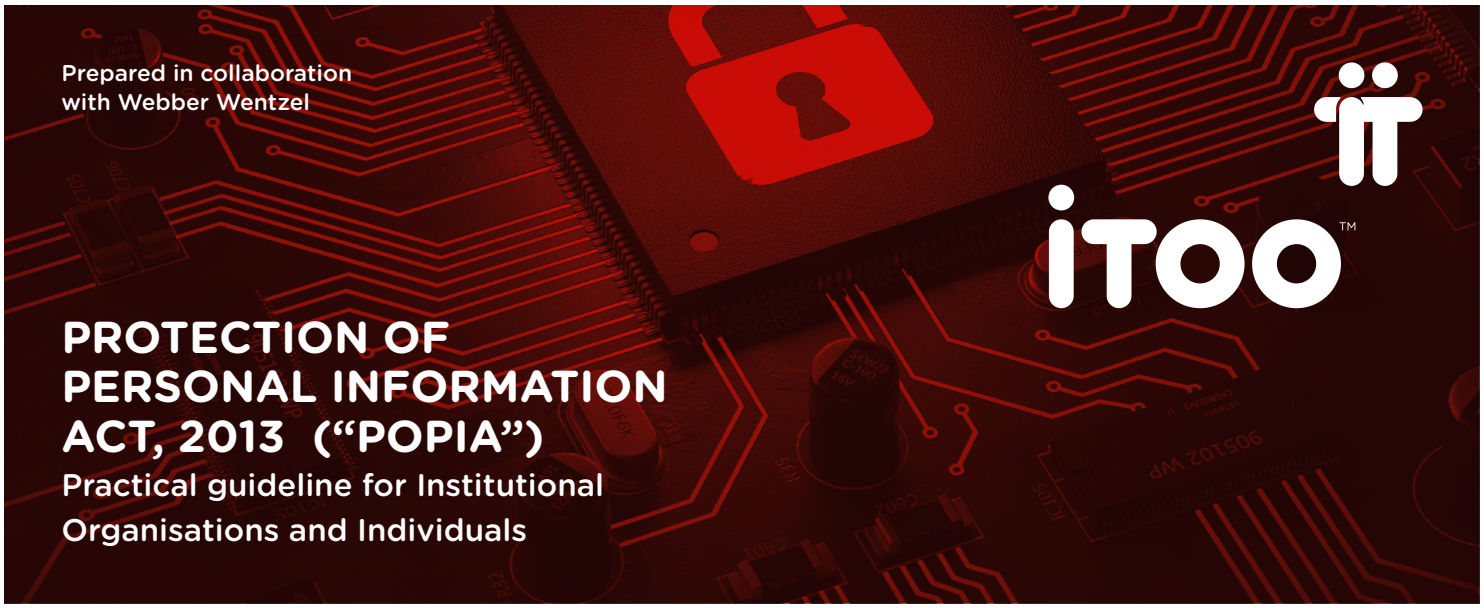

Prepared in collaboration with Webber Wentzel

PROTECTION OF PERSONAL INFORMATION ACT, 2013 ("POPIA")

Practical guideline for Institutional Organisations and Individuals

Introduction

The Protection of Personal Information Act, 2013 **("POPIA")** came into full effect on 1 July 2021. It gives effect to the constitutional right to privacy by regulating the processing of personal information of individuals and where appropriate, juristic persons such as companies or associations (called data subjects) which is processed by public and private bodies as well as individuals (responsible parties). It affects all areas of business including how organisations deal with their customers' and employees' personal information.

Personal information has a wide meaning and includes information which identifies and relates to living individuals (for example gender, marital status, national, ethnic or social origin, age, biometric information, employment history) or existing corporates (for example, company information such as tax number, registration number, contact details and information of a confidential nature relating to the company). Personal information relating to children (i.e. persons under the age of 18 years) and special personal information (which includes private information relating to religious beliefs, race, and health or sex life) is deemed sensitive information and subject to more onerous processing obligations.

POPIA safeguards and protects the personal information by imposing minimum standards for the lawful processing of that personal information.

This note sets out at a practical guideline to assist institutional organisations and individuals comply with the obligations under POPIA. As a matter of priority, you must designate an internal Information Officer (e.g. legal officer or practice administrator) who must register with the Information Regulator (the enforcement agency responsible for monitoring and enforcing compliance with POPIA).
The Information Officer deals with requests made to your business operations under POPIA and will generally be responsible for your organisation's compliance with POPIA.

This guidance note is not an exhaustive list of the obligations under POPIA. It does not constitute legal advice and should not be considered a substitute for legal advice.

Consent to processing of personal information

Except in certain circumstances, a data subject must consent to the processing of their personal information. This is usually at contract entering stage.

Consent under POPIA is a voluntary, specific, and informed expression of willingness to give permission to process personal information.

As a responsible party, you would be held accountable for the personal information that you process. Where information is collected for any use that requires consent, you must take steps to ensure that the data subject is made aware of your identity as the responsible party, what the information will be used for and who the recipients will be.

Personal information should only be used for the purpose that it was collected, and the data subject should be informed and give their consent if the information is to be used for any other purpose unless if you reasonably consider that you need to use it for another reason which is not compatible with the original purpose. For example, if your original purpose is to collect personal information for COVID screening of your premises to comply with the Disaster Management Act, 2002 this would be lawful. If you use that information to inform those data subjects that there were multiple positive cases on a particular day, that would be compatible with the original purpose and thus lawful. However, if you use that information to advertise those persons or you sell that information (without their consent) to a third party that would not align with the original purpose and therefore unlawful. l

You must ensure that the personal information is complete, accurate and up to date and is accessible to the data subject if they require it.

Keep personal information confidential and do not disclose it

You must keep the personal information that comes to your knowledge confidential.

It is likely that business sector or trade that you are in already has a legal and professional duty to maintain the confidentiality. By way of example, medical professionals have a duty of confidentially in respect of a patient's health. Banks have a duty to keep their clients' information confidential (also known as bank secrecy Accounting professionals are required to maintain confidentiality in accordance with the IRBA cod and educational institutions have a duty to sensitively deal with information in relation to children. POPIA continues this requirement but also explains that you can disclose information to third parties or to persons within your respective institution without the data subject's consent if the disclosure is necessary to perform a contract to which a data subject is a party or where consent is necessary for the responsible party's legitimate interests or those of a third party.

You can also disclose personal information if required by law, for example, where the information is required to be disclosed in terms of the Promotion of Access to Information Act or to a regulator.

The safest method however is to ensure that you only share the information with people who need to know.

Where you use third party service providers (called operators) such as: fin-tech providers that provide data analytics solutions to banks and FSPs for example, Computer Aided Design (CAD) software providers for entities or professionals in the built environment, uniform and textbook suppliers for educational institutions, or entities that assist you with the processing of FICA information they will need to your authorization or knowledge to process information on your behalf. This is because POPIA requires an operator or anyone processing personal information on behalf of a responsible party to do so with the knowledge or authorization of the responsible party. In other words, an operator must process the information based on the instructions of the responsible party. However, you need to ensure that your third-party service providers are processing the personal information in accordance with the POPIA requirements and ensure that contracts with your service providers contain appropriate warranties and indemnities regarding POPIA compliance.

Security of personal information is paramount
The biggest exposure under POPIA is the required security safeguarding of personal information. You must take reasonable measures to prevent the loss or damage to or the unauthorized destruction of personal information that is in their possession. You must ensure that you or any operator who processes personal information on your behalf establish and maintain the security measures required by POPIA. To give effect to the above, you must identify: the risks to personal information, establish and maintain safeguards against risks, regularly verify the effectiveness of those safeguards and update the safeguards if new risks are identified.

A lot of data breaches occur due to hacking but also due to human error, for example, leaving a client, employee, or customer file out in the open and it gets lost. Or a flash stick is misplaced. It is often the human element that places institutions most at risk when it comes to data privacy and protection and you need to ensure that you have secure and modern systems in place to protect the information of your patients and of your employees.

Any operator who processes personal information on your behalf will also need to establish and maintain the security measures required by POPIA.

Direct marketing
A separate chapter in POPIA is devoted to the rights of data subjects regarding direct marketing.

An organization may not contact a prospective customer through automated calls, email or SMS to promote any products or services without that person's consent. This is especially so for the financial services industry. A data subject must be given the opportunity to object to the use of their contact details for direct marketing purposes and may request that such communications cease.

This is in line with the direct marketing provisions of the Consumer Protection Act, 2008.

Cross-border transactions
Restrictions are placed on the cross-border transfer of personal information in and out of South Africa including the requirement of consent or contractual necessity. The person receiving the data offshore must be subject to laws specifying an adequate level of data protection that is no less than that in the country of origin of the information. Data or personal information collected and sent to, for instance, the UK or the EU will be sufficiently protected but the data subject must be told and consent to the information going offshore.

Record retention periods
Personal information may not be retained longer than is necessary to fulfil the original purpose for collection except where 1) the data subject consents, 2) the retention is required by contract between the parties or 3) where the further retention of the records is required by law.

You must destroy or delete or de-identify personal information as soon as reasonably practicable after authorisation to retain the records ends. Deleting information from an IT system is not the same as destroying it. Destroying requires physical deletion such as shredding or burning of the information in hardcopy or de-encrypting or using software to overwrite electronic records.

By way of example, the Financial Intelligence Centre Act of requires accountable institutions (banks, attorneys, investment brokers, insurance companies board of executors or trust company, accountants) to keep certain personal information for specified transaction or relationships for a period of 5 years.

Enforcement: Penalties and offences
POPIA creates significant civil and criminal law exposure where there are breaches. A civil remedy is provided to the person whose data privacy is breached, whether or not there is intent or negligence on the part of the responsible party.

Contraventions of certain provisions of POPIA are a criminal offence, rendering the offender liable to a fine (with a maximum of R10 million) or imprisonment up to 10 years or to both a fine and imprisonment. So, ensuring efficient and working systems to protect the confidentiality of personal information is essential.

Conclusion
Generally, obtaining the data subject's consent will overcome any hurdles to the provision of processing personal information during processing and thereafter. However, consent is not the preferred method as it can be easily withdrawn and cumbersome to keep record of. As such, and before drafting obtaining consent or including consent clauses in your contracts, you should ask: are you asking for consent where you do not need it? Where you do need the consent, is it valid under POPIA? What information do you hold for personal identifiable clients, suppliers or employees etc.

Your contracts with third parties or operators need to include POPIA compliant clauses including appropriate warranties and indemnities as to compliance by those third parties in so far as confidentiality and security measures is concerned.

As institutions or practices that generally deal with sensitive and confidential information, you should already have adequate systems in place to protect personal information. But a thorough review of your current systems and security safeguards is necessary as good business practice but also in terms of POPIA.