Mortgage Max
The Future of Homeloans

POPIA Infopack

Protection of Personal Information Act (POPI Act)

Why do we need the Protection of Personal Information Act (POPIA)?

POPIA legislation was passed in 2013, "To promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic(.)"

POPIA officially commenced on 1 July 2020, with a one-year grace period. This gives public and private bodies until 1 July 2021 to ensure all processing of personal data complies with POPIA.

The purpose of POPIA is to protect people from harm by safeguarding their personal information. For example, preventing money being stolen, averting identity theft, and generally protecting privacy, which is a fundamental human right that is enshrined in the South African Constitution.

POPIA sets out the conditions for the processing of personal information.

A person's right to privacy entails having a form of control over their personal information and being able to protect their identity.

Infringement of this right could include acts of unauthorised collection or processing of personal data, and unauthorised disclosure of such data.

POPIA was designed to protect personal information that is processed by both private and public bodies, including government.

Under POPIA, everyone who processes, collects, stores, modifies or uses someone's personal information is a responsible party, and must therefore comply with the conditions required for the lawful processing of personal information.

What are the objectives of POPIA?

The objectives of POPIA are to protect data subjects (natural and juristic persons) from:

A. Security breaches
B. Theft of personal information
C. Discrimination

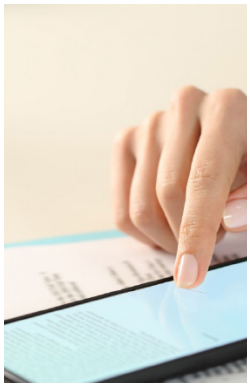
POPIA aims to promote the protection of privacy by way of eight principles that guide the processing of personal information in a confidential manner by data processors in South Africa.

These principles encourage responsibility, security and consent.

The eight POPIA principles that we as a company, and you as a data processor, must adhere to, are:

1. Accountability

- An accountable or responsible party is a “public, private or any other person who determines the purpose of and means for processing personal information, alone or in conjunction with others”.
- Each responsible party must be held accountable for its actions.
- The process must be voluntary, specific, and informed.



2. Lawful Processing

- Processing involves the collection, receipt, filing, storage, updating, alteration, retrieval, dissemination, linking, merging, erasing or destruction of personal information, and must be done lawfully.
- Consent must be obtained to process and share personal information with relevant parties.
- Personal information must be processed lawfully and in a reasonable manner that does not unnecessarily infringe on privacy.
- For example, we would need to obtain consent from a client to:
    - Process the information contained in their home loan application.
    - Do a credit check.
    - Obtain, retain and share their information with banks, estate agents and BetterSure.
    - We must also delete records as soon as reasonably possible. The National Credit Act and our bank contracts provide that we must retain records for five years. We are in the process of establishing systems that will enable the deletion of records when required.

3. Purpose Specific

- There must be a clear understanding of the reason or purpose for which the personal information you collect, will be processed and used.
- We must state the purpose and our intentions, and limit processing to the original purpose.
- Data must be used for a lawful purpose, in line with the consent given.
- For example, we collect financial information to assist clients with their home loan applications.

Purpose 1

Purpose 2

4. Further Processing

- Further processing of personal information must be in accordance, or compatible with, the original purpose for which it was collected.
- For example, a client applies for a home loan (purpose 1) and we also obtain consent to share their information with BetterSure, who will contact them for Homeowners Insurance (purpose 2). This is already included in our application forms.

Complete

Accurate

Not misleading

Updated

5. Information Quality

- We need to take reasonable and realistic steps to ensure that the personal information we process is:
  - Complete
  - Accurate
  - Not misleading
  - Updated, where necessary, in line with the reason such information was collected.
- If the information that we have on record changes, the client must be able to update their information by contacting us.

6. Transparency / Openness

- We must make clients aware:
  A. Information may be obtained from a source that is not the client themselves, for example a credit report from a credit bureau.
  B. Whether information is mandatory or voluntary.
  C. They have the right to lodge a complaint with the Information Regulator.
- While the client has the right to lodge a complaint, we will also have procedures in place to handle complaints. We will manage and register complaints, and attempt to resolve them first. Only if we are unable to do so, will it be escalated to the Information Regulator.
- We must maintain documentation relating to all processing operations under our responsibility.

7. Security Safeguards

- The integrity and confidentiality of personal information must be secured.
- We are responsible for ensuring that personal data is kept secure from both external threats (for example, malicious hackers) and internal threats (for example, poorly trained or negligent employees).
- Where processing is outsourced, the business should be satisfied that the service provider is treating the data with the same level of security as the business would.
- We must ensure that we have adequate safety measures in place to protect our systems.

8. Data Subject Participation

- Clients have certain rights, including being notified when their data is collected, and the right to request its deletion, correction or destruction.
- The right to object to processing and direct marketing.
- Our clients also have the right to opt out of any future marketing messages.

Who are the role players within POPIA?

Information Regulator – The Information Regulator has been newly created by POPIA. It has investigative powers and can issue fines.

Responsible Party – The person or entity that collects or processes personal information. They are liable and could be held responsible in terms of any data breaches.

Data Subject – The person or entity from whom the personal information is collected.

Information Officer – The individual who enforces the policy.

Data Processor – The third party who acts as a data processor, for example Cloud service providers or SwitchX. They must have a written mandate, as well as proper and adequate security measures.

What qualifies as 'personal information'?

Personal information is essentially any information that can be used to identify a person (whether natural person, or an existing juristic person/legal entity). It includes:

- Names, identity numbers, age, nationality
- Addresses
- Marital status
- Mental health or wellbeing
- Biometrics
- Education, medical, financial, criminal or employment history
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particulars assigned to a person.
- Correspondence sent by a person that is implicitly or explicitly of a private/confidential nature.

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 ethnicity
- Trade union membership
- Political persuasion
- Health or sex life
- Biometrics
- Criminal behaviour/record

POPIA also specifically regulates the personal information of children.

What does 'processing' of personal information involve?

Any activity or set of operations, including by automatic means, that concerns personal information, including:

- Collection, receipt, recording, collation, storage, updating;
- Modification, retrieval, alteration, consultation, or use;
- Dissemination by means of transmission;
- Distribution or making available in any other form;
- Merging and linking; and
- Any restriction, degradation, erasure, or destruction of information.

What does POPIA *not* regulate?

- Household or personal activities, for example data such as the Contacts list on your smartphone.

- Information that has been de-identified, i.e. it has been made anonymous to such a degree that it cannot be used to identify someone.
- Information that is processed by, or on behalf of, a public body, national security, defence or public safety, or for the prevention, investigation or proof of offences, the prosecution, or the execution of sentences. Why? Because there is a greater public interest in having this information available.
- Processing for purely journalistic purposes, if subject to a code of ethics that provides adequate safeguards for protection.

When can we process personal information?

Personal information can only be processed:

- With the consent of the data subject.
- If necessary, for the conclusion or performance of a contract to which the data subject is a party.
- An obligation imposed by law on a responsible party, for example FICA, FAIS etc.
- If it protects a legitimate interest of the data subject, for example in a health emergency if you cannot consent to personal information being processed.
- If necessary for the proper performance of a public law duty by a public body.
- If necessary to pursue the legitimate interests of the responsible party, or the interest of a third party to who the information is supplied, for example taking down information when entering an office space, etc.

The responsible party must prove that they had at least one of the grounds listed above to process personal information.

Once you have consent/lawful permission to process the personal information of a data subject (client) you must process that information under POPIA, meaning you must comply with its eight principles.

Where is personal information stored?

Personal information can be electronically or physically stored, processed and transferred by various mechanisms and devices. Examples include:

- Laptops and notebooks
- Smartphones or tablets
- Paper or files on workstations (or other places)
- Storage devices (hard-drives and USB or 'flash' drives)
- Servers
- Networks (during information transfer)
- Cloud
- Email
- Databases

What are your duties and responsibilities in terms of POPIA?

Handling personal information is a huge responsibility. Your clients entrust their information to you. If you misuse, lose or allow their personal information to fall into the wrong hands, it could cause serious harm or distress to your clients, and to our business.

You need to protect and safeguard personal information, regardless of whether you are working from the office, on the road, or at home. You can do this in the following ways:

Use strong and secure passwords.

- Passwords should never be shared or left on display. They ensure that only the right people have access to the information.
- Passwords should not be too simple.
- The most common password is 'Password', or the numbers 1234. Never use either of these!

Never share your passwords.

- There is a tendency to share passwords in the workplace because of trust and familiarity between colleagues.
- Because of the information-related risks in our business, you should never share passwords with anyone else.
- Do not save your username and password anywhere that requires you to log in, for example DealMaker.

Always lock your computer and smartphone, when not in use.

- Make sure that you lock your computer when it is unattended, to prevent unauthorised access.
- This protects the information and safeguards you from blame if the computer is misused while you are away.

Be vigilant and do not allow unauthorised people into work areas.

- It is important that lanyards are visible while in the workplace. They are a clear indicator that the wearer is authorised to be there.
- Be on the lookout for people who do not belong there, and immediately report any suspicion to the relevant manager.
- No unauthorised persons may use your work equipment, for example a family member using your laptop for whatever purpose.

Clean your desk at the end of each day.

- If your desk is messy, you could accidentally leave sensitive information out in the open. It also makes it less likely you'll notice if something goes missing.
- Lock away physical files and documents – do not leave them lying around.

Dispose of documents containing personal information correctly and responsibly.

- Ensure that physical files and documents containing personal information are for shredding.
- Do not throw away, donate or recycle (without shredding) documents containing personal information.
- This applies to any work environment, even your office space at home.

Never use your personal email account to send or receive work-related information.

- Only make use of your work email when dealing with client details.
- Personal email accounts are not secure.
- Personal communication channels, like WhatsApp, should not be used to share or collect any client information.

Always check if a person requesting large amounts of data has a legitimate reason to do so.

- Data breaches can have major consequences for our business.
- If someone is requesting unusually large amounts of personal information or business sensitive information, ALWAYS investigate whether they have the authority to request such information.
- Never execute such requests over the telephone, always ask for an email so that you have the request in writing.
- As a general rule, "If in doubt, shout it out!", i.e. escalate it to your manager.

What to do when working on the go

Information immediately becomes more vulnerable when we're working outside the office. So, take extra care to avoid unnecessary risks.

Check before you leave.

- Ensure that you have not left anything behind when you leave. USB or 'flash' drives, documents, or your laptop. Check and check again.

Work neatly.

- Work tidily and with care. Ensure that information is not on display, or visible to others.

Be vigilant.

- Make sure your laptop screen is not visible to others. The same applies to your smartphone and other mobile or electronic devices.

Avoid discussing sensitive details.

- Do not discuss anything sensitive where people could overhear your conversation. Always be aware and pay attention to who is around you. Information that is overheard can be used by criminals in many ways.

Do not leave files or laptops in vehicles for extended periods of time.

- Remove the files or your laptop from your vehicle whenever possible. Remember, your vehicle could be stolen, and all that sensitive information would be lost with it. Always ensure that your laptop and files are stored in your boot while travelling.

Avoid working with paper, as far as possible.

- Paper poses a huge risk. It is advisable to avoid using physical paper documents as far as possible. Ensure that documents are scanned and emailed to your work email address.

What can you do to keep virtual information safe?

It is best to connect to a business network via a Virtual Private Network (VPN)

- VPN is important for online privacy whenever you are logging into the internet in public or from home because cyber snoops could track your online activity when you are using public wi-fi, whether it's on your laptop or smartphone.

Always protect your work computer

- Understand that there is a risk when using personal laptops or desktops when processing deals or client information.
- You need to ensure that you have the latest anti-virus programs on your computers.
- Avoid using your work laptop for personal purposes, like downloading music or movies, as it could put your customer information at risk.
- Never let anyone else use your business computer.

Always run updates on your computer and mobile devices.

- Software updates do a lot of things, including the repair of security issues that have been identified, and fixing or removing bugs.
- Updates add new features to your devices and remove outdated ones.
- Updates are essential to keep information safe.

Do not click on a link embedded in an email.

- Scammers use links with malware and viruses to infect your devices.
- Always check the email address, a Gmail, Yahoo, or any other non-business-related account is a dead give-away.
- Look out for obvious spelling mistakes in the email.
- Out of the ordinary or poorly written subject lines could be an indication of fraudulent or spam email.

Use common sense.

- Does a website look strange to you?
- Is it asking for sensitive personal information?
- If it looks unsafe, do not risk it. Do not click on pop-ups or allow sites to track your location.

What to look for on a secure website

Signs of legitimacy.

- Does the website list contact information or give some indication of a real-world presence, for example a physical address?
- If in doubt, contact them by phone or email to establish their legitimacy.
- Look at their web address carefully. If this is a website you frequent, is the web address spelled correctly?
- Often, phishing attacks will set up websites with a web address that is almost identical to a site you go to often. A small typo could lead you to a fraudulent version of the site you thought you were visiting.

If it looks too good to be true, it probably is.

- Is the website offering you a product or service at an incredibly good price?
- Are they promising you a huge return on investment?
- If the offer looks too good to be true, then it probably is! Trust your instincts. Do some research and look for reviews and warnings from other users.

HTTPS

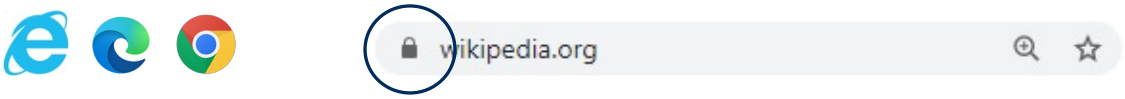
- The web address or URL of the website could give you a good indication of online security.
- A secure website's URL should begin with 'https' rather than just 'http'.
- The 's' after 'http' stands for 'secure' and indicates that it is using a Secure Sockets Layer (SSL) connection. This means your information will be encrypted before being sent to a server.

The 'lock' icon

Another sign to look for is the 'lock' icon that should be displayed in the window of your web browser. Different browsers position the lock in different places, but here are a few examples of to look out for:

Google Chrome/ Internet Explorer / Microsoft Edge

Click the lock icon, far-left on the address bar, for information about the security of a website.



IMPORTANT NOTE: Be sure to click the lock icon to verify that a website is trustworthy. Do not assume that a website is secure if you see this icon!

What are the consequences of personal data falling into the wrong hands?

There could essentially be two legal consequences and penalties for the responsible party:

1. A fine of R1 million to R10 million, or imprisonment of one to 10 years in jail.
2. Having to pay compensation to data subjects for damage/s suffered.

Jail time is unlikely, and the fines are relatively small, compared to other jurisdictions.

Other penalties include:

- Reputational damage.
- Business disruptions (through malware or viruses)
- Losing clients and employees.
- Failure or difficulty in attracting new business.

However, our main aim and motivation in complying with POPIA, is always to protect people from risk and harm.