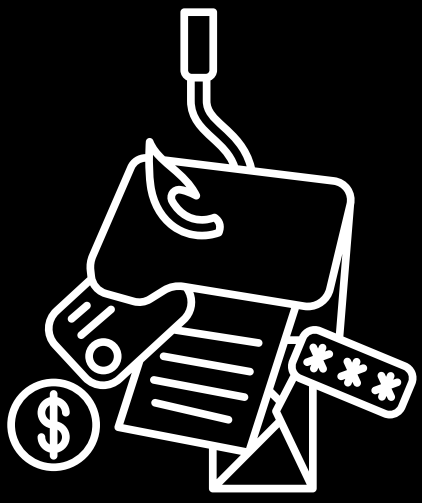


SMBsecure™

# POPIA & Device Security

**Your Compliance Questions Answered**

*Drafted by:*

michalsons

Leading Legal Insight on the POPIA.
www.michalsons.co.za


***smbsecure.co.za***

# I. What POPIA Requires

POPIA includes a number of stated conditions, and each must be fulfilled in order for an organisation to remain in compliance with the law. POPIA's provisions require the Responsible Party to define the purpose for which they collect personal information, and inform the individual of what that purpose is.

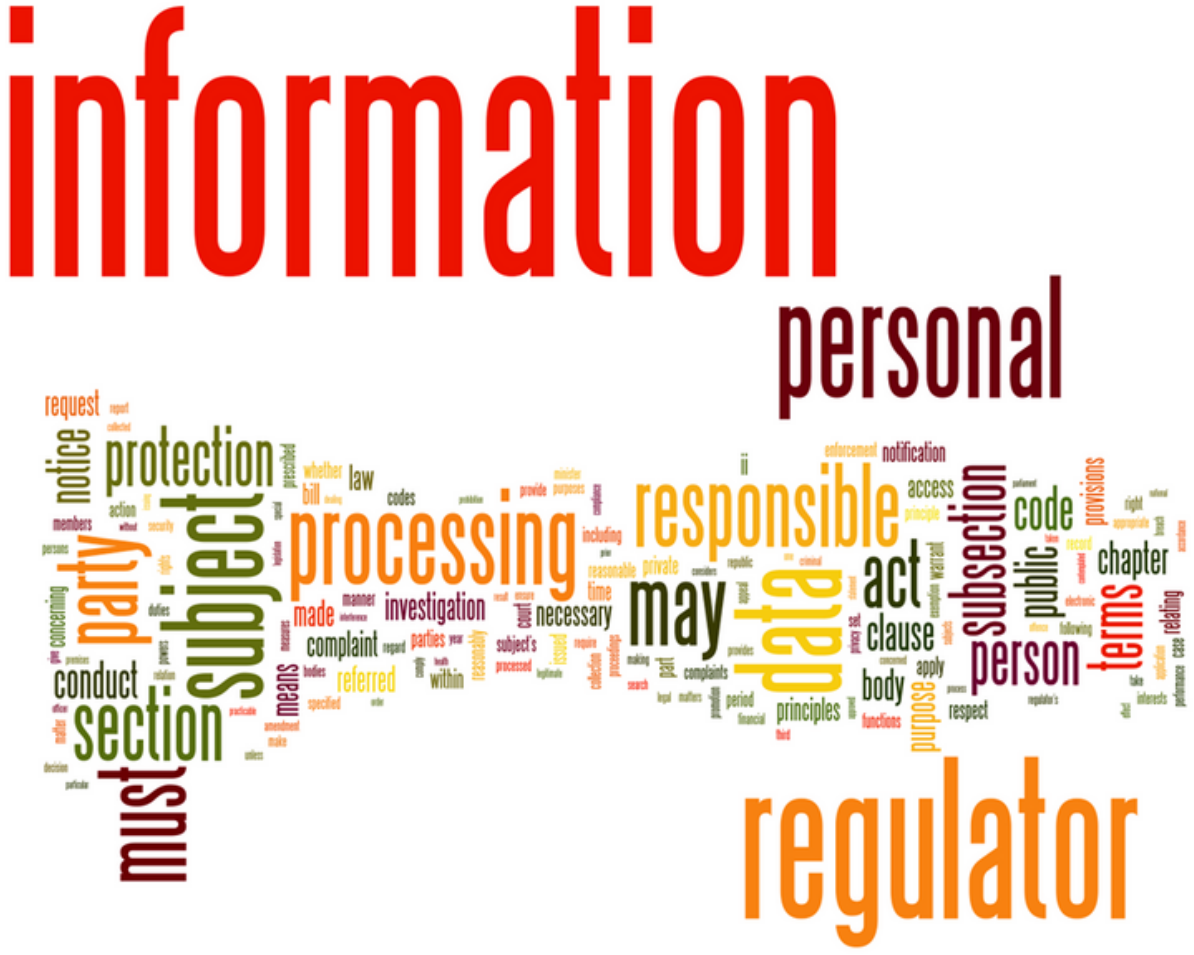
The personal information must be complete, accurate and kept up to date.

Organisations should secure the integrity of the personal information that they process. POPIA requires the party who is processing the information to inform both the Information Regulator and the data subject if they suspect a breach.

The Information Regulator regulates POPIA (https://inforegulator.org.za). Parliament has gone to great lengths to give this regulator teeth. There are significant consequences for non-compliance, including:

- Suffer reputational damage.
- Lose customers and fail to attract new ones.
- Pay out millions in damages in a civil class action.
- Be fined up to R10 million or face 10 years in jail for committing an offence.

Of these, reputational damage is likely the biggest risk and most potentially harmful to an organisation.



# II. How POPIA affects South African Businesses and Organisations

POPIA sets conditions that any organisation processing personal information must comply with. Under POPIA, organisations in South Africa are required to protect the personal information they process.

Organisations store data (including personal information) on many different types of devices, from PCs and company networks to mobile devices (such as phones, tablets and USB drives), including employee-owned BYOD devices. POPIA requires you to protect the personal information on those devices. Some organisation will require special permission from the regulator for processing certain types of information as defined by the Act.

## Q&A:

## Does POPIA apply to everybody?

Yes, virtually everybody. POPIA applies to anyone who processes personal information. It applies to all public (like Municipalities and SARS) and private bodies (like financial institutions, healthcare providers and direct marketers).

### Key Ponts and Possible Actions

- POPIA applies to Government, companies, close corporations, and partnerships.
- POPIA has a big impact on anybody in the financial services, healthcare or marketing sectors.
- POPIA also applies to small and micro businesses, including sole proprietors.
- Charities, Non-Governmental Organisations (NGOs), and Not-for-Profit Organisations (NPOs) are all required to comply with POPIA
- POPIA also applies to Schools and Further Education and Training (FET) colleges.

## Who is exempt from complying with POPIA?

Very few people, examples are SAPS and Cabinet, and journalists who process personal information for journalistic reasons.

Some processing of personal information is exempt as well, for example, processing personal information in the course of a purely personal or household activity.

## Do you have to comply with POPIA?

Yes, you must comply with POPIA (and the consequences for non-compliance are quite severe). While this is the case, you do want to adhere to the law efficiently and get business value from your efforts.

### Key Ponts and Possible Actions

- POPIA almost certainly applies to you and you are not exempt. You must comply.
- You should do what is reasonably practicable to protect personal information.

## Who is the responsible party when personal information is processed?

If you have decided to process personal information in a certain way, then you are the responsible party. The responsible party is the person that, alone or in conjunction with others, determines the purpose of and means (the why and the how) for processing personal information.

If you are processing personal information for somebody else, you are their operator and they are the responsible party. The responsible party can and should subject operators to requirements of POPIA in support of its own compliance initiatives.

## Does POPIA only relate to consumer data?

No, it relates to all personal information. Almost all consumer data is personal information, but personal information is much broader than just consumer data. For example, personal information includes any personal information pertaining to employees.

## Does POPIA apply outside of South Africa?

Yes, POPIA does apply outside of South Africa. A responsible party does not need to be domiciled in South Africa for POPIA to apply. If the responsible party uses equipment in South Africa to process information, then POPIA applies to that information.

# III. What POPIA means to you as a custodian of personal Information

Personal information includes information like race, gender, age and education, as well as the medical, financial, criminal or employment history of a person. Contact details like an email address, telephone number or location information are also included.

Personal information is any information that relates to an identifiable, living, natural person. In other words it is information that identifies a human being. In some circumstances it can also be information that identifies an existing juristic person, such as a company, close corporation or trust.

**The conditions for lawful processing under POPIA apply even if personal information is public knowledge.**

### Key Ponts and Possible Actions

- Personal information includes a broad category of information.
- Personal information will likely be included amongst all of your records and devices.
- Information that has had the person's identity removed is not personal information.
- Information about a company can also be personal information.
- POPIA applies to personal information that is public information.

# Q&A:

## Does the law now require information Security?

Yes, it does. You may have already been securing the information that you hold because it made business sense to do so. POPIA now places a legal obligation on you to secure the information you process. You must secure both the integrity and confidentiality of any personal information by taking appropriate, reasonable technical (such as using encryption) and organisational (such as policy) measures to prevent loss and unlawful access (hacking).

## What is appropriate and reasonable information security

Considering the type of personal information that needs to be protected, there are certain preparations that will be considered appropriate and reasonable measures to take. One of those is to use encryption and policies to secure personal information on mobile devices. Mobile devices containing personal information put that data at higher risk of loss or theft. You need to secure that information, and be in a position to adequately prove the security measures.

### Key Ponts and Possible Actions

- The law requires you to take both technical and organisational measures.
- If you allow employees to use mobile data devices including laptops, phones, tablets and USB drives, you must take measures to secure them. This will include both company and employee-owned devices, and could extend to operator devices.

## What will happen to you if you recklessly disclose personal information?

You could be fined R10 million or jailed for up to 10 years, if you:

- Obstruct the Regulator.
- Fail to comply with an Enforcement Notice from the Regulator.
- Give false evidence before the Regulators under oath.

## What will happen to you, if you recklessly disclose a bank account number?

You could be fined R10 million or jailed for up to 10 years, if you:

- Fail to comply with the conditions when processing account numbers.
- Knowingly or recklessly obtain or disclose an account number.
- Sell (or offer to sell) an account number.

### Key Ponts and Possible Actions

- Focus on account numbers. It is important to secure devices that have account numbers on them.
- If you get fined, seriously consider paying the fine. If you don't, you could get a criminal record, suffer reputational damage, have to pay huge legal fees, risk a Magistrate making an adverse finding against you.

# Does cost play a role in determining what is reasonable?

Yes it does. POPIA requires the responsible party to do what is reasonably practicable to comply with POPIA. The organisation must be able to show that they have taken the appropriate steps in protecting the information.

In considering whether an organisation took reasonable measures to protect data, the information regulator (or a court) will take into account how much money the organisation had available to protect this information.

# Must you encrypt personal information?

Yes, because it is a key technical measure for securing data. Encryption is the first line of defence for sensitive data and is a key aspect of complying with POPIA. However, encryption is often not fully sufficient on its own. For example, if somebody knows or hacks a password they can bypass the encryption.

Your chosen technical measure should include functionality to go beyond encryption to provide adequate security safeguards where encryption alone cannot protect the data.

# Must you use email encryption when sending emails containing personal infromation?

Yes. Although POPIA does not explicitly deal with email encryption, it does require you to take security measures that are appropriate and reasonable in relation to the nature of the personal information you process. If you send an email that contains personal information of such a nature that data subjects could suffer adverse harm if the email were hacked, it would be appropriate and reasonable to ensure that it is encrypted. The regulator would not look kindly on you if you were to send it unencrypted. Further to this point, data protection authorities around the world recognise encryption as one of the generally appropriate and reasonable security measures that you must take.

While the answer under POPIA requires you to consider a number of factors before you can determine whether to encrypt an email or not, policies like the Minimum Information Security Standards (MISS) have more explicit requirements for both public and private bodies transmitting important government information.

## Key Ponts and Possible Actions

- Email encryption is one of the ways to protect data subjects from harm and further comply with POPIA.
- When determining whether to encrypt an email, ask yourself, "would data subjects suffer adverse harm if this email were hacked or if the content were accessed by an unauthorized person on the recipient's device or mailbox?"

# Can I still make use of cloud services?

Yes, you can. A business-grade cloud service provider usually provides strong security to offer their services and to earn the trust from the market, often with sufficient audit certifications and privacy policies to validate their practices and their treatment of customer data.

Consumer cloud services (also referred to as personal clouds) must be carefully reviewed for business use.

Under POPIA, to deal with data sovereignty it will require a data transfer agreement or for you to be made aware and consent to the transfer of data.

SMBsecure is cloud-based service. It allows you to protect your information and manage the security of your devices using remote encryption and policy management from the cloud.

### Key Ponts and Possible Actions

- POPIA allows for use of the cloud.
- Using the cloud can be an effective way of protecting personal information.

# If you lose a device, must you tell the regulator?

Yes. If there are reasonable grounds for you to believe that an un-authorised person has accessed the personal information, you must notify:

- the Information Regulator, and
- each of the data subjects involved.

**Note:** This can have serious practical and reputational issues for you and your organisation.

# Can an employee complain that you have access to the device?

No, but if you want to take extra measures along these lines, you can secure employees' consent as part of your device security policy. Often this is done through a company policy, such as a Monitoring Policy, BYOD Policy or Acceptable Use Policy.

# Is it lawful to monitor apps on devices?

Yes, you don't need to get consent. A Monitoring or BYOD Policy often covers this. Personal devices used to carry on business can be monitored without the consent of the data subject.

# What about protection of state information?

The Protection of state information Act (POSI) and POPIA are different laws, and are not to be confused!

# What laws are linked to POPIA?

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

1. Consumer Protection Act (CPA)
2. National Credit Act (NCA)
3. Regulation of interception of Communication and Provision of Communication Information Act (RICA)
4. Promotion of access to Information Act (PAIA)
5. Cybercrimes Act

If there is a conflict between POPIA and another law, POPIA prevails. However, if another law gives greater protection to personal information, that other law prevails. For example, if POPIA says you do not need to get consent to market to someone and another law (like the NCA) says you do, the NCA will apply, and you will have to get the persons consent.

There are various other laws, rules, codes or standards that relate to (Information Technology) IT as well.

# What is PCI-DSS and is this different?

PCI DSS stands for the Payment Card Industry Data Security Standard. It requires organisations that process credit card information to keep it secure. It is different to POPIA and requires greater security than POPIA when it comes to credit card holder information.

### Key Ponts and Possible Actions

- Be aware of laws, rules, codes or standards that relate to IT.
- You must comply with PCI-DSS if you process credit card holder information.

# What about the rest of the world?

There have been data protection laws in the EU and UK for many years. South Africa is rightly following in the footsteps of the rest of the world – it is not trying to lead the way or be different. POPIA brings South Africa in line with the rest of the world.

The United States is currently enacting many new data privacy laws. As are many countries in Africa.

### Key Ponts and Possible Actions

- The EU and the UK data protection laws prohibit the transfer of data to countries that do not have the same level of data protection as them.
- The United States is no longer recognized as a safe harbor for personal information and therefore personal information can only be transferred there on meeting certain requirements.

# Can data be transferred across borders?

You as a responsible party must protect the personal information of your data subjects when the data is transferred to a third party in another country. The other country may not have the same level of data protection as your country.

POPIA says that personal information may not cross borders unless there are measures in place, like:

- There are binding agreements providing adequate protection between the responsible party and the third party;
- The data subjects gives their consent;
- The data transfer is necessary for the performance of a contract;
- The transfer is for the benefit of the data subject.

# What are useful links for more information?

- https://www.michalsons.com
- https://inforegulator.org.za
- https://www.beachheadsolutions.com/
- https://encryption4outlook.com/

# IV. Practical guidance on POPIA and how to comply

### Key Ponts and Possible Actions

1. Be responsible when processing personal information.
2. Take practical effective steps to protect personal information whenever possible.
3. Monitoring solutions for organisational owned mobile devices can be effective in recovering lost or stolen items and safeguarding crucial data.
4. There are both legal and business benefits to be gained from securing your information.
5. Fines, reputational damages, legal fees and customer communication costs will be more dire impacts of POPIA on any organisation.

# Q&A on SMBsecure as a practical solution:

- SMBsecure helps you to comply with the POPIA law, while also offering significant business benefits.
- SMBsecure can help you to protect and safeguard the personal information you might possess as a Responsible Party on mobile devices, including laptops, phones, tablets, and USB drives.
- With SMBsecure you can encrypt data or devices, as well as remotely monitor and quarantine or wipe data as necessary to keep it from being exposed.
- SMBsecure Email Encryption can help you secure and encrypt personal or sensitive data being emailed from the Outlook desktop client on Windows PC. The plugin for Microsoft Outlook uses open standard portable document format (PDF) so it is very easy for the recipient to open an encrypted PDF on any device (using a password), just as banks do when sending bank statements to you.
- By using SMBsecure, you do not only apply, but can adequately prove the technical controls for compliance, through adequate auditing and reporting. Such validations are vital, but often missed and forgotten when standalone solutions are implemented, especially in smaller organisations.

# If you use SMBsecure, must you still notify regulators in the event of a lost or stolen device?

No, you do not have to notify the information regulator or the data subjects, because an unauthorised person is unlikely to have accessed the personal information. There are three key elements to SMBsecure that make this happen:

1. Encryption
2. Access controls & Security policies
3. Reporting for auditing and validations

Encryption is a way of using keys to lock access to electronic data. Security policies may make it so that if the device does not check-in with the server after a period of time, or a user enters an incorrect password too many times, the device is locked. These policies will execute even though the device is not connected to the Internet, and you are able to set custom rules. SMBsecure takes protective actions even though the device may not be connected to the Internet when using the premium service.

### Key Ponts and Possible Actions

- SMBsecure prevents an unauthorised person accessing the personal information.
- If you use SMBsecure and a device is lost or stolen, you do not need to notify the information regulator or data subjects.
- SMBsecure reports can be leveraged to audit and validate the reasonable steps and action taken on a lost or stolen device to mitigate the risk of personal information exposure as proof to an auditor or the regulator.

# Is the SMBsecure datacenter secure?

Yes, it is. SMBsecure is powered by Beachhead whose servers are hosted with Rackspace, one of the biggest and most trusted cloud companies in the world. They take information security very seriously, and take appropriate, reasonable technical and organisational measures to prevent loss and unlawful access of the data. They are certified for ISO27001 Service Organisational Control (SOC 2) and Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization, abbreviated as SSAE16, which replaced the Statement on Auditing Standards No. 70, commonly abbreviated as SAS 70.

# Does SMBsecure store my data files on its servers?

No, SMBsecure does not store any data files on its servers. SMBsecure only stores data related to the device, like username, computer (or device) name and specifications, IP address, filenames, and users' email address, mobile number and name. It stores just the names of files and not the contents. SMBsecure does not store anything more than the active directory. In fact, it is less than the active directory. If location is switched on, SMBsecure may know the location of the mobile device. But SMBsecure will only process this information if the user allows location permissions to the app.

SMBsecure is not like a backup service and therefore does not store any data files, encrypted or not, on its servers.

No company data other than what is described above can be found on the SMBsecure servers.

### Key Ponts and Possible Actions

- SMBsecure stores very little data. It only stores data related to the device.
- Actual data files are not stored within the SMBsecure cloud-based accounts.

# Will SMBsecure reduce the performance of my device?

No it does not, because SMBsecure simply builds on what is natively resident on the device. It is not a foreign module - it simply leverages off the crypto technologies that are on the device (for example BitLocker Volume Encryption on a Windows PC).

# Does SMBsecure intercept data messages?

No. SMBsecure may store information about communications, but it does not intercept the communications themselves or have access to the communications.

# Can it help with staff exit procedures?

Yes it can. As soon as an employee resigns or contractors exit a project, you can schedule SMBsecure to execute data removal policies on their PC the date the person leaves when using the Premium service.

# Can SMBsecure safeguard personal information on USB drives and memory sticks?

Yes, Memory sticks are high risk because people can copy large amounts of personal information onto them and they be easily lost or stolen because they its small size and portability. SMBsecure can do port blocking and when using the Premium service it can also protect the data on a memory stick the same way it does with other mobile devices, but provides protection and traceability beyond just creating an encryption vault; spanning functions including access control to rights management.

# Can SMBsecure safeguard personal information we send via email and help us comply with POPIA?

Yes. Email encryption is one of the ways to protect data subjects from harm and further comply with POPIA. The neat and simple SMBsecure plugin for Outlook on PC can help you to accomplish end-to-end encryption for personal data being emailed and provides sufficient features and functions to accommodate most requirements.

## Key benefits of SMBsecure

- It is an appropriate and reasonable measure you can take to the protect personal information on devices, which will prevent reputational damage and fines.
- It is cloud based, which makes it easy to use, flexible and easy to access.
- It has a low impact on the user, which means users can get the most out of their devices.
- It is simple, which will save you money not having to train people and spend excessive administrator time.
- It will prevent legal problems and disputes.
- It will protect people from harm by protecting their personal information.
- It will ensure you get a better return on your investment when leveraging existing native technology (like Bitlocker).