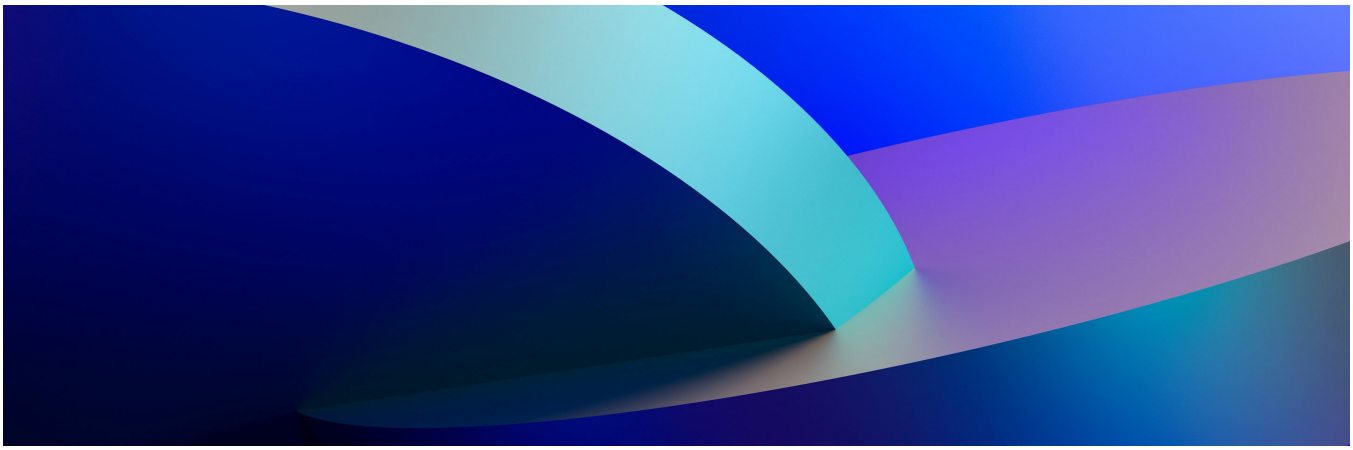

Data protection and cybersecurity laws in South Africa

Data protection

1. Local data protection laws and scope

The Protection of Personal Information Act 4 of 2013 (“POPI”). It is a comprehensive piece of data protection legislation that is comparable to the GDPR.

POPI came into effect on 1 July 2020. Businesses must ensure POPI compliance by no later than 30 June 2021.

POPI applies to the processing of personal information entered into a record by or for a responsible party (referred to as a data controller in the GDPR) by making use of automated or non-automated means, where the responsible party is domiciled in South Africa.

If not domiciled in South Africa, POPI applies if that responsible party makes use of automated or non-automated means in South Africa (unless those means are used only to forward personal information through South Africa).

‘Automated means’ is defined as any equipment capable of operating automatically in response to instructions given for the purpose of processing information.

‘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.

2. Data protection authority

Information Regulator (South Africa)

3. Anticipated changes to local laws

There are no anticipated changes.

4. Sanctions & non-compliance

Non-compliance with POPI may result in complaints, Information Regulator audits and/or orders, administrative fines as well as civil and/or criminal proceedings.

Administrative sanctions:

The Information Regulator may deliver an infringement notice to a responsible party alleged to have committed an offence.

The infringement notice will specify the amount of the administrative fine payable. This may not exceed ZAR 10m.

Factors that will be considered when determining an appropriate fine include:

- the nature of the personal information involved;
- the duration and extent of the contravention;
- the number of data subjects affected or potentially affected by the contravention;
- the likelihood of substantial damage or distress;
- whether the responsible party or a third party could have prevented the contravention from occurring; and
- whether the responsible party has previously committed an offence in terms of POPI.

Criminal sanctions:

This will depend on the nature of the specific offence. Generally, a person convicted of an offence may be held liable to a fine or to imprisonment for period of up to ten years, or to both a fine and imprisonment.

Others:

A data subject or the Information Regulator (at the request of the data subject), may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of POPI. A court hearing the proceedings may award an amount that is just and equitable.

5. Registration / notification / authorisation

Registration

Businesses are required to register their respective Information Officers (referred to as Data Protection Officers in the GDPR).

Notification

Generally, there is no obligation to notify the Information Regulator of each and every data processing activity. However, there are certain instances when prior authorisation may be required to be obtained from the Information Regulator for certain processing activity.

Authorisation

Processing of special personal information

There is a general prohibition on the processing of special personal information. This information includes:

- 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 to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

POPI contains a general authorisation in terms of which the prohibition on processing special personal information does not apply. These are instances where the:

- processing is carried out with the data subject's consent;
- processing is necessary for the establishment, exercise or defence of a right or obligation in law;
- processing is necessary to comply with an obligation of international public law;
- processing is for historical, statistical or research purposes subject to certain requirements being met;
- information has deliberately been made public by the data subject; or
- the provisions of sections 28 to 33 of POPI (as may be applicable) are complied with.

The Information Regulator may also (upon application by a responsible party) authorise a responsible party to process special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject.

Processing of personal information of children

There is a general prohibition on the processing of personal information concerning a child.
However, there is general authorisation on processing the personal information of children in terms of which the aforementioned prohibition on processing personal information of children does not apply. These are instances where the processing is:

- carried out with the prior consent of a competent person;
- necessary for the establishment, exercise or defence of a right or obligation in law;
- necessary to comply with an obligation of international public law;
- for historical, statistical or research purposes subject to certain requirements being met; or
- of personal information which has deliberately been made public by the child with the consent of a competent person.

The Information Regulator may (upon application by a responsible party) authorise a responsible party to process the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information the child.

Prior authorisation

A responsible party is required to obtain prior authorisation from the Information Regulator prior to any processing, if that responsible party plans to:

- process any unique identifiers of data subjects: (i) for a purpose other than the one for which the identifier was specifically intended at collection; and (ii) with the aim of linking the information together with information processed by other responsible parties;
- process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;
- process information for the purposes of credit reporting; or
- transfer special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

A responsible party is required to notify the Information Regulator if the processing of any personal information is subject to prior authorisation.

6. Main obligations and processing requirements

There are eight conditions for the lawful processing of personal information.

Accountability

- The conditions for the lawful processing of personal information must be met.

Processing limitation

- Processing must be done in a reasonable and lawful manner that does not infringe the privacy of a data subject.
- Processing must be adequate, relevant and not excessive.
- Personal information may only be processed if:
  - the data subject has consented;
  - processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;
  - processing complies with an obligation imposed by law;
  - processing protects the legitimate interest of the 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 interests of the responsible party or of a third party to whom the information is supplied.
- Personal information must be collected directly from the data subject. However, there are certain exceptions to this.

Purpose specification

- Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party;
- Records of personal information must not be retained any longer than is necessary for achieving the purpose for which it was collected or subsequently processed. However, there are certain exceptions to this.

Further processing limitation

- Further processing must be in accordance or compatible with the purpose for which the personal information was initially collected.

Information quality

- Reasonably practicable steps must be taken to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

Openness

- Documentation of all processing operations must be maintained.
- Reasonably practicable steps must be taken to notify a data subject of, amongst others, the information being collected (or the source, if not collected from the data subject), the purpose for collection, the name and address of the responsible party, whether the supply of the information is voluntary or mandatory, and the consequences of a failure to provide the information.

Security safeguards

- Appropriate, reasonable technical and organisational measures must be taken to prevent loss of, damage to or unauthorised destruction of personal information, and unlawful access to or processing of personal information.

Data subject participation

- A data subject has the right to, amongst others, request confirmation of whether or not the responsible party holds his, her or its personal information as well as the record or a description of the personal information that is held;
- A data subject has a right to request (in certain instances) the correction and/or deletion of the

data subject's personal information.

7. Data subject rights

- Right to have personal information processed in accordance with the conditions for the lawful processing of personal information;
- Right to be notified regarding collection or unauthorised acquisition/access;
- Right of access by the data subject;
- Right to rectification or erasure;
- Right to object to processing;
- Right to object to processing for purposes of direct marketing;
- Right not to have personal information processed for purposes of direct marketing by means of unsolicited electronic communications except when consent is given or data subject is a customer of the responsible party (subject to certain requirements being met);
- Right not to be subject to a decision based solely on automated processing, including profiling;
- Right to submit a complaint to the Information Regulator;
- Right to institute civil proceedings regarding alleged interference with the protection of personal information.

8. Processing by third parties

An operator (referred to as a data processor in the GDPR), or anyone processing personal information on behalf of a responsible party or an operator, is required to process such information only with the knowledge or authorisation of the responsible party.

They are also required to treat personal information which comes to their knowledge as confidential and not disclose it, unless required by law or in the course of the proper performance of their duties.

A written contract between the responsible party and the operator is required to be entered into to ensure that the operator establishes and maintains the security measures required in terms of POPI.

The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

An operator is defined in POPI as a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the director authority of that party.

9. Transfers out of country

A responsible party may not transfer personal information about a data subject to a third party who is in a foreign country unless one or more of the following conditions apply:

- that third party is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection that:
  - upholds principles for reasonable processing that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject; and
  - includes provisions that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;
- 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;
- 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 data subject's consent; and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

10. Data Protection Officer

The Data Protection Officer is referred to as an Information Officer in POPI.

The Information Officer has responsibilities in terms of both POPI and the Promotion of Access to Information Act No 2 of 2000 ("**PAIA**").

The Information Officer of a juristic person that is a private body is the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or a person acting as such (or any person duly authorised by such acting person).

Information Officers are required to be registered with the Information Regulator.

The Information Officer's duties and responsibilities include:

- the encouragement of compliance with the conditions for the lawful processing of personal information;
- dealing with requests made to the organisation pursuant to POPI;
- working with the Information Regulator in relation to investigations conducted in relation to the organisation;
- ensuring compliance by the organisation with the provisions of POPI; and
- as may be prescribed.

11. Security

The integrity and confidentiality of personal information is required to be secured by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information.

These measures include:

- identifying all reasonably foreseeable internal and external risks;
- establishing and maintaining appropriate safeguards against the risks identified;
- regularly verifying that the safeguards are effectively implemented; and
- ensuring that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

Due regard must be given to generally accepted information security practices and procedures which may apply to a responsible party generally or be required in terms of specific industry or professional rules and regulations.

12. Breach notification

A responsible party is required to notify the Information Regulator and the data subject (unless the identity of the data subject cannot be established) when there are reasonable grounds to believe that the personal data of that data subject has been accessed or acquired by any unauthorised person.

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.

13. Direct marketing

The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or email is prohibited unless the data subject has consented; or is a customer of the responsible party.

Personal information of a data subject who is a customer of the responsible party may only be processed:

- if the contact details of the data subject are obtained in the context of the sale of a product or service;
- for the purpose of direct marketing of the responsible party's own similar products or services; and
- if the data subject has been given a reasonable opportunity to object to such use of his, her or its electronic details at the time when the information was collected; and on the occasion of each communication with the data subject for the purpose of marketing (if the data subject has not initially refused such use).

14. Cookies and adtech

POPI does not specifically mention cookies. However, to the extent that cookies collect personal information, the requirements regarding the processing of personal information in POPI need to be complied with.

Generally, organisations must:

- notify users that cookies are used;
- explain what the cookies are used for and why;
- get the user's consent to store a cookie on their device unless the cookie is strictly necessary (essential) for the operation of the organisation's website.

15. Risk scale

Severe.

16. Useful links

- Overview of POPI: https://popia.co.za/
- Information Regulator: https://www.justice.gov.za/inforeg/

Cybersecurity

1. Local cybersecurity laws and scope

There is currently no dedicated cybersecurity statute in South Africa. Provisions relating to cybersecurity are fragmented and found in various pieces of legislation.

The Electronic Communications and Transactions Act No 25 of 2002 ("**ECTA**") contains several provisions specifically addressing cybercrime.

The Regulation of Interception of Communications and Provision of Communication-related Information Act No 70 of 2002 ("**RICA**") is aimed at, amongst others, regulating the interception of certain communications.

The Criminal Procedure Act No 51 of 1977 ("**CPA**") contains provisions dealing with the investigation and prosecution of crimes (including cybercrimes) in South Africa.

POPI promotes the protection of personal information processed by public and private bodies and introduces certain conditions to establish minimum requirements for the processing of personal information. See “Data Protection” section above for full details of data protection laws.

2. Anticipated changes to local laws

The Cybercrimes Bill is one step away from becoming law, having been passed by the Parliament of South Africa on 2 December 2020. It is unclear at this stage when the president will sign this Bill.

The Cybercrimes Bill, once it becomes law, will be a comprehensive statute regulating cybercrime in South Africa. It contains comprehensive provisions addressing cybercrime and criminalises, amongst others, the following offences:

- unlawful access to data, a computer program, a computer data storage medium or a computer system (commonly known as ‘hacking’);
- unlawful interception of data;
- the unlawful and intentional use or possession of software and hardware tools that are used in the commission of cybercrimes;
- cyber fraud;
- cyber extortion;
- cyber forgery and uttering; and
- malicious communications. This is the distribution of data messages with the intention to incite the causing of damage to any property belonging to, or to incite violence against, or to threaten a person or group of persons, including the distribution of “revenge porn”.

The Cybercrimes Bill also contains provisions dealing with, amongst others, the investigation of cybercrimes, the provision of mutual assistance between States, as well as reporting obligations of electronica communications service providers and financial institutions.

3. Application

ECTA

ECTA applies in respect of any electronic transaction or data message. It criminalises, amongst others, the unauthorised access to, interception of or interference with data as well as computer related extortion, fraud and forgery.

RICA

RICA contains a general prohibition on the interception of direct and indirect communications. This prohibition is subject to certain exceptions which includes, amongst others, the interception of communication by a party to a communication, under an interception direction, with the consent of a party to a communication, in connection with carrying on a business, to prevent serious bodily harm or for the purposes of determining a location in the case of an emergency.

POPI

POPI applies to the processing of personal information entered into a record by or for a responsible party by making use of automated or non-automated means, where the responsible party is domiciled in South Africa. If not domiciled in South Africa, POPI applies if that responsible party makes use of automated or non-automated means in South Africa (unless those means are used only to forward personal information through South Africa).

4. Authority

POPI

Information Regulator (South Africa): https://www.justice.gov.za/inforeg/

5. Key obligations

RICA

Before a telecommunication service provider enters into a contract with any person for the provision of a telecommunication service to that person, he/she is required to obtain certain information (as detailed more fully in RICA) from that person and take steps to verify that information. The relevant telecommunication service provider is required to ensure that proper records of such information is kept.

An electronic communications service provider who provides mobile cellular electronic communications services may not activate a SIM card on its electronic communications system unless it implements a process to record and store and does record and store:

- the Mobile Subscriber Integrated Service Digital Network number (MSISDN number) of the SIM card that is to be activated;
- the full names and surname, identity number, country where the passport was issued (in the case of a non South African citizen) and at least one address of the person who requests that a SIM card be activated on that electronic communications service provider's electronic communication system;
- the full names, surname, identity number and an address of the authorised representative of a juristic person as well as the name and address of the juristic person (and, where applicable, the registration number of the juristic person), in the case of a juristic person.

The electronic communications service provider is required to verify the information collected. Furthermore, the electronic communications service provider must ensure that the information recorded and stored as well as the facility in or on which the information is recorded and stored, are secure and only accessible to persons specifically designated by that electronic communications service provider.

POPI

See "Data Protection" section above.

Cybercrimes Bill

When the Cybercrimes Bill becomes law, an electronic communications service provider or a financial institution that is aware or becomes aware that its computer system is involved in the commission of any of the cybercrime offences set out in the Cybercrimes Bill, will be required to report the offence to the South African Police Service without undue delay and, where feasible, not later than 72 hours after having become aware of the offence.

6. Sanctions & non-compliance

Administrative sanctions:

POPI

See "Data Protection" section above.

Criminal sanctions:

ECTA

This would ultimately depend on the nature of the offence and may include liability to a fine or

imprisonment for a period of up to five years.

RICA

This would ultimately depend on the nature of the offence and may include liability to a fine not exceeding ZAR 2m or to imprisonment for a period not exceeding ten years. In certain instances, in the case of a telecommunication service provider, liability may include a fine not exceeding ZAR 5m.

POPI

See “Data Protection” section above.

Others:

ECTA

Any person who has suffered damages as a result of a contravention of any of the provisions of ECTA may, depending on the circumstances of the case, institute a civil claim for damages suffered against the wrongful party.

RICA

Any person who has suffered damages as a result of a contravention of any of the provisions of RICA may, depending on the circumstances of the case, institute a civil claim for damages suffered against the wrongful party.

POPI

See “Data Protection” section above.

7. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?

The Electronic Communications Security - Computer Security Incident Response Team (**ECS_CSIRT**) serves as the South African Government Security Incident Response Team. Its core services are primarily offered to Organs of State, with the intention to create a single point of contact, where the constituency can obtain CSIRT services and receive assistance on cybersecurity issues.

The Cybersecurity Hub is South Africa’s National Computer Security Incident Response Team (**CSIRT**) and strives to make Cyberspace an environment where all residents of South Africa can safely communicate, socialise, and transact in confidence. It achieves this by working with stakeholders from government, the private sector, civil society and the public with a view to identifying and countering cybersecurity threats. It is mandated by the National Cybersecurity Policy Framework (NCPF) which was passed by Cabinet in March 2012.

8. National cybersecurity incident management structure

Yes, see above.

9. Other cybersecurity initiatives

The National Cybersecurity Advisory Council is mandated to:

- advise the Minister of Telecommunications and Postal Services on policy, legal and technical issues as well as other matters pertinent to cybersecurity in line with the Department’s roles and responsibilities as outlined in the NCPF, the establishment and operationalisation of the national Cybersecurity Hub and the alignment and adoption of standards in South Africa;
- promote and encourage coordinated public-private partnerships on issues regarding cybersecurity,

including threat and risk information in South Africa pursuant to building confidence and trust in the secure use of ICTs;
- develop an annual report on, amongst others, cybersecurity risk assessment measured against international best practices, measures available to promote the culture of cybersecurity, recommendations on how South Africa will enhance prevention and address threats and vulnerabilities; and
- investigate and report on other matters that may be referred to the Council by the Minister.

10. Useful links

- Cybersecurity Hub
- Information Regulator

Authors

Zaakir Mohamed
Director
left_cms