ACFE™
Association of Certified Fraud Examiners
South Africa Chapter #91

POPIA COMPLIANCE GUIDELINES

ACFE™
Association of Certified Fraud Examiners
South Africa Chapter #91

CONTENTS

ACFE™
Association of Certified Fraud Examiners
South Africa Chapter #91

CONTENTS

TABLE OF IMAGES

ABOUT THIS GUIDELINE

1. WHY THIS GUIDELINE?

The South African chapter of the Association of Certified Fraud Examiners (ACFE SA) has prepared this guideline to help the fraud examiner industry interpret the requirements of the Protection of Personal Information Act (POPIA). This guideline explains how, where, when, what and why you may use and share Personal Information to prevent, detect and investigate fraud and white-collar crimes. It will also help organisations and individuals to protect Data Subjects' right to privacy when preventing, detecting and investigating fraud.

We see this guideline as the first step towards creating a POPIA Code of Conduct for the industry.

2. WHAT IS THIS GUIDELINE ABOUT?

This guideline will help ACFE SA members and all other fraud examiners in South Africa to assess and improve their POPIA compliance. This guideline should be read with members' compliance frameworks and standard operating procedures. This guideline will help you to:

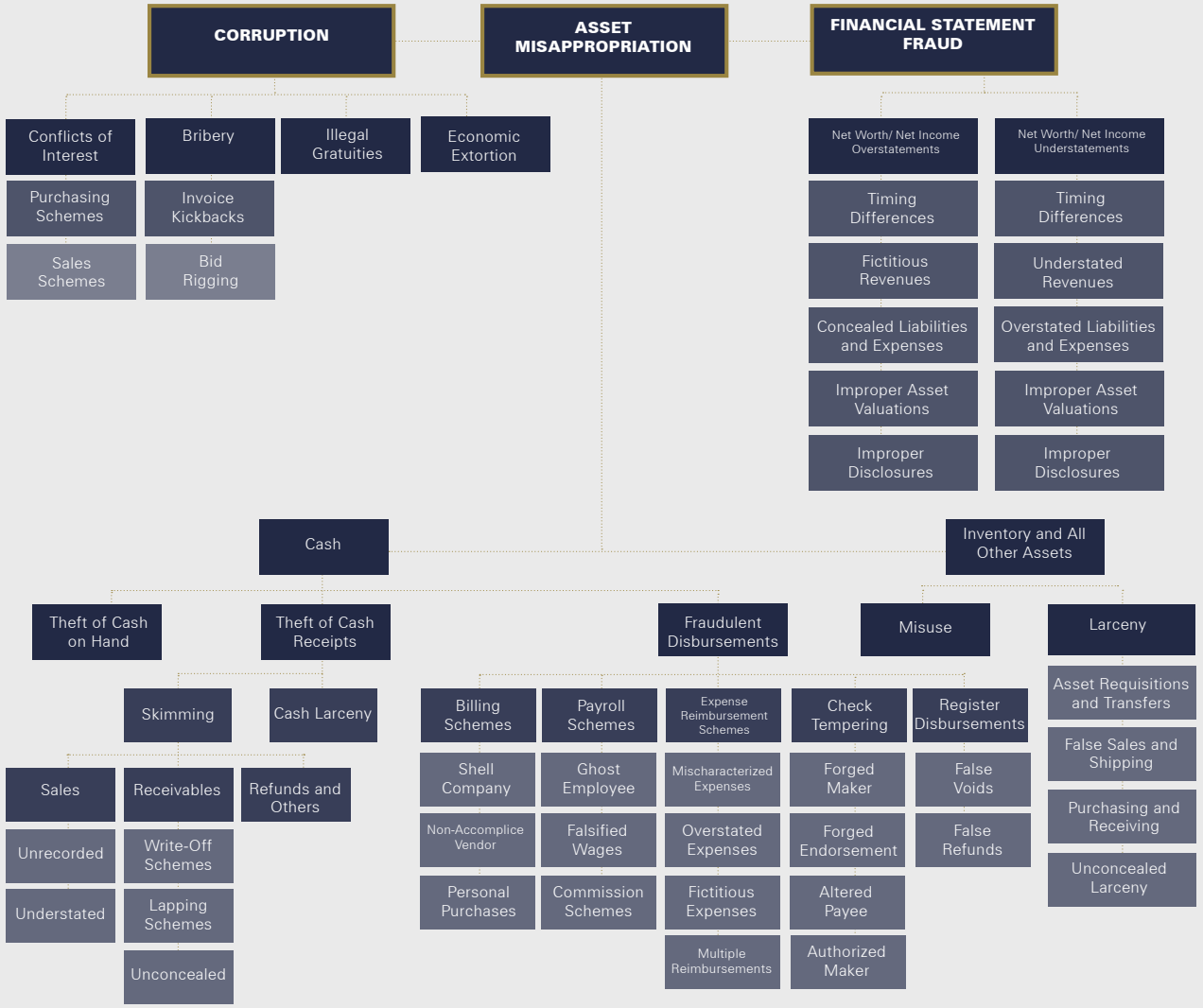
- determine when POPIA applies to your activities;
- assess your POPIA compliance;
- improve your POPIA compliance;
- respond to complaints and Security Compromises; and
- respond to notices from and investigations by the Regulator.

When this guideline refers to 'fraud', it includes all occupational fraud categories:

ACFE™
Association of Certified Fraud Examiners
South Africa Chapter #91

THE FRAUD TREE

OCCUPATIONAL FRAUD AND ABUSE CLASSIFICATION SYSTEM



01. 1. WHEN POPIA APPLIES

1. WHEN DOES POPIA APPLY?

POPIA applies to all Processing of Personal Information that a Responsible Party enters into a Record in South Africa. Ask yourself:

Are you Processing Personal information?	**Y/N**
Is the Personal information entered into a Record or, in the case of manual Processing, a Filing System?	**Y/N**
Are you in South Africa? OR Are you doing the Processing in South Africa?	**Y/N**

ASK YOUR LAWYER

Foreign companies or multinationals may find this question complicated to answer. If you are unsure, ask your lawyer for advice.

Even if you answer yes to all three questions, there may be exceptions when POPIA does not apply. We discuss these exceptions next in When does POPIA not apply.

DEFINE IT

PERSONAL INFORMATION is all information that can be linked to an identifiable living individual or existing juristic person (such as a company or government institution).

READ MORE: EXAMPLES OF PERSONAL INFORMATION.

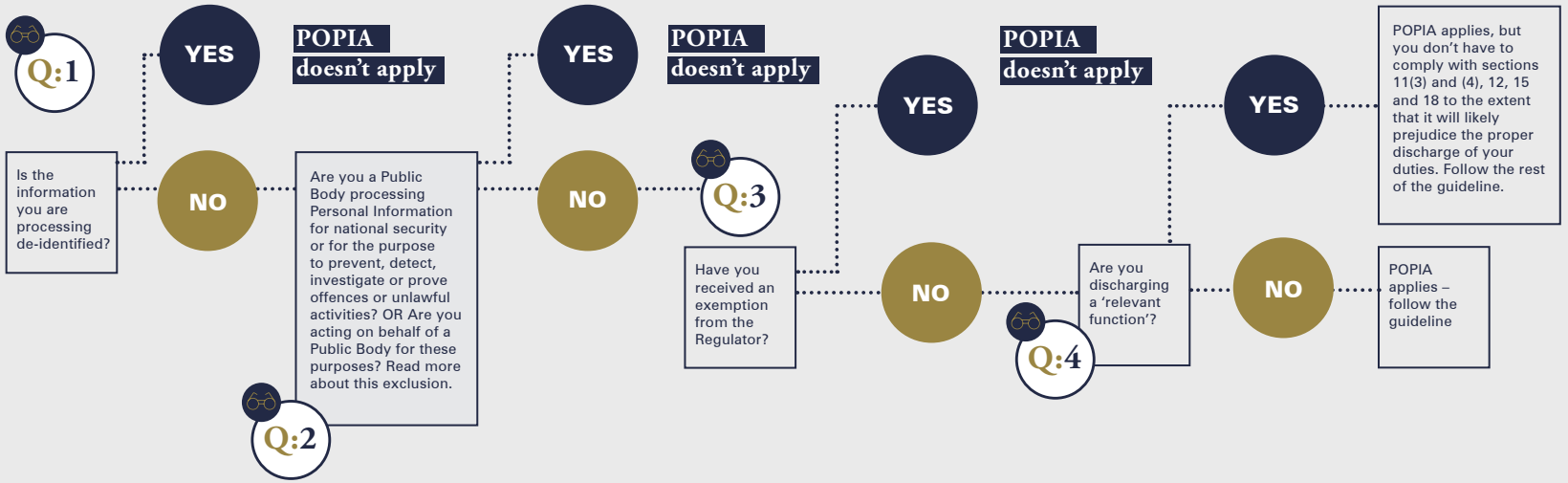
PROCESSING covers all activities that involve Personal Information from collection to destruction. It includes collecting, receiving, recording, organising, collating, storing, updating, modifying, retrieving, consulting, using, disseminating, linking, restricting, deleting, erasing, and destroying Personal Information.

A **RECORD** is any form of information recorded such as writing on any material, or information produced or recorded or stored on a tape-recorder or a computer or other device, or labels, or markings, or other writing that describes anything of which it forms part, or to which it is attached to by any means, or books, maps, plans, graphs or drawings, or photographs, films, negatives and tapes.

2. WHEN DOES POPIA NOT APPLY?

In some instances, you are exempted from complying with the requirements of POPIA, and for some activities you are partially exempted from complying with specific conditions of POPIA. Answer these questions to determine whether an exclusion applies to your activity.

DOES POPIA APPLY TO YOUR ACTIVITY?



QUESTION 1: IS THE INFORMATION DE-IDENTIFIED?

POPIA does not apply to De-identified information.

DEFINE IT

PERSONAL INFORMATION is De-identified if you have deleted the information that can identify a Data Subject, or that can be used or manipulated to identify a Data Subject, or that can be linked to other information that identifies a Data Subject.

QUESTION 2: ARE YOU INVESTIGATING FRAUD ON BEHALF OF A PUBLIC BODY?

POPIA does not apply to the Processing of Personal Information by or on behalf of a Public Body when:

- the Processing relates to national security, including identifying financing used for terrorist and related activities or the defence of public safety; or
- the Public Body is involved in preventing, detecting, investigating, or proving offences, prosecuting offenders, executing criminal sentences, or providing security measures. This includes activities to identify the proceeds of unlawful activities and the combating of money laundering activities. This means that many of the Processing activities that law enforcement undertakes will be excluded.

NB

This exception is limited. It only applies when there is other legislation in place to protect this Personal Information. If not, POPIA will still apply. The Regulator issued an Enforcement Notice against SAPS. The Regulator indicated that the SAPS Act does not provide adequate protection of Personal Information and therefore POPIA applied to the officers' conduct. This means that you cannot assume that this exception applies when you investigate fraud on behalf of a Public Body and that you should always aim to follow this guideline. Read more about this and other findings here.

QUESTION 3: DO YOU HAVE AN EXEMPTION FROM THE REGULATOR?

You can apply to the Regulator to exempt you from POPIA for your activities if:

- the PUBLIC INTEREST in your activity substantially outweighs any interference with the privacy of the Data Subject that could result from your activity; or
- your activity involves a clear benefit to the Data Subject or a Third Party which substantially outweighs any interference with the privacy of the Third Party that could result from your activity.

The Regulator's guidance note on exemptions explains how to apply for an exemption.

QUESTION 4: ARE YOU DISCHARGING A RELEVANT FUNCTION?

When you discharge a Relevant Function, there are some conditions you are exempted from for the lawful Processing of Personal Information. You are exempted from having to:

- notify Data Subjects when you collect Personal Information;
- collect Personal Information directly from the Data Subject;
- limit further Processing of the Personal Information; and
- allow for the Data Subject to object to the Processing of their Personal Information.

This exemption only applies if complying with these conditions in POPIA would likely prejudice the proper performance of that function. The Regulator's guidance note on exemptions provides more information about this exemption. You must document your reasons if you rely on this exemption.

We will indicate the conditions you are exempted from when you discharge a Relevant Function in this guideline.

DEFINE IT

Both public and private bodies may discharge a **RELEVANT FUNCTION.** You are discharging a Relevant Function if you perform a function in terms of a law, and if that function is to protect members of the public against:

- financial loss due to dishonesty, malpractice, or other serious improper conduct by, or the unfitness or incompetence of, persons concerned with the provision of banking, insurance, investment or other financial services or in the management of corporate bodies; or
- dishonesty, malpractice or other serious improper conduct by, or unfitness or incompetence of persons authorised to carry on any profession or other activity.

Examples: When a bank implements measures to prevent fraud and money laundering, they may collect Personal Information from Third Parties without notifying the Data Subject because they are discharging a Relevant Function.

When you investigate a medical practice for alleged fraud, you are exempted from collecting Personal Information directly from that medical practice. This makes sense because you might want to collect information from other sources without necessarily alerting the medical practice to your investigation.

ASK YOUR LAWYER

If you are unsure whether you are discharging a Relevant Function, ask your lawyer for advice.

3. WHO IS ACCOUNTABLE FOR COMPLIANCE WITH POPIA?

The person or organisation that determines why Personal Information is Processed (purpose) and how it is Processed (means), is accountable for POPIA compliance. They are called Responsible Parties. The Responsible Party will be accountable even if another person or organisation causes non-compliance of the Responsible Party's activities.

Sometimes multiple parties are jointly responsible for compliance. For instance, when they make joint decisions about why and how to process Personal Information.

A Responsible Party may appoint an Operator to Process Personal Information on their behalf through a written contract. The Responsible Party is accountable for their Operator's compliance, although the Operator may be liable for non-compliance in terms of the contract.

You should always consider accountability and liability in the context of POPIA and contractual obligations.

Example: An insurer appoints a consultant to investigate alleged fraud by an employee. The consultant performs the investigation in terms of a contract or mandate from the insurer. The insurer is the Responsible Party and must ensure that the consultant is POPIA compliant. The consultant is an Operator.

NB

Because fraud examiners often work independently, such as when you decide what information to use in your investigations and how to use it, you will almost always bear some responsibility for POPIA compliance. That is why you must always comply with this guideline.

02. HOW TO ASSESS COMPLIANCE

1. WHEN MUST YOU ASSESS COMPLIANCE WITH POPIA?

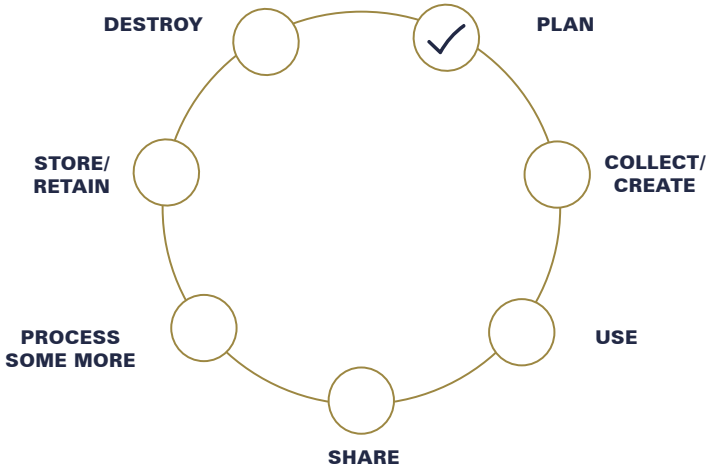
You must assess your compliance with POPIA every time you Process Personal Information. You should consider POPIA requirements at each step of the information life cycle.

It may seem daunting at first, but once you've done this a few times, it will become second nature.

Here are some examples of when you should assess compliance with POPIA. When you:

- introduce a new system or technology
- change a process or create a new process
- change from paper to electronic Records
- share Personal Information with Third Parties
- obtain Personal Information from Third Parties
- consider using Personal Information for a new purpose
- re-identify anonymised data

THE INFORMATION LIFECYCLE:



2. WHY MUST YOU USE PERSONAL INFORMATION?

Your specific purpose for Processing Personal Information is to investigate fraud. This means that you may collect and use Personal Information only if you need it to investigate fraud.

When you start an investigation, you must consider and document the information you need and why you need it.

NB

IT IS IMPORTANT TO DOCUMENT YOUR PURPOSE AND ACTIVITIES IN A RECORD SO THAT YOU CAN:

- notify the Data Subject (Read more)
- determine whether you may use the Personal Information for fraud investigations (Read more)
- determine whether you only have information that is adequate, relevant, and not excessive for your purpose (Read more)
- determine how long you may keep the information (Read more)

3. WHAT PERSONAL INFORMATION DO YOU NEED FOR YOUR PURPOSE?

The principle of minimality states that you can only Process Personal Information that is adequate, relevant, and not excessive considering the purpose of the Processing. This means that you must have a clear purpose for each piece of Personal Information you collect and that you may only use the information for the purpose of investigating fraud.

To comply with the minimality requirement, you must:

- only collect Personal Information that you actually need to do your job;
- have sufficient Personal Information to properly fulfil your purpose; and
- periodically review the Personal Information you have and delete or destroy all the information that you do not need.

Example: You are asked to do a lifestyle audit on a client. You search various databases using the client's name. You receive reports on three people who share the same name as the client. Once you are sure which report is relevant to your client, you must destroy the irrelevant reports.

4. WHEN MAY YOU PROCESS PERSONAL INFORMATION?

4.1. WHEN YOU MAY COLLECT PERSONAL INFORMATION

Whether you may collect Personal Information will depend on the type of information you plan to collect. The requirements to collect Special Personal Information or the Personal Information of Children are stricter than for less-sensitive information.

You may collect and process personal information (that is less sensitive) to examine fraud when:

- you have a legal obligation (e.g., to comply with FICA or AML legislation), or when you need to help the Responsible Party fulfil a legal obligation
- you need the information to conclude a contract or fulfil your responsibilities in terms of a contract with the Data Subject (e.g., when you verify a job applicant's qualifications);
- you need the information to pursue the Responsible Party's legitimate interests (e.g., a financial institution has a legitimate interest to pro-actively prevent fraud and to share evidence of fraud with SAPS); or
- you have the Data Subject's Consent to collect their information.

To collect Special Personal Information or the Personal Information of Children you must be able to prove that:

- you need the information to establish, exercise, or defend the Responsible Party's legal rights or obligations (e.g., a bank identifies a client using biometric information);
- the Data Subject deliberately made the information public (e.g., a person published an article about their health on a public website);
- you have the Data Subject's Consent, or in the case of Children, you have the Consent of their parent or guardian to collect their information; or
- the Regulator gave you prior authorisation (Read more).

In most instances, you will be authorised to collect Special Personal Information or the Personal Information of Children because, when investigating fraud, it is necessary to establish, exercise or defend a legal right or obligation. However, if you cannot prove that you may collect the Special Personal Information or Personal Information of Children based on one of the above authorisations, you may still be able to collect the Personal Information, in terms of other authorisations that may be available to you.

READ MORE: AUTHORISATIONS FOR PROCESSING SPECIAL PERSONAL INFORMATION.

ASK YOUR LAWYER	*This gets technical, so, if you are unsure, ask your lawyer.*

DEFINE IT

SPECIAL PERSONAL INFORMATION includes religious and philosophical beliefs, race and ethnic origin, trade union membership, political persuasion, health and sex life, inherited characteristics, biometric information and criminal behaviour.

READ MORE: CATEGORIES OF SPECIAL PERSONAL INFORMATION.

PERSONAL INFORMATION OF CHILDREN includes the information of individuals younger than 18 years who are not legally competent to make decisions without the assistance of a parent, guardian, or another Competent Person.

4.2. WHEN YOU MAKE AUTOMATED DECISIONS BASED ON PROFILES

RULE:

Responsible Parties must implement additional measures to protect Data Subjects if they make decisions:

- based solely on the automated Processing of Personal Information profiles; and
- that could result in legal consequences for or significantly affect Data Subjects.

Decisions related to fraud investigations will likely always have legal consequences or a substantial effect on the Data Subject. You must assess whether you make decisions based on a profile and without any human intervention. If so, you must implement additional measures to protect the Data Subject's interests.

READ MORE: MEASURES THAT RESPONSIBLE PARTIES MUST IMPLEMENT WHEN MAKING AUTOMATED DECISIONS BASED ON PROFILES.

Examples: A bank monitors credit card spending patterns and automatically blocks the credit card if fraud is suspected. In this case, the bank makes automated decisions based on spending profiles.

A mobile network operator monitors for fraudulent data tunnelling using a VPN and blocks the relevant SIM card automatically.

The minimum measures that the Responsible Party must implement are to:

- provide an opportunity for the Data Subject to make representations about a decision; and
- provide the Data Subject with sufficient information about the underlying logic of automated Processing to allow the Data Subject to make representations.

EXCEPTION:

You do not have to implement the minimum measures if a law or a code of conduct governs your automated decisions in which appropriate measures are specified for protecting the legitimate interests of Data Subjects.

Example: The POPIA Code of Conduct of the Banking Association of South Africa contains measures for protecting the legitimate interests of Data Subjects when banks make automated decisions based on profiles.

READ MORE: ABOUT EXAMPLES OF THE MEASURES YOU SHOULD IMPLEMENT WHEN MAKING AUTOMATED DECISIONS BASED ON PROFILES.

DEFINE IT

PROFILING happens when information is structured in such a way that questions about a person can be answered by using that information. Examples include profiles created to assess a Data Subject's performance at work, creditworthiness, reliability, location, health, personal preferences, or conduct.

AUTOMATED PROCESSING happens when there is no human involvement in the decision-making process.

4.3. WHEN YOU USE PERSONAL INFORMATION FOR A NEW PURPOSE (FURTHER PROCESSING) (SECTION 38 EXEMPTION)

When investigating fraud, you may want to use Personal Information you already have, however, this information was probably collected for a different purpose. POPIA limits the circumstances under which you may use Personal Information for a 'new' purpose.

Example: You investigate an employee of suspected fraud. In your investigation, you use the employee's banking details, originally collected to process payroll.

RULE:

Your 'new' reason for Processing Personal Information must be compatible with the original purpose for the collection.

To assess if your reason is compatible with the original purpose for collecting the Personal Information you must consider:

- the relationship between the original purpose and the new purpose;
- the nature of the Personal Information concerned (e.g., is the Personal Information particularly sensitive);
- the consequences that further Processing would have for the Data Subject;
- the way in which the Personal Information was collected; and
- any contractual rights between the Responsible Party and the Data Subject.

Example: You investigate an employee for suspected fraud. You use the employee's banking details, address and emergency contact information. This information was not originally collected with the purpose of investigating fraud. Your organisation has various internal policies and procedures that deal with fraudulent activity in the workplace and the disciplinary proceedings that may result from fraudulent activities. The 'new' purpose is compatible with the original purpose because there is a clear relationship between the original purpose and the new purpose, and the contractual rights that exist between the employer and employee.

EXCEPTION:

Even if your purpose (fraud investigation) is not compatible with the original purpose, you may still use previously collected Personal Information if:

- the information is available in or could be derived from a Public Record (e.g., CIPC or Deeds Office Records);
- the information was deliberately made public by the Data Subject (e.g., the information is available on their public social media profile);
- Processing is necessary to avoid prejudice to the maintenance of the law by any Public Body (including the prevention, detection, investigation, prosecution and punishment of offences)(e.g., investigations by SAPS);
- Processing is necessary for the interest of national security (e.g., to prevent terrorist attacks);
- Processing is necessary to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue (as defined in section 1 of the South African Revenue Service Act, 1997) (e.g., investigations by SARS);
- Processing is necessary for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated (e.g., collecting evidence for a criminal court case);
- Processing is necessary to prevent or mitigate a serious and imminent threat to public health or public safety (e.g., COVID-19 screening); or
- you have the Data Subject's Consent, or the Consent of a Competent Person if the Data Subject is a Child.

5. WHEN DO YOU NEED PRIOR AUTHORISATION FROM THE REGULATOR?

Responsible Parties need authorisation from the Regulator before they can undertake certain high-risk activities. You must apply for authorisation before you:

- use Unique Identifiers to link information held by multiple Responsible Parties, and if the linking activity constitutes further Processing that is incompatible with the original purpose for which the Unique Identifiers were collected or created;
- Process criminal behaviour or unlawful or objectionable conduct on behalf of Third Parties. This may apply if you are contracted to conduct a criminal record enquiry, to do a reference check about past conduct, or to take disciplinary action against a Data Subject; or
- transfer Special Personal Information or the Personal Information of Children to foreign countries.

READ MORE: ON THIS TOPIC IN THE REGULATOR'S GUIDANCE NOTE ON THE APPLICATION FOR PRIOR AUTHORISATION.

ASK YOUR LAWYER	*It is unlikely that you would ever have to apply for authorisation, but if you are unsure, get a formal legal opinion.*

DEFINE IT

UNIQUE IDENTIFIERS are identifiers assigned to Data Subjects that Responsible Parties use for the purpose of their operations and that uniquely identify a Data Subject in relation to that Responsible Party. For example, a bank or other Account Number, policy number, identity number, employee number, student number, telephone number or reference number.

6. HOW AND FROM WHAT SOURCE MAY YOU COLLECT PERSONAL INFORMATION? (SECTION 38 EXEMPTION)

RULE:

You must collect Personal Information directly from a Data Subject.

EXCEPTION:

There are some exceptions to this rule. You are exempted from having to collect Personal Information directly from a Data Subject if:

- you can derive the Personal Information from a Public Record or if it is contained in a Public Record (e.g., Deeds Office or CIPC Records);
- the Data Subject deliberately made the information public (e.g., the Data Subject published their address on their own publicly available website);
- you have the Data Subject's Consent, or the Consent of a Competent Person if the Data Subject is a Child, to collect the Personal Information from another source;
- collecting the Personal Information from another source would not prejudice a legitimate interest of the Data Subject (e.g., you verify a job applicant's education);
- it means that to collect the Personal Information directly from the Data Subject would negatively affect a lawful purpose why the information was collected (e.g., when you investigate an employee for fraud you must collect financial information from other sources as evidence);
- it is not reasonably practical to collect the Personal Information

directly from the Data Subject (e.g., you perform a criminal check on a job applicant);

- you have to collect Personal Information from another source to avoid negatively affecting the ability of any Public Body to enforce the law, including prevention, detection, investigation, prosecution, and punishment of offences (e.g., when you investigate money laundering and you must not tip off the subject of the investigation);
- you must collect Personal Information from another source to comply with a legal obligation or to enforce legislation concerning the collection of revenue (as defined in section 1 of the South African Revenue Service Act, 1997) (e.g., investigations undertaken by SARS);
- you must collect Personal Information from another source for the conduct of proceedings in any court or tribunal (e.g., when you collect evidence for a court case);
- you have to collect the Personal Information from another source for purposes of national security (e.g., when investigating terrorist activities); or
- you have to collect the Personal Information from another source to maintain the legitimate interests of the Responsible Party or Third Party that you supply the information to (e.g., you perform credit checks on clients of a bank).

RECOMMENDATION

When you conduct fraud investigations and you want to collect Personal Information from a Third Party, you must identify the relevant exception. If the Third Party asks, you can tell them which exception you are relying on. You should also get an undertaking from the Third Party that they have a legal justification to share the Personal Information with you.

DEFINE IT

A PUBLIC RECORD is a Record that is accessible in the public domain and is in the possession or under the control of a Public Body whether or not it was created by that Public Body.

Examples of Responsible Parties' legitimate interests are:

- Processing which is strictly necessary to prevent fraud
- transmitting information within a group of organisations for internal administration
- Processing to ensure network and information security
- preventing misuse of services and money laundering
- debt collection and enforcement of other legal claims

7. WHEN MUST YOU TELL PEOPLE THAT YOU ARE COLLECTING THEIR PERSONAL INFORMATION? (SECTION 38 EXEMPTION)

RULE:

POPIA requires you to inform Data Subjects that you are collecting their Personal Information, why you are collecting it, how you will use it, etc. Publishing a privacy notice or statement on your website will help you comply with this requirement.

READ MORE: THE DISCLOSURES A RESPONSIBLE PARTY MUST MAKE WHEN COLLECTING PERSONAL INFORMATION.

Notifying Data Subjects about a fraud investigation will often not be possible, nor will it be ideal for the investigation. Luckily, POPIA provides several exceptions to this notification rule.

Example:

You are exempted from having to notify Data Subjects that you are collecting their Personal Information if:

- they consented that you do not have to notify them;
- you can demonstrate that not notifying them will not have a negative impact on their legitimate interests (e.g., you collect Personal Information to prove the innocence of an employee who are suspected of theft);
- your notification would have a negative impact on a Public Body's maintenance of the law, for instance, when Personal Information is used to prevent, detect, investigate, prosecute or punish offences (e.g., when SAPS investigate a crime);
- you require the Personal Information to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue (as defined in section 1 of the South African Revenue Service Act, 1997) (e.g., investigations undertaken by SARS);
- their Personal Information is necessary in the interest of national security (e.g., to prevent an act of terrorism);

- their Personal Information is necessary for the proceedings in any court or tribunal that have commenced or are reasonably contemplated (e.g., when you collect evidence for a criminal court case);
- your notification would prejudice a lawful purpose of the collection (e.g., when there is a chance that the Data Subject will destroy evidence if they know about the investigation); or
- your notification is not reasonably practical considering the circumstances of the particular case (e.g., if you do not have the Data Subject's contact details).

RECOMMENDATION

Fraud investigations will almost always fall within one or more of the exceptions provided in terms of POPIA. However, Responsible Parties must publish a manual in terms of the Promotion of Access to Information Act 2 of 2000 (PAIA) that includes a description of the Personal Information they collect and use, the purposes for collecting the information, etc. Remember to include fraud prevention, detecting and investigation as a purpose for Processing Personal Information in your privacy notice and in your PAIA Manual. Read more about the notification requirements in terms of PAIA.

DEFINE IT

A **PAIA MANUAL** is a document that all organisations must publish in terms of sections 14 and 51 of the Promotion of Access to Information Act 2 of 2000.

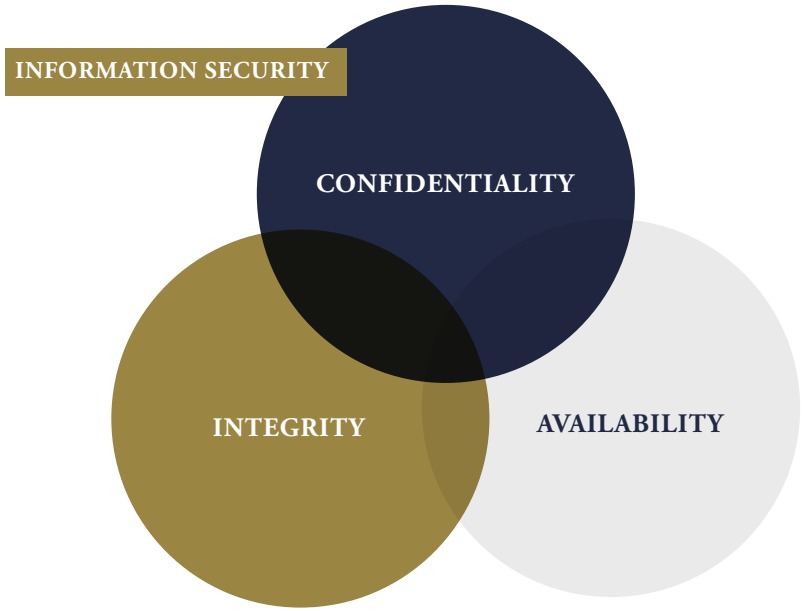
Examples: You are investigating an employee for suspected fraud. You learn that the employee has a brother. Because you have reason to believe that the employee transferred funds to this brother, you want to collect information from a credit bureau about the brother. Do you have to notify the brother? No, because notifying him would prejudice your lawful purpose of collecting the information, i.e., investigating fraud.

8. HOW MUST YOU SECURE PERSONAL INFORMATION?

You must protect Personal Information from loss, damage, unauthorised destruction, unlawful access, and unlawful Processing. In addition, you must ensure that the Personal Information you process is complete, accurate, not misleading and updated where necessary (i.e., ensure information quality).

DEFINE IT

INFORMATION SECURITY is defined as 'the preservation of confidentiality, integrity and availability of information'.



POPIA requires you to follow a risk-based approach and to implement reasonable measures to:

- identify risks to Personal Information in your possession;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are properly implemented; and
- regularly update safeguards in response to new risks or deficiencies in safeguards.

NB If you suspect or confirm that you have had a Security Compromise, you may have to notify the Regulator and Data Subjects of the incident.

READ MORE: WHAT MUST YOU DO WHEN YOU HAVE A SECURITY COMPROMISE?.

When you process Personal Information, it is important for you to have the following minimum safeguards in place:

- updated software, apps, browsers, and operating systems
- backed-up Records on a secure offline drive or the cloud
- locked cabinets to store paper Records
- no unattended Records lying around

- strong passwords on all devices that lock automatically after a maximum of five minutes of inactivity
- encrypted devices and other media that contain Special Personal Information or the Personal Information of Children
- multi-factor authentication to access special categories of Personal Information
- cross-cutting shredders to destroy paper Records
- secured wi-fi routers by changing the default name and password, turning off remote management, and logging out as the administrator once the router is set up
- a wi-fi router with up-to-date secure encryption that it is turned on
- training given to all employees at induction and regularly after that about how to avoid phishing scams, how computers and devices become infected, and how to spot and report ransomware attacks.

9. WHEN MAY SERVICE PROVIDERS (OPERATORS) PROCESS PERSONAL INFORMATION ON YOUR BEHALF?

Operators may process Personal Information on the Responsible Party's behalf if you and the Operators agreed in writing that:

- they will only use Personal Information where you authorised it in writing;
- the Personal Information is confidential and that they must not share it with Third Parties without your knowledge and authority;
- they will comply with the security requirements in section 21 of POPIA; and
- they must notify you immediately in the case of a Security Compromise.

These are the minimum requirements that Operators must agree to. Responsible Parties may add more responsibilities for Operators in a contract.

DEFINE IT

An **OPERATOR** is anyone who processes Personal Information for a Responsible Party in terms of a contract or mandate without coming under the direct authority of the Responsible Party.

Example: SARS contracts consultants to assist in an investigation. The consultants are Operators and SARS is the Responsible Party.

10. WHEN MUST YOU DELETE OR DESTROY PERSONAL INFORMATION?

RULE:

You must delete or destroy Personal Information when you no longer need it to achieve your purpose (i.e., to examine fraud).

EXCEPTION:

There are some exceptions to this rule that allow you to keep Personal Information. You may only keep Personal Information after you achieved your purpose if:

- a law requires you to keep the information (e.g., FICA, NCA or labour laws);
- you require the information for lawful purposes related to your functions or activities (e.g., as Record of a disciplinary enquiry, CCMA proceedings, civil proceedings, criminal trial);
- a contract requires you to keep the information (e.g., an employment contract);
- the Data Subject consented that you keep their information;
- you must keep the information for historical, statistical or research purposes and as long as you ensure that the information is not used for any other purposes; or
- you used the Personal Information to make a decision about a Data Subject, and a law or code of conduct requires you to keep the information. If no law or code of conduct applies, you must keep the information for a period which will afford the Data Subject a reasonable opportunity to request access to the information (e.g., when an algorithm decided to include a Data Subject in an investigation).

RECOMMENDATION

You should create and implement a Records retention schedule that determines default rules for how long and why you must retain Records of Personal Information.

When a retention period ends, you must delete, destroy or De-identify the Personal Information as soon as reasonably possible but at least within six months after the retention period ends or within the period that you documented in your policies and procedures. If Personal Information is held in the cloud or by a service provider, you must ensure that the Personal Information, and any backups, are securely deleted, destroyed or de-identified.

11. WHAT RIGHTS DO DATA SUBJECTS HAVE?

POPIA gives Data Subjects the right to:

- be notified that you are collecting their Personal Information (Read more);
- be notified that an unauthorised person accessed or acquired their Personal Information (Read more);
- access their Personal Information (Read more);
- correct or delete their Personal Information (Read more);
- object to the Processing of their Personal Information (Read more);
- withdraw the Consent they have previously given (Read more);
- not be subject to a decision based solely on automated Processing of their Personal Information profiles (Read more);
- complain to the Regulator about the alleged interference with the protection of their Personal Information (Read more); and
- institute civil proceedings about the alleged interference with the protection of their Personal Information (Read more).

You must have processes in place to deal with the requests and objections of Data Subjects.

12. WHEN AND HOW MAY YOU SHARE PERSONAL INFORMATION WITH THIRD PARTIES?

12.1. YOU MUST ASSESS ALL SHARING ACTIVITIES

Before you share Personal Information with a Third Party (such as SAPS), you must make sure that you are legally allowed to share the Personal Information with that Third Party by assessing the planned Sharing against all the conditions for the lawful Processing of Personal Information.

DEFINE IT

SHARING includes transferring and giving access to Personal Information.

NB

This section deals with Sharing Personal Information with other Responsible Parties. It does not apply to sharing information with your employees, employer, or Operators.

Make sure you can tick these boxes before you share Personal Information with a Third Party:

- ✓ Document what information you are Sharing, who you are Sharing it with, and how you are Sharing it.
- ✓ Identify and document why you are Sharing the information.
- ✓ Obtain prior authorisation from the Regulator if you need it.
- ✓ Ensure that you meet the requirements for Sharing information across borders if the Third Party is in a foreign country.
- ✓ Make sure you have a legal justification to share each piece of information. Remember, the rules are different when you share Special Personal Information, or the Personal Information of Children.
- ✓ Make sure you comply with the requirements for further Processing if you are Sharing Personal Information for a new purpose.

NOTE ASSESS EITHER LEGAL JUSTIFICATION OR FURTHER PROCESSING. EITHER CAN APPLY, BUT THEY CANNOT BOTH APPLY.

- ✓ Ask the Third Party to confirm which exception to the direct collection rule applies to them so that they may receive the information from you instead of directly from the Data Subject.
- ✓ Make sure that you let the Data Subject know that you will share their information with Third Parties before you collect their information, or while you collect their information, unless there is an exception to the notification rule.
- ✓ Share only the necessary information.
- ✓ Share the information securely.
- ✓ Keep a Record of the information that you shared and with whom you shared it.

Example: You want to share an employee's bank statements that you collected during a fraud investigation with SAPS. You must make sure that you can check all the boxes before you can share the employee's Personal Information. For instance:

- ✓ Document which bank statements you are Sharing with SAPS, who at SAPS you are sending it to, how you are Sharing it, and why you are Sharing it.
- ✓ You do not need prior authorisation to share bank statements.
- ✓ You are not Sharing information with foreigners.
- ✓ You have a legal justification for Sharing the information because it is in the Responsible Party's legitimate interest to combat fraud.
- ✓ SAPS may collect the bank statements from you because it is necessary for them, a Public Body, to detect and investigate a crime.
- ✓ You do not have to notify the employee that you are Sharing the bank statements with SAPS because the information will be used in court proceedings.
- ✓ You are Sharing only the necessary information, no irrelevant information.
- ✓ You use a secure channel (e.g., encrypted email) to send the information to SAPS.
- ✓ You keep a Record of this assessment.

12.2. WHEN YOU MAY TRANSFER PERSONAL INFORMATION TO A THIRD PARTY OUTSIDE SOUTH AFRICA OR TO AN INTERNATIONAL ORGANISATION

RULE:

You may not transfer Personal Information to a Third Party in a foreign country.

EXCEPTIONS:

There are some exceptions to this rule that allow you to transfer Personal Information. You may transfer Personal Information to a Third Party in a foreign country if:

- the Third Party receiving the information provides an adequate level of protection (i.e., if they are subject to a law, binding corporate rules, or contract that protects Personal Information in the same way that POPIA does);
- the Data Subject consented to the transfer;
- the transfer is necessary to perform in terms of a contract or to implement pre-contractual measures between you and the Data Subject;
- the transfer is necessary to perform in terms of a contract between you and the Third Party in the interest of the Data Subject; or
- the transfer is for the benefit of the Data Subject, and it was not reasonably practical to obtain Consent (and if it were, the Data Subject would have likely given Consent).

RECOMMENDATION

You should always have a written contract with foreign Third Parties with whom you share Personal Information.

ASK YOUR LAWYER	*Ask your lawyer to check that you have the correct contracts in place.*

03. WHAT COULD HAPPEN IF YOU DO NOT COMPLY WITH POPIA

1. HOW SHOULD YOU RESPOND TO A COMPLAINT FROM A DATA SUBJECT?

When Data Subjects learn that you are using their Personal Information in a fraud investigation, they may want to complain about it. If the Data Subject is the subject of the investigation, they might claim that you did not have their Consent to collect and use their Personal Information. However, in these circumstances it is seldom that you need the Data Subject's Consent and you should be able to explain that what you are doing is legal.

When you receive a complaint from a Data Subject, you should:

- acknowledge their complaint and that you are investigating it;
- confirm the complainant's identity;
- determine what Personal Information you have, why you have it (your purpose and legal justification), where you collected it from, and how you used it; and
- respond to the Data Subject within a reasonable time.

When you respond to the Data Subject, you should:

- confirm whether you have the Data Subject's Personal Information;
- explain why you have the Data Subject's Personal Information (see the purpose you documented when you started with the fraud investigation);
- confirm the legal reasons why you are using the Data Subject's Personal Information;
- confirm from which source you collected the Data Subject's Personal Information and why you were allowed to collect it from this source;
- explain how you notified the Data Subject that you will collect and use their Personal Information, or if you did not notify them, why you did not have to notify them;
- explain why you may keep the Data Subject's Personal Information and when you will delete or destroy it; and
- inform the Data Subject of their rights to request access to, update, or delete their Personal Information.

	**ASK YOUR LAWYER**	*Attorney-client privilege covers any discussions between you and your lawyer, so ask your lawyer for advice when you prepare your response. There may be valid reasons why it is not appropriate to supply all the information mentioned here.*

2. WHAT COULD HAPPEN WHEN A DATA SUBJECT COMPLAINS TO THE REGULATOR?

When a Data Subject complains to the Regulator, the Regulator could implement the following steps.

2.1. HOW TO RESPOND TO A PRE-INVESTIGATION NOTICE FROM THE REGULATOR

When a Data Subject complains to the Regulator, the Regulator may decide not to take action or to send you a pre-investigation notice. The pre-investigation notice must contain details of the complaint or subject matter of the investigation and your right to submit a written response within a reasonable time – the Regulator will give you a deadline.

When you respond to a pre-investigation notice, you should:

- investigate the complaint (determine who complained, why you have their Personal Information, where you got their information from, what you used the information for, and whether you still have a valid reason to have the information);
- respond before the deadline;
- respond only to the details of the complaint or subject matter of the investigation and not give unnecessary or irrelevant information;
- involve your lawyer (remember the attorney-client privilege); and
- explain which relevant measures you have taken to ensure POPIA compliance (e.g., we have implemented a data privacy policy through training, or we informed the Data Subject why we collect and use their Personal Information on our website).
- If you find that you did breach POPIA, explain to the Regulator how and when you will change your process and activities to avoid non-compliance in future.

When the pre-investigation is complete, the Regulator may decide to launch a full investigation.

NB

The Regulator may also act as a conciliator or attempt to reach a settlement. When this happens, the Regulator will likely invite you to a meeting.

ASK YOUR LAWYER	*Ask your lawyer for advice before you attend a meeting of the Regulator.*

2.2. HOW THE REGULATOR MAY INVESTIGATE YOU

When the pre-investigation is complete, the Regulator may launch a full investigation.

ASK YOUR LAWYER	*Ask your lawyer for advice before responding to any investigation notices from the Regulator.*

In an investigation, the Regulator may:

- summon and force people to testify before the Regulator;
- administer oaths;
- issue Information Notices;
- receive any evidence and other information that the Regulator sees fit;
- search the premises of the Responsible Party, conduct interviews with people on the Responsible Party's premises in terms of a warrant issued by a high court, regional magistrate or a magistrate; and
- conduct a private interview with anyone in any premises the Regulator has a warrant to search.

DEFINE IT

The Regulator may issue an **INFORMATION NOTICE** if it reasonably requires any information to determine whether the Responsible Party has interfered or is interfering with the Personal Information of a Data Subject.

The Responsible Party may appeal an Information Notice. An Information Notice also cannot compel a Responsible Party to provide communication between them and their Professional Legal Adviser.

After completing the investigation the Regulator may refer the complaint to the Enforcement Committee. The Regulator must inform the Responsible Party and Data Subject of the process and whether they may make further submissions to the Enforcement Committee. If the Regulator finds that a Responsible Party has interfered with the protection of the Personal Information of a Data Subject, the Regulator can serve an Enforcement Notice on the Responsible Party.

An Enforcement Notice may require that the Responsible Party:

- take or not take certain steps by a specific date; or
- stop Processing the Personal Information entirely, or for a specific purpose, or in a specific way by a specific date.

The Responsible Party may appeal the Enforcement Notice to the high court. If the Responsible Party fails to comply with an Enforcement Notice, they will be guilty of an offence and may be fined up to R10 million or the Information Officer could be imprisoned.

3. WHAT MUST YOU DO WHEN YOU HAVE A SECURITY COMPROMISE?

If you suspect that you had a Security Compromise, report it to the Responsible Party (your employer or the organisation on whose behalf you are investigating fraud).

DEFINE IT

A **SECURITY COMPROMISE** happens when a Responsible Party has 'reasonable grounds to believe' that Personal Information was 'accessed or acquired by an unauthorised person'.

NB

Even if only one Record falls in the wrong hands, it is a Security Compromise that you must report.

The Responsible Party must notify the Regulator as soon as reasonably possible after discovering a Security Compromise using Form SCN1. The Regulator published guidelines to help Responsible Parties complete the form.

DEFINE IT

What does **'AS SOON AS REASONABLY POSSIBLE'** mean? Responsible Parties may take the needs of law enforcement and the measures that are reasonably necessary to determine the scope of the compromise and to restore the integrity of its information system into account when deciding when to report a Security Compromise. This means that the Responsible Party may first investigate and contain the Security Compromise and report it to law enforcement before reporting it to the Regulator.

The Responsible Party must also notify all affected Data Subjects as soon as reasonably possible after discovering the Security Compromise unless a Public Body in law enforcement or the Regulator asks for a delay. To allow the Data Subject to protect themselves against potential consequences of the Security Compromise the notification must include:

- the possible consequences of the Security Compromise;
- the measures that the Responsible Party intends to take or have taken to address the Security Compromise;
- recommended measures the Data Subject can take to mitigate the possible adverse effects of the Security Compromise; and
- the identity of the unauthorised person (if known) who may have accessed or acquired the Personal Information of the Data Subjects.

The notice to Data Subjects must be given by:

- mail;
- email;
- placing a prominent notice on your website; or
- publishing a notice in the news media.

NB

Sometimes it will be impossible for you to identify the Data Subjects affected by the Security Compromise. For instance, when your files were encrypted in a ransomware attack. In these instances the Information Regulator may require that you publish a notice in national newspapers and on social media platforms.

4. WHAT IS THE DIFFERENCE BETWEEN NON-COMPLIANCE AND COMMITTING AN OFFENSE?

There is a difference between non-compliance with POPIA and committing an offense in terms of POPIA. Non-compliance with POPIA is when someone interferes with the protection of the Personal Information of Data Subjects, whereas committing an offense is when someone deliberately violates certain sections of POPIA.

Example: In terms of POPIA it is an offense if someone:

- destroys, damages, alters, conceals or falsifies a Record with the intent to deny a Data Subject their right to access their Personal Information;
- fails to comply with an Enforcement Notice;
- knowingly or recklessly makes false statements in response to an Information Notice;
- fails to appear or produce information if summoned by the Regulator; and
- fails to ensure that the conditions for the lawful Processing of Personal Information are complied with in relation to Account Numbers assigned by a financial institution.

5. WHEN CAN RESPONSIBLE PARTIES GET FINED?

The types of fines and penalties Responsible Parties may face depend on the type of offense they committed. When a Responsible Party commits an offense, they will not immediately receive a fine, penalty, or imprisonment. The Regulator will first investigate the cause and circumstances surrounding the offence. The Regulator can then issue an Enforcement Notice and if the Responsible Party ignores the notice, the Regulator may issue fines.

The following are fines and penalties that may be given to the persons indicated if the particular offences were committed:

TYPE OF OFFENCE	POSSIBLE CONSEQUENCES	WHO
Destroying, damaging, altering, concealing or falsifying a Record with the intent to deny a Data Subject's right to access to Personal Information	A fine or imprisonment for a period not exceeding two years	The person that committed the offence
Failing wilfully or in a grossly negligent manner to make a complete PAIA Manual available	A fine or imprisonment for a period not exceeding two years	The Information Officer
Charging a fee to make a PAIA Manual available	A fine or imprisonment for a period not exceeding two years	The Information Officer
Charging a fee other than as Prescribed by PAIA	A fine or imprisonment for a period not exceeding two years	The Information Officer
Failing to comply with an Enforcement Notice in terms of PAIA	A fine or imprisonment for a period not exceeding three years	The Information Officer
Failing to comply with an Enforcement Notice in terms of POPIA	A fine or imprisonment for a period not exceeding 10 years	The Responsible Party

TYPE OF OFFENCE	POSSIBLE CONSEQUENCES	WHO
Knowingly or recklessly making false statements in response to an Information Notice	A fine or imprisonment for a period not exceeding 12 months	The Responsible Party
Failing to treat Personal Information which comes to a person's knowledge in the course of the performance of their official duties, confidential	A fine or imprisonment for a period not exceeding 12 months	The person acting on behalf of or under the direction of the Regulator
Hindering, obstructing or unlawfully influencing the Regulator or any person acting on behalf of the Regulator	A fine or imprisonment for a period not exceeding 10 years	The person that committed the offence
Intentionally obstructing a person executing a warrant or failing (without a reasonable excuse) to provide assistance to a person executing a warrant	A fine or imprisonment for a period not exceeding 12 months	The person that committed the offence
Failing to appear or produce information if summoned by the Regulator	A fine or imprisonment for a period not exceeding 12 months	The person that committed the offence
Giving false evidence under oath	A fine or imprisonment for a period not exceeding 10 years	The person that committed the offence
Failing to ensure that the conditions for the lawful Processing of Personal Information are complied with in relation to Account Numbers assigned by a financial institution	A fine or imprisonment for a period not exceeding 10 years	The Responsible Party
Obtaining, disclosing, selling or trying to sell an Account Number assigned by a financial institution without the permission of the Responsible Party or getting someone else to obtain or disclose an Account Number	A fine or imprisonment for a period not exceeding 10 years	The person that committed the offence

6. WHO CAN BE HELD LIABLE FOR OFFENCES?

Some of the offences listed refer to 'the person that committed the offence', whereas other offences refer to the 'Responsible Party'. If you commit these offences in your personal capacity in contravention of or without instruction from a Responsible Party, you can go to jail or receive these fines and penalties, but if you act in the course and scope of your employment or on the instruction of a Responsible Party, the Responsible Party will be accountable.

If a Responsible Party commits an offence, the Regulator could issue fines and notices to the Responsible Party. If the Responsible Party faces imprisonment, the organisation's Information Officer will go to jail as they are ultimately accountable for the Responsible Party's POPIA compliance. Although the Information Officer can delegate their duties and responsibilities to a Deputy Information Officer, they cannot delegate their accountability.

7. WHEN MAY DATA SUBJECTS OR THE REGULATOR INSTITUTE A CIVIL CLAIM?

Any Data Subject who suffers harm because of a Responsible Party's interference with the protection of their Personal Information, may institute a civil claim for damages in their personal capacity or request that the Regulator institute civil action on their behalf.

A Responsible Party will be liable when there is interference with the protection of the Personal Information of a Data Subject, including:

- any breach of the conditions for the lawful Processing of Personal Information;
- non-compliance with the sections of POPIA that deal with notifications of a Security Compromise, duty of confidentiality, Direct Marketing by means of unsolicited Electronic Communication, directories, automated decision-making, and transfers of Personal Information outside South Africa; or
- a breach of the provisions of an approved POPIA Code of Conduct.

RESOURCES

1. EXAMPLES OF PERSONAL INFORMATION

TYPE	EXAMPLES
Identifiers	A name, identity number, staff number, Account Number, customer number, company registration number, tax number, IP address, a phone's IMEI number and usernames on websites and social media
Biometric information	Blood types, fingerprints, DNA, retinal scans and voice Records Important: Biometrics is defined as 'a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition. This means that a photograph by itself is not biometric information, there must be some technical Processing (i.e., use of facial recognition software) before it is considered biometric information
Demographic information	Race, gender, sex, pregnancy, marital status, nationality, ethnicity, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture and language
Contact details and location	Physical and postal addresses, location information, email addresses, telephone numbers and social media handles
Financial information	Bank and other Account Numbers, statements, account balances, financial Records, salary information and credit histories
Background information	Educational, financial, employment, medical, criminal or credit history
Behavioural information	Likes, dislikes, preferences, opinions, views, posts on social media, browser history, location information, shopping history and who you associate with
Correspondence	Emails, direct messages, SMSs, letters, video chats and video meetings
Opinions about a Data Subject	Opinions expressed about an individual or organisation, such as preferences, trade references or reviews

2. PUBLIC INTEREST

You may apply for an exemption in terms of POPIA if the public interest in your activities is so significant that it outweighs the Data Subject's right to the protection of their Personal Information.

You may also apply for authorisation to Process Special Personal Information or the Personal Information of Children, or both, if the Processing is in the public interest and appropriate safeguards are in place to protect that information.

In their guidance note on exemptions, the Regulator states that public interest is a wide and diverse concept that should not be limited in its scope and application. The Regulator defines public interest as 'the notion that an action or process or outcome widely and generally benefits the public at large and should be accepted, imposed, or pursued in the spirit of equality and justice.'

POPIA provides the following examples of activities that are in the public interest:

- activities in the interests of national security
- the prevention, detection, and prosecution of offences
- important economic and financial interests of a Public Body
- fostering compliance with legal provisions that were established in the interests of the prevention, detection, and prosecution of offences, and the important economic and financial interests of a Public Body
- historical, statistical or research activities
- the special importance of the interest in freedom of expression

NB

The Regulator's guidance note provides the following example: A Public Body which intends investigating fraud and corruption that impacts its economic and financial interests may apply for an exemption from any condition for lawful Processing of Personal Information.

3. CATEGORIES OF SPECIAL PERSONAL INFORMATION

3.1. RELIGIOUS AND PHILOSOPHICAL BELIEFS

A religious belief is when a person does or abstains from something in the name of religion. To enjoy protection under the constitutional right to freedom of religion, that belief must be central to the religion, the person holding the belief must be genuine in practicing their religion, and the belief and the person's observance of this belief must be considered essential in that they hold a clear purpose.

A philosophical belief must:

- be genuinely held;
- be a belief as to a weighty and substantial aspect of human life or behaviour;
- attain a certain level of cogency, seriousness, cohesion, and importance;
- be worthy of respect in a democratic society, not be incompatible with human dignity and not be in conflict with the fundamental rights of others; and
- be more than just an opinion.

3.2. RACE OR ETHNIC ORIGIN

Race is a social construct referring to a group of people with distinct and similar physical characteristics. In the BBBEE and Employment Equity Act, the race categories used for employment equity and empowerment targeting purposes include 'Black African', 'Coloured', 'Indian or Asian', 'White' and 'Other'.

Ethnic origin includes shared cultural practices, perspectives, and distinctions that set one group of people apart from another, such as ancestry, territorial possession, language, forms of dress, a sense of history, and religion.

3.3. TRADE UNION MEMBERSHIP

A trade union is an association of employees whose principal purpose is to regulate relations between employees and employers. A person's membership is considered Special Personal Information in POPIA.

3.4. POLITICAL PERSUASION

A person's political persuasion (or political opinion) is their set of beliefs about government or public affairs. It is not limited to information relating to membership of a political party. It could include information such as a person's voting Records, whether they have ever interacted with a political party or expressed political views on social media.

3.5. HEALTH INFORMATION

Health information comprises any information about a person's injury, disease, disability, inherited characteristics, or disease risk, including medical history, medical opinions, diagnoses and clinical treatments, medical examination data, test results, data from medical devices, or data from fitness trackers, information collected from the person when they register for health services or access treatment, and any appointment details, reminders and invoices which tell you something about the health status of a person.

3.6. INFORMATION CONCERNING A PERSON'S SEX LIFE

Information concerning a person's sex life includes information about their sexual activity, relationships, sexual orientation, or sexual preferences.

3.7. BIOMETRIC INFORMATION

'Biometrics' is defined in POPIA as 'a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.'

3.8. CRIMINAL BEHAVIOUR

Criminal behaviour means allegations of criminal behaviour of a person (e.g., allegations of fraud) and does not include actual criminal convictions of a person. Criminal convictions are not Special Personal Information.

4. AUTHORISATIONS FOR PROCESSING SPECIAL PERSONAL INFORMATION

4.1. WHEN PROCESSING OF SPECIAL PERSONAL INFORMATION WILL BE AUTHORISED

You may collect and use Special Personal Information in fraud investigations if:

- the Data Subject consented;
- it is necessary for the establishment, exercise, or defence of a right or obligation in law;
- it is necessary to comply with an obligation of international public law;
- it is for historical, statistical or research purposes;
- it was deliberately made public by the Data Subject;
- the Regulator has authorised you to process Special Personal Information;
- a medical institution must provide proper treatment or care;
- bodies charged by law requires it to supplement information about the Data Subject's criminal behaviour or biometric information in order to apply criminal law; or
- a specific authorisation for certain types of Special Personal Information applies.

4.2. SPECIFIC AUTHORISATIONS FOR CERTAIN TYPES OF SPECIAL PERSONAL INFORMATION

RELIGIOUS OR PHILOSOPHICAL BELIEF

Spiritual or religious organisations may process Personal Information relating to their members' religious or philosophical beliefs.
This authorisation extends to information about the 'religion or philosophy of life' of the family members of the Data Subject if the organisation maintains regular contact with them in connection with its aim and the family members have not objected in writing to the Processing.

Institutions founded on religious or philosophical principles (e.g., a religious school or other organisation with a religious 'ethos') may also process information about religious or philosophical beliefs of their members, employees or other Data Subjects if it is necessary to achieve their aims and principles.

Others may process this type of Personal Information if 'the Processing is necessary to protect the spiritual welfare of the Data Subjects unless they have indicated that they object to the Processing'. For instance, an organisation may want to know whether people require vegan, Halaal or Kosher meals to meet their needs. This will be authorised if the Data Subjects have the opportunity to object to providing the information.

NB

Responsible Parties may only share Personal Information concerning religious or philosophical beliefs with Third Parties if the Data Subject Consents or if one of the general authorisations in section 27 of POPIA applies to that sharing activity.

RACE OR ETHNIC ORIGIN

You may process Personal Information relating to race or ethnic origin if:

- the Processing is essential to identify the Data Subject; and
- the Processing is required to comply with legislation and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

TRADE UNION MEMBERSHIP

A trade union (or the trade union federation to which the trade union belongs) can process the trade union membership of its members if the Processing is necessary to achieve the aims of the trade union or that of the trade union federation.

NB

The trade union or trade union federation is not permitted to share this Personal Information with Third Parties without the Data Subject's Consent unless one of the general authorisations in section 27 of POPIA applies to that sharing activity.

POLITICAL PERSUASION

Institutions founded on political principles may process information that relates to the political persuasion of its members if it is necessary to achieve the aims and principles of the institution. They may also process information relating to the political persuasion of other Data Subjects if the Processing is necessary to:

- form a political party;
- participate in activities of a political nature, to recruit members, or to canvass for supporters or voters for an election or referendum; or
- campaign for a political party or cause.

HEALTH OR SEX LIFE

Several types of Responsible Parties may have to process Personal Information about a person's health or sex life. POPIA provides the following authorisations:

Type of Responsible Party	The Responsible Party is authorised to process Special Personal Information about a person's health or sex life if it is necessary:
Medical professionals, healthcare institutions or social services	• for the proper treatment of the person or for administrative purposes.
Insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations	• to assess the risk that the insurance company or medical scheme must insure; • to perform in terms of an insurance or medical scheme agreement; or • to enforce any contractual rights and obligations.
Schools	• to provide special support or make special arrangements for the pupil in question.
Any Responsible Party who manages the care of a Child	• to carry out the Responsible Party's lawful functions.
Any Public Body responsible for prison sentences or detention measures	• to implement prison sentences or detention measures.
Administrative bodies, pension funds, employers, 'or institutions working for them'	• to implement legislation, pension regulations or collective agreements that create rights that are dependent on the Data Subject's health or sex life; or • to reintegrate, or support workers or persons who are entitled to benefits in relation to their sickness or work incapacity.

Responsible Parties must always treat information relating to health or sex life as confidential and may only share it with others if:

- it is required by law; or
- it is necessary for the performance of their duties.

Responsible Parties must adhere to additional requirements when they process inherited characteristics. You may only process this type of health information if:

- a serious medical interest prevails; or
- the Processing is necessary for historical, statistical or research purposes.

CRIMINAL BEHAVIOUR OR BIOMETRIC INFORMATION

Personal Information relating to criminal behaviour or biometric information may be processed by:

- bodies charged by law with applying criminal law (e.g., SAPS); or
- Responsible Parties who have obtained the information in accordance with the law.

4.3. APPLYING FOR AUTHORISATION TO PROCESS SPECIAL PERSONAL INFORMATION OR THE PERSONAL INFORMATION OF CHILDREN

A Responsible Party may apply for authorisation from the Regulator to process Special Personal Information or the Personal Information of Children, or both. The Responsible Party must prove that:

- the Processing is in the PUBLIC INTEREST; and
- appropriate safeguards have been put in place to protect the Personal Information.

The Regulator may also impose additional conditions in respect of the authorisation which will be decided on a case-by-case basis. Read the Regulator's guidance note for more information.

5. MEASURES THAT RESPONSIBLE PARTIES MUST IMPLEMENT WHEN MAKING AUTOMATED DECISIONS BASED ON PROFILES

When you rely on automated decisions based on profiles, you must implement additional safeguards to sufficiently protect the rights of Data Subjects. Here are some examples of safeguards that you could implement:

- Provide an opportunity for the Data Subject to make representations about the decision.
- Use anonymised Personal Information in automated decision-making activities where possible.
- Notify Data Subjects about any automated decision-making activities.
- Give Data Subjects the right to object to the use of automated decisions to an individual with authority who could review and change the decision.
- Provide Data Subjects with a plain language explanation of the categories of Personal Information that will be used, why these categories are considered important for the activity, how the profile used in the activity is built (including any statistics involved in the analysis), why this profile is relevant to the activity and how this profile is used to make an automated decision concerning the Data Subject.
- Explain the type of consequences or impacts that automated decisions could result in for a Data Subject and provide honest, tangible examples.
- Provide a simple way for the Data Subject to obtain human intervention in the automated decision, to express their point of view, and to contest the automated decision, e.g., placing a link to the appeals process at the point when the automated decision

is delivered to the Data Subject with specified periods of the review and a named contact point for any queries.

- Carry out frequent assessments of the Personal Information the Responsible Parties process as part of the automated decision-making activity to check for any bias, and develop ways to address any prejudicial elements, including any over-reliance on correlations (such as algorithm audits).
- Introduce appropriate procedures and measures to prevent errors, inaccuracies, or discrimination.

6. THE DISCLOSURES A RESPONSIBLE PARTY MUST MAKE WHEN COLLECTING PERSONAL INFORMATION

When collecting Personal Information you must notify the Data Subject of:

- what information you are collecting;
- where you are collecting the information from;
- the name and address of the Responsible Party;
- the purposes for which the information is being collected;
- whether the Data Subject is supplying the information voluntary or mandatory;
- the consequences if the Data Subject choose not to provide the information;
- any particular law that authorises or requires the collection of the information;
- the Responsible Party's intention to transfer the information to a foreign country or international organisation and the level of protection which that foreign country or international organisation can provide to the information;
- a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the Responsible Party to ensure the confidentiality, integrity, and availability of the information which is to be processed;
- the recipient or category of recipients of the information;
- the nature and category of the information;
- the existence of Data Subject rights; and
- the contact details of the Regulator.

7. HOW DATA SUBJECTS MAY EXERCISE THEIR RIGHTS

7.1. THE RIGHT TO ACCESS PERSONAL INFORMATION

Data subjects have the right to know what Personal Information you have about them and to access a Record of their Personal Information. Data Subjects may also ask which Third Parties have had access to their Personal Information.

You must implement a procedure to ensure that you can verify the identity of Data Subjects and that you can respond to their requests:

- within a reasonable time;
- in a reasonable manner and format; and
- in a form that is reasonably understandable.

Data Subjects' right to access Personal Information is not absolute. You may or must refuse to disclose information on the grounds provided for refusal as stated in Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act.

Examples: Data Subjects are not entitled to their own Personal Information if giving access would:

- reveal the Personal Information of someone else without that other person's permission;
- disclose privileged documents (in the context of legal proceedings), unless the person entitled to the privilege has waived that privilege;
- endanger the life or safety of an individual;
- breach your contractual duty of confidence that you have to a Third Party; or
- compromise someone else's intellectual property or confidential information.

If you may or must refuse to disclose a part of the Personal Information that the Data Subject requested, you must disclose every other part of the information to them.

7.2. THE RIGHT TO CORRECT OR DELETE PERSONAL INFORMATION

Data Subjects may ask you to:

- correct inaccurate, out-of-date, incomplete, or misleading Personal Information that you possess or control;
- delete excessive, irrelevant, out-of-date, incomplete, misleading, or unlawfully obtained Personal Information that you possess or control; and
- destroy or delete Personal Information you control in contravention of POPIA.

When you receive such a request, you must either:

- correct, delete, or destroy the Personal Information; or
- provide evidence of the accuracy and validity of the Personal Information to the satisfaction of the Data Subject (in the interim, you must restrict the use of that Personal Information).

DEFINE IT

RESTRICTING the use of Personal Information means that the Responsible Party must stop any further Processing of the information and that they must ensure that the information cannot be changed or deleted. The Responsible Party must mark the information as 'restricted'.

Examples: Responsible Parties can restrict the Processing of Personal Information by:

- temporarily moving the information to another Processing system;
- making the information unavailable to users; or
- temporarily removing published information.

7.3. THE RIGHT TO OBJECT TO THE PROCESSING OF PERSONAL INFORMATION (SECTION 38 EXCEPTION)

If you are Processing Personal Information to protect a legitimate interest of the Data Subject, or to pursue your or a third party's legitimate interest, the Data Subject has the right to object to that Processing. To exercise this right, i.e., to object, the Data Subject must demonstrate that there are reasonable grounds relating to their situation that justify their objection.

If you receive a valid objection, you must stop Processing the Data Subject's Personal Information and restrict access to that Personal Information.

NB

If you perform a Relevant Function, Data Subjects do not have this right to object.

7.4. THE RIGHT TO WITHDRAW CONSENT PREVIOUSLY GIVEN

Data Subjects have the right to withdraw previously given Consent at any time. When they withdraw their Consent, you must stop Processing the Personal Information for the purposes for which the Consent was withdrawn. The Processing that happened before the Data Subject withdrew their Consent will stay valid.

7.5. THE RIGHT TO MAKE REPRESENTATIONS ABOUT AUTOMATED DECISIONS WITH A LEGAL OR SUBSTANTIAL EFFECT BASED ON PROFILES

Data Subjects have additional rights if your activities involve automated decisions based on Profiling.
When your activities involve automated decision-making based on profiles, you must:

- allow Data Subjects to make representations about that decision; and
- provide Data Subjects with sufficient information about the underlying logic of the automated decision to allow them to make representations.

GLOSSARY

ACCOUNT NUMBER	Any unique identifier that has been assigned a) to one data subject only b) jointly to more than one data subject by a financial or other institution which enables the data subject(s) to access their own or joint funds or to access credit facilities.
BIOMETRICS	A technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.
CHILD	A natural person under the age of 18 years who is not legally competent without the assistance of a competent person to take any action or decision in respect of any matter concerning him- or herself.
CODE OF CONDUCT	This means a code of conduct issued in terms of Chapter 7 of POPIA.
COMPETENT PERSON	Any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.
CONSENT	Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
CONSTITUTION	The Constitution of the Republic of South Africa, 1996
DATA SUBJECT	The person to whom personal information relates.
DE-IDENTIFY	In relation to personal information of a data subject, means to delete any information that: a) identifies the data subject; b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.
DIRECT MARKETING	To approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or b) requesting the data subject to make a donation of any kind for any reason.

ELECTRONIC COMMUNICATION	Any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
ENFORCEMENT NOTICE	A notice issued in terms of section 95 of POPIA.
FILING SYSTEM	Any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.
INFORMATION OFFICER	Of, or in relation to, a: a) public body, means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or b) private body, means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act (PAIA). If you are a sole proprietor you are both the responsible party and the information officer.
OPERATOR	A person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
PERSON	A natural person or a juristic person
PERSONAL INFORMATION	This is information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including, but not limited to: a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; b) information relating to the education or the medical, financial, criminal or employment history of the person; c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or another particular assignment to the person; d) the biometric information of the person; e) the personal opinions, views or preferences of the person; f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; g) the views or opinions of another individual about the person; and h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
PRESCRIBED	Means prescribed by regulation or by a code of conduct.

PRIVATE BODY	Means: a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity; b) a partnership which carries or has carried on any trade, business or profession; or c) any former or existing juristic person but excluding a public body.
PROCESSING	Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including: a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; b) dissemination by means of transmission, distribution or making available in any other form; or c) merging, linking, as well as restriction, degradation, erasure or destruction of information.
PROFESSIONAL LEGAL ADVISER	Any legally qualified person, whether in private practice or not, who lawfully provides a client, at their or its request, with independent, confidential legal advice.
PROFILING	Means any form of automated processing of personal information to evaluate certain aspects relating to a data subject's personality, behaviour, interests, and habits (e.g., creditworthiness, location, performance at work, health, or conduct).
PROMOTION OF ACCESS TO INFORMATION ACT (PAIA)	The Promotion of Access to Information Act, no. 2 of 2000
POPIA	The Protection of Personal Information Act, no. 4 of 2013
PUBLIC BODY	Means: a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or a) any other functionary or institution when: i. exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or ii. exercising a public power or performing a public function in terms of any legislation.
PUBLIC RECORD	A record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.

RECORD	Any recorded information: a) regardless of form or medium, including any of the following: i. writing on any material; ii. information produced, recorded or stored by means of any tape recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; iii. label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; iv. book, map, plan, graph or drawing; v. photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; b) in the possession or under the control of a responsible party; c) whether or not it was created by a responsible party; and d) regardless of when it came into existence.
REGULATOR	Means the Information Regulator established in terms of section 39 of POPIA.
REPUBLIC	The Republic of South Africa
RESPONSIBLE PARTY	A 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.
RESTRICTION	To withhold any personal information from circulation, use or publication that forms part of a filing system, but not to delete or destroy such information.
SPECIAL PERSONAL INFORMATION	Personal information as referred to in section 26 of the Protection of Personal Information Act. According to section 26, this is personal information concerning: a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or b) the criminal behaviour of a data subject to the extent that such information relates to: i. the alleged commission by a data subject of any offence; or ii. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
THIRD PARTY	An organisation or individual other than the a) data subject; b) responsible party; c) operator; or d) sub-operator.
UNIQUE IDENTIFIER	Any identifier that is assigned to a data subject and that a responsible party uses for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.