RESPECT

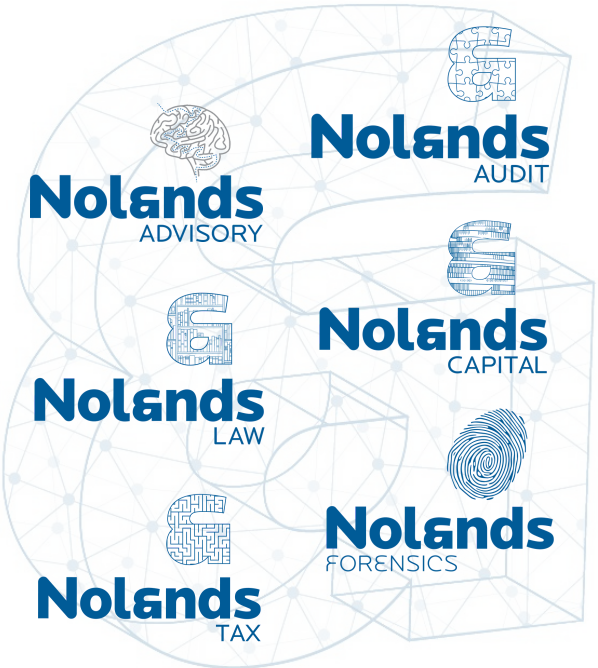
PROTECT

POPIA GUIDE 2021/22

Nolands
AUDIT • ADVISORY • LAW

Nolands

THE COMPANIES



INDEX

INTRODUCTION AND TERMINOLOGY

The Protection of Personal Information Act (no.4 of 2013) (hereinafter referred to as 'POPIA' or 'the Act'), which gives effect to the Constitutional right to privacy in South Africa, commenced on the 1st July 2020. It is compulsory for all public and private bodies (subject to some exclusions) who process personal information, to comply with the Act. This includes personal information about employees, customers, clients, and/or suppliers, collectively known as 'Data Subjects'.

In certain other countries, SME's are exempt from similar legislation, however in South Africa, this is not the case. It may be that in the future, SME's will be exempted by the Information Regulator. The correct use of terminology for the Act is very important. The Information Regulator has requested that everyone uses 'POPIA' when referring to the Act, and the term 'POPI' is rather to be used when referring to the action or process of protecting personal information. In order to comply with POPIA, public and private bodies or 'organisations' are required to implement a 'POPI' programme to ensure that the safety and privacy of the personal information for their 'Data Subjects' is protected.

Some important terms which are defined in the Act, and are vital to understand from the outset are:

- "processing" this is defined very broadly in the Act, and means any operation or activity (including automatic means) concerning personal information - and includes the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use, dissemination by means of transmission, distribution or making available in any other form or merging, linking, and restriction, degradation, erasure or destruction - of personal information.
- "personal information" is also defined very broadly in the Act, and includes a wide range of information that can be used to identify a Data Subject. It relates to information pertaining to an identifiable, living natural person, and where it is applicable, an identifiable existing juristic person, including (and not limited to) information relating to race, gender, sex, marital status, pregnancy, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health,

well-being, disability, religion, conscience, belief, culture, language and birth. It also includes information relating to the education, or the medical, financial, employment or criminal history of the person, any identifying number, all contact details, biometric information, 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, (including emails, reply to all, copy in etc.) 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 (such as his identity number), or if the disclosure of the name itself would reveal information about the person. Note that personal information is not limited to these categories, but can be any personal information which is used to identify the Data Subject.

GRACE AND IMPLEMENTATION

All organisations have a grace period, and will be required to be fully compliant with POPIA within 12 months of the commencement date, in other words, by the 1 July 2021. The Act applies retrospectively, which means that these bodies will need to ensure that they have been compliant as from the commencement date (1 July 2020). On the 18 June 2021, the Information Regulator announced that they are granting an extension on the application or processing as set out in Section 58(2) from 1 July 2021 to 1 February 2022.

PURPOSE AND OBJECTIVES

The purpose of the Act is, inter alia, to introduce measures that will ensure that the personal information processed by these organisations is done in a fair, transparent and secure manner. And that section 14 of the Constitution – the right to privacy - is upheld. This right to privacy is, however, subject to "justifiable limitations" - such as the access to information and the free flow of information within South Africa, and

across international borders. The right of access to information is given effect to in the Promotion of Access to Information Act (no.2 of 2000) (PAIA).

In a nutshell, the Act provides codes of conduct so that the processing of such personal information is regulated. This regulation is in place in order to prevent unsolicited electronic communications and automated decision making, as well as to regulate the flow of personal information. POPIA introduces certain conditions to establish minimum requirements for the lawful processing of such information, in order to, inter alia:

- protect the public from harm,
- stop people's money being stolen,
- stop people's identity being stolen, and
- generally to protect the right to privacy.

APPLICATION OF THE ACT

POPIA applies to most organisations in South Africa – both public and private, as follows:

A private body – being a:

- natural person (sole proprietor) who carries (or has carried) on any trade, business or profession, but only in such capacity.
- a partnership which carries (or has carried) on a trade, business or profession, or a former or existing juristic person (but excludes a public body) – in other words a private company, non-profit company, close corporation, or personal liability company.

A public body – being any department of state or administration in the national or provincial sphere of government, or any municipality in the local sphere of government. It also includes any other entity when exercising a power or performing a duty in terms of the Constitution (or provincial constitution), or when exercising or performing public power or function in terms of any legislation.

POPIA also will also apply to those organisations which are not domiciled in South Africa, yet which processes personal information within South African borders (for example, a call centre for an international organisation).

EXCLUSIONS FROM THE APPLICATION OF THE ACT

Certain exclusions from the application of the Act are allowed. These specific instances are, where information:

- Is processed in the course of a purely personal or household activity.
- Has been de-identified to the extent that it cannot be re-identified again (to de-identify personal information means to delete any information that specifically identifies the Data Subject, or can be used to identify the Data Subject, or can be linked by a reasonably foreseeable method to other information that identifies the Data Subject). For example anonymous information used for statistical reporting.
- Is processed by or on behalf of a public body which involves national security, e.g. in the identification of the financing of terrorist activities, defence or public safety, or in the prevention/detection of identifying the proceeds of unlawful activities, the combating of money laundering activities, or the investigation of offences, prosecution of offenders and the execution of sentences or security measures – but only to the extent that adequate safeguards for the protection of this personal information has been provided for in other legislation.
- Is processed by the Cabinet and its committees or Executive Council of a province.
- Is in relation to the judicial functions of a court in regard to section 166 of the Constitution (in other words, the Constitutional Court, the Supreme Court of Appeal, the High Court of South Africa, the Magistrates' Courts and any other court established or recognised in terms of an Act of Parliament, including any court of a status similar to either the High Court of South Africa or the Magistrates' Courts).

- Is processed for journalistic, literary or artistic expression – but only where it is necessary to reconcile the right of privacy vs the right to freedom of expression - as being in the public interest. And also where the Responsible Party (by virtue of office, employment or profession) - who processes such personal information for solely journalistic purposes - is subject to a code of ethics that provides adequate safeguards for the protection of personal information.

ROLE PLAYERS

The Information Regulator

This is an independent body established in terms of the Act. The Information Regulator is appointed by the President on the recommendation of the National Assembly and is answerable to the National Assembly. It exercises powers and performs duties in terms of both POPIA and the Promotion of Access to Information Act (no.2 of 2000). It is responsible for issuing of codes of conduct, and the monitoring and enforcement of compliance with the Act. The Information Regulator must be immediately advised by the Responsible Party in the event of a breach which resulted in personal information falling into the wrong hands.

The Responsible Party

This can be a natural or juristic person, who/which keeps personal information of Data Subject(s). The Act defines the Responsible Party as a public or private body or any other person which alone, or in conjunction with others, determines the purpose for processing information (the "why"), and the means for processing personal information (the "how" i.e. what information is processed and for how long and how it is processed). A Responsible Party could fall into the category of a profit company, a non-profit company, government, state agencies, a sole proprietor, a club or a school, or even an international organisation, who processes personal information within South Africa.

The Responsible Party can outsource the processing of the information function to an Operator, however, the Responsible Party will still determine the purpose for the processing and will still make all decisions in relation to the information. The

Operator acts in accordance with these decisions and on the instructions from the Responsible Party.

- **The Information Officer**

Usually the role of the Information Officer is, by default, assigned to the Chief Executive Officer, Managing Director or an equivalent officer of a private company, or the sole proprietor of a "trading as" entity. He is then entitled to delegate this role to someone else. The Information Officer needs to be identified and registered with the Information Regulator by the Responsible Party, before he can start performing his duties.

He is responsible for:

- Encouraging compliance within the organisation, to the conditions for the lawful processing of personal information as set out in the Act,
- Dealing with requests made in terms of the Act,
- Working with the Information Regulator, with regards to any investigations the Information Regulator may conduct in terms of Chapter 6 of the Act (which requires prior authorisation from the Information Regulator when processing certain information).

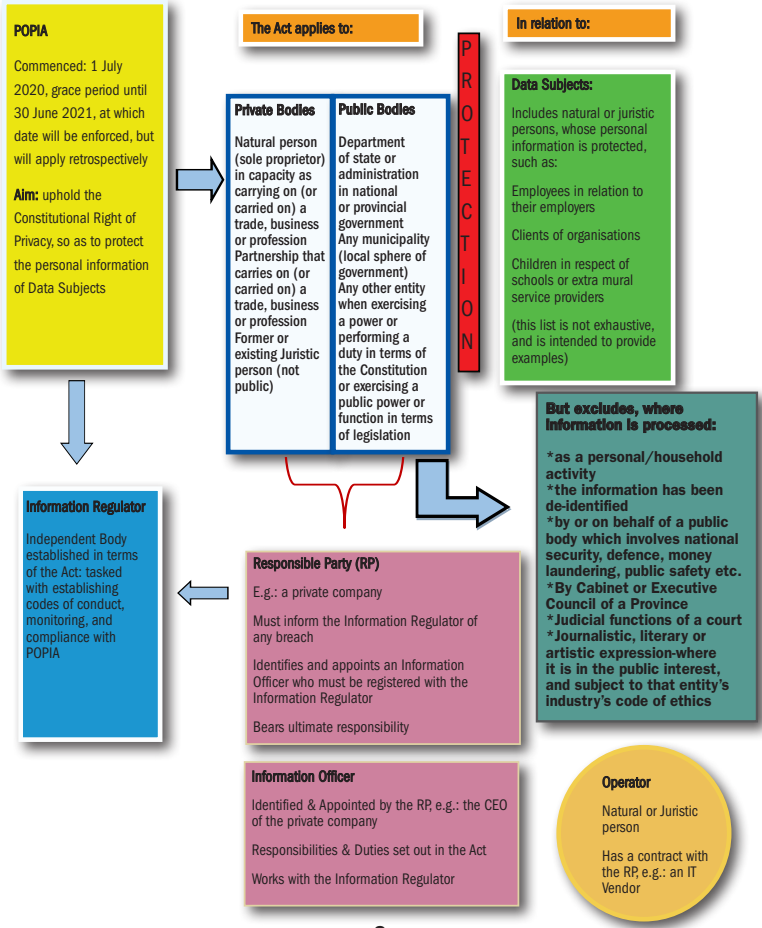
- **The Operator**

This is the person who processes personal information on behalf of the Responsible Party in terms of a contract or mandate, without coming under the direct authority of that party. It can be a natural person or a juristic person. An example would be an IT vendor, a Payroll Service Provider etc. The Operator must not process the information otherwise than in accordance with the Responsible Party's mandate or instructions.

- **The Data Subject**

The person to whom the information relates- this can be an indentifiable living natural person and/or identifiable existing juristic person or legal entity. Since the definition of Data Subject refers to the personal information of juristic entities, businesses are thus also able to enforce their data protection rights under POPIA.

An Illustration of the Role Players



PERSONAL INFORMATION

“Personal information” is defined very broadly in the Act, and includes a wide range of information that can be used to identify a Data Subject.

"Personal information" can be clarified even further, by dividing it into categories, as follows:

Personal Data (General)

This includes information about a person's:

- Age, colour, race, gender, sex, pregnancy, marital status, biometric information
- National, ethnic or social origin
- Sexual orientation, personal opinions, preferences or views of the Data Subject and/or the views or opinions of another person about the Data Subject
- Physical or mental health, wellbeing, disability
- Religion, conscience, belief, culture, language and birth
- Education, medical, financial, criminal or employment history
- Identifying number, symbol, email address, physical address, telephone number, location information, online identifier
- Correspondences sent by the Data Subject that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence
- 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.

Sensitive Data

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 (fingerprints or blood type)**
- **Criminal behaviour (that is alleged or any proceedings relating to any alleged offence of the Data Subject, or the disposal of such proceedings).**

The data of Children

POPIA also specifically regulates the personal information of a child, and there is an extra duty of care placed on the Responsible Party when it deals with the personal information of a child.

LAWFUL GATHERING AND PROCESSING OF PERSONAL INFORMATION (GENERAL)

- There are 8 general conditions for the lawful processing of personal information set out in the Act, which a Responsible Party must adhere to, as follows:

1. Accountability

- The Responsible Party has the responsibility of ensuring that these 8 conditions for lawful processing are met and adhered to.
- The Responsible Party must decide who will be tasked with this responsibility within the organisation, and that Policies and Procedures are put in place.

2. Processing limitation

- Personal information must be processed in a manner which does not infringe on the Data Subject's privacy, and which is only relevant to the defined purpose for which it has been collected.
- Only the minimal amount of information required for the purpose for which it is being gathered should be collected.

3. Purpose specification

- The purpose for collecting the information must be specific, explicit for a lawful purpose related to a function or activity of the Responsible Party. It must tie in with the Responsible Party's general business activities.
- The Data Subject has the right to know what information is in the Responsible Party's possession and for what purpose it was gathered.
- The personal information may only be used for the specific purpose for which it was gathered and thereafter it must be destroyed. This procedure should be covered in the POPIA Policies and Procedures Manual of the Responsible

Party, which should set out how the information is to be destroyed, which should also be in a manner that prevents its reconstruction.

- The Responsible Party is required to set a date that the information must be destroyed by.

4. Further processing limitation

- Further processing is to be compatible with the original purpose of collection.
- Personal information may not be processed for a secondary purpose - unless that processing is compatible with the original purpose.
- The Responsible Party will be required to obtain specific consent from the Data Subject in the event that it wishes to use his existing personal information for any other purpose other than what the information was initially gathered for.
- When gathering information, the Responsible Party is required to advise the Data Subject what the information will be used for, and for how long it will hold the information.

5. Information quality

- The Responsible Party must take reasonably practical steps to ensure that the personal information collected is complete, accurate, not misleading and updated where necessary.
- In most cases, the Responsible Party must obtain the information directly from the Data Subject, or send it to the Data Subject for validation. There are some instances where the Responsible Party may obtain the information from another source, for example where the information has already been made public by the Data Subject, or where the Data Subject has provided consent for the collection of the information from a third party.

- The Responsible Party must advise the Data Subject on how he can update his information or withdraw consent.

6. Openness

- The Data Subject must be made aware that the Responsible Party is collecting his or her personal information and for what purpose it will be used.
- A process needs to be in place for the gathering of this information and the process required to obtain consent (where applicable).
- Where consent is obtained, proof thereof must be retained to safeguard the Responsible Party against potential claims made by the Data Subject.
- Data Subjects must also, at the time the Responsible Party gathers the information, be advised of: the name and contact number of its Information Officer, as well as that of the Information Regulator. They must be advised of their rights to complain to the Information Regulator, should they wish to do so.
- The Data Subject should also be advised of their rights to access their information, and to object to the processing of their information.

7. Security Safeguards

- The integrity and confidentiality of the personal information must be secured (includes physical access controls, computer passwords, firewalls, encryption, backups of data, and anti-virus software).
- Security measures should be in place regarding information processed by the Operator or person acting under authority.
- The Responsible Party must ensure that there are strict policies and procedures in place to safeguard personal information (in both hard copy

and digital format).

- These policies and procedures should set out who has access, how access is gained (employees), and how an alert will arise when personal information is accessed or modified without authorisation.
- The Information Officer must ensure that there are processes in place to identify the source of a data breach and the procedure to follow to neutralise such a breach, and the processes to prevent the re-occurrence of a data breach.
- There also needs to be policies and procedures in place in regard to the Responsible Party's contractual arrangement with its Operator – there needs to be a written contract in place and the Responsible Party needs to ensure that the Operator establishes and maintains the required security measures.
- Procedures also need to be in place to inform the Data Subject when their personal information has been compromised, and the Information Regulator when there has been a security breach.

8. Data subject participation

- The Data Subject has certain access rights to its personal information (free of charge) including a right to request from the Responsible Party as to whether it (or a third party) is holding any of their personal information and its correction and/or deletion.
- The Information Officer must ensure that the process for providing access to information to a Data Subject is adhered to and followed (and that there are procedures and policies in place in this regard).
- The Data Subject has the right to withdraw consent at any time, and procedures should be in place to process such a withdrawal of consent.

*Note: these lists are not exhaustive, and are intended to provide the reader with examples of what is required by the Responsible Party when complying with each of the 8 general conditions.

PROCESSING OF SPECIAL PERSONAL INFORMATION

The processing of sensitive data is prohibited unless specific consent is provided by the Data Subject (or competent person on behalf of a child). Failure to obtain consent makes processing of this sensitive data strictly prohibited, **unless** it is necessary for the establishment, exercise or defence of a right or obligation in law, or is done for historical, statistical or research purposes to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned or it appears to be impossible to ask for consent and there are sufficient guarantees to ensure that the processing does not adversely affect the privacy of the Data Subject, or the information has been deliberately made public by the Data Subject.

For example, where special personal information is required to be processed in terms of the Basic Conditions of Employment Act (no.75 of 1997), or in terms of the Employment Equity Act (no. 55 of 1998) the information may be processed lawfully by the Responsible Party, in terms of the law as set out in that particular piece of legislation.

In addition, Sections 27 to 33 of the Act provide specific authorisations under certain circumstances for the processing of specific sensitive personal information of a Data Subject, as follows:

- **Section 27 - General:** This Section sets out the same requirements as those set out in Section 35 (where Section 35 specifically applies to children, this Section applies to all Data Subjects' sensitive data). A Responsible Party may make an application to the Information Regulator to authorise the processing of special personal information where such processing is deemed by the Information Officer to be in the public interest and subject to adequate safeguards.
- **Section 28 - Religious or philosophical beliefs:** Where the processing is carried out by spiritual or religious organisations regarding a Data Subject who belongs to the organisation, or it is necessary to do so to achieve its aims and principles. It would also apply to such Data Subjects' family members - if there is regular contact between the association and the family members in connection with its aims, and they have not objected in writing to the processing of their

data. However, personal information relating to a Data Subject's religious or philosophical beliefs may not be supplied to third parties without the consent of the Data Subject.

- **Section 29 - Race or ethnic origin:** The prohibition on processing this data without consent falls away where it is essential to process such information, in order to identify the Data Subject, and/or also where the information is used in order to comply with laws designed to protect and advance certain previously disadvantaged categories of persons (those who were subject to unfair discrimination).
- **Section 30 - Trade Union membership:** Where the data is processed by the Trade Union to which the Data Subject belongs, where the processing is necessary to achieve the aims of the Trade Union. No such information may be supplied to third parties by the Trade Union without the Data Subject's consent.
- **Section 31 - Political persuasion:** A political institution may process the personal information of its members or employees if: it is necessary to achieve the aims or principles of the institution, or if it is necessary to do so in order to form a political party, or the campaigning for a political party or cause, participating in activities of the political party or engaging in the recruitment of members for or canvassing of supporters etc. No personal information may be supplied to third parties without the consent of the Data Subject.
- **Section 32 - Health or sex life:** Inter alia medical professionals, healthcare institutions, social services may process this information if it is necessary for the proper treatment and care of the Data Subject. Insurance companies, medical schemes etc. may also if it is necessary to assess the risk to be insured or covered by the medical scheme and the Data Subject has not objected to the processing. Schools may also process medical information where it is necessary in order to provide special support for learners or making special arrangements in connection with their health or sex life, and any public or private body which is managing the care of a child if such processing is necessary for the performance of their lawful duties, and any public body if it is necessary in regard to the implementation of prison sentences or detention measures. Pension funds may process this information in regard to the implementation of pension regulations etc. This information may only be processed by Responsible

Parties who are subject to an obligation of confidentiality by virtue of their office, employment, profession or legal provision or by virtue of a written agreement between the Responsible Party and the Data Subject. Personal information concerning a Data Subject's inherited characteristics may not be processed unless a serious medical interest prevails or the processing is necessary for historical, statistical or research activity.

- **Section 33 - Criminal behaviour or biometric information:** Processing of this information may take place if the processing is carried out by bodies charged by law with applying criminal law or by Responsible Party's who have obtained that information in accordance with the law. Any information gathered on personnel in the service of a Responsible Party must be done so in compliance with labour legislation. The prohibition on processing of any of the categories of sensitive data as dealt with in Sections 27 to 32, does not apply if it is necessary to process such information in order to supplement the processing of information on criminal behaviour or biometric information permitted by this Section.

The Information Regulator may also on application, grant a specific authority (for example it being in the public interest) for special personal information to be processed, as long as appropriate safeguards have been put in place to protect the personal information of the Data Subject. The Information Regulator may also impose reasonable conditions on the processing of this information.

Should the criteria set out in Sections 27 to 33 be met, then the information may be processed, but also subject to the 8 general conditions for the lawful processing of personal information.

THE RIGHTS OF DATA SUBJECTS

Data Subjects have certain rights, and these are set out in the Act as follows:

- To have personal information processed in accordance with the Conditions set out in POPIA.
- To be notified that personal information about them is being collected in accordance with Condition 6 (Openness).
- To be notified that personal information about them has been accessed or

acquired by an unauthorised person, in accordance with Condition 7 (Security Safeguards).

- The right to establish whether a Responsible Party holds personal information of that Data Subject, and to request access thereto, in accordance with Condition 8 (Data Subject Participation).
- To request, where necessary, the correction, destruction or deletion of his, her or its personal information, in accordance with Condition 8 (Data Subject Participation).
- The right to object, on reasonable grounds relating to their particular situation, to the processing of his, her or its personal information in terms of section 11(3).
- The right to object to the processing of his, her or its personal information if it is for the purposes of direct marketing.
- The right not to have his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications except where he, she or it has given his consent or is a customer of the Responsible Party (subject to certain requirements).
- The right not to be subject to a decision which is based solely on the basis of automated processing of his, her or its personal information intended to provide a profile of such person.
- The right to submit a complaint to the Information Regulator regarding alleged interference with the protection of personal information of any Data Subject, or in respect of a determination of an adjudicator.
- The right to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information.

RESPONSIBILITIES AND DUTIES OF THE RESPONSIBLE PARTY

The Responsible Party has the following duties and responsibilities:

- To ensure compliance with the Act and that an Information Officer is appointed.
- To ensure that personal information is collected directly from the Data Subject

(some exceptions apply here).

- To ensure that personal information is only processed if it is fair and lawful to do so.
- To keep a record of what information is being held, its purpose, and on which date it must be destroyed. This can be called a "Records Retention Register".
- To ensure that the process to destroy personal information is done in such a way as to prevent its reconstruction.
- To ensure that personal information is not processed for a secondary purpose unless it is compatible with the original purpose. If the Responsible Party wishes to use the personal information for a secondary purpose, it will need to obtain the consent from the Data Subject to do so.
- To ensure that at all times, the personal information collected is complete, accurate, not misleading and updated where necessary.
- To ascertain whether its activities fall into the ambit of "direct marketing" as it is widely defined in the Act, to include "any approach" to a Data Subject, "for the direct or indirect purpose of…promoting or offering to supply, in the ordinary course of business, any goods or services to the Data Subject." A Responsible Party can, as a general rule, market to existing customers in respect of similar products or services (there are limits and recipients must be able to "opt-out" at any stage). Potential new customers can only be marketed with their consent, i.e. on an "opt-in" basis.
- To keep personal information secure against the risk of loss, unlawful access, interference, modification, unauthorised destruction and disclosure.
- To process information in a transparent manner, and have a Privacy Policy, which is available for perusal – which sets out its data processing procedure.
- To train its staff on POPIA, the new procedures, and the implementation thereof.
- To review its agreements, letters of engagement (where applicable), contracts with suppliers, and employment contracts, and amend these in order to so as to align them with POPIA.
- Where there is a data breach, the Responsible Party and the Operator must

provide notification thereof. The Responsible Party must formulate a 'Breach Plan' and 'Breach Incident Management Process'.

- To allow Data Subjects to access their personal information and to request that it be corrected or deleted. Data Subjects may also decline to share their information.
- To maintain documentation of all processing operations and specific information must be disclosed in a PAIA manual, which is published on a platform that is easily accessible by Data Subjects and provided on request.

PRIOR AUTHORISATION

There are certain instances where a Responsible Party is required to obtain prior authorisation from the Information Regulator, before it is able to process certain information.

These instances where prior authorisation is required, are set out in more detail in Section 57, as follows:

- Where unique identifiers of Data Subjects will be processed 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 (for example a bank account number, student number, policy number etc.).
- Where criminal behaviour or unlawful or objectionable conduct information on the Data Subject is processed on behalf of third parties (for example a reference check pertaining to past conduct).
- Where information is processed for the purpose of credit reporting on the Data Subject.
- Where special personal information (sensitive data) or the personal information of children is to be transferred to a third party in a foreign country that does not provide an adequate level of protection for the processing of this information.

The Information Regulator may include other types of information processing to this list, by law or regulation, if the processing thereof carries a particular risk for the legitimate interests of the Data Subject.

Section 58(2) states that a Responsible Party is required to provide a notice to the Information Regulator requesting prior authorisation to process the information set out in Section 57, and may not carry out information processing that has been notified as such to the Information Regulator until the Information Regulator has completed its investigation or until they have received notice that a more detailed investigation will not be conducted. **The Information Regulator has granted an extension on the application of this Section 58(2), to 1 February 2022.** In effect, this means that Responsible Parties who are processing such information should continue to do so, but should still submit their application/s to the Information Regulator, providing the latter with additional time to process the applications.

BODIES CORPORATE AND HOMEOWNERS ASSOCIATIONS

Bodies Corporate, Sectional Title Schemes and Homeowners Associations are also subject to POPIA.

Personal information is held by these community schemes in regard to Data Subjects such as scheme owners, Homeowners Associations members', the Trustees, Auditors, Attorneys, and Managing Agents. In addition, information gathered on visitors who enter a security estate via a security gate (such as the scanning of license plates and driver's licenses), is required to be processed in compliance with the 8 general conditions of lawful processing of personal information, as set out in POPIA.

THE PERSONAL INFORMATION OF A CHILD

The gathering and processing of the personal information of a child is prohibited by the Act. There are only a select few situations where this kind of information may be processed, and these are set out in Section 35. Some relevant terms used in this Section, which are defined in the Act, are:

'competent person' means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child, for example, a parent.

'child' means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter.

Section 35 states that the processing of information about children is only allowed if: (i) it is carried out with the prior consent of a competent person (ii) it is necessary for the establishment, exercise or defence of a right or obligation in law (iii) it is necessary to comply with an obligation of international public law (iv) it is for historical, statistical or research purposes or (v) it is of personal information which has deliberately been made public by the child with the consent of a competent person.

In addition, the Information Regulator may, upon application by a Responsible Party, and by notice in the Government Gazette, 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 of the child.

Schools and POPIA

POPIA applies to all schools – and in fact, any entity which requires membership or the registration of a child – such as a cricket club, a gymnastics club, a scout's club, and so on. In fact, children's rights are carefully protected in any situation where the processing of their personal information occurs. Schools are increasingly embracing the digital world. In addition, the Covid-19 pandemic has accelerated the use of online communication and teaching. Schools need to make sure that they have the systems in place to keep learners' and parents' details secure. Parents should hold schools and clubs accountable for the way they store, process, and retain information, and have the right under POPIA to request a breakdown of what information the institution holds about them and their children, and the institution is obliged to provide that information. Schools, in turn, should only keep the minimum information required to fulfil their obligations, and ensure that this information is stored securely whether it's in electronic or physical form. Cybersecurity and network security are critical for electronic data, while access control and physical security measures need to also be addressed for hard-copy information.

There is thus an extra duty of care when processing the personal information of a child. Should the specific criteria laid out on Section 35 be met, then the information must also be processed in accordance with the 8 general conditions for the processing of personal information.

THE CONCEPT OF CONSENT

The Act defines consent as "any voluntary, specific and informed expression of will – in terms of which permission is given for the processing of personal information."

"Voluntary" implies a choice as to whether to consent or not, in other words, where consent is made conditional on using a product or service, such consent will probably not be deemed to have been given voluntarily.

"Specific" implies that the consent must have been given for a specific purpose, and cannot be vague.

"Informed" implies that the Responsible Party must provide its Data Subject with sufficient information to enable them to make an informed decision as to whether or not they want to consent to the processing of their information. The Act does not set out a prescribed manner in which such consent must be obtained, however it must be expressed in some form or another. How this consent is expressed - such as by signature or the press of a button on a website - will have to be determined in each case.

By providing consent, Data Subjects agree to the processing of their personal information, and, by understanding what they are consenting to, it helps avoid disputes when their data is processed or transferred to third parties in accordance with the consent provided. The Responsible Party bears the burden of proof for that consent. The Data Subject may withdraw his or her or its consent at any time.

There are certain instances where consent **is not** required, and personal information may be processed lawfully. These instances are as follows:

- When it is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is party; or
- The processing complies with an obligation imposed by law on the Responsible Party (for example, during the course of carrying out auditing services for a client, an auditor may obtain the personal information of his client's employees. The carrying out of the auditor's duties in this respect is in terms of the Companies Act (no. 71 of 2008) and the Auditing Profession Act (no.26 of 2005); or
- It protects a legitimate interest of the Data Subject; or
- It is necessary for the proper performance of a public law duty by a public body; or
- It is necessary for pursuing the legitimate interests of the Responsible Party or of a third party to whom the information is supplied (for example the tracing of a person to collect outstanding debt).

GENERAL EXEMPTIONS IN CERTAIN CIRCUMSTANCES

The Information Regulator may, by notice in the Gazette, grant an exemption to a Responsible Party to process personal information, even if that processing is in breach of any of the 8 general conditions or special conditions set out in the Act (and may impose reasonable conditions in regard to this exemption), where:

The public interest* in the processing outweighs, to a substantial degree, any interference with the privacy of the Data Subject that could result from such processing

The processing involves a clear benefit to the Data Subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the Data Subject or third party that could result from such processing.

*"Public interest" includes: (a) the interests of national security (b) the prevention, detection and prosecution of offences (c) important economic and financial interests of a public body (d) fostering compliance with legal provisions established in the interests referred to under (b) and (c), (e) historical, statistical or research activity (f) or the special importance of the interest in freedom of expression.

Exemption in respect of certain functions

Where personal information is processed for the purpose of discharging a relevant function which is described as one of these scenarios:

- Of a public body,
- Conferred on any person in terms of the law,
- Performed with the purpose of protecting the general public against: Financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate. Dishonesty, malpractice or other seriously

improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity.

Then, such processing is exempt from the provisions of the following Sections in the Act:

- Sections 11(3) and (4) (objection by a Data Subject to the processing of their information), Section 12 (collection of personal information directly from a Data Subject),
- Section 15 (further processing to be compatible with the original purpose of the collection of the data),
- Section 18 (requirement for the notification to the Data Subject when collecting personal information) in any case to the extent to which the application of those provisions to the personal information would be likely to prejudice the proper discharge of that function.

For example, if a Responsible Party requires certain information from a Data Subject in terms of the Financial Intelligence Centre Act (no. 38 of 2001), then the Data Subject cannot object thereto.

CODES OF CONDUCT

Specific Codes of Conduct may be developed in order to clarify how the 8 conditions for the lawful processing of personal information are to be applied within a particular sector.

These codes may be developed either by the Information Regulator itself, or by the stakeholder/s within that particular sector, who would then make an application to the Information Regulator to issue and approve the codes. In other words, the Information Regulator may either issue a code for a particular sector on its own initiative (after first consulting with affected stakeholders), or it may issue and approve them after receiving an application from affected stakeholders (as long as the Information Regulator believes that such applicants are sufficiently representative of the industry, profession, vocation or class of bodies applying for the Codes of Conduct).

These sectors include specific industries, professions, vocations or specific bodies or class of bodies.

The process that then takes place is that a notice will be placed in the Government

Gazette by the Information Regulator that the issuing of a Code of Conduct is being considered. This notice must set out the details of the particular code being considered and that a draft of the proposed code can be obtained from the Information Regulator by any interested party. There is then a period of time for the public (affected parties) to make submissions in writing relating to that code, these submissions must be considered by the Information Regulator. As long as the code remains in force, copies of it are available on the Information Regulator's website and at its offices. The Information Regulator must keep a register of all the approved Codes of Conduct.

These sectors will then be governed by these codes in terms of the lawful processing of personal information of Data Subjects within their sphere of operation.

The Information Regulator may also issue Codes of Conduct in relation to specific types of information to be processed and may also provide written guidelines to assist bodies to develop their own Codes of Conduct, and also on how to apply them.

The Journalistic Profession and Codes of Conduct

In regard to the journalistic profession, where there is no Code of Ethics governing a Responsible Party, the Information Regulator must have regard to the principles set out below, when considering the approval of a Code of Conduct for the processing of any personal information for exclusively journalistic purposes:

- The special importance of the public interest in freedom of expression.
- Domestic and international standards balancing the free flow of information in recognition of the right of the public to be informed.
- Domestic and international standards balancing the public interest in safeguarding of personal information of Data Subjects.
- The need to secure the integrity of personal information.

Failure to comply with a Code of Conduct that has been approved and issued by the Information Regulator is deemed to be a breach of the conditions for the lawful processing of personal information and may be subject to the enforcement procedures set out in Chapter 10 of the Act.

DIRECT MARKETING

Section 69 states that 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, faxes, SMS's or email is prohibited unless the Data Subject has given his consent to the processing, or is a customer of the Responsible Party (subject to certain conditions).

Direct Marketing by means of unsolicited Electronic Communications

In order for the processing of personal information of a Data Subject to be lawful when a Responsible Party undertakes Direct Marketing, the Data Subject must first:

A. **Have given his express consent to the processing:** The consent must be expressly given, through a clear, specific and affirmative act, or "opt-in". The Data Subject may withdraw his or her consent at any time. A Responsible Party may approach a Data Subject in order to obtain his specific consent only for a specific processing purpose, provided that Data Subject has not previously withheld such consent. The Responsible Party can only do this once. It must be requested in the prescribed manner and form (although the Act does not set out what this should look like). Consent can be managed by:

   - Having an unsubscribe function, so that Data Subjects are able to withdraw their consent at any time (without being penalised).
   - Having a process in place to update consents regularly.
   - Removing Data Subjects from contact lists when they unsubscribe.

B. **Must be an existing customer of the Responsible Party:** Only where the Responsible Party has:

- Obtained the contact details of the Data Subject 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.
- If the Data Subject has been given a reasonable opportunity to object, free of charge, to the use of his 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.

Direct marketing by means of unsolicited electronic communications under POPIA includes any form of electronic communication including automatic calling machines (a machine that is able to do automated calls without human intervention), faxes, SMS's or email.

If telephone calls are coming from a telemarketing company, registering on the national "opt-out" database can enable a person to opt-out of all direct marketing communication. The National Opt-Out Register is run by the Direct Marketing Association of South Africa (DMASA).

Requirements for lawful direct marketing communication

In order to be lawful, all direct marketing communications:

- Must have the details of the identity of the sender or the person on whose behalf the communication was sent, as well as the contact details of any third party that the Responsible Party will share the information with.
- Must have an address or other contact details to which the recipient may send a request that such communications cease.

A Data Subject has the right to object to the processing of personal information if it is for the purposes of direct marketing.

Other Legislation relating to electronic marketing

The Consumer Protection Act

The Consumer Protection Act (no. 68 of 2008) deals with the consumer's right to restrict unwanted direct marketing.

Section 32 states that a person who directly markets goods or services to a consumer and who concludes a transaction or agreement with the consumer, must inform the consumer of the right to rescind that agreement in terms of the cooling-off period of 5 business days from the date of the transaction, as set out in Section 16 of that Act.

Electronic Communications and Transactions Act

The Electronic Communications and Transactions Act (no.25 of 2002), or "ECTA", applies to any form of communication by email, the internet, SMS's etc. except possibly for voice communications between 2 people. Provision is made for consumer protection in Chapter VII of ECTA – whereby suppliers of goods or services must provide consumers with a minimum set of information, including the price of the product or service, the name, contact details, a brief description of the business, and the right to withdraw from an electronic communication before its completion. The consumer is protected in that they are also afforded a cooling-off period (7 days) within which they may cancel certain types of transactions concluded electronically – without incurring a penalty. In addition, ECTA specifically requires that each electronic message be accompanied by an option to cancel ("opt-out") of a subscription to a mailing list.

Section 45 of ECTA also provides some protection against spam communications. The sender of such unsolicited communications, who continues to send them, even although the consumer has advised that he does not welcome the communications, will be committing an offence.

ECTA also regulates the electronic collection of personal information, although compliance with these provisions is voluntary. The provisions of ECTA pertaining to the protection of personal information will, however, be repealed on 30 June 2021.

DIRECTORIES

A Data Subject who is a subscriber* to a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which his personal information is included, must be informed, free of charge and before the information is included in the directory about the purpose of the directory, and about any further uses to which the directory may possibly be put, based on search functions embedded in electronic versions of the directory. He must be given a reasonable opportunity to object, free of charge to the use of his personal information or to request withdrawal of such information if he did not initially refuse such use.

This will not apply to editions of directories that were produced in printed or off-line electronic form prior to the commencement of this section in the Act.

*For the purposes of this Section, subscriber means any person who is a party to a contract with the provider of publicly available electronic communications services, for the supply of such services.

AUTOMATED PROCESSING OF PERSONAL INFORMATION

A Data Subject has the right not to be subject to a decision which is based solely on the basis of automated processing of his personal information intended to provide a profile of such person, including his performance at work, or his credit worthiness, reliability, location, health, personal preferences or conduct.

This does not apply however, where the decision is taken in connection with the conclusion of a contract and the request of the Data Subject in terms of the contract has been met or appropriate measures have been taken to protect the interests of the Data Subject. It will also not apply where the decision is governed by a law or Code of Conduct.

TRANS-BORDER INFORMATION FLOWS

In the context of Section 14 of the Constitution, (which encompasses the right to privacy), balanced against principle of free flow of information within South Africa and across international borders, Section 72 of the Act deals with the transfer of personal information about a Data Subject to a third party who is in a foreign country.

This can only be done lawfully by a Responsible Party, if the requirements of Section 72 are met. These requirements are as follows:

Protection: The third party is subject to a law, binding corporate rules or a binding agreement which provides an adequate level of protection that:

- Upholds principles that are substantially similar to the conditions of lawful processing in South Africa.
- Includes similar provisions re the transfer of such information from the recipient to a third party in another foreign country.

Consent: the Data Subject consents to the transfer.

Contract: the transfer is necessary for the performance of a contract between the Data Subject and the Responsible Party.

Interest of Data Subject: the transfer is necessary for the performance of a contract concluded in the interest of the Data Subject between the Responsible Party and a third party.

Benefit: 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 the transfer, and
- if it were reasonably practicable to obtain such consent, the Data Subject would be likely to give it.

In a nutshell, in order to lawfully transfer personal information outside South Africa to a foreign country, the transferor will need to ensure that it will be protected in that foreign country.

EMPLOYERS

The general provisions under POPIA will apply equally to any personal information processed by an employer as part of an employee's employment, and all employers have until 1 July 2021 to ensure that their workplaces are fully POPIA compliant.

The processing of an employee's general personal information is necessary for a variety of reasons, such as:

- Concluding employment contracts.
- Recruitment and training.
- The requirements of the Occupational Health and Safety Act (no. 85 of 1993), the Basic Conditions of Employment Act (no. 75 of 1997), and the Employment Equity Act (no.55 of 1998).
- The Covid-19 Pandemic.

POPIA does also specifically include an employee's employment history within the definition of personal information.

Employers may also be required to process special personal information of an employee, including religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information.

The processing of this information attracts special additional rules of compliance and employers need to be cognisant of these special rules.

A POPIA Compliance Programme in the Workplace

- **Designate an Information Officer**

The Information Officer's responsibilities in terms of compliance in the workplace, include ensuring that the employer is compliant with the lawful processing

of personal information of the employees (such as the health information of employees relating to Covid-19), and dealing with employee access to information requests.

- **Develop a procedure ensuring personal information of employees are processed in a lawful manner.**
- **Ensure that the processing of personal information is done in accordance with the 8 conditions for the lawful processing of the personal information.**
- **Obtain consent from employees for the processing of their personal information**

The first step employers can take to guard against liability in terms of POPIA is to ensure that the consent of employees is obtained, and the processing of the employee's personal information is for a specified purpose. An employee should be in a position to "opt-in" and know what their personal information will be used for. The way this can be done is by:

  - providing consent forms for signature, when consent is required – these forms will set out the specific purpose for which the employee's personal information will be processed, or
  - amending all contracts of employment to include special reference to the processing of personal information and consent.

- **Provide training to employees so as to ensure that the information of clients and customers (where applicable) are processed lawfully, and also to ensure that employees themselves, as 'Data Subjects' are aware of their rights.**

Employees have certain rights under POPIA. These include:

- the lawful processing of their personal information;
- to consent to the processing and further processing of personal information;
- to be notified when their personal information is being collected or has been subject to a breach;
- to be able to request access to their personal information;
- to object to the processing of their personal information; and
- to request the correction, destruction or deletion of their personal information.

- **Putting in place measures to ensure the processing of 'special personal information' is lawful.**

- **Putting in place a Manual on Workplace Policies and Procedures**

It is the responsibility of the Information Officer to put a manual in Place on Workplace Policies and Procedures for POPIA. This manual should function as an important tool in training staff on the requirements, implications, implementation, and consequences of POPIA. Compliance with every aspect of POPIA should be understood by everyone in the workplace. By setting up the manual, the policies and procedures will be documented. But they also need to be seen to be implemented. Checklists for procedures and protocols for recording actions are thus also important to have in place.

Depending on the size, scale and services of an employer, it may be necessary to consolidate the policies or establish new ones to adequately address high risk areas when processing personal information of employees, and/or clients, customers, services providers etc. (Data Subjects). These policies form a basis of compliance and awareness, however regular training of employees on and about the policies is essential.

- **Ensure that adequate safeguards are in place**

Employers are required to identify reasonably foreseeable risks, in respect of non compliance with POPIA, and then develop safeguards, in order to respond thereto. For example, in relation to cybersecurity and access control.

- **Implementing procedures to address and deal with any complaints from employees regarding the processing of their personal information.**

COVID-19, THE WORKPLACE AND POPIA

On the 15th March 2020, a national state of disaster was declared by the South African Government due to the Covid-19 pandemic that reached our shores in early 2020. Regulations and Directives have been published to provide for procedures to be followed during the period of lockdown. In terms of these, employers are required to process personal information and special personal information of both employees and clients/customers/service providers (i.e. third party visitors to the workplace) to prevent and mitigate the spread of Covid-19.

The Regulations issued in terms of Section 27(2) of the Disaster Management Act (no.57 of 2002), state (inter alia), that employers are required to implement measures for employees who are over 60 years of age, or those with co-morbidities, to facilitate their safe return to work, which may include special measures at the workplace to limit employees' exposure to Covid-19 infection and where possible that the employees work from home. In addition, firms must adhere to any sector-specific health protocols intended to limit the spread of Covid-19 in the sector concerned.

The Occupational Health and Safety Labour Directive 20.11 states (inter alia) that if a worker has been diagnosed with Covid-19, an employer must:

- Inform the Department of Health and the Department of Employment and Labour, and
- Investigate the mode of exposure including any control failure and review its risk assessment to ensure that the necessary controls and PPE requirements are in place;
- Give administrative support to any contact-tracing measures implemented by the Department of Health.

Workers are to immediately inform the employer if they experience any symptoms such as cough, sore throat, shortness of breath, loss of smell or taste, fever, body aches, redness of eyes, nausea, vomiting, diarrhea, fatigue, weakness or tiredness – while at work. Directive 16.4, on the other hand, requires employers to notify employees that if they are sick or have symptoms associated with Covid-19, that they must not come to work and to take paid sick leave in terms of Section 22 of the Basic Conditions of Employment Act.

Employers are thus obligated to process health information of employees in terms of these Regulations and Directives by way of screening, recording of symptoms, test results, and the registering of co-morbidities.

This information, by its nature, is special personal information, as defined by POPIA. Ideally, proper, written, clear, voluntary and specific consent should be obtained by the employee / third party in regard to the processing of such information. Where there is no such consent, or a refusal to give consent, Section 27 of POPIA would apply – whereby an employer (as a Responsible Party) may make an application

to the Information Regulator to authorise the processing of special personal information where such processing is deemed by the Information Regulator to be in the public interest and subject to adequate safeguards.

Section 32(1)(f) of POPIA entitles employers to process health information of employees if necessary, for (i) the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on health or sex of the data subject or (ii) the reintegration of or support for workers or persons entitled to a benefit in connection with sickness or work incapacity.

Directive 41 of the Occupational Health and Safety Directive also places an obligation on workers to comply with measures introduced by employers in regard to Covid-19.

The 8 conditions for the lawful processing of the personal information as set out in POPIA would also apply in these circumstances. By way of example, we have listed three of these conditions below, and how they would be implemented in regard to Covid-19 in the workplace:

- Condition 3: Purpose Specification: whereby records on Covid-19 information should not be retained for longer than necessary to achieve this purpose.
- Condition 5: Information Quality: it is important to ensure that the correct symptom screening results are stored in respect of the correct employee.
- Condition 8: Data Subject Participation: employees are entitled to request access to their personal information on Covid-19 as processed by the employer.

Regulation 8(17) has clarified the situation relating to Condition 3, by stating that:

"Within 6 weeks after the national state of disaster has lapsed or been terminated –

a. The information on the Covid-19 Database (Department of Health) shall be de-identified,

b. The de-identified information on the Covid-19 Database shall be retained and only used for research, study and teaching purposes.

c. All information on the Covid-19 database which has not been de-identified shall be destroyed."

RETENTION PERIODS

When retaining records of personal information of its Data Subjects, the first point of call for the Responsible Party is that the records must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed. Thereafter, the records should be deleted or destroyed.

However, the records may be retained for longer, but only where:

- The retention is required or authorised by law.
- The Responsible Party reasonably requires the record for lawful purposes related to its functions or activities (see the table below, which sets out various pieces of legislation which specify a minimum period for the retention of records).
- The retention is required by contract between parties.
- The Data Subject or a competent person (where the Data Subject is a minor child) has consented to the retention of the record for a longer period.
- For historical, statistical or research purposes if the Responsible Party has established appropriate safeguards against the records being used for any other purposes.

The following table sets out some of the retention periods which are prescribed by various pieces of legislation in South Africa, as follows:

Document	Retention Period
Companies Act	
■ Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Companies Act and other public regulation.	7 years or longer (as specified in other public regulation).
■ Registration certificate. ■ Memorandum of Incorporation. ■ Rules. ■ Securities register and uncertificated securities register. ■ Register of company secretary and auditors.	Indefinite.

■ Notice and minutes of all shareholders' meetings. ■ Copies of reports presented at the annual general meeting of the company.	7 years.
■ Minutes and resolutions of directors' meetings, audit committee and directors' committees. ■ Copies of annual financial statements. ■ Copies of accounting records. ■ Record of directors and past directors, after the director has retired from the company. ■ Written communication to holders of securities.	
Close Corporations Act	
■ Accounting records. ■ Annual financial statements.	15 years.
■ Founding statement (Form CK 1). ■ Amended Founding statement (forms CK 2 and CK 2A). ■ Microfilm image of any original record reproduced directly by the camera – the "camera master." ■ Minutes books as well as resolution passed at meetings.	Indefinite.
Income Tax and VAT Act	
■ In respect of each employee the employer shall keep a record showing: amount of remuneration paid or due by him to the employee; the amount of employees' tax deducted or withheld from the remuneration paid or due; the income tax reference number of that employee; any further prescribed information; Employer Reconciliation return (EMP501). ■ The following records of importation of goods and documents: Bill of entry or other documents prescribed by the Custom and Excise Act, proof that the VAT charge has been paid to SARS. ■ VAT Vendors are obliged to keep the following records: record of all goods and services, the rate of tax applicable	5 years from date of submission of the return (documents relating to the acquisition of assets should be retained indefinitely for future capital gains tax calculations).

■ to the supply and the suppliers or their agents, invoices, tax invoices, credit notes, debit notes, bank statements, deposit slips, stock lists and paid cheques. ■ Documentary proof for zero-rating of supplies.	
Consumer Protection Act	
■ There are specific requirements for information to be kept by intermediaries for auctions and promotional competitions, for example a written agreement that contains the terms and conditions upon which the auctioneer accepts the goods for sale.	3 years.
Co-operatives Act	
■ Constitution and rules (and amendments), minutes of general meetings, minutes of meetings of the board of directors, list of members setting out their details, register of directors.	Indefinite.
National Credit Act	
■ Records of registered activities to be retained by Credit Providers in re each consumer includes: application for credit, application for credit declined, reasons therefore,	3 years from the earliest of the dates on which
■ pre-agreement statement and quote, documentation in terms of S81(2), record of payments made, documentation in support of any steps taken after default by consumer.	the registrant created, signed or received the document.
Electronic Communication and Transaction Act	
■ Personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information. All personal data which has become obsolete must be destroyed.	As long as the information is used, and at least 1 year thereafter.

Financial Intelligence Centre Act	
■ Accountable Institution (AI) to keep a record (inter alia) of the identity of the client, the nature of the business relationship, in the case of a transaction, the amount involved and the parties thereto, all accounts involved in transactions concluded by that AI in the course of that business relationship and that single transaction, any	
document obtained by the AI Records must be kept (and may be kept in electronic format) as follows: ■ From termination of business relationship ■ From the date the transaction is concluded	 5 years. 5 years.
Compensation for Occupational Injuries and Diseases Act	
■ A register or other record of the earnings and other prescribed particulars of all the employees.	4 years after the date of the last entry in that register or record.
Occupational Health and Safety Act	
■ An employer or user shall keep at a workplace or section of a workplace a record in the form of Annexure 1 for a period of at least 3 years which record shall be open for inspection by an inspector of all incidents which he is required to report in terms of section 24 of the Act and also of any other incident which resulted in the person concerned having had to receive medical treatment other than first aid. ■ Records of assessments and air monitoring and the asbestos inventory. ■ Medical surveillance records.	3 years. Minimum of 40 years. Minimum of 40 years.
Basic Conditions of Employment Act	
■ Written particulars of employee must be kept after termination of employment.	3 years after termination.

Employment Equity Act	
■ An employer must establish and maintain records in respect of its workforce, its employment equity plan and other records relevant to its compliance with the Act.	5 years after expiry of the plan.
Labour Relations Act	
■ Employers should keep records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions.	Indefinite.
Sectional Title Schemes Management Act	
■ The body corporate must ensure that all the body corporate's books of account and financial records are retained.	6 years after completion of the transactions, acts or operations to which they relate.
Securities Transfer Tax Administration Act	
■ A company or close corporation that issued an unlisted security must keep records of every transfer of an unlisted security issued by it as may be required to enable the company to observe the requirements of the Act.	5 years from the date of transfer.
Trust Property Control Act	
■ A trustee shall not without the written consent of the Master destroy any document which serves as proof of the investment, safe custody, control, administration, alienation or distribution of trust property, before the expiry of a period of 5 years from the termination of the trust.	5 years from the date from termination of a trust.
Auditing Profession Act	
■ Engagement documentation, including working papers, statements, correspondence, books or other documents in the possession or under the control of the registered auditor.	Ordinarily no shorter than 5 years from the date of the

	auditor's report, or if later, the date of the group auditor's report.

Notes: Where different legislation refers to the retention of the same records/ information, the Responsible Party must consider adhering to the most stringent of the legislative requirements. For example, the Value Added Tax (VAT) Act (no. 89 of 1991) states that invoices should be kept for five years from the submission of the return. However, if the entity is a company, the Companies Act (no. 71 of 2008) would require the financial records to be kept for a minimum of seven years and therefore the Responsible Party should adhere to the most stringent requirement of seven years.

The records, books of account and documents must be retained in their original form in a safe place, or electronic format as prescribed by the Commissioner or in a form authorised by a senior SARS official.

This table does not attempt to include all legislation, or all of the provisions within a particular piece of legislation, regarding retention periods, but instead, is intended to give the reader a general overview of the retention requirements of documents in South Africa.

THE REGULATIONS

The Regulations are largely administrative in nature and deal with:

- How a Data Subject can object to the processing of their personal information.
- How a Data Subject can request the correction or deletion of information.
- The responsibilities of an Information Officer. Regulation 4 sets out more of the duties and responsibilities of the Information Officer.
- How to apply to the Information Regulator to issue a code of conduct.
- How to request marketing consent. Form 4 of the Regulations sets out how to get consent to the direct marketing(by electronic communications) of a Data

Subject.

- How to submit a complaint to the Information Regulator.
- How the Information Regulator will act as a conciliator in investigations.
- What the Information Regulator must do before it investigates a Responsible Party.
- How the Information Regulator will try to settle complaints.
- How the Information Regulator will conduct assessments.
- How the Information Regulator will notify people during investigations.

There are two people who have the power to make Regulations. The Information Regulator and the Minister of Justice and Constitutional Development - who has the limited power to make Regulations [under section 112(1)] but only about establishing the Information Regulator, and the fees that Data Subjects must pay to a Responsible Party for accessing the personal information it processes, and to the Information Regulator when lodging a complaint with it.

ENFORCEMENT AND REMEDIES

Non-compliance with the provisions of POPIA by a Responsible Party could lead to the Data Subject lodging a complaint with the Information Regulator, which would lead to an investigation and possible civil action. The process of lodging a complaint with the Information Regulator, is set out in Chapter 10 of the Act, and may be summarised as follows:

- Investigation by the Information Regulator
- Issue and Execution of Warrants
- Communication between legal adviser and client are exempt
- Complaints
- Action on receipt of complaint
- The Information Regulator may decide to take no action
- Or referral to Regulatory Body
- Pre-Investigation proceedings of Information Regulator
- Settlement of Complaints

- Objections to Search and Seizure
- Return of Warrants
- Assessment
- Information Notice
- Parties informed of result of assessment
- Matters referred to Enforcement Committee
- Parties to be informed during and regarding the result of the investigation
- Enforcement Notice
- Cancellation of Enforcement Notice
- Right of Appeal
- Consideration of Appeal
- Civil remedies

Examples of non-compliance by a Responsible Party are:

- Breach of any of the 8 lawful conditions,
- Not informing the Information Regulator of a data breach
- Sending unsolicited direct marketing
- Sharing information cross-border where it is not allowed

The outcome may be monetary compensation for the Data Subject, as set out in an infringement notice by the Information Regulator, in terms of an Administrative Fine.

OFFENCES, PENALTIES AND ADMINISTRATIVE FINES

The Responsible Party may commit a criminal offence. Chapter 11 lists the offences under POPIA as follows:

- Obstruction of information
- Obstruction of the execution of a warrant
- Failure to comply with an Enforcement or Information Notice issued by the Information Regulator
- Unlawful acts by Responsible Party with an account number
- Unlawful acts by third parties in connection with an account number
- Breach of confidentiality (breach of Section 54 - where a person acting on

behalf of or under the direction of the Information Regulator must keep all personal information that he is privy to during the course of his duties, as confidential).

- Offences by witnesses (e.g. failure to attend and give evidence when summoned to do so).

Penalties: Any person convicted of an offence in terms of this Act (as listed above), will be liable to penalties which range from R1 million and/or 1 year imprisonment to R10 million and/or 10 year's imprisonment – depending on the severity of the offence.

Administrative fines of up to R10 million may be imposed by the Information Regulator on the Responsible Party – as set out in an infringement notice.

A Responsible Party may also be subject to civil claim for damages brought by Data Subjects (or the Information Regulator at the request of the Data Subject), as well as reputational damage. Directors may also be declared unfit to serve as a director in terms of the Companies Act (no. 71 of 2008).

TYPICAL EXAMPLES OF A POPIA BREACH

Some typical examples of a POPIA breach would be:

- Sending an email containing personal information to the wrong person,
- Losing a laptop,
- Processing special personal information of a Data Subject without following the correct procedures,
- The Responsible Party's database is hacked,
- Collecting personal information without consent, where it is required,
- Using current information of a Data Subject for purposes other than was originally consented to (such as marketing to a person without consent),
- Not complying with enforcement notices issued by the Information Regulator.

POPIA PROGRAMME CHECKLIST

- The Responsible Party will need to compile a checklist as a starting point to develop a POPI programme*. For example:

1. Assemble a project team, define the roles and responsibilities, and accountability within the organisation.
2. Identify and appoint an Information Officer. Register him with the Information Regulator.
3. The project team should conduct a "Gap Analysis" of the current processes, and identify compliance risks: for example, asking questions such as:

- What data do we process and why? Is it for a contractual or legal purpose? Is it due to a legitimate interest?
- For whom do we process data?
- Is it for clients, suppliers or individuals? Do we process information of children?
- Do we mandate someone else (an Operator) to process personal information?
- Where is it stored?
- Is it securely stored? Is there access control?
- Who do I share it with, and why? Is it shared across the South African border? Does it come from a public source? Is it being shared for a contractual or legal reason (e.g. to SARS)?
- Do we have processes in place to ensure that the data is lawfully obtained? Who do we obtain data from - is it from a data source, a public source, from 3rd Parties for a valid reason or legitimate interest?
- Are our email disclaimers compliant with POPIA?

4. Develop a **"Project Plan"**, which would include working out a budget, reviewing current policies, determining what changes to these policies and procedures are required in order to protect personal information, and then setting a timeline for implementation.

5. **"Implementation",** would include items such as:

- The drafting of new policies and adjustment of existing policies.

- Drafting a POPIA compliance framework manual for the organisation. This is not compulsory but is recommended.
- Preparing documentation such as checklists to ensure the procedures are met, and "ticked off", in order to provide proof of compliance, should the Information Regulator ever conduct an inspection. A process for continual monitoring and enforcement thereof should be put into place.
- Raising awareness and conduct training with employees.
- Amending contracts with employees.
- Amending letters of engagement with clients (where applicable).
- Amending contracts with Operators where applicable. A contractual agreement between the Responsible Party and Operator is highly recommended in order to govern the roles of each party and the boundaries of this relationship.
- Ensuring that systems are in place to protect data – such as disaster recovery systems, backups and firewalls relating to electronically stored data.
- Reporting data breaches to the Information Regulator and Data Subjects.
- Only sharing personal information when lawfully able to. Of the organisation's privacy policy.
- Reviewing of the organisation's privacy policy.
- Creating a database whereby all Data Subjects and their personal information that the organisation deals with, is identified.
- Communicating with Data Subjects.
- Reducing record retention where possible, and destroying data that the organisation does not need to retain.

*this checklist is intended to give the reader an idea of what should be included - as a starting point, and is not intended to be exhaustive, but merely as an illustrative example.

NOTES

Disclaimer:

The information contained in this guide is of a general nature and is not intended as legal advice. The reader is advised to consult a professional adviser for further assistance and information, and for guidance on new and existing legislation which may affect the business owner, directors and officers of companies.

All references to the masculine gender shall include the feminine (and vice versa).

While every care has been taken in the compilation of this guide, no responsibility of any nature whatsoever shall be accepted for any inaccuracies, errors or omissions.

RELATIONSHIPS & SOLUTIONS

Through experience, Nolands has built productive working relationships with many companies in related service sectors, to the benefit and convenience of our clients

Amandla OBUNYE Consulting

Carbon VECTOR

SA PRIME TRUSTEES

Amandla OBUNYE
The Power Of Learning Together

GREATSOFT FINANCIAL SERVICES

taxrisk underwriting managers

OBUNYE PRIVATE EQUITY

Kabusha ADVISORY

ROCKMAN CAPITAL

BR360 INTEGRATED BUSINESS RESCUE

Landsbury
Institute Of Applied Learning

ROCKMILLS FINANCIALS LTD

BALLITO	032 032 0500
BLOEMFONTEIN	051 430 0931
CAPE TOWN	021 658 6600
DURBAN	031 309 1931
GEORGE	044 873 6579
JOHANNESBURG	011 7894966
PORT ELIZABETH	041 379 4173
STELLENBOSCH	021 612 0921
TYGERBERG	021 943 4340

Nolands

AUDIT • ADVISORY • LAW