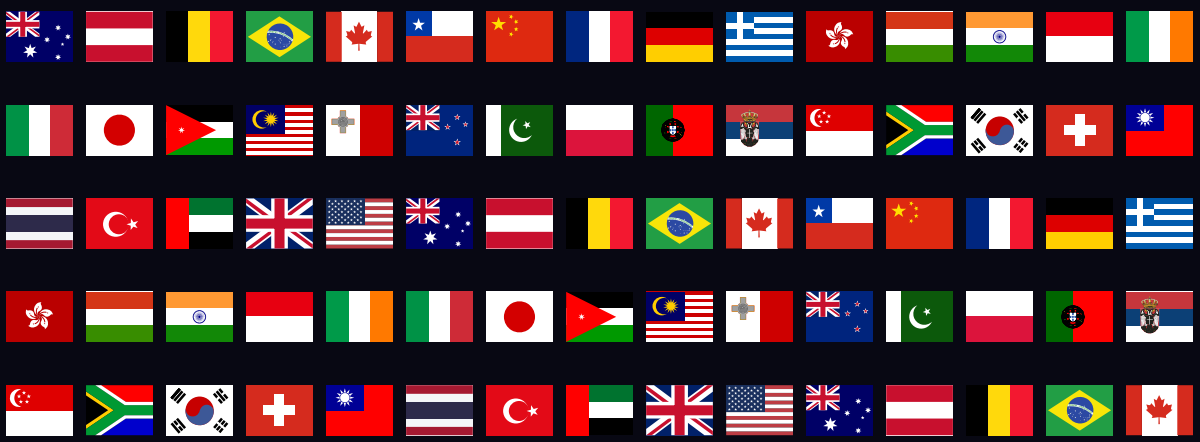
DATA PROTECTION & PRIVACY

South Africa



LEXOLOGY
Getting The Deal Through

Consulting editor
Hunton Andrews Kurth LLP

Data Protection & Privacy

Consulting editors

Aaron P Simpson, Lisa J Sotto

Hunton Andrews Kurth LLP

Quick reference guide enabling side-by-side comparison of local insights into the legislative framework; relevant authorities; treatment of breaches; legitimate processing; data handling responsibilities of PII owners; security obligations; internal controls, including the data protection officer; registration formalities transfer and disclosure of PII; rights of individuals; judicial supervision; specific data processing use cases such as cookies, electronic communications marketing, and cloud services; and recent trends.

Generated 17 July 2023

Table of contents

Contributors

South Africa

Dan Cooper
dcooper@cov.com
Covington & Burling LLP

Ben Haley
bhaley@cov.com
Covington & Burling LLP

Deon Govender
dgovender@cov.com
Covington & Burling LLP

Ahmed Mokdad
amokdad@cov.com
Covington & Burling LLP

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The Protection of Personal Information Act 2013 (POPIA) and the Regulations relating to POPIA (POPIA Regulations) are South Africa's primary data protection laws. POPIA is wide in its application and impacts all persons processing PI. Other key laws relating to privacy and data protection include:

- the Constitution of the Republic of South Africa, which guarantees the right to privacy.
- the Electronic Communications and Transactions Act 2002 (ECTA), which regulates the electronic collection of PI. The provisions of the ECTA pertaining to the protection of PI were repealed on 30 June 2021.
- the Consumer Protection Act 2008, which applies to the direct marketing of goods as well as services to consumers telephonically.
- the Cybercrimes Act 2020, which creates new offences that criminalise the theft and interference of data and impose sanctions that relate to cybercrime.
- the Promotion of Access to Information Act 2 of 2000 (PAIA), which regulates access to information and enables individuals to gain access to information held by both public and private bodies. PAIA also deals with the appointment of an information officer (the equivalent of a data protection officer in other jurisdictions) to manage the requirements to access information held by an organisation.

Law stated - 31 May 2023

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

POPIA provides for the establishment of the office of the Information Regulator , an independent supervisory authority established for the purpose of administering POPIA. In exercising its investigative powers, the Information Regulator may :

- summon and enforce the appearance of persons;
- compel the provision of written or oral evidence under oath;
- receive evidence irrespective of whether such evidence is admissible in a court of law; and
- enter and search any premises occupied by a responsible party (the equivalent of a controller in other jurisdictions); and
- where necessary apply to a judge of the High Court or a magistrate to issue a warrant to enable the Information Regulator to enter and search premises.

Law stated - 31 May 2023

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

POPIA provides that the Information Regulator is tasked with facilitating cross-border cooperation in the enforcement of privacy laws by participating in any initiative that is aimed at such cooperation.

Law stated - 31 May 2023

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Generally, an offence committed under POPIA could expose a responsible party to a maximum fine of 10 million South African rand, or to imprisonment for a period not exceeding 10 years, or both.

Law stated - 31 May 2023

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Responsible parties have a right to lodge an appeal with the High Court to set aside or vary a decision of the Information Regulator, namely, an enforcement notice. The Court must allow the appeal and may set aside or substitute the enforcement notice: (1) if it is not in accordance with the law; or (2) if it involved an exercise of discretion by the Information Regulator that ought to have been exercised differently.

The Court may review any determination of fact on which the enforcement notice was based.

Law stated - 31 May 2023

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

POPIA (section 6) does not apply to processing of PI by or on behalf of a public body where it involves national security or where its purpose is to prevent or detect unlawful activities.

The Information Regulator may, in terms of section 37(1) of POPIA and on application by a responsible party, grant an exemption from complying with a specific condition when processing PI, even if such processing is in breach of any of the conditions for the lawful processing of such information, or any measure that gives effect to such condition. The responsible party applying for an exemption must either satisfy the Information Regulator that (1) the processing is in the public interest; or (2) the processing involves a clear benefit to the data subject. In terms of section 37(2) of POPIA, public interest includes interests of national security; the prevention, detection and prosecution of offences; and important economic and financial interests of a public body. The Information Regulator has published a Guidance Note on Exemptions from the Conditions for Lawful Processing of Personal Information in terms of Section 37 and 38 of

POPIA , which includes the exemption application form to be completed by the responsible party.

Law stated - 31 May 2023

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Direct marketing by means of unsolicited electronic communications is regulated by POPIA (section 69). Processing of a data subject's PI for the purposes of direct marketing by means of unsolicited electronic communications is prohibited, unless the data subject has given his or her consent, or the recipient of the electronic marketing is an existing customer of the responsible party. The responsible party may only approach a data subject once in order for the data subject to opt in to receive marketing information. When sending electronic marketing to a data subject who is an existing customer: (1) the responsible party must have obtained the details of the data subject through the sale of a product or service; (2) the marketing should relate to its own similar products or services; and (3) the data subject must have been given a reasonable opportunity to opt out, free of charge, of the use of its PI 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 PI for electronic marketing purposes.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002 (RICA) generally regulates the interception of communications, the monitoring of radio signals and radio frequency spectra and the provision of communication-related information. In February 2021, the Constitutional Court of South Africa (CC) declared certain parts of RICA to be unconstitutional insofar as they fail to provide adequate safeguards to protect the right to privacy, freedom of expression, the rights of access to the courts, and legal privilege. The CC's order of invalidity has been suspended for a period of three years, during which time South Africa's parliament is expected to cure the various constitutional defects. RICA therefore remains in force during the period of suspension of the CC's order. However, notwithstanding the suspension of the order of invalidity, the CC has directed that RICA's provisions must be read in, to provide for post-surveillance notification as a default position.

Law stated - 31 May 2023

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

There are several sector-specific laws and regulations that include data protection provisions to be read in conjunction with POPIA. Most notable are those in the financial sector, which include:

- the Financial Advisory and Intermediary Services Act 2002;
- the Financial Advisory and Intermediary Services Act: General Code of Conduct for Authorised Financial Services Providers and their Representatives;
- the Financial Intelligence Centre Act 2001;
- the Financial Sector Regulation Act 2017; and
- the National Credit Act 2005.

Law stated - 31 May 2023

PI formats

What categories and types of PI are covered by the law?

PI is defined broadly in POPIA to include information relating to both an identifiable, living, natural person, and where applicable, an identifiable juristic person or legal entity, and include things such as information about a person's race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language, birth, education, medical, financial, criminal, or employment history, any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person, such as biometric information.

POPIA provides for a separate category of information called 'special personal information', which includes all information relating to a person's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information or criminal behaviour. POPIA also specifically regulates children's PI (ie, persons under the age of 18 years).

POPIA generally applies to the processing of PI entered in a 'record' by or for a responsible party. A record is defined broadly in POPIA to include any recorded information regardless of form or medium; in other words, both information recorded on physical materials and information produced, recorded or stored electronically.

Law stated - 31 May 2023

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

POPIA (section 3(1)) specifies that the responsible party must either be domiciled or use means in South Africa in order to fall under its scope; namely, POPIA applies where a responsible party is: (1) domiciled in South Africa; or (2) not domiciled in South Africa but makes use of automated or non-automated means in South Africa to process PI, unless those means are used only to forward PI through South Africa (eg, a responsible party outside of South Africa who processes PI in South Africa with the assistance of a third party local service provider).

For the purposes of section 3 of POPIA, 'automated means' means any equipment capable of operating automatically in response to instructions given for the purpose of processing information.

Law stated - 31 May 2023

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

POPIA does not apply to the processing of PI:

- in the course of a purely personal or household activity;
- that has been de-identified to the extent that it cannot be re-identified;
- by or on behalf of the state with regard to national security, defence or public safety, or the prevention, investigation or proof of offences, 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 PI;
- for exclusively journalistic purposes by responsible parties who are subject to, by virtue of office, employment, profession, or a code of ethics that provides adequate safeguards for the protection of PI;
- solely for the purposes 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 the Cabinet and its committees, the executive council of a province or 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.

POPIA does not directly address the rights and responsibilities of a responsible party and an operator (the equivalent of a processor in other jurisdictions). Instead, these are incorporated in the eight conditions for lawful processing, which allow for processing (including collection) of PI.

A responsible party retains ultimate accountability for an operator and must ensure that an operator or anyone processing PI on behalf of a responsible party:

- only does so with the knowledge or authorisation of a responsible party; and
- treats the PI that comes to their knowledge as confidential and will not disclose it, unless required by law or in the course of the proper performance of their duties.

A responsible party must ensure that it enters into a written agreement with each operator that a responsible party relies on to process PI on its behalf.

Law stated - 31 May 2023

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The Protection of Personal Information Act 2013 (POPIA) prescribes the following eight conditions for the lawful processing of PI by or for a responsible party:

- Accountability: A responsible party must ensure compliance with all the conditions under POPIA and is responsible for implementing such conditions.
- Processing limitation: Processing of PI must be undertaken lawfully and done in a reasonable manner.
- Purpose specification: PI must be collected for a specific, explicitly defined and lawful purpose relating to a responsible party's business.
- Further processing: Further processing of PI must be undertaken in accordance with, or be compatible with, the purpose for which the PI was originally collected.
- Information quality: A responsible party is required to take reasonably practicable steps to ensure that the PI it processes about a data subject is complete, accurate, not misleading and updated where necessary.
- Openness: This condition seeks to ensure transparency between a responsible party and a data subject.
- Security safeguards: A responsible party must secure the integrity of PI in its possession or under its control with

appropriate and reasonable technical and organisational measures.
- Data subject participation: A data subject, having provided adequate proof of identity, has the right to request a responsible party to confirm, free of charge, whether or not a responsible party holds PI about that particular data subject.

Law stated - 31 May 2023

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

POPIA provides for a separate category of information called 'special personal information', which includes all information relating to a person's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information or criminal behaviour. Processing of special PI is generally prohibited, unless:

- processing is necessary for the establishment, exercise, or defence of a right or obligation in law;
- processing is carried out with consent;
- processing is necessary to comply with an obligation of public international law;
- processing is for historical, statistical, or research purposes to the extent that:
  - it serves a public interest and processing is necessary for the purpose; or
  - getting consent is impossible or would involve a disproportionate effort;
- there is sufficient guarantee that processing would not adversely affect the privacy of a data subject to a disproportionate extent; and
- information is deliberately made public by a data subject.

POPIA also affords special protection to children's PI, placing a general prohibition on the processing of PI concerning a child, unless:

- it is carried out with the prior consent of a competent person (ie, the parent or guardian);
- it is necessary for the establishment, exercise or defence of a right or obligation in law;
- it is necessary to comply with an obligation of international public law;
- for historical, statistical or research purposes:
  - it serves a public interest and the processing is necessary for the purpose concerned or it appears to be impossible or would involve a disproportionate effort to ask for consent; and
  - sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent, or the PI has deliberately been made public by the child with the consent of a competent person.

Law stated - 31 May 2023

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

A responsible party must take reasonably practicable steps to notify a data subject (either before the PI is collected, or

as soon as reasonably practicable after collection) of:

- the information being collected and, where the information is not collected from a data subject, the source from which it is collected
- the name and address of a responsible party
- the purpose for which the information is being collected
- whether or not the supply of the information by that data subject is voluntary or mandatory
- the consequences of failure to provide the information
- any particular law authorising or requiring the collection of the information
- the fact that, where applicable, a responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation
- further information such as: (1) the recipient or category of recipients of the information (2) the nature or category of the information (3) the existence of the right of access to and the right to rectify the information collected (4) the existence of the right to object to the processing of PI and (5) the right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator.

Law stated - 31 May 2023

Exemptions from transparency obligations

When is notice not required?

It is not necessary for a responsible party to provide notice if:

- a data subject (or a competent person where a data subject is a child) has consented to the noncompliance with the notice requirement
- noncompliance would not prejudice the legitimate interests of a data subject
- noncompliance is necessary:
  - to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences
  - to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in the South African Revenue Service Act 1997
  - for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated or
  - in the interests of national security
- compliance would prejudice a lawful purpose of the collection
- compliance is not reasonably practicable in the circumstances of the particular case or
- the information will (1) not be used in a form in which a data subject may be identified or (2) be used for historical, statistical or research purposes.

Law stated - 31 May 2023

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

A responsible party is required to take reasonable steps to ensure that the PI it processes about a data subject is complete, accurate, not misleading and updated where necessary.

Law stated - 31 May 2023

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

PI may only be processed if (given the purpose for which it is processed) it is adequate, relevant, and not excessive.

Law stated - 31 May 2023

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Records of a data subject's PI should not be retained for any longer than is necessary for achieving the purpose for which the information was collected or processed, unless:

- retention of the record is required or authorised by law;
- a responsible party reasonably requires the record for lawful purposes related to its functions or activities;
- retention of the record is required by a contract between the parties thereto; or
- a data subject (or a competent person where a data subject is a child) has consented to the retention of the record.

Law stated - 31 May 2023

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

PI must be collected for a specific, explicitly defined and lawful purpose relating to a responsible party's business. A responsible party must obtain prior authorisation from the Information Regulator if it is processing or intends to process any 'unique identifiers' of a data subject for a purpose other than the one for which the identifier was specifically intended at collection, and with the aim of linking the information together with information processed by other responsible parties.

The Information Regulator's Guidance Note on Application for Prior Authorisation includes, among other things, practical guidance on the completion and submission of an application for prior authorisation.

Law stated - 31 May 2023

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The Protection of Personal Information Act 2013 prohibits automated processing of PI where a data subject will be subjected to a decision that has legal consequences for a data subject or that affects a data subject to a substantial degree, in other words, automated processing of PI intended to provide a profile of a data subject, including their

performance at work, credit worthiness, reliability, location, health, personal preferences or conduct.

Law stated - 31 May 2023

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Protection of Personal Information Act 2013 (POPIA) requires a responsible party to implement security safeguards that ensure PI collected is appropriately safeguarded against loss, destruction, or unlawful access. POPIA does not prescribe the exact requirements to be followed, instead referring to industry and internationally accepted principles. There is also a duty on a responsible party to ensure that an operator processing information on its behalf has and maintains security safeguards as required under POPIA, and to only process information of a responsible party with a responsible party's authorisation.

Law stated - 31 May 2023

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Data breach is not specifically defined in POPIA. POPIA describes a 'security compromise' or 'breach' as access to and acquisition of data of a data subject by an unauthorised person. There is no distinction between serious breaches and minor breaches.

POPIA requires a responsible party to notify the Information Regulator, and an affected data subject (except where it is not possible to identify them) of a compromise of PI should be notified as soon as it is discovered, or as soon as is reasonably possible. The Information Officer of a responsible party will be responsible for notifying the Information Regulator on behalf of the responsible party.

On 12 August 2022, the Information Regulator published guidelines on how the security compromise notification form to the Information Regulator must be completed. These guidelines provide a step-by-step guide as to the process to be followed by a responsible party.

The Cybercrimes Act 2020 requires electronic communications service providers and financial institutions to notify the South African Police Service if they become aware that their electronic communications service or electronic communications network has been involved in the commission of any category or class of offence listed in the Cybercrimes Act 2020, including unauthorised access of the data or PI within their possession.

Law stated - 31 May 2023

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

The Protection of Personal Information Act 2013 (POPIA) does not specifically address the implementation of internal controls or the implementation of a compliance programme. However, POPIA provides that any failure to carry out a risk assessment or a failure to operate good policies, procedures and practices to protect PI will be considered in determining an appropriate fine for non-compliance with POPIA.

Regulation 4(1)(b) of the POPIA Regulations also provides that, as part of the responsibilities of information officers, a personal information impact assessment (PIIA) must be performed to ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of PI.

Law stated - 31 May 2023

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

A data protection officer, known as an 'information officer' is appointed automatically in terms of the Promotion of Access to Information Act 2 of 2000 (PAIA) and POPIA. The default position is that the head of a private company (ie, the chief executive officer, the managing director, or an equivalent officer) is the information officer. PAIA allows the default information officer of a company to authorise any employee of the company as an information officer. Companies may also designate any number of deputy information officers as necessary. Each subsidiary of a group of companies should appoint and register its own information officer, and multinational companies based outside of South Africa must authorise a person within South Africa to act as their information officer.

POPIA provides that an information officer is responsible for:

- encouraging compliance with POPIA and the conditions for lawful processing;
- dealing with any requests made to the organisation;
- cooperating with the Information Regulator in respect of any investigation; and
- any other duties as may be prescribed.

The Information Regulator has issued a Guidance Note on Information Officers and Deputy Information Officers , which provides that the information officer is responsible for, among others, developing a policy or circular for implementing the conditions of lawful processing under POPIA among employees, and obtaining prior authorisation from the Information Regulator where required. Regulation 4 of the POPIA Regulations also requires the information officer to:

- develop, implement, monitor, and maintain a compliance framework;
- ensure personal impact assessments are conducted and that adequate measures exist for compliance;
- ensure adequacy of systems to process requests for information;
- ensure that internal awareness sessions are conducted; and
- develop, monitor, maintain, and make available a manual as prescribed in sections 14 and 51 of PAIA, and, upon request by any person, provide copies of the manual upon the payment of a fee determined by the Information Regulator.

An information officer does not need to meet any specific criteria or qualifications to be appointed information officer. However, the guidance note provides that only an employee of a company at a level of management and above should be considered for authorisation as an information officer of that company.

Law stated - 31 May 2023

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

POPIA provides that a responsible party must maintain documentation of all processing operations under its responsibility.

Law stated - 31 May 2023

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

POPIA Regulation 4(b) requires a responsible party to undertake a PIIA to ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of PI. A PIIA must:

- describe the nature, scope, context, and purposes of the processing;
- assess necessity, proportionality, and compliance measures;
- identify and assess risks to data subjects; and
- identify any additional measures to mitigate those risks and ensure compliance with the eight conditions for lawful processing.

Law stated - 31 May 2023

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

POPIA does not prescribe how PI processing systems must be designed.

Law stated - 31 May 2023

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

Responsible parties are required to register information officers with the Information Regulator before they can take up their duties in accordance with the Protection of Personal Information Act 2013 (POPIA). However, POPIA does not specifically prescribe any penalty for a failure to do so. Generally, non-compliance with POPIA could expose a responsible party to a maximum fine of 10 million South African rand, or to imprisonment for a period not exceeding 10 years, or both.

Law stated - 31 May 2023

Other transparency duties

Are there any other public transparency duties?

POPIA does not impose any public transparency obligations.

Law stated - 31 May 2023

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

A responsible party must enter into a written contract with an operator aimed at ensuring that an operator that processes PI for a responsible party establishes and maintains the security measures as prescribed under the Protection of Personal Information Act 2013 (POPIA).

POPIA does not prescribe any specific contractual obligations between a responsible party and an operator. However, POPIA provides that an operator or anyone processing PI on behalf of a responsible party or an operator, must, unless required by law or in the course of the proper performance of their duties:

- process such information only with the knowledge or authorisation of a responsible party; and
- treat PI that comes to their knowledge as confidential and must not disclose it.

Law stated - 31 May 2023

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

It is an offence to share PI with or sell PI to third-party recipients that are not processors or service providers. A person found guilty of an such offence under POPIA is liable on conviction to a fine up to 10 million South African rand, or imprisonment for a period of no longer than 10 years, or both.

Law stated - 31 May 2023

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

POPIA generally prohibits the transfer of PI outside South Africa unless the transfer satisfies one or more of the following conditions:

- the recipient is subject to a law, binding corporate rules or binding agreement that provides an adequate level of protection that effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for lawful processing under POPIA;
- a data subject consents to the transfer;

- the transfer is necessary for the performance of a contract between a data subject and a responsible party, or for the implementation of pre-contractual measures taken in response to a data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of a data subject between a responsible party and a third party; or
- the transfer is for the benefit of a data subject, and it is not reasonably practicable to obtain the consent of a data subject to the transfer, but if it were, a data subject would be likely to give it.

POPIA (section 57 (1)(d)) provides that prior authorisation must be obtained from the Information Regulator where a responsible party intends to transfer special PI, or children's PI to a third party in a foreign country that does not provide an adequate level of protection for the processing of PI unless: (1) the recipient is subject to a law, binding corporate rules or binding agreement that provides an adequate level of protection that effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for lawful processing under POPIA; or (2) a data subject consents to the transfer.

Law stated - 31 May 2023

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Onward transfers outside of South Africa fall outside the scope of POPIA.

Law stated - 31 May 2023

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

POPIA does not include data localisation requirements.

Law stated - 31 May 2023

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

A data subject, having provided adequate proof of identity, has the right to request a responsible party to confirm, free of charge, whether or not that responsible party holds PI about that particular data subject. A data subject may also request a description of the PI, including information about third parties who have had access to the information, within a reasonable time and at a prescribed fee (if any). In addition, the information must be provided to a data subject in a reasonable manner and in a form that is generally understandable (ie, a physical copy, or in a readily accessible electronic form).

A responsible party may refuse a request on the grounds for refusal or access to records as set out in the Promotion of Access to Information Act 2 of 2000. Private bodies may refuse access to records where:

- the disclosure would involve the unreasonable disclosure of PI about a third party;
- the record contains trade secrets of a third party;
- the record contains confidential information of a third party; or
- the record contains legally privileged documents.

Law stated - 31 May 2023

Other rights

Do individuals have other substantive rights?

A data subject may also request a responsible party to correct, delete, or destroy PI about a data subject in its possession or under its control. The Protection of Personal Information Act 2013 (POPIA) allows a data subject the right to request that a responsible party correct or delete PI that is inaccurate, irrelevant, or excessive, or which a responsible party is no longer authorised to retain.

POPIA also specifically governs direct marketing activities via electronic communication. Generally, POPIA follows an opt-in approach whereby the direct marketer must obtain a data subject's consent before sending them a direct marking communication, and every subsequent direct marketing communication must include an opportunity for a data subject to opt out from receiving further marketing materials from the direct marketer.

Law stated - 31 May 2023

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

A data subject has the right to institute a civil action for damages in a court against a responsible party for breach of any provision of POPIA. Claims for damages under South African law are financial claims that are brought to compensate a plaintiff as a result of a loss-causing event that occurred because of the fault of the defendant. There are hurdles under South African law to any claim for non-pecuniary loss. Damages for mental distress, inconvenience or disappointment would be typified as non-pecuniary loss.

Law stated - 31 May 2023

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

A data subject may submit a complaint to the Information Regulator regarding an alleged interference with the protection of PI, or submit a complaint in respect of a determination of an adjudicator. A data subject may also institute civil proceedings in a court regarding the alleged interference with the protection of their PI.

Law stated - 31 May 2023

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

The Protection of Personal Information Act 2013 (POPIA) provides that the Information Regulator may, by notice in the Government Gazette, grant an exemption to a responsible party to process certain PI, even if that processing is in breach of a condition for the lawful processing of such information, or any measure that gives effect to such condition if the Information Regulator is satisfied that the requirements that are stated therein are met.

The Information Regulator has published a Guidance Note on Exemptions from the Conditions for Lawful Processing of Personal Information in terms of Section 37 and 38 of POPIA, which describes the process of submitting an exemption application.

Law stated - 31 May 2023

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

The Information Regulator has not yet issued any guidance regarding the regulation of cookies or similar technologies. The Protection of Personal Information Act 2013 (POPIA) requires a responsible party to notify a data subject when collecting personal information. This notification usually takes the form of a pop-up website notification on the collection of cookie identifiers.

POPIA also requires a responsible party to obtain prior authorisation from the Information Regulator in the case of processing any unique identifiers of a data subject for a purpose other than the one for which the identifier was specifically intended at collection, and with the aim of linking the information together with information processed by other responsible parties. Since cookie identifiers may constitute unique identifiers, a responsible party may in certain instances require prior authorisation to process cookie identifiers.

Law stated - 31 May 2023

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

Processing PI for the purposes of direct marketing is prohibited unless the data subject has given their consent or the recipient is a customer of the responsible party. The responsible party must have obtained the details of the data subject through sales of a product or service and the marketing should relate to similar products or services of the responsible party. The data subject must be given a reasonable opportunity to object to the use of his or her personal information for marketing each time the responsible party communicates with the data subject for marketing purposes.

Law stated - 31 May 2023

Targeted advertising

Are there any rules on targeted online advertising?

The Information Regulator has not yet issued any guidance regarding targeted online advertising.

Law stated - 31 May 2023

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

Processing of special PI is generally prohibited, unless:

- processing is necessary for the establishment, exercise, or defence of a right or obligation in law;
- processing is carried out with consent;
- processing is necessary to comply with an obligation of International Public Law;
- processing is for historical, statistical, or research purposes if it:
  - serves a public interest and processing is necessary for the purpose; or
  - getting consent is impossible or would involve a disproportionate effort;
- there is sufficient guarantee that processing would not adversely affect the privacy of a data subject to a disproportionate extent; and
- information is deliberately made public by a data subject.

Law stated - 31 May 2023

Profiling

Are there any rules regarding individual profiling?

POPIA prohibits automated processing of PI where a data subject will be subjected to a decision that has legal consequences for that data subject or that affects that data subject to a substantial degree; in other words, automated processing of PI intended to provide a profile of a data subject, including their performance at work, credit worthiness, reliability, location, health, personal preferences or conduct.

Law stated - 31 May 2023

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

South Africa has implemented a cloud and data framework (the Framework), which is set out in various legislative, regulatory and policy instruments. A key component of the Framework is the draft National Data and Cloud Policy , which was published in the Government Gazette on 1 April 2021 (the Draft Policy).

Save for the Draft Policy, all of the components of the Framework are in final form. The Draft Policy is yet to take effect.

Law stated - 31 May 2023

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

On 16 February 2023, the Information Regulator published draft rules on the Protection of Personal Information Act No. 4 of 2013 ('POPIA'): Rules of Procedure Relating To The Manner In Which A Complaint Or Any Matter In Terms Of The POPIA May Be Referred To And Considered For A Finding, And Recommendation By The Enforcement Committee, 2023 , for public comment. The draft rules indicate the Secretariat's duties and functions and the powers of the Enforcement Committee. The draft rules also detail, among other things, the following:

- the manner in which the Enforcement Committee should adjudicate a complaint, or any other matter referred to it;
- the types of matters that may be referred to the Enforcement Committee;
- the manner and the form in which a complaint or other matter may be referred to the Enforcement Committee;
- notification to the parties; and
- the manner in which the responsible party and data subject may make submissions to the Enforcement Committee.

On 5 April 2023, the Information Regulator published a report on the outcomes of complaints investigated under POPIA and the Promotion of Access to Information Act 2000 , noting that for the financial year 2022–2023: (1) the Promotion of Access to Information (PAIA) Division of the Information Regulator received over 309 complaints, of which 209 were resolved; and (2) the POPIA Division received 895 complaints during the reporting period, of which 616 were resolved. The report also includes details of the process for investigation of complaints.

On 9 May 2023, the Information Regulator published an announcement that it issued an Enforcement Notice to the Department of Justice and Constitutional Development (the Department) following a finding of the contravention of various sections of the POPIA. The Enforcement Notice orders the Department to take a number of corrective measures, and to institute disciplinary proceedings against the official(s) who failed to take the necessary steps to safeguard the Department against security compromises.

Law stated - 31 May 2023

Jurisdictions

Australia	Piper Alderman
Austria	Knyrim Trieb Rechtsanwälte
Belgium	Hunton Andrews Kurth LLP
Brazil	Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados
Canada	.
Chile	Magliona Abogados
China	Mayer Brown
France	Aramis Law Firm
Germany	Hoffmann Liebs Fritsch & Partner
Greece	GKP Law Firm
Hong Kong	Mayer Brown
Hungary	VJT & Partners
India	AP & Partners
Indonesia	SSEK Law Firm
Ireland	Walkers
Italy	ICT Legal Consulting
Japan	Nagashima Ohno & Tsunematsu
Jordan	Nsair & Partners - Lawyers
Malaysia	SKRINE
Malta	Fenech & Fenech Advocates
New Zealand	Anderson Lloyd
Pakistan	S.U.Khan Associates Corporate & Legal Consultants
Poland	Kobylanska Lewoszewski Mednis
Portugal	Morais Leitao Galvao Teles Soares da Silva and Associados
Serbia	BDK Advokati

South Africa	Covington & Burling LLP
South Korea	Bae, Kim & Lee LLC
Switzerland	Lenz & Staehelin
Taiwan	Formosa Transnational Attorneys at Law
Thailand	Formichella & Sritawat Attorneys at Law
Turkey	Turunç
United Arab Emirates	Bizilance Legal Consultants
United Kingdom	Hunton Andrews Kurth LLP
USA	Hunton Andrews Kurth LLP