PROTECTION OF PERSONAL INFORMATION ACT: FREQUENTLY ASKED QUESTIONS

What does POPIA stand for?

The Protection of Personal Information Act 4 of 2013.

What is the purpose of POPIA?

The purpose is to regulate the processing of Personal Information. It is aimed to encourage the flow of information in a secure and responsible manner. The spirit of POPIA is to ensure that organisations that hold and process personal information do so carefully and with respect for the rights and interests of the people to whom it pertains.

Who does POPIA apply to?

Public and Private Sector

Natural and Juristic persons (meaning registered companies and organisations)

Paper and electronic records

What is considered personal information?

Personal information is information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing, juristic person. Therefore, any information about an identifiable human being or an identifiable company.

Examples of personal information include: race, gender, sex, marital status, nationality, sexual orientation, age, physical or mental health, disability, religion, language, education, medical, financial, employment information, ID number, email, address, telephone number, location information, blood type, biometric information, personal opinions, preferences, private or confidential correspondence, and views or opinions of another person.

Why did POPIA come into effect?

It is becoming more difficult to protect the privacy of information, as information becomes more vulnerable to new threats that keep emerging. Worldwide data protection (e.g General Data Protection Regulation or GDPR of Europe) is becoming more recognised as a fundamental business practice which cannot be ignored. Failure to do so could have dire consequences for a business' brands and reputation.

POPIA aims to give effect to the constitutional right to privacy, whilst balancing this against competing rights and interests, particularly the right of access to information.

By when do we have to comply to POPIA?

POPIA was signed into law on 19 November 2013 and has come into force incrementally.13 Section 114 of POPIA, which came into force on 1 July 2020, requires compliance with POPIA within one year from the date of its commencement. Accordingly, all responsible parties will be required to have compliance measures in place by 30 June 2021.

What is the definition of a Responsible Party?

The public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

Who is an Operator?

A person or body which processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, if a third-party company is contracted to manage your employees' tax then they would be considered an operator, because they process personal information on your behalf.

What laws are linked to POPIA?

There are various other laws that also protect personal information. The key ones are:

- Consumer Protection Act (CPA)
- National Credit Act (NCA)
- Regulation of Interception of Communications Act (RICA)
- Promotion of Access to Information Act (PAIA)
- Electronic Communication Act (ECTA)
- Cybercrimes Bill
- your Constitutional Right to Privacy as defined in the Bill of Rights

Who is a Data Subject?

A person who provides information about himself/herself. These can be individuals or businesses.

How much information about a person can I collect, process and use?

POPIA requires you to apply the principle of minimality and only collect personal information that you absolutely need to be able to service a customer, staff member or third party. Since POPIA also requires that you specify the reasons for the collection of personal information, if you don't have a valid reason for why you need certain personal information, you shouldn't be collecting it.

What is the Information Officer?

An individual who works within a private or public body and has been designated, in compliance with section 56 of POPIA, to be responsible for ensuring compliance with POPIA and the Promotion of Access to Information Act (PAIA). They must be registered with the Information Regulator.

Why must I worry about personal information leaving South Africa?

Not all countries have adequate data protection or privacy legislation. Transferring personal information to such countries without taking appropriate measures will render the transfer illegal. It is important to have a contract in place with the other party where they agree to abide by POPIA.

Can I transfer personal information into and out of South Africa?

You may, when the recipient in the other country is subject to a law, binding corporate rules or agreements that provide an adequate level of protection that effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject in South Africa. If the other country does not have such rules in place, you can copy POPIA stipulations into the contract agreement and ensure the other third party complies with it.

What does “consent” mean?

Consent is one of the justifications for the lawful processing of personal information. If the data subject is a child, consent must be provided by a competent person.

Consent is defined in POPIA to mean any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

A data subject may withdraw consent at any time, provided that the withdrawal will not affect the lawfulness of the processing which occurred before the withdrawal of consent.

What is “processing”?

Processing means any operation or activity, whether or not by automatic means, concerning personal information including:

OBTAINING:
Collection, Receipt, Recording, Organisation, Collation, Storage, Updating, Modification, Retrieval, Alteration

DISSEMINATION:
Transmission, Distribution, Making available

DESTROYING:
Merging, Linking, Restriction, Erasure, Destruction

What are common examples of breach of POPIA?

- Loss of personal information due to inadequate security safeguards

- Collecting personal information without having obtained the necessary consent
- Sending personal information to people who are not supposed to have it
- Breach of security safeguards (network with personal information is hacked)
- Not complying with an enforcement notice issued by the Information Regulator
- Processing special personal information without there being a necessity

What can I not do with personal information?

Use it for any purpose other than the purpose for which it was authorised.

Who can I send personal information to?

Only people and organisations authorised by the data subject or those people and organisations allowed under POPIA. Once you have established justification for forwarding the personal information you must ensure that those people or organisations also comply with POPIA and have appropriate security safeguards.

What are the POPIA conditions POPIA prescribes of protecting personal information?

There are eight conditions and four special conditions. The eight conditions are Accountability, Processing Limitation, Purpose Specification, Further Processing Limitation, Information Quality, Openness, Security Safeguards and Data Subject Participation. The four special conditions are Secure Cross Border Flow, Permission for Direct Marketing, Secure Special Personal Information and Automatic Decision Making.

How should we get consent?

- A person must have a choice whether to consent or not (it must be voluntary)
- The consent must relate to a specific purpose and you must specify your purpose.
- You must notify the data subject of various things as set out in section 18 of POPIA.
- You must inform the person sufficiently to enable them to make a decision.
- The person must express their will in some form.

Who can have access to personal information?

Authorised people using the specific personal information for its intended purpose.

How does POPIA apply to company information?

A juristic person (non-natural) is regarded as an entity covered by POPIA. Therefore, organisations also have personal information and special personal information as defined by POPIA.

What happens if we don’t comply with POPIA?

There are significant consequences for non-compliance, including up to R10m in fines per offence and/or up to 10 years in prison per offence.

How long must I retain Personal Information?

This must be defined in the Records Retention Policy on how long you retain personal information and other confidential information for all data subjects. Only for as long as to fulfil the intended purpose for which the information was collected or processed. Keep in mind other legislative requirements.

Can I keep personal information for longer than the legally prescribed period?

Your Records Retention Policy will inform retention periods for all types of personal information you collect from your data subjects. If there is a valid business reason as to why you should keep the information beyond the prescribed retention periods, you can do so, provided that you have informed the Regulator and the Data Subject of the intention and purpose.

When am I exempt from following what POPIA prescribes?

When certain permissions were obtained from the Information Regulator. Certain laws may trump certain POPIA rules, for example data subject requests in the insurance industry where the only information available on a person is that they are a beneficiary on a person's policy. In this instance, the Insurance Act forbids that a company disclose to a person if they are a beneficiary on someone's policy. There may be other scenarios that emerge that could justify certain exemptions to POPIA (these may typically be fraud-related issues where disclosing to data subjects the use of their information for investigations could be detrimental to the case).

I hear a lot of talk about changing behaviour. Why is it so important?

The challenge and success of becoming POPIA compliant will depend largely on people's adoption of various data protection practices. If you don't bring your people on board, you will fail to achieve the desired behaviours you are trying to achieve (i.e. people taking personal accountability for protecting personal information).

Am I responsible for the security of documents that I store at a storage company?

Absolutely. You have the responsibility to ensure that we have a contract in place with your storage vendor to ensure that they have the appropriate controls in place to ensure all physical documents stored on their premises will be safeguarded and protected.

What do I have to do to be a lawful processor of personal information?

You must be registered with the Informational Regulator as a lawful processing entity.

Is anyone exempt from complying with POPIA?

No, although there are all sorts of exemptions in the Act for specific scenarios and everyone must be aware of what they are as they need to comply with certain criteria to then be able to invoke the exemption.

Can POPIA be compared to the Secrecy Bill?

No, as they are designed for two different reasons. The Secrecy Bill is not actually a well–favoured piece of legislation as it is designed to classify certain pieces of data as “secret” which then means there is the concern that bodies with a vested interest can declare the detail “secret” and then conduct their activities in “secret” without being obliged to inform Joe Public. They are expressly protected by making it a crime if the data or information is divulged. POPIA is the opposite as it protects our right to privacy and puts the accountability on the responsible parties to ensure they apply practical and reasonable measures to protect data subjects’ information from being comprised.

Does POPIA put an end to Direct Marketing?

No. POPIA is not going to put an end to direct marketing. Direct marketing happens all over the world in many countries that have had data protection laws for decades. Direct marketing is a legitimate interest that organisations can pursue to find new customers. The big change or implication of POPIA is that in future direct electronic marketing to potential customers will be on an opt-in basis.

Can we email or SMS someone to sell them something?

Yes, you can. POPIA will have a big impact on email and SMS marketing. You can currently email market on an opt-out basis. This means you can send anyone emails until the person asks you to stop. Under POPIA, you will only be able to direct market on an opt-in basis – you can email someone only once to get their consent to send them more emails.

Can I store job applicants’ CVs indefinitely, even after their application have failed?

No, unless you have obtained their specific consent for this.

Can I keep personal information about employees that have left our employment?

You are required by certain laws to keep records of staff (even when they leave) for certain periods of time. Beyond this retention period, you should dispose of the information. The retention period for employees that have left the organisation should be defined in the Records Retention Policy.

Can employees keep customer information on desktops?

For the purposes on Business as Usual (BAU) and BAU only, with respect to POPIA, employees may keep electronic records on their desktops and hard copies on their desks. The Record Retention Policy will shed more light on the retention of information held on desktops and local drives.

Can employees exchange customers’ personal details?

Yes and no. It depends on the context of the situation. If it is business-related, i.e. for the intention of servicing the customer (e.g. resolving a query or complaint) then yes, it is normal that a customer’s information would need to be shared across departments to get an issue resolved. Sharing a customer’s information with a friend or relative to assist their business in finding customers or for example is sending a customer list to a competitor is strictly forbidden.

What's in it for me?

Your privacy is protected.

How does POPIA apply to supplier information?

As the responsible party, you share certain personal information with suppliers that you interact with. It is important to have formal third–party agreements with all your suppliers, especially the ones that make use of your data subject's personal information to provide services on your behalf. This contract between you and your supplier prescribes the privacy and requirements that you can hold your suppliers accountable to with regards to the processing of personal information.

Will I be held liable if I get a third party to process personal information on my behalf?

Yes, if a third party or supplier breaches any of your customer, employee or other suppliers' information, you will still remain accountable and liable to the data subject. You can be found to be in breach of POPIA and will be liable for the penalties.

What happens when a third party breaches POPIA?

A third party is held to be Operator in terms of POPIA. That means they are still responsible for what happens by way of the contract they would have concluded with you before they started to act on your behalf. Your Head of Privacy will then have to deal with the breach according to your Incident and Breach Management procedures.

Do cloud solutions have to comply with POPIA?

Absolutely. There is a vast array of concerns. While in transit, the personal information must be protected (encrypted, de-identified if possible). The cloud environment, if in another country, must provide the same if not more protection as is required in South Africa.

Do cross-border cloud solutions have to be compliant?

Absolutely. If your cloud service is based in another country, it is your responsibility to ensure that the contracted provider, meet certain privacy requirements. You should also ensure that, if you enter into a relationship with them, they will uphold the same principles as prescribed in POPIA.