Rand Safety Equipment CC - Personal Information Protection Policy

Introduction

You may be aware that South Africa has introduced a new law called the Protection of Personal Information Act, or POPIA. This law has introduced many requirements for organisations to act responsibly when using individuals' personal information. POPIA calls these individuals, data subjects. Failure to comply with POPIA could severely impact our organisation's reputation and possibly lead to litigation with, potentially, serious financial consequences. This document outlines our organisation's intent with regards the implementation and maintenance of our on-going Personal Information Protection Program.

As an employee, you are a data subject and we use your personal information such as your name, identification, address and banking details' or perhaps sensitive data such as your health status or trade union membership. Our clients and customers are also data subjects. POPIA states that this personal information must be protected, it must remain fresh and valid and that data subjects must be able to access their personal information.

Requirements

We expect our leadership to:

- Understand the requirements of POPIA, especially for areas under their influence and especially where they have responsibilities as information owners
- Drive the adoption of the appropriate behaviours throughout our organisation
- Understand and regularly assess and respond to any privacy risk to their areas of operation

Policy Statement

This Policy defines the responsibilities and expected behaviours of all our employees, contractors and relevant organisation partners which will uphold a data subject's right to have his or her personal information processed in accordance with the requirements of the Protection of Personal Information Act.

Scope

This Policy applies to:

- the personal information of all data subjects with whom we interact
- all types of and uses for personal information within our organisation
- all our employees and organisation partners, especially those who deal directly with personal information
- all our organisation's processes and all systems (both manual and digital, internal and external) that process personal information
- all our data processing locations, whether in, or out of country

Data Protection Rules

We shall:

Only process personal information which is relevant to our organisational needs

Together with our data subjects, keep their personal information up to date

Not keep personal information in the hope that it may become useful later on

Only grant access to the data to people who need to use it for their jobs

Protect the data from accidental loss or theft

Where required, always seek the data subject's consent

Where required, always seek the consent of a competent person in respect of a child

Only process sensitive personal information where we are legally able or required to do so

When communicating with our data subjects, always be open and transparent, using language that is easily understandable

Be aware of possible data subjects requests to access and manage their personal information and how to respond to such requests

Be aware of possible compromises in the security of personal information and how to respond to such security compromises

Be aware of and respond timeously to any training and awareness programs and communications within our organisation

Rand Safety Equipment CC - Privacy Notice

This privacy notice provides details of the personal information we collect from you, what we do with it, how you might access it and who it might be shared with.

Our Organisation

Rand Safety Equipment CC

10 Miracle Park

Tshiomate Close, Hennopspark, Centurion

0157

South Africa

Mobile: +27828590895

Telephone: +27126532870

Organisation email: info@randsafety.co.za

What we do with your personal information

We use your personal information only for the purpose for which it is collected. Among others, this purpose could be to provide a service, assist us with administration, recruit prospective employees or even to comply with a legal obligation. We may use your personal information for other similar purposes, including marketing and communications, but that will only occur in the case where we have your consent or another lawful justification for doing so.

From our **Service Providers** we collect, use and retain personal information for the following purposes and periods, with the applicable lawful basis..

Processing purpose	Lawful basis	Retention period
Auditing and taxation services	S11 - It is in our organisation's legitimate interest (Employment data processing)	Until consent withdrawn
Business advisory	S11 - It is in our organisation's legitimate interest (Organisation operations and due diligence)	Upon conclusion of the service, event or promotion
Legal advice and representation	S11 - It is in our organisation's legitimate interest (Legal and regulatory compliance)	Until consent withdrawn

From our **Suppliers** we collect, use and retain personal information for the following purposes and periods, with the applicable lawful basis..

Processing purpose	Lawful basis	Retention period
Customer sales, service and support	S11 - We have the data subject's consent	Until consent withdrawn

From our **Consultants** we collect, use and retain personal information for the following purposes and periods, with the applicable lawful basis..

Processing purpose	Lawful basis	Retention period
Business advisory	S11 - We have the competent person's consent	Until consent withdrawn

From our **Customers / Clients** we collect, use and retain personal information for the following purposes and periods, with the applicable lawful basis..

Processing purpose	Lawful basis	Retention period

Customer sales, service and support	S11 - We have the data subject's consent	Until consent withdrawn

From our **Prospective Employees** we collect, use and retain personal information for the following purposes and periods, with the applicable lawful basis..

Processing purpose	Lawful basis	Retention period
Employee recruitment	S11 - We have the competent person's consent	Until consent withdrawn

What personal information do we collect?

We only collect the minimum amount of information that is relevant to the purpose. If you interact with us on the internet, the personal information we collect depends on whether you just visit our website or, use our services. If you visit our website, your browser transmits some data automatically, such as your browsing times, the data transmitted and your IP address. Our website does not make use of Online Identifiers or any 3rd party analytics tools, however, trackers may follow users from other sites to our website. Our online store captures user billing and shipping information.

If you use our services, personal information is required to fulfil the requirements of that service.

Generally, we collect the following personal information. If there is any *specific* personal information to collect, we will indicate as such, at or near the time of collection.

1. Physical address
2. Telephone number
3. Email address
4. Financial & banking details
5. Location information
6. Name, together with other identifying information
7. Identification Number
8. Education history
9. Employment history

Who might we share your personal information with?

To maintain and improve our services, your personal information may need to be shared with or disclosed to our service providers, other organisations such as ours or, in some cases, public or legal authorities.

We transfer personal information to the following organisations and countries:

Data subject type	Organisation name	Type	Country
Service Providers	Margaret Mostert	Accountant	South Africa
Service Providers	Sentinel Systems (Pty) Ltd	IT Company	South Africa
Prospective Employees	Beverley Evans	Operator	South Africa

If we transfer your personal information outside of South Africa, we apply the necessary safeguards which include, confirming whether the receiving country has the proper data protection law, ensuring that there is a binding agreement between parties or, if the transfer is internal to our organisation, commitment to binding corporate rules. Details of these safeguards may be obtained by contacting us directly.

How do we look after personal information?

We limit the amount of personal information collected to only what is fit for the purposes as described above. We restrict, secure and control all of our information assets against unauthorised access, damage, loss or destruction; whether physical or electronic. We retain personal information only for as long as is described above, to respond to your requests, or longer if required by law. If we retain your personal information for historical or statistical purposes we ensure that the personal information cannot be used further. While in our possession, together with your assistance, we try to maintain the accuracy of your personal information.

How can you access your personal information?

You have the right to request access to any of your personal information we may hold. If any of that information is incorrect, you may request that we correct it. If we are improperly using your information, you may request that we stop using it or even delete it completely.

If you would like to make a request to see what personal information of yours we might hold, you may make a request from our organisation website or contact us as per the details above

Where you have previously given your consent to process your personal information, you also have the right to request that we transmit your personal information to a different service provider.

Where it may have been necessary to get your consent to use your personal information, at any moment, you have the right to withdraw that consent. If you withdraw your consent, we will cease using your personal information without affecting the lawfulness of processing based on consent before your withdrawal.

Our Information Officer

Shaun Evans

shaun@randsafety.co.za

Telephone: +012 653 2870

Mobile: +082 859 0895

The SA Information Regulator

You have the right to lodge a complaint with the SA Information Regulator. See the Information Regulator contact details below.

The Information Regulator (South Africa)

PO Box 31533

Braamfontein

27 Stiemens St

Braamfontein

2017

The Information Regulator (South Africa)

complaints.IR@justice.gov.za

27827464173

inforeg@justice.gov.za

Rand Safety Equipment CC - Employee Privacy Notice

Details of the personal information we collect from you, what we do with it, how you might access it and who it might be shared with.

Why do we need your personal information?

Personal information is required to fulfill the requirements of an employment, contractual or service relationship which may exist between you and our organisation.

From our **Contracting Staff** we collect, use and retain personal information for the following purposes and periods, with the applicable lawful basis..

Processing purpose	Lawful basis	Retention period
Employee recruitment	S11 - We have the competent person's consent	Until contract completed

From our **Employees** we collect, use and retain personal information for the following purposes and periods, with the applicable lawful basis..

Processing purpose	Lawful basis	Retention period
Employee monitoring	S11 - We have the competent person's consent	Until consent withdrawn
Employee recruitment	S11 - We have the competent person's consent	Until consent withdrawn

What personal information do we collect?

- Physical address
- Identification Number
- Telephone number
- Education history
- Employment history
- Email address
- Financial & banking details
- Location information
- Name, together with other identifying information

Special personal information could be about your health, your racial or ethnic origin, your trade union membership etc. We collect the following special personal information, under the appropriate lawful basis.:

- Criminal behaviour - allegations
    - S27 - We have the data subject's consent

Should we intend to use the information for any other purpose, we will always inform you beforehand. We may collect the personal information of children, but this data will be required to maintain records e.g., with tax authorities or medical aid societies.

Who might we share your personal information with?

To maintain and improve our services, your personal information may need to be shared with or disclosed to service providers, other similar organisations or, in some cases, public authorities. We may be mandated to disclose your personal information in response to requests from a court, police services or other regulatory bodies. Where feasible, we will consult with you prior to making such disclosure and, in order to protect your privacy, we will ensure that we will disclose only the minimum amount of your information necessary for the required purpose.

We transfer personal information to the following organisations and countries.

Data subject type	Organisation name	Type	Country
Contracting Staff	Margaret Mostert	Responsible Party	South Africa

Employees	Beverley Evans	Operator	South Africa
Employees	Margaret Mostert	Operator	South Africa
Employees	Margaret Mostert	Responsible Party	South Africa
Employees	Sentinel Systems (Pty) Ltd	Responsible Party	South Africa

If we transfer your personal information outside of South Africa, we apply the necessary safeguards which include, confirming whether the receiving country has the proper data protection law, ensuring that there is a binding agreement between parties or, if the transfer is internal to our organisation, commitment to binding corporate rules. Details of these safeguards may be obtained by contacting HR directly.

How do we look after personal information?

We limit the amount of personal information collected only to what is fit for the purpose of the employment relationship. We restrict, secure and control all of our information assets against unauthorised access, damage, loss or destruction' whether physical or electronic, and we ask that our employees assist us in these activities. We retain personal information only for as long as is necessary to fulfil the requirements of the employment relationship, respond to requests from employees, or longer, if required by law. If we retain your personal information for historical or statistical purposes we ensure that the personal information cannot be used further. While in our possession, together with your assistance, we try to maintain the accuracy of your personal information.

How can you access your personal information?

As an employee you have the following rights.

You have the right to request of our organisation, access to your personal information which we might hold as well as the rights to rectify, erase or restrict the processing of such information. You may make a request for access to your personal information from our organisation website, or directly to our HR department. Where you have previously given consent to process your personal information, you have right to request that your personal information be ported (transferred) to a different service provider, or to yourself.

Where it may have been necessary to get your consent to use your personal information, at any moment, you have the right to withdraw that consent. If you withdraw your consent, we will cease using your personal information without affecting the lawfulness of processing based on consent before your withdrawal.

Our Organisation

Rand Safety Equipment CC
10 Miracle Park
Tshiomate Close, Hennopspark, Centurion
0157
South Africa
Mobile: +27828590895
Telephone: +27126532870
Organisation email: bev@randsafety.co.za

Our Information Officer

Shaun Evans
shaun@randsafety.co.za
Telephone: +012 653 2870
Mobile: +082 859 0895

The SA Information Regulator

You have the right to lodge a complaint with the SA Information Regulator. See the Information Regulator contact details below.

The Information Regulator (South Africa)
PO Box 31533
Braamfontein

27 Stiemens St
Braamfontein
2017
The Information Regulator (South Africa)
complaints.IR@justice.gov.za
27827464173
inforeg@justice.gov.za

Rand Safety Equipment CC - Record of Processing

Regulator

Name	The Information Regulator (South Africa)
Address	PO Box 31533 Braamfontein 2017
Email	complaints.IR@justice.gov.za
Contact Person	inforeg@justice.gov.za
South Africa	The Information Regulator (South Africa)

Responsible Party

Responsible Party Name	Rand Safety Equipment CC
Head of Organisation / Owner	Shaun Evans
Postal Address	10 Miracle Park Tshiomate Close, Hennopspark, Centurion 0157
Physical Address	10 Miracle Park Tshiomate Close, Hennopspark, Centurion 0157
Landline	27126532870
Email	info@randsafety.co.za
Country	South Africa

Information Officer

Name	Shaun Evans
Email	shaun@randsafety.co.za
Landline	012 653 2870
Mobile	082 859 0895
Address	10 Miracle Park, Tshiomate Close, Hennopspark, Centurion, 0157

1. Details of Processing

Data Subject Type	Processing Purpose	Personal Information Category
Service Providers (Contractor /Supplier)	**Auditing and taxation services** Lawful basis: *S11 - It is in our organisation's legitimate*	Education history Email address Employment history Financial & banking details

	interest Retention Period: *Until consent withdrawn*	Identification Number Location information Name, together with other identifying information Physical address Telephone number	
		Special Personal Information Category	**Lawful basis**
		specialPersonalInformationType.custom.name.993	S27 - We have the data subject's consent
	Business advisory Lawful basis: *S11 - It is in our organisation's legitimate interest* Retention Period: *Upon conclusion of the service, event or promotion*	**Personal Information Category** Education history Email address Employment history Identification Number Location information Physical address Telephone number	
	Legal advice and representation Lawful basis: *S11 - It is in our organisation's legitimate interest* Retention Period: *Until consent withdrawn*	**Personal Information Category** Email address Employment history Identification Number Location information Name, together with other identifying information Physical address Telephone number	
Contracting Staff (Employee)	**Employee recruitment** Lawful basis: *S11 - We have the competent person's consent* Retention Period: *Until contract completed*	**Personal Information Category** Education history Email address Employment history Financial & banking details Identification Number Location information Name, together with other identifying information Physical address Telephone number	
Suppliers (Contractor /Supplier)	**Customer sales, service and support**	**Personal Information Category** Email address	

	Lawful basis: *S11 - We have the data subject's consent* Retention Period: *Until consent withdrawn*	Financial & banking details Location information Name, together with other identifying information Physical address Telephone number
Consultants (Contractor /Supplier)	**Business advisory** Lawful basis: *S11 - We have the competent person's consent* Retention Period: *Until consent withdrawn*	**Personal Information Category** Email address Location information Name, together with other identifying information Physical address Telephone number
Customers / Clients (Other)	**Customer sales, service and support** Lawful basis: *S11 - We have the data subject's consent* Retention Period: *Until consent withdrawn*	**Personal Information Category** Email address Financial & banking details Location information Name, together with other identifying information Physical address Telephone number
Employees (Employee)	**Employee monitoring** Lawful basis: *S11 - We have the competent person's consent* Retention Period: *Until consent withdrawn*	**Personal Information Category** Education history Email address Employment history Financial & banking details Identification Number Location information Name, together with other identifying information Physical address Telephone number
		Special Personal Information Category / **Lawful basis** Criminal behaviour - allegations / S27 - We have the data subject's consent
	Employee recruitment Lawful basis: *S11 - We have the competent person's consent* Retention Period: *Until consent withdrawn*	**Personal Information Category** Education history Email address Employment history Financial & banking details

		Identification Number	
		Location information	
		Name, together with other identifying information	
		Physical address	
		Telephone number	
		Special Personal Information Category	**Lawful basis**
		Criminal behaviour - allegations	S27 - We have the data subject's consent
Prospective Employees (Other)	**Employee recruitment** Lawful basis: *S11 - We have the competent person's consent* Retention Period: *Until consent withdrawn*	**Personal Information Category**	
		Education history	
		Email address	
		Employment history	
		Identification Number	
		Location information	
		Name, together with other identifying information	
		Physical address	
		Telephone number	

2. We disclose personal information to the following recipients

Organisation name	Type	Category	Country
Beverley Evans	Operator	Bookkeeping & Payroll	South Africa
Margaret Mostert	Operator	Accountant	South Africa
Iron Tree Internet Services CC	Operator	Cloud Storage	South Africa
Margaret Mostert	Responsible Party	Accountant	South Africa
Sentinel Systems (Pty) Ltd	Responsible Party	IT Support	South Africa

Where relevant, we confirm whether the destination country has an appropriate law in place, else we make use of the appropriate binding agreement. If the transfer is internal to our organisation, we ensure that we have Binding Corporate Rules in place.

3. Security Measures

Through regular risk assessment, we are able to identify security measures necessary to secure the confidentiality and integrity of processing of personal information.

Examples of some of our Technical security measures are as follows:

- Encrypted storage and transfer
- Employee access controls
- Regular updating of security software and systems
- Monitoring to detect potential breaches

Examples of some of our Organisational security measures are as follows:

- Employee awareness and training on relevant policies and procedures

- Undertaking Data Protection Impact Assessments
- A documented disaster recovery program, including regularly tested backups
- Limiting employee access to personal data
- We maintain a risk management program to address information security risks and breaches

Rand Safety Equipment CC - CCTV Policy

INTRODUCTION

Purpose

This CCTV Usage Policy establishes the guidelines for the use of closed circuit television (CCTV) within all of the relevant properties of Rand Safety Equipment CC

The CCTV equipment is in use for the following purpose:

- Prevention, investigation and detection of crime
- Apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings)
- Visitor, contractor and employee safety
- Monitoring the security of premises

Scope

This Policy applies to all areas controlled by Rand Safety Equipment CC

This Policy applies to all Rand Safety Equipment CC employees, contractors, operators and visitors

This Policy is guided by and supports the requirements of relevant regulation

REQUIREMENTS

Siting and usage of cameras

Data shall not be used for purposes other than as stated above

Cameras shall be sited such that they will only monitor those spaces which are intended to be covered

Equipment operators (such as Security Companies) shall be aware that they are only able to use the equipment to achieve the purpose for which Rand Safety Equipment CC installed them

The cameras shall be limited / restricted in their movement so that they cannot be manipulated beyond their intended coverage zones

Equipment operators shall be aware of the privacy implications of CCTV usage

Clearly visible and legible signs shall be placed in the common areas making people aware that they are entering a zone that is covered by surveillance equipment

Image quality

- We shall procure technology that provides the best images suited to our purposes for usage of CCTV
- The equipment shall be checked on initial installation and'shall perform to required standard
- The media on which the images are captured shall be cleaned so that images are not recorded on top of images recorded previously
- The media on which the images have been recorded shall not be used when it has become apparent that the quality of images has deteriorated
- The system shall record such features as the location of the camera and date and time reference
- These features shall be checked daily for accuracy and a record shall be kept
- We shall carry out constant, real time recording
- Cameras shall be properly maintained and serviced
- A maintenance log shall be maintained
- Damaged equipment shall be replaced within 5 working days

Image processing

- Generally, data shall be retained for a period of 28 days, after which it must be deleted

- Specifically, if data is in use for investigation or evidential purposes then the data shall be retained for as long as required by the investigation
- If the data is retained for evidential proposes, it shall be retained in a secure place to which access is controlled
- Monitors displaying images from areas in which individuals have an expectation of privacy shall not be viewed by anyone other than authorised operators of the equipment
- Access to and viewing of the recorded images is restricted to the manager or designated member of staff, who will decide whether to allow requests for access by third parties in accordance with our documented disclosure procedure
- The removal and return of media for viewing purposes, shall be documented
- All operators and employees with access to images shall be aware of the procedure for accessing the images
- The removal and return of media for use in legal proceedings shall be documented

Access by, and disclosure of images to third parties

- Access to recorded images is restricted to accredited employees or operators
- All access to storage media shall be documented
- Disclosures shall be governed by a disclosure agreement, unless such disclosure is required by law
- All requests for access or for disclosure shall be documented. If access or disclosure is denied then the reason shall be documented
- Disclosure to third parties is limited to the following circumstances:
    - Law enforcement agencies where the images recorded would assist in a specific criminal enquiry
    - Prosecution agencies
    - Relevant legal representatives
    - People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)
    - No disclosures shall be made to the media unless under direction of our communications policy and in accordance with the requirements of the relevant agency
    - Images are NOT to be made widely available - such as on the Internet

Data subject access

All relevant employees or CCTV equipment operators must be able to recognise a request for access and shall be familiar with and follow our data subject access request procedure

Records storage and retention

All relevant employees or CCTV equipment operators shall be familiar with and shall follow our policies and procedures on records retention and storage

Rand Safety Equipment CC - Work from Home Policy

POLICY - Working from Home

When working from home, it is your responsibility to ensure our organisation's information remains secure at all times. This includes information of our business, our employees, our customers and suppliers. This policy provides guidance and best practice to follow for employees who are permitted or requested to work from home.

Do's and Don'ts

In the context of our organisation's business, your home is also considered a public place. While it is largely restricted to just your family, it is nevertheless a space to which people (who do not work for us) have unrestricted access. Therefore, you must follow the same practices when working from home with our company's information, as you would outside of the organisation's premises.

When working from home, ensure your office environment and network is secure, and your laptop and our organisation's information is protected at all times.

Physical security

Never leave your laptop visible to an intruder. Store our laptop, documents and any other devices in a secure place e.g. in a locked cabinet, when not in use;
If you are permanently home-based, you must ensure appropriate arrangements are in place to maintain the security of our laptop and documents. If possible, use a dedicated office room that you can keep locked when you are not working.

Personal security

Ensure that only you have access to the laptop and working papers. Never let outsiders use our laptops or view our data or applications.

Acceptable Use of our equipment and information

Only use a laptop issued by our organisation;
All equipment connecting to our networks must be used in accordance with instruction. Only limited and occasional personal use of our technology systems is permitted;
Do not install unlicensed software on our laptops.

Protection of information

If working with confidential or personal information, ensure you access and save data on our organisation-approved servers, and not the laptop. If you are required to save confidential or personal information to the laptop, business approval is required beforehand.
Removable storage devices such as memory sticks, DVD's and CD's containing confidential or personal information must not be stored at home. These must be left at our premises, in a locked secure cabinet or safe;
Do not use private e-mail accounts or non-approved instant messaging services for our organisation's work;
Avoid printing documents on your home printer. If there is a need to print, dispose paper documents by shredding;
When making phone calls or attending or running a teleconference, ensure you are not overheard if discussing a sensitive topic. Also ensure that you do a roll-call to confirm the legitimacy of attendees.
Avoid discussing sensitive or personal information when out and about.

Protection of our laptop

Do not modify or remove the security functionality that is pre-installed on the laptop or prevent the device from installing mandated security updates. Ensure you connect regularly to our organisation's network to receive the latest security updates for your laptop;
When leaving your laptop unattended, activate the screen saver;
Do not share passwords or write them down.

Security of your home network

Do not allow wireless connections from un-trusted, unknown sources or open Wi-Fi network e.g. free wireless hotspots, neighbour's router. Using unsecured connections can allow intruders to intercept your information;
Only connect to the internet using a secure wireless or Ethernet connection. Ensure your Wi-Fi is adequately secure. You can secure this by WPA encryption. Your network provider will provide you with instructions on how to switch on WPA.

Rand Safety Equipment CC - POLICY: Personal Information Security Compromise

Introduction

A personal information security compromise, if not addressed appropriately and timeously, could result in physical, material or non-material damage to individuals as well as financial and reputational damage to our organisation. Where we collect, use and retain personal data, every care must be taken to both, protect that personal data and use it in a lawful manner.

Purpose and Scope

The Personal Information Protection Act (POPIA), has a requirement for our organisation to have a suitable data security framework in place. This policy is an essential part of that framework and sets out the procedure to be followed that ensures a consistent and effective response to a security incident. The policy applies to all employees, contractors and other stakeholders who might have access to or be responsible for the collection and processing of personal data.

Definition

A personal information security compromise means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information transmitted, stored or otherwise processed.

Reporting an incident

Report any discovery of an incident immediately to your most senior manager. Senior management will ensure that they are contactable for emergencies outside our regular hours of operation. Anyone reporting an incident is encouraged to record as much detail as possible. Be aware that failure to report an incident could potentially attract disciplinary action.

Containment and recovery

The first responder will determine if the incident is still occurring and, if so, the steps that will be taken to minimise the effects of the incident. Thereafter, an initial assessment will be done to determine - severity; what can be done to limit damages or recover losses; who may need to be notified in terms of the initial containment; any involvement of law enforcement; and the course of action to be followed.

Investigation and risk assessment

Our breach procedure will, at the very least, determine - the lead investigator; when the investigation must start; how will risks be assessed and treated; the individuals affected, the effect of the incident on them and what they can to minimise impact.

Notification

If an incident has been contained, it may not be necessary to inform the Regulator. If we do have to inform the Regulator, it must be made as soon as reasonably possible after the discovery of the compromise.

Be aware that law enforcement may prevent us from informing individuals whose personal data may be affected by the breach. Where we do need to inform individuals, we will do so timeously and in simple but specific language. We will also consider whether it's necessary to inform other stakeholders - insurers, banks, credit card agents, trade unions. We will keep a record of every incident/breach regardless of whether notification was required.

Evaluation and response

Every incident will require a full review of the causes, the effectiveness of the response and the impact on existing systems and/or procedures. Existing controls will be reviewed to determine whether any optimisation is necessary. We will determine whether any training and awareness of incident detection and response may be necessary. As such, regular desktop training exercises are to be encouraged.

Rand Safety Equipment CC - POLICY: Data Subject Access Requests

Policy Statement

A data subject is the individual to whom personal information relates. The Protection of Personal Information Act, gives data subjects certain rights, for example, to confirm whether we're processing their personal information lawfully; to rectify or delete their personal information; and to obtain copies of the personal information. This policy demonstrates our approach to identifying and responding to such requests.

Scope

This policy relates to our data subjects which may include employees, contractors, clients, suppliers and the like. This policy applies to all who may be responsible for identifying and responding to data subject access requests, including any external organisations who might process personal data on our behalf.

Duties and Responsibilities

Leadership Accountability-The leadership is accountable for implementation and oversight of this policy. They must understand its requirements, especially for areas under their control, and drive the adoption of the appropriate behaviours throughout our organisation.

Data Privacy Team-The team is responsible for the implementation, monitoring and review of the overall procedure. The team must ensure that the individuals directly involved in processing requests are aware of their responsibilities and are adequately trained. Regular table-top exercises are encouraged.

The Manner of Requests

Data subject access requests can be made in writing, electronically or verbally. We must therefore, develop and implement the mechanisms to quickly identify and respond to requests.

Verifying Identity

If we have doubts about the identity of the person making the request, we can ask for more information. However, it is important that we only request information that is necessary to confirm who they are. It should be the minimum amount and only what is relevant in the particular context. The prescribed forms like Form C do actually ask for the requester to provide an ID number. However, in many cases, asking for a copy of an identity document, passport or birth certificate could be considered disproportionate and, contrary to what some believe, does not necessarily provide proper assurance as to the real identity of the person. We must therefore ensure that we have in place, the appropriate procedures and mechanisms to verify the requester's legitimacy to make such requests.

Request Detection and Response

All persons responsible must be able to recognise and properly escalate a request. The request must be evaluated for legitimacy and then processed according to the nature of the request and the POPIA's specific requirements.

Promotion of Access to Information Act (PAIA)

PAIA provides for the way in which we must respond in respect of matters such as response times, prescribed fees we may charge, the types of information we may or may not include in our response or whether we need to inform third parties. Our responses must be guided by both POPIA and PAIA.

Rand Safety Equipment CC - Information Protection Training and Awareness

What is POPIA?

The South African Protection of Personal Information Act, or POPIA, is a law that aims to protect the personal information of individuals while that information is being used by various organisations.

What is Personal Information?

Personal information is information relating to an individual, including, but not necessarily limited to name, contact details, identity number, bank details, race, gender, age, health status, email address, location, online identifier and the like

What is Special Personal Information?

This is sensitive information concerning racial or ethnic origin, political persuasion, health or sex life, religious or philosophical beliefs, criminal behaviour or biometric data

What is a data subject?

A data subject means the person to whom personal information relates. For example, some of the data subjects of an organisation could be its customers and employees

What are the Rights of data subjects?

In order to protect the rights that POPIA grants to data subjects, organisations need to observe the following:

- The head of any organisation is accountable for complying with POPIA
- Personal information must be collected and used only for the specific and lawful purpose for which the organisation is established
- Only the essential amount of personal information must be collected from the data subject
- The personal information of a child may only be collected and used upon consent of a competent person, such as a parent or guardian
- Personal information must, as far as is practicable, be collected directly from a data subject
- Do not retain personal information for longer than is necessary for that specific purpose for which it was collected
- Where the personal information might be used for a purpose different to the original reason for collection, in most cases, the data subject's consent must be confirmed
- Organisations must ensure that the personal information remains complete, accurate and up to date
- Always be transparent in your communications with data subjects
- Protect personal information from loss, theft, damage and unauthorised access
- Where personal information is processed by an external service provider (called an Operator), ensure that contracts are in place which demand that the Operator also complies with these conditions
- Where personal information must be shared, and jointly controlled between Respsonsible Parties, ensure that the proper consent has been obtained and that the sharing is governed by the relevant data sharing agreement
- Have a system in place to notify data subjects and the Information Regulator of any security compromises (breakdowns in security)
- Have a system in place to allow data subjects to access and manage their personal information
- You can only market electronically to data subjects if they are your bona fide customers
- If you plan to approach a prospective customer with the intention of marketing directly, using electronic means, then you need the consent of that data subject. Do not contact a data subject more than ONCE for a particular product if you plan to get his or her consent
- Always give data subjects the option to object to such processing of their personal information. For example, an unsubscribe link in every marketing email.
- Do not profile a data subject using purely automated means, (i.e. without human intervention) if your intention is to make any decisions which might significantly impact the data subject - unless you have the relevant safeguards in place
- Ensure that whenever consent is needed and given, that the consent is in writing and that you retain the evidence of consent having been given

- Consent means any **voluntary, specific and informed** expression of will in terms of which permission is given for the processing of personal information

What is a 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

What is an 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. For example, if our organisation were to outsource the processing of our payroll to an external organisation, that organisation would be the Operator. Of course, if our organisation is to process payrolls on behalf of other Responsible Parties, we would also be an Operator - and, therefore, both Responsible Party and Operator

What is a Personal Information Protection Policy?

A Policy is internal to an organisation and demonstrates management's intent with regards to compliance with legislation such as POPIA

What is a Privacy Notice?

A Privacy Notice is an externally facing document that draws special attention to the manner in which our organisation is complying with POPIA. It is usually displayed at points where we collect personal information and informs data subjects as to their rights

Data Subject's access to his or her Personal Information

Data subjects have the right to enquire whether an organisation holds their personal information and also to request the records or descriptions of those records. They have the right to challenge and even stop the processing of their personal information. They may request that their personal information be changed - e.g. where a name, surname or contact details change. When a data subject makes a request for access, the data subject's identity must be confirmed before you may continue with the response. POPI365, our privacy management system, has a has a special section to assist with data subject access management. If you recognise a request for information you need to alert your manager.

What is 'limited personal use'?

Often the line between personal use and organisation use of systems becomes blurred. Our systems are primarily and exclusively for organisation use. Where we allow limited personal use of our organisation's IT systems you must be aware of the following:

- DO NOT make personal use of an unreasonable amount, of our organisation's network or other technology resources (e.g. to stream audio or video, download or store large files, or large amounts of printing)
- DO NOT allow personal use to interfere with your productivity or the productivity of others who are doing organisational work
- DO NOT violate copyright, privacy laws, or licensing arrangements (e.g. file sharing of content protected by copyright, such as movies and music)
- DO NOT use our organisation's IT systems and services to run or support your private organisation
- DO NOT use our organisation's IT systems and services to distribute SPAM, personal solicitations or unsolicited advertising
- DO NOT assume that our organisation has an obligation to store or recover your personal content saved on organisation IT systems, if lost
- DO NOT break local laws, cause harm or offence to others or negatively impact our organisation's reputation or interests

How do I play my part in protecting Personal Information?

Understand and respect the rights of data subjects

Be aware that some information within our organisation may be classified as 'Confidential' and must be treated accordingly

All *personal* information in our organisation is classified as 'Confidential'

Understand what we mean by the 'Acceptable Use' of our digital systems

Use strong passwords and keep them to yourself

Understand how to recognise suspicious emails and links

Think twice before clicking on any suspicious links

Keep your workstation clear, especially with regards to sensitive information

Practice discretion when you are outside and discussing our organisation

Keep our IT equipment safe, especially when you are outside the organisation premises

Be aware of the limitations we set with regards to internet access and usage

Understand what we mean by 'limited use' of our organisation's systems for personal reasons

If you know and understand your rights as a data subject, it will be much easier for you to apply this knowledge in the execution of your own job, especially where you handle personal information

Personal Information Protection Training and Awareness

The Protection of Personal Information Act (POPIA) brings South Africa's privacy protection regulation in line with the rest of the world

This regulation seeks to protect the collection and use of an individual's personal information while trying not to restrict the free flow of data.

It harmonises personal information protection with international standards.

Key Concepts

To fully understand the POPIA and its impact on our organisation and your role here, there are some core concepts you need to understand first.

What is personal information?

Personal information is any information relating to an identifiable individual. This includes not only obvious data like names, contact details, identity numbers, location, images, bank details, gender and age, but also less obvious items like online identifiers (think IP addresses).

What is processing and what is an operator?

Processing is very broad. It includes any operation or activity or any set of operations, whether or not by automatic means, concerning personal information. So any collection, recording, structuring, storage, adaptation or alteration, retrieval, consultation use, disclosure by transmission, dissemination, restriction, erasure or destruction - basically anything that is done with data.
An operator means a person who processes personal information for a responsible party (our organisation) in terms of a contract or mandate, without coming under the direct authority of that party. For example, a company doing payroll processing for its clients would be an operator.

What is a responsible party?

A responsible party means 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. Our organisation is a responsible party.

What is a data subject?

A data subject is the person to whom personal information relates For example, customers and employees would be data subjects of almost every organisation.

Special personal information

Special personal information requires higher levels of security as well as an extra lawful basis for processing. Special personal information concern race or ethnic origin, political persuasion, religious or philosophical beliefs, trade union membership, health or sex life or biometric information of a data subject.

The Conditions (Principles)

To fully understand the POPIA you need to understand conditions (or principles) that underpin the regulation. They are:

1. Processing, and further processing limitations

Personal information must be processed lawfully, and in a manner that does not infringe data subjects' rights. Any further processing of personal information must be in accordance or compatible with the original purpose for which it was collected. If all you do is sell tyres, don't send your customers' marketing material for babies shoes. The personal information you collect must be relevant and kept to a minimum. Collect the personal information directly from the data subject; unless there are other lawful reasons not to collect directly.

2. Purpose specification

Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. Take note - there are three conditions in this statement. Personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed - unless there are other lawful reasons to retain the information. There are certain instances where the processing must be restricted - in other words, held back from processing until such time that certain conditions are met.

3. Information security

A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control.

4. Openness

If personal information is collected, the responsible party must ensure that the data subject is aware of a host of information including the organisation's contact details, the source of the personal information, if not directly, the lawful basis for collection, the types of information, who the information might be shared with, how the personal information can be accessed etc.

5. Data subject participation

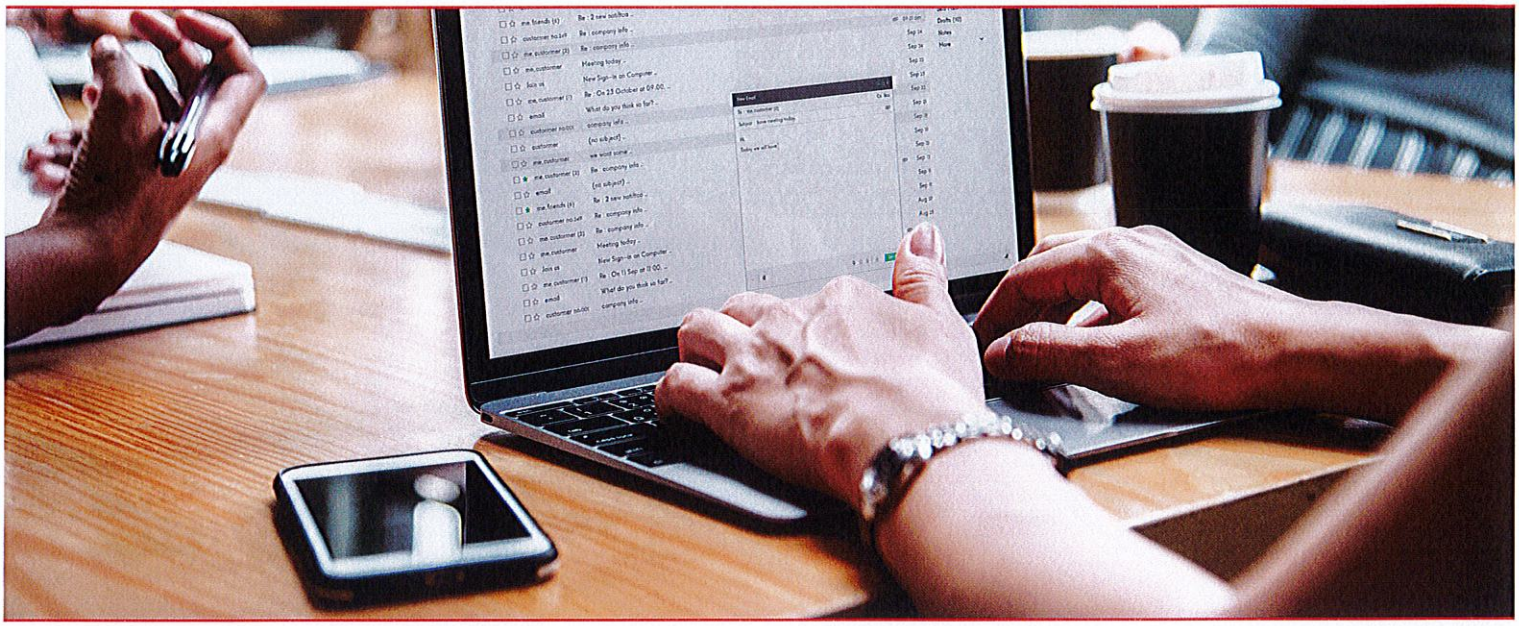
A data subject has the right to request a responsible party to confirm whether they hold any personal information of the data subject and the right to request a record or a description of the personal information held. A data subject has the right to have any incorrect personal information rectified as well as the right to object to certain processing of their personal information.

6. Information quality

A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

What rights do data subjects have?

In order to protect an individual's rights over their own personal information, POPIA grants the following rights to data subjects:



- **Right to be notified -** individuals have the right to be notified when their personal information is being collected as well as when their personal information has been accessed or acquired by an unauthorised person.
- **Right to object to certain processing of their personal information.**
- **Right to correction or deletion -** data subjects have the right to request the correction, deletion or destruction of their personal information..
- **Right to object to direct marketing -** direct electronic marketing requires consent and individuals must be able to opt out of any direct marketing..
- **Right to complain to the Regulator and to civil proceedings.**
- **Right not to be profiled -** in some cases you cannot profile people and take decisions based on the profiling, using computers to do the profiling.

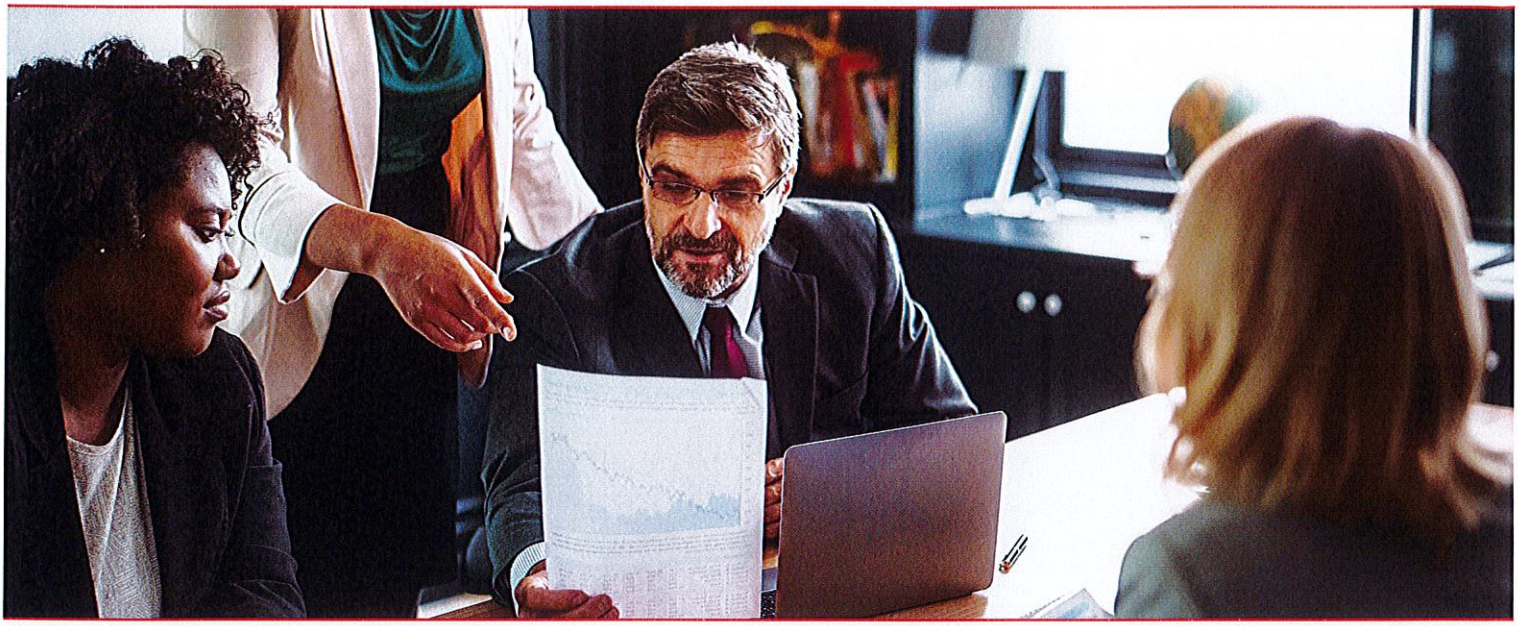
Protecting a data subject's rights

By remaining true to the conditions (principals), an organisation would easily be able to demonstrate compliance with the regulation.

An important point to remember is that compliance is not a once-off - it's a cyclical journey that requires regular review and upkeep.

Accountability

Each responsible party is responsible for demonstrating how it complies with POPIA and will need to:



- Create the environment to be able to implement and maintain the compliance journey and to appoint the relevant individuals to manage the journey.
- Collect personal information, as far as is practicable, directly from a data subject.
- Ensure that the personal information processing is lawful. Create and maintain an inventory of processing that can easily identify where the processing might not be lawful.
- Keep individuals informed through clear privacy notices.
- Have a system in place to allow data subjects to access and manage their personal information.
- Protect personal information from unwanted change, loss, and unauthorised access.
- Have a system in place to notify data subjects and the Regulator of any breaches in security of personal information.
- Where personal information is processed on your behalf by another organisation (operator), ensure that the relevant contract is in place.
- Where personal information must be shared with another organisation (responsible party), ensure that proper consent has been obtained. It's good practice to have a written agreement between parties - especially when it comes to data subjects understanding of how their rights will be upheld.
- Maintain the proper manual as provided for in both POPIA and PAIA (Promotion of Access to Information Act).
- Conduct privacy impact assessments to assess and treat any high risk processing of personal information.

What is a personal information protection policy?

A policy is usually a document, internal to an organisation, that demonstrates management intent with regards to (in this case), complying with POPIA.

Privacy notice

A privacy notice is used to inform individuals about their rights and about how your organisation processes and protects their personal information.

Consent

Having the data subject's (or competent person's) consent is one of the lawful bases for processing of personal information. Consent must be voluntary (not coerced or incentivised); it must be specific to the processing purpose (not broad-based) and the data subject must be fully informed in order to make the decision around granting of consent.

Children's personal information.

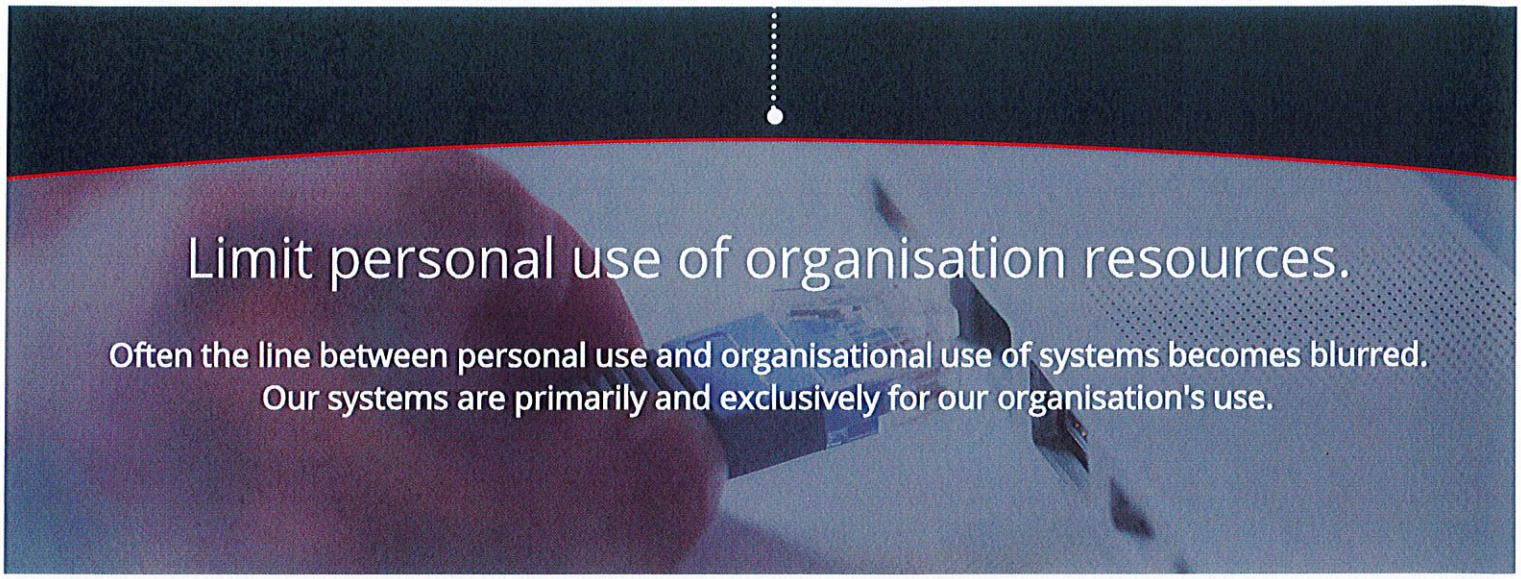
A child is a person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself. There are instances where the personal information of a child cannot be processed without the consent of a competent person.

Best practices for protecting personal information

There are some basic actions each one of us can take to make sure we're protecting the personal information we hold on individuals. Here are some of the things you can do:

Play my part in protecting personal information

- Understand and respect the rights of data subjects.
- Be aware that some information within our organisation is classified as 'confidential' and must be treated accordingly. Better yet, go beyond that and treat all personal information in our organisation as confidential.
- Understand what we mean by the 'acceptable use' of our digital systems.
- Understand how to recognise suspicious emails and links, and think twice before clicking on any link.
- Keep your workstation clear, especially in regard to sensitive information.
- Practice discretion when you're out of the office and discussing our organisation, our clients and our suppliers.
- Keep our IT equipment safe, especially when you're outside the organisation premises. If you have personal data files on your PC make sure they're encrypted or require password access.



Limit personal use of organisation resources.

Often the line between personal use and organisational use of systems becomes blurred. Our systems are primarily and exclusively for our organisation's use.

Where we allow limited personal use of our organisation's IT systems you must take note of the following:

- Do not make personal use of an unreasonable amount of our organisation's network or other technology resources (e.g. to stream audio or video, download or store large files, or do large amounts of printing).
- Do not allow personal use to interfere with your productivity or the productivity of others who are doing organisation work.
- Do not violate copyright and data protection laws or licensing arrangements (e.g. file sharing of content protected by copyright, such as movies and music).
- Do not use our organisation's IT systems and services to run or support a private organisation.
- Do not use our organisation's IT systems and services to distribute spam, make personal solicitations or unsolicited advertisements.
- Do not assume that our organisation has an obligation to store or recover your personal content saved on organisation IT systems, if lost.
- Do not break local laws, cause harm or offense to others or negatively impact the organisation.

Know your rights as a data subject. It'll be much easier for you to apply this knowledge in the execution of your own job.