FACTSHEET: SOUTH AFRICA

Last updated: 30 September 2019
Prepared by Justin Bryant

FAST FACTS

Population: 57,725,600
Capitals: Pretoria (executive), Bloemfontein (judicial), Cape Town (legislative)
President: Cyril Ramaphosa
2019 Freedom House Score: 79/100
Data protection law? Exists, partially enforced

LAW

Section 14 of the Constitution of South Africa establishes privacy as a fundamental human and the right to privacy is protected under the common law.

The Protection of Personal Information Act (POPIA) was signed in 2013 and provides clarity around the rights of South Africans regarding their personal information. Only limited sections of POPIA have come into force, and organisations are not yet required to comply. POPIA, in its entirety, was expected to come into force in 2019, but this may be delayed. Once POPIA comes into force, organisations will have a one-year grace period to become compliant with its regulations.

Under POPIA, the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information. This includes the right to be notified of the collection of one's information, and to be informed of unauthorised access to personal information by an unauthorised party.

Other rights held by data subjects include rights to:

- establish whether personal information is held by a responsible party, and request access to such information;
- request that if necessary, their personal information be deleted, corrected or destroyed;
- object to the processing of their personal information, provided that such objection is reasonable, unless the data subject was allowed to object free of charge, and failed to do so upon the initial collection of the data;
- object to the processing of personal information for direct marketing purposes at any time, unless the data subject gave their consent and is a customer of the responsible party;
- not have their personal information processed by means of unsolicited electronic communications;
- submit a complaint to the Information Regulator regarding alleged interference with their personal information; and
- institute civil proceedings in relation to the alleged interference with the protection of their personal information.

PERSONAL DATA

Personal information includes information relating to an identifiable, living, natural person, and in particular instances to juristic persons (social entities or communities that bear the same rights and legal obligations as a natural person). Personal information includes, but is not limited to:

- information relating to gender, sex, pregnancy, marital status, and nationality;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;
- personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly private and would reveal the contents of the original correspondence;
- 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.

The following types of information constitute *special personal information* and certain conditions must be met for their processing to be lawful:

- religious or philosophical beliefs;
- race or ethnic origin;
- political persuasion or trade union membership;
- health or sex life;
- biometric information; and
- criminal behaviour.

COLLECTION AND PROCESSING

There are eight conditions required for the lawful processing of personal information by or on behalf of a responsible party:

1. **Accountability**
    - The responsible party must ensure that the conditions for lawful processing are satisfied.
2. **Processing limitation**
    - Processing must be conducted lawfully, for necessary and not excessive purposes, in a manner that protects the legitimate interests of the data subject and does not infringe on their rights.
    - Personal information may only be processed with the consent of the data subject (or competent person where the subject is a minor). Such consent is revocable at any time, and at such point, the responsible party must cease processing the information.
    - Generally, personal information must be obtained directly from the data subject unless an exception applies.
3. **Purpose specification**
    - Personal information must be collected for a specific, explicitly defined, lawful purpose related to a particular function or activity of the responsible party. In most circumstances, the responsible party must act to ensure the data subject is aware of this purpose.

- Personal information may not be retained for any longer than is necessary to achieve the purpose for which it was collected, barring certain exceptions.

4. **Further processing limitation**
   - Further processing of personal information must be compatible with the original purpose for which it was collected, as determined by factors such as the nature of the information concerned, possible consequences of further processing on the data subject, the manner in which the information was collected, and contractual rights and obligations existing between parties.
5. **Information quality**
   - The responsible party must take reasonably practicable measures to ensure that the personal information provided is accurate, complete and not misleading. The purpose for which the personal information is collected or further processed determines what is reasonably practical under the circumstances.
6. **Openness**
   - The responsible party must keep documentation of all processing operations and notify the data subject when collecting personal information, barring certain exceptions.
7. **Security safeguards**
   - The responsible party is required to safeguard the integrity and confidentiality of personal information in its possession and / or under its control by taking the appropriate, reasonable technical and organisational measures to prevent loss, damage or unauthorised destruction. Necessary measures are also to be taken to prevent unlawful access to or processing of personal information.
8. **Data subject participation**
   - The responsible party must allow data subjects to exercise their rights under POPIA regarding their personal data.

REGISTRATION AND ENFORCEMENT

POPIA established the Office of the Information Regulator (Information Regulator), comprised of a Chairperson and additional members. Its functions include providing education on protection and processing of personal information; monitoring and enforcing POPIA compliance; consulting and mediating; investigating and resolving complaints; issuing enforcement notices; and facilitating cross-border cooperation.

The body will announce the date at which the law will take effect and enforce the relevant provisions thereafter. Public and private bodies who process personal information are expected to designate an information officer (and if necessary, deputy information officers) and register them with the Information Regulator. These individuals will deal with requests made to the responsible party regarding POPIA and assist the Information Regulator during the course of investigations related to the responsible party.

Responsible parties must obtain prior authorisation from the Regulator to:

- process and transfer special personal information;
- process unique identifiers for purposes other than initially specified;
- process information for the purposes of credit reporting; or
- transfer the personal information of children to a third party in a foreign country that does not offer adequate protection.

CROSS-BORDER TRANSFER

Transferring the personal information of a data subject outside of South Africa to a third party located in a foreign country is prohibited unless the following can be shown:

- the third party who is receiving of the information is subject to a set of legal rules or regulations that provide an adequate level of protection;
- the data subject consents to the transfer;
- the transfer of such information is necessary for the performance of a contract between the responsible party and data subject, or for other pre-contractual measures taken in response to a request made by the data subject;
- the transfer is required for the conclusion or performance of a contract concluded in the interest of the data subject, between the responsible party and third party; or
- the transfer is to the benefit of the data subject and it is not reasonably possible to obtain the consent of the data subject, and it is highly likely that consent would be given if it were possible to obtain.

SECURITY AND BREACH PROTOCOL

In the event that the personal information of a data subject is believed to have been accessed or acquired by any unauthorised person, the responsible party must notify the Information Regulator and the data subject if they can be identified. Notification is to occur as soon as reasonably possible after the discovery of the data breach.

Delayed notification to the data subject is only permitted if a public body determines that notification will impede a criminal investigation. The notification to a data subject must be in writing and sufficiently informative. The Information Regulator may direct a responsible party to publicise a breach of personal information if it is of the view that doing so will protect data subjects.

Read the legal notice and terms of use for this factsheet.