1. Purpose, scope and target group

1.1 Purpose

This Data Privacy procedure refers to SAPREF's commitment to treat personal information which we process, with reasonable care and confidentiality.

Personal information: relates to information that makes a person identifiable, such as:

- Names.
- ID numbers.
- Information relating to the race, gender, sex, pregnancy, marital status, nationality, 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.
- Addresses.
- Blood type and fingerprints.
- Views or opinions.
- Usernames & passwords.
- Digital footprints.
- Photographs.
- Passport numbers.
- Educational, criminal or employment history, as well as information pertaining to financial transactions.

There are two laws which govern data privacy **Protection of Personal Information** (POPI) in South Africa and **General Data Protection Regulation** (GDPR) in EU. GDPR applies in S.A. where an entity processes the personal data of EU citizens. Impact of these:

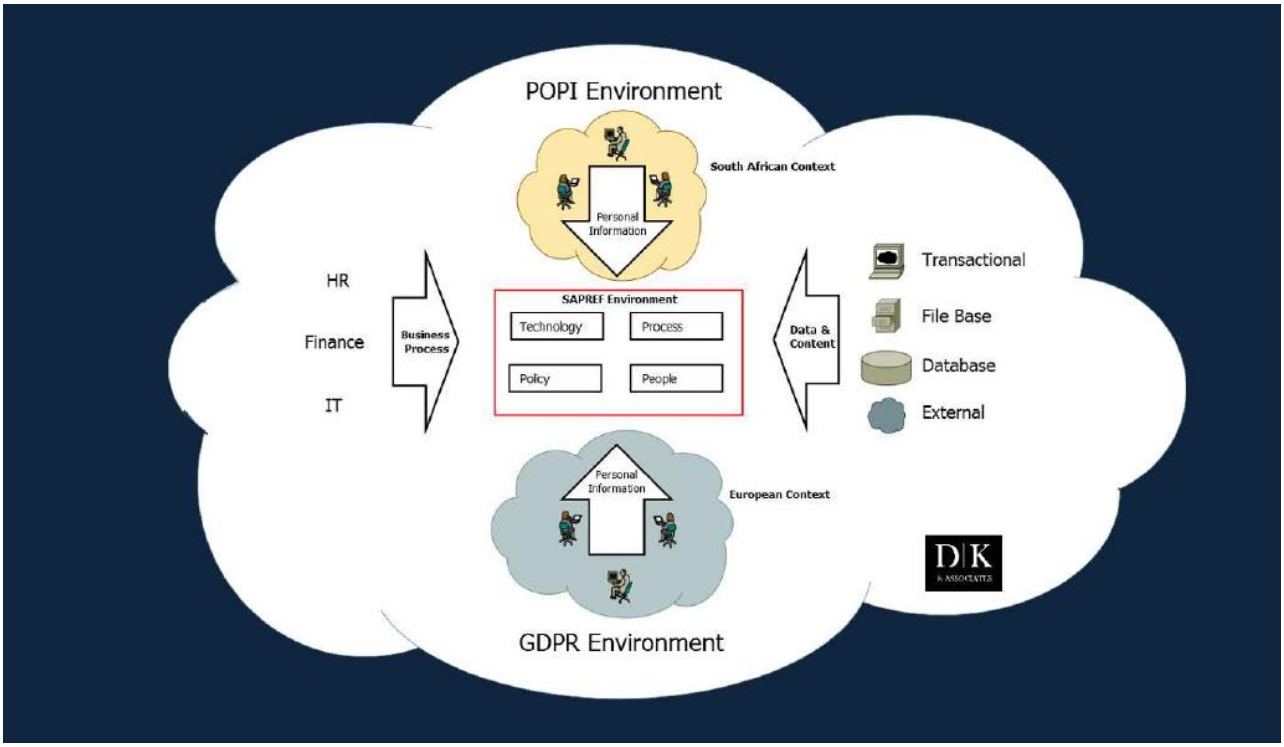
Business Area	Impact
Human Resources	Collection and processing of employee information e.g. employees medical and banking processed and stored in SAPREF database repository
Information Management	Developing policies for Information Security, Data Classification and Retention
Governance	Detailing who has the overall accountability for compliance e.g. Appointing a Chief Privacy Officer
Contract Management	Identification and Management of 3rdparty processing and hosting partners e.g. All service providers hosting Personal Information will be subject to yearly privacy audits.
Customer Relations	Collection and processing of customer personal information e.g. Call center processing customer personal details for returned or defective items and queries.
International Transacting	Identification and restrictions on cross border information transfers

Source: DK Associates presentation, 14 March 2018.

Processing definition: When a person attempts to collect personal information, this will be known as "Processing". The word Processing includes the collecting, receiving, storing, using, updating, modifying, disseminating and destruction of personal Information. Reasonable care must be exercised to gather, store and handle personal data fairly, transparently and with respect towards individual rights.

1.2 Scope

This procedure provides guidance for the protection of all personal information (physical and electronic) processed at SAPREF.



Source: DK Associates presentation, 14 March 2018.

1.3 Target Group

All SAPREF employees and Service providers must follow this policy in processing any personal data which might be required to execute SAPREF business processes. This also extends to the protection of personal information by anyone we collaborate with or who acts on our behalf.

2. Description [back to TOC]

- As part of our operations, we need to obtain and process personal information.
- Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties.

In alignment with the 8 POPI principles, SAPREF will employ reasonable endeavors to ensure that this personal information is:

- Collected from the data subject.
- Of good quality - accurate and kept up-to-date.
- Collected fairly and for lawful/ specific purposes only.
- Processed by the company within its legal boundaries.
- Technical and organisational measures applied to secure the integrity of personal information, and to guard against the risk of loss, damage or destruction of personal information.

This personal information will not be:

- Communicated informally.
- Stored for more than is necessary to support SAPREF's business processes or satisfy a regulatory requirement.
- Transferred/distributed to organizations, states or countries that do not have adequate data protection policies. As such, due diligence should be applied to determine this e.g. requesting proof of POPI compliance OR proof of GDPR compliance, as is applicable (exempting legitimate requests from law enforcement authorities). Personal information must be properly safeguarded when it is shared with a Third Party.

- Processed further in a way that is incompatible with the purpose for which the information was collected initially.

We endeavor to protect the personal information against any unauthorized or illegal access by internal or external parties.

Should parties erroneously gain access to personal/ confidential information, it is expected as per our code of conduct, that they will speedily flag the issue for remedy.

- In addition to ways of handling the data, the company has direct obligations towards people to whom the data belongs. Specifically, we must upon request:
    - Let people know which of their data is collected. (Ref table 1 below)
    - Inform people about how we'll process their data.
    - Inform people about who has access to their information.
    - Allow an individual's record to be modified, erased, reduced or corrected.
    - Inform the data subject in the event of a breach. A responsible person has a duty where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorized person, to notify:
        - the Regulator.
        - the Data Subject, unless the identity of the Data Subject cannot be established.
    - Notification must take place in writing, as soon as reasonably possible (ideally within 72 hrs.), unless a public body responsible for the prevention, detection or investigation of offences, or the Regulator determines that notification will impede a criminal investigation.

Should there be requests by the data subjects to view their information. The request will be processed through the relevant department (owning the information) head with the relevant System Administrator, Internal audit, ICT Risk and compliance, and legal having been consulted/ informed for any input.

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action. Any suspected violations should be reported via tip offs anonymous.