POPI and Device Security:

Your Compliance Questions Answered

Drafted by

michalsons

Leading legal insight on the POPI Act.
www.michalsons.co.za

With Compliments

ASG
Your Outsourced IT Department

www.asg.co.za 011 975 7521

info@asg.co.za

Contents

Summary

This guide will answer your questions about the impact that the South African Protection of Personal Information Act (POPI) will have on device security and how to prepare your organisation for the enforcement of POPI.

POPI, signed by the President in November 2013, is an extensive piece of legislation that will affect the business practices of any organisation that processes personal information of any natural or juristic person.
POPI is intended to protect people from harm, for example becoming victims of identity theft.

This guide will cover:

I. What POPI requires
II. How POPI affects South African businesses and organisations
III. What POPI means to you as a custodian of personal information
IV. Practical guidance on POPI & How to comply

I. What POPI requires

POPI stands for the South African ***Protection of Personal Information Act*** (Nov, 2013) and includes a number of stated conditions, and each must be fulfilled in order for an organisation to remain in compliance with the law. POPI's provisions require the ***responsible party*** to define the purpose for which they collect personal information, and to inform the individual or ***data subject*** 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. POPI 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 POPI (www.informationregulator.co.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 .[i]
- Be fined up to R10 million or face 10 years in jail for committing an offence.

Reputational damage is likely the biggest risk and most potentially harmful to an organisation.

II. How POPI affects South African businesses and organisations

POPI sets conditions that any organisation processing personal information must comply with. Under POPI, 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 (phones, tablets and USB drives), including employee-owned BYOD devices. POPI requires you to protect the personal information on these devices too. Some organisations will require special permission from the regulator for processing certain types of information as defined by the Act.

Q&A:

Does POPI apply to everybody?

Yes, virtually everybody. POPI applies to any organisation 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 points and possible actions

- POPI applies to Government, companies, close corporations, and partnerships.
- POPI has a big impact on anybody in the financial services, healthcare or marketing sectors.
- POPI 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 POPI.
- POPI also applies to Schools and Further Education and Training (FET) colleges.

Who is exempt from complying with POPI?

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 [v].

Do you have to comply with POPI?

Yes, you must comply with POPI (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 points and possible actions

- POPI 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 any 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 POPI in support its own compliance initiatives.

Does POPI 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 POPI apply outside of South Africa?

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

III. What POPI 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 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 ***personal information 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 or trust.***

Under POPI, these are known as your data subjects.

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

Key points and possible actions

- Personal information includes a broad category of information.
- Personal information will likely be included amongst all of your records and data-devices.
- Information that has had the person's identity removed is not personal information.
- Information about a company can also be personal information.
- POPI can apply 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. ***POPI 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) [vii].

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.*** Mobile devices containing personal information, be it company or employee-owned BYOD devices, 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 points 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 as well.

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 [i]
- Fail to comply with an Enforcement Notice from the Regulator
- Give false evidence before the Regulator 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 points and possible actions

- Focus on account numbers. It is especially 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, 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. POPI requires the responsible party to do what is reasonably practicable to comply with POPI. The company 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 POPI. 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 alone to provide adequate security safeguards to protect the data.

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 POPI, to deal with data sovereignty, cloud services will require a data transfer agreement; or it must make you aware and you consent to the transfer of data.

ASG Managed Endpoint Encryption is a 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 points and possible actions

- POPI allows for use of the cloud.
- Using the cloud can be an effective way of protecting personal information.
- Encrypt your company and employee-owned devices as a key technical measure; extend to operator devices if required to minimise your own risk.

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

Yes. If there are reasonable grounds for you to believe that an unauthorised person has accessed 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 activities can be monitored without the consent of the user.

What about the protection of state information?

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

What laws are linked to POPI?

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 Communications and Provision of Communication-related Information Act (RICA)
4. Promotion of Access to Information Act (PAIA)

If there is a conflict between POPI and another law, POPI prevails. However, if another law gives greater protection to personal information, that other law prevails. For example, if POPI 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 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 POPI and requires greater security than POPI when it comes to credit card holder information.

Key points and possible actions

- Be aware of all laws, rules, codes or standards that relate to IT.
- You must adhere to PCI-DSS requirements 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. POPI 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 points 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. POPI is therefore a vital business enabler for South Africa.
- The United States have been recognised as a safe harbour for personal information and therefore personal information can be transferred there.

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.

POPI 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 transfer is necessary for the performance of a contract;
- The transfer is for the benefit of the data subject.

IV. Practical guidance on POPI and how to comply.

Key points 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 mobile devices can be effective in recovering lost or stolen devices 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 POPI on any organisation.

Q&A on ASG Managed Endpoint Encryption as a practical solution:

- **ASG Managed Endpoint Encryption** helps you to comply with the POPI law, while also offering business benefits.

- **ASG Managed Endpoint Encryption** 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 **ASG Managed Endpoint Encryption** you can encrypt data or devices, remotely monitor devices, as well as quarantine or wipe data as necessary to keep it from being exposed.

- By using **ASG Managed Endpoint Encryption**, 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.

If you use ASG Managed Endpoint Encryption, 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 **ASG Managed Endpoint Encryption** that make this happen:

1. ***Encryption***
2. ***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.

ASG Managed Endpoint Encryption takes protective actions even though the device may not be connected to the Internet.

Key points and possible actions

- **ASG Managed Endpoint Encryption** prevents an unauthorised person accessing the data on devices.
- If you use **ASG Managed Endpoint Encryption** and a device is lost or stolen, you do not need to notify the Information Regulator or the data subjects.
- **ASG Managed Endpoint Encryption** reports can be leveraged to audit and validate the reasonable steps and actions 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 ASG Managed Endpoint Encryption datacentre secure?

Yes, it is. Its 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.

If an ASG Managed Endpoint Encryption customer needs proof of certification it can contact ASG for this.

Does ASG Managed Endpoint Encryption store my data files on its servers?

No, ASG Managed Endpoint Encryption does not store any data files on its servers. ASG Managed Endpoint Encryption only stores data related to the device, like username, computer (or device) name and specifications, IP address, filenames, and users' email address and name. It stores just the names of files and not the contents. ASG Managed Endpoint Encryption does not store anything more than the active directory. In fact, it is less than the active directory. If location-services on a device is switched on, ASG Managed Endpoint Encryption may know the location of the mobile device.

ASG Managed Endpoint Encryption 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 ASG Managed Endpoint Encryption servers.

Key points and possible actions

- ASG Managed Endpoint Encryption stores very little data. It only stores data related to the device for performance of the service / contract .
- Actual data files are not stored within the ASG Managed Endpoint Encryption cloud-based accounts.

Will ASG Managed Endpoint Encryption reduce the performance of my device?

No it should not, because ASG Managed Endpoint Encryption 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 (much like BitLocker Volume-Encryption on a Windows PC or On-Board-Encryption on a phone / tablet.)

Does ASG Managed Endpoint Encryption intercept data messages?

No. ASG Managed Endpoint Encryption 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 ASG Managed Endpoint Encryption to execute data removal policies on their PC the date the person leaves. Military-grade data delete functions can also allow PC hard drives to be reused!

Can ASG Managed Endpoint Encryption 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 can be easily lost or stolen because of its small size and portability. ASG Managed Endpoint Encryption can 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 encrypted secure-vault; spanning functions including access control to rights management.

Key benefits of ASG Managed Endpoint Encryption

- It is an appropriate and reasonable measure you can take to protect personal information on devices, which will prevent reputational damage and fines.
- It is cloud based, which makes it easy to use, flexible, and affordable 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 & spend excessive administrator time.
- It will mitigate 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).

What are useful links for more information?

- www.michalsons.co.za ; www.informationregulator.co.za

About this guide

Disclaimers

1. The content is provided for the jurisdiction of South Africa and is not suitable for other jurisdictions.
2. We give no warranty about it, and none may be implied. We are not responsible for any mistake in the information or any direct or indirect loss that may follow from it.
3. The guidance has been prepared by Michalsons and is based on their interpretation of the principles of South African law at the time of publication. The law may change due to future legislative enactments and court decisions.
4. It is a summary or opinion on general principles of law and is published for general guidance purposes only. The content does not constitute specific legal, tax, investment, accountancy or other professional advice.
5. Seek individual advice from a suitably qualified professional adviser before dealing with any specific situation.

End Notes

i POPI, section 99

ii POPI, section 109.

iii POPI, definition of responsible party iv POPI, 7 v POPI, section 6(1)(a) vi POPI, definition of responsible party vii POPI, section 19 viii POPI, section 100 ix POPI, section 103 x POPI, section 104 xi POPI, section 105(1) xii POPI, section 106(1) xiii POPI, section 106(3) and (4) xiv POPI, section 22(1) xv Section 5 of RICA. xvi http://www.michalsons.co.za/it-laws-ict-laws-rules-codes-and-standards-list/3219 xvii POPI, section 72 xviii http://www.beachheadsolutions.com/privacy-policy/

Drafted by Michalsons – leading legal insight on the POPI Act. Copyright © 2015 Michalsons www.michalsons.co.za

ASG Managed Endpoint Encryption for PCs & Macs

Still the heart and soul of user productivity, there's more data here for thieves than any other mobile device. Plus, industry, national, state and local regulations require encryption – and sometimes elimination – of all at risk consumer data. Still, many businesses fail to comply, leaving customers and employees vulnerable to identity theft, opening the possibility for lawsuits, and allowing sensitive corporate information to escape. Why don't they simply put encryption in place? Many reasons: user productivity is often impaired with traditional encryption software on PCs, implementation can be difficult and often requires purchase of additional software and hardware, and recovery from unintended data access elimination can be arduous (or impossible). And to make matters even more complicated, it is usually impossible to manage PCs from the same console as Macs, phones and tablets.

None of that is true of ASG Managed Endpoint Encryption PC. Managed from the same console as other mobile devices, ASG Managed Endpoint Encryption PC layers an intelligent engine on top of encryption built into the operating systems of all PCs, so the user burdens are wiped away. Plus, ASG's tool can instantly remove user access to data, and uses a patented method to immediately restore the data by pushing one button on the ASG Managed Endpoint Encryption Management Console. Pretty neat trick, huh?

Great, but what about Macs you ask? Fear not – ASG Managed Endpoint Encryption Mac handles this need smoothly.

Features include:

- Immediate data access elimination through patented "quarantine" – persistent shutdown, and elimination of local encryption key (PC only). Instant remote restoration of data access with administrator approval
- Complete data wipe capability when devices are stolen
- Broad range of both administrator-enabled and automatic security responses to threat conditions
- Remote enforcement of password and security policy
- Customisable reporting of status and device risks/conditions plus auditing to support compliance, for example GDPR, Cyber Essentials, POPIA etc.
- Enforced encryption of all sensitive data on the PC or Mac

ASG Managed Endpoint Encryption for Phones & Tablets

Smartphones have become the single most carried, most valuable life tool for many people. Often owned by employees, they are personalized, yet have unlimited access to wads of sensitive data. What happens to that data if the phone is lost or stolen? Is the employee a good corporate citizen who password protected the phone, saved no sensitive materials, and encrypted everything else? Maybe? Who are we kidding? No, we cannot assume ideal phone security.

And what about iPads and Android tablets? They are nearly as portable as phones, but can carry and display data like PCs. Wow, a perfect storm of security risk! And the more tablets get used instead of PCs, the greater the data holdings and the greater the risks.

ASG Managed Endpoint Encryption Phones & Tablets to the rescue! Encryption, application management, password enforcement, location awareness and data elimination are some of the capabilities that are at your disposal, accessed via the same, single, easy to operate policy management console that can be used to manage all your phones, PCs and other devices.

Features include:

- Remote network access shutoff
- Immediate data access elimination through instant lock (All platforms), password reset and - Persistent shutdown (Android only)
- Complete data wipe capability when devices are stolen
- Remote enforcement of password and security policy
- Customisable reporting of status and device risks/conditions plus auditing to support compliance, For example GDPR, Cyber Essentials, POPIA etc.
- Broad range of both administrator-enabled and automatic security responses to threat conditions
- Enforced encryption of all sensitive data on the phone or tablet

This little device may be your biggest data loss vulnerability.

ASG Managed Endpoint Encryption for USB Storage

Talk about a BYOD invasion, how about R100 flash drives? Four times as much data as some iPads, fits in a shirt pocket, and is smaller than your thumb. Sounds like a security problem! Often unintentional, but these tiny storage devices are so very portable that they can go – and be lost – anywhere. Thieves are not bothered by form factors – the data is the same. Fortunately, ASG Managed Endpoint Encryption USB Storage is here to rescue you from this nightmare. Your company doesn't have to issue expensive, specialty secure flash drives. ASG Managed Endpoint Encryption USB Storage can be applied to any flash drive, from any manufacturer, even after it has been initialized by the user. It can also be set up to only allow reading of the drive by certain employees, or in certain circumstances (e.g., with an Internet connection), across a defined grouping of PCs.

Features include:

- Enforced encryption of all sensitive data on the drive
- Configurable to include requirement for remote authentication (cloud) to open any file, limita tions on which computers can be used to open files, instant data lock and wipe capability when devices are stolen
- Broad range of both administrator-enabled and automatic security responses to threat conditions
- Remote enforcement of password and security policy
- Customisable reporting of status and device risks/conditions plus auditing to support compliance, for example GDPR, Cyber Essentials, POPIA etc.

www.asg.co.za **011 975 7521**

ASG
Your Outsourced IT Department