLA Piper

Monique Jefferson
Director
T +27 11 302 0853
monique.jefferson@dlapiper.com

Justine Katz
Associate
T +27 (0)11 302 0846
justine.katz@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.