SANRAL SOUTH AFRICAN NATIONAL ROADS AGENCY SOC LTD BUILDING SOUTH AFRICA THROUGH BETTER ROADS	**SANRAL**	**DOCUMENT NUMBER**	5763841
		REVISION NUMBER	**01**
		ORIGINAL IMPLEMENTATION DATE	**New**
		REVISION EFFECTIVE DATE	**01 June 2020**
		UPDATED BY	**Adolph Tomes**
		CLASSIFICATION	**Public**

TITLE: EXTERNAL PRIVACY PROTECTION POLICY

1. PURPOSE

The purpose of this memorandum is to request the SANRAL Board of Directors approval of the External Privacy Policy.

2. BACKGROUND

This policy document sets out the South African National Roads Agency SOC Limited's (SANRAL) commitment to adhering to privacy and data protection principles. The policy sets out the responsibilities of everyone who handles personal and special category data within SANRAL.

3. RECOMMENDATION

It is recommended that the External Privacy Policy be approved.

RECOMMENDED / NOT RECOMMENDED

21/05/2020

CHAIRPERSON EXCO **DATE**

Comments (if any):

_____

_____

_____

RECOMMENDED / NOT RECOMMENDED

_____ _____

CHAIRPERSON ARC **DATE**

Comments (if any):

_____
_____
_____

APPROVED / NOT APPROVED

_____ _____

CHAIRPERSON BOARD **DATE**

Comments (if any):

_____
_____
_____

Table of contents

1 Document Administration

1.1 Revision History

Version	Date	Author	Description of change
1.0	2020/21/02	Adolph Tomes	Draft

1.2 Recommendation List

Name	Designation	Date	Signature
	Business Operations Executive		
	Executive Committee		
	Audit and Risk Committee		

1.3 Approval List

Name	Designation	Date	Signature
	Board of Directors: Chairperson		

1.4 Definitions / Acronyms

Term	Description
Customers	Anyone who uses (or is affected by) SANRAL's road network. Customers are not only the end-users of transportation services; they can also be members of the community directly affected by the use of the transportation systems.
Customer Information	Means any information contained on a customer's subscription/application documents or other form and all non-public personal information about a customer that SANRAL receives. "Customer Information" shall include, but not be limited to, name, address, telephone number, ID number, vehicle information and personal financial information (which may include consumer account number).
Data / Information asset	Refers to all data and information, in either electronic or paper form, that is processed and owned by or on behalf of SANRAL.
Data / Information asset owner: The responsible Executive	The Executive accountability for the management of the information asset in order to attain the business objective, while satisfying the demands of legislation and information management best practice.
Data / Information processing	Any operation or activity or any set of operations, whether or not by automatic means, including A. the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use; B. dissemination by means of transmission, distribution or making available through any other form; or C. merging, linking, as well as restriction, degradation, erasure, pseudonymizing or destruction of information.
Data / Information processing facilities	Any device, equipment, service, system, hardware, software or network that is used to process SANRAL owned information in either

Term	Description
	electronic or paper form, or any physical location that houses any of the aforementioned.
Data Protection personnel	The individual(s) tasks with the protection of data and information privacy operationally.
Data Subject	Refers to the individual to whom the Personal Data / Information relates
Encryption	Methods used to convert or re-organise data or information into a form that hides the original content of the data or information for protection.
Functional unit	Any SANRAL functional unit, business unit or supporting function.
Functional head	The leader of a SANRAL functional unit, business unit or supporting function.
General Data Protection Regulation (GDPR)	The primary legislation governing Privacy in the European Union Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016
Information Asset Owner or creator (Data Owner): Business Owner	The party with the authority to determine who may create, access, modify or delete information. This is usually a line function, not IT function.
Information Officer	The individual accountable with satisfying the requirements of PoPIA and relevant regulations are complied with.
information Security personnel	Information Technology staff responsible for the security and protection of information systems.
Intercept	The acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person

Term	Description
	other than the sender or recipient or intended recipient of that communication, and includes the: • Monitoring of any such communication by means of a monitoring device; • Viewing, examination or inspection of the contents of any indirect communication; and • Diversion of any indirect communication from its intended destination to any other destination. Note that this will include activities such as the viewing of static mails or files residing on servers.
Juristic Body	As opposed to a Natural Person, a Juristic Body is a non-living entity regarded by law to have the status of personhood. In the context of this policy: Companies, Partnerships, Corporations, Limited Liability Companies, Non-Profit and Tax-Exempt Corporations, Sole Proprietorships, Governmental and Semi-Governmental Organizations.
Legal Person	Any entity (Natural Person or Juristic Body) that can do the things an everyday person can usually do in law - such as enter into contracts, etc.
Logical access	The process of being identified, authenticated and authorized in order to use IT systems.
Natural Person	An individual human being, as opposed to a Legal Person. In the context of this policy: staff, contractors, customers and all persons engaging with SANRAL.
Need-to-know principle	A principle that states that individuals should only be granted access to information if they require that information to carry out their duties or any tasks assigned to them.

Term	Description
Personal Data / Information	Information relating to an identifiable, living, natural person, and where applicable and identifiable, existing juristic person[1], including but not limited to A. information relating to 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 other particular assignment to the person D. the biometric information of the person, including identifiable video imagery of a person, and fingerprint data retained for access control purposes E. 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 F. the views or opinions of another individual about the person G. 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 H. information relating to call data records which is a data record produced by telecommunications equipment that documents the details of a telephone call or other telecommunications transaction that passes through the mobile network. I. From GDPR: Genetic data, defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or

[1] Note that not all privacy legislation or regulations include Juristic Bodies (companies) in the definition of personal data / information. For purposes of this policy, in the interests of creating a common set of principles, and as it does not significantly change the operating procedures Juristic Bodies are included in the ambit of this policy.

Term	Description
	from the analysis of another element enabling equivalent information to be obtained.
PoPIA	Protection of Personal Information Act, 4 of 2013; the primary legislation governing Privacy in South Africa
PAIA	The Promotion of Access to **Information Act** 2 of **2000** (PAIA) is legislation in the Republic of **South Africa** allowing access to any **information** held by the State, and any **information** held by private bodies that is required for the exercise and protection of any rights.
Privacy Policy	Means this policy or the SANRAL External Privacy Policy and Data Protection policy.
SANRAL	The South African National Roads Agency SOC Limited
System Owner(s)	The party responsible for defining the business requirement to be addressed through a system implementation, budgeting for the acquisition and deriving business value from the system operation.
User	User refers to any individual, whether employee, contractor or third party, that makes use of SANRAL information systems or information assets. This includes connecting to SANRAL information systems remotely.

2 Overview

2.1 Purpose

The aim of this Policy is to:

- ensure compliance to the relevant privacy legislation /regulations across the different jurisdictions of SANRAL's operations;
- educate the business on why the adherence to privacy legislation / regulation is important and the potential consequences of failing to comply; and
- inform the business of the procedures in place for dealing with any breaches that affect SANRAL Stakeholders.

2.2 Scope

This policy applies to all individuals authorized to access SANRAL information processing facilities. This Policy is also applicable to the information (electronic or physical) that is handled and processed by contractors and third parties for SANRAL and Operating / Outsourced Companies but not limited to:

- All personal data / information including but not limited to customer information, SANRAL employees, vendors, third party and SANRAL company related information generated, processed and stored by operating companies at SANRAL to perform its activities and delivery of services;
- All systems and processes used in the course of managing personal data / information;
- Unless stated otherwise, this policy applies to all employees, contractors and third-party personnel of SANRAL and operating companies accessing SANRAL information processing facilities. SANRAL information processing facilities include, but not limited to; SANRAL outsourced partners / operators, facilities, offices, work areas, storage areas, critical infrastructure rooms (i.e. server rooms), warehouses and depots as well as solutions that may be used in road-, water- and air-borne vehicles.

2.3 Non-Compliance

Non-compliance with this policy must be reported to the SANRAL information Security personnel. Any breach may result in disciplinary action being taken, which may include dismissal.

Any disciplinary action arising from breach of this policy will be taken according to the disciplinary code and grievance procedure of SANRAL. Where an employee is suspected of

breaching the privacy policy, an internal investigation will be undertaken, depending on the outcome, civil and/or criminal legal action could be taken against the employee, contractors and third parties.

3 Policy Statements

3.1 Introduction

3.1.1. SANRAL takes the Privacy of Sensitive and Personal Information of all its stakeholders seriously. SANRAL understands that sensitive and personal information is important to all stakeholders and is committed to protecting stakeholder privacy. SANRAL's Privacy Policy incorporates relevant legislation as a guideline on how sensitive or personal information should be treated in as far as it relates to the following:

3.1.1.1. Data Collection;

3.1.1.2. Data Retention and Security;

3.1.1.3. Data Usage and Disclosure;

3.1.1.4. Data Accessibility;

3.1.1.5. Data Correction; and

3.1.1.6. Data Breach procedures.

3.2 Information Collected by SANRAL

3.2.1. SANRAL generally collects some or all the following sensitive/personal information or a combination of internal and/or external sources (e.g. employment data, toll systems, suppliers or from third parties). Information collected relates specific to information acquired for specific business purposes:

3.2.1.1. Name including any use of a pseudonym;

3.2.1.2. Address, phone details and email contact details;

3.2.1.3. Employment history;

3.2.1.4. Vehicle Information;

3.2.1.5. Bank account details;

3.2.1.6. Financial information;

3.2.1.7. National identifiers;

3.2.1.8. Referee opinions;

3.2.1.9. Interview opinions; and

3.2.1.10. Any other information that is supplied on documentation, electronically based systems or in communications with an SANRAL representative.

3.2.1.10.1. Other information gained for business purposed may include but not limited to these:

3.2.1.10.1.1. Identification Number

3.2.1.10.1.2. Vehicle owner information

3.2.1.10.1.3. Vehicle information; and

3.2.1.10.1.4. Any personal information

3.2.1.10.1.5. Credit card information

3.3 How SANRAL Obtains Data

3.3.1. Information acquired from other entities, including our Service Providers, third parties, government agencies, and toll agencies and operators. Information is obtained when motorists use The Toll Roads, the systems will automatically collect certain information, which may be Personal Information, including:

3.3.1.1. The toll road used, along with the date, time, and lane of travel;

3.3.1.2. Transponder unique identifier (e.g., the transponder number)

3.3.2. Information customers provide directly to SANRAL or its service providers using our Website, App(s), and interactions with SANRAL – including creating or managing an account – customers may provide the following categories of information, which may include Personal Information, such as:

3.3.2.1. Identifiers - name and other similar information (for example, first and last names, email address[es], mailing address[es], phone number[s]).

3.3.2.2. Account numbers as assigned to customers.

3.3.2.3. Transponder numbers as assigned.

3.3.2.4. Transaction and payment information

3.3.2.5. Vehicle information registered to customer accounts (for example, the vehicle type, license plate number, registration, year, make, model, colour, and clean expiration date).

3.3.2.6. Data entered when paying and/or calculating a toll on our Website or App.

3.3.2.7. Responses to surveys and promotional events (such as responses to questions and interactions with us on social medial or through surveys provided to customers).

3.3.2.8. Correspondence and communications information (for example, records of information provided by customers when you contact us, including audio and electronic information).

3.3.3. Information About transactions with SANRAL through toll systems when customers make payments, payment information is collected, such as the date, type, amount, and

category of any payment. Additionally, when customers provide financial, credit or debit card payment information, relevant data is collected for processing payment like what is listed above.

3.3.4. Other Sources Outside of SANRAL's direct interactions with customers or third parties in order to carry out our business functions including billing, accounting, enforcement, operation, and management of The Toll Roads. Information – including Personal Information – from the following sources (collectively "Other Sources"):

3.3.4.1. eNatis

3.3.4.2. Service Providers

3.3.4.3. Law enforcement

3.3.4.4. Government records or other publicly accessible directories and sources

3.3.4.5. Public record and information service providers

3.3.5. Other Sources shall include the following for internal/external for relevant business processes:

3.3.5.1. employee management, include the screening of curriculum vitae;

3.3.5.2. individuals utilizing the SANRAL website; and

3.3.5.3. business purposes, including communication by phone, fax, email, in person or other method of communication (i.e. eNatis).

- Individuals and companies who transact with SANRAL through the use of toll systems as a customer or road user.
- Individuals and companies who provide services to SANRAL as contractors and or service providers across various service areas locally and abroad.

3.3.6. SANRAL may also, with consent from the data subject, collect personal information from third parties including:

3.3.6.1. reference checks with referees; and

3.3.6.2. through networking with peers.

3.4 The Purpose of Collection

3.4.1. SANRAL collects sensitive and personal information about stakeholders to carry out its business functions and fulfil its obligations. These may include (but are not limited to):

3.4.1.1. the pursuit of legitimate business objectives;

3.4.1.2. complying with government legislation (e.g.: Employee information of contractors or third parties, SANRAL collects Income tax and Value Added Tax numbers to comply with taxation requirements);

3.4.1.3. meeting employment obligations to contractors and employees, which may include the processing of sensitive information (e.g.: Identification numbers, salary, age, disability and gender).

3.4.2. In addition, SANRAL may occasionally be required by law to collect, use and disclose personal information, for example in order to comply with the requirements of government departments for business data, or in support of a criminal investigation.

3.5 Collection, Use and Disclosure of Sensitive/Personal Information

3.5.1. SANRAL may only collect, store, process or disclose personal data / information pertaining to an individual:

3.5.1.1. if it is lawful to do so;

3.5.1.2. by individuals authorised to do so in the course of their duties;

3.5.1.3. with the knowledge of the data subject of the personal data / information, unless directed otherwise by legal authority; or

3.5.1.4. either

- with the express or implied consent of
  - the data subject;
  - guardian of the data subject of the personal data / information, or;
  - individual legally authorised to act on behalf of the data / information subject; or
- in order to satisfy a legitimate commercial purpose; or
- if required to do so meet a legislative or regulatory obligation.

3.5.2. Sensitive and Personal information may be disclosed to:

3.5.2.1. staff of SANRAL responsible for administering the processes described above;

3.5.2.2. health service providers in the event of the administering of emergency health services;

3.5.2.3. related bodies and third parties for the administration and provision of selected benefits and services but not limited to these (e.g.: debt recovery, training or policy administration); and

3.5.2.4. statutory authorities that may require personal information as per legislative requirements.

3.5.3. SANRAL may collect only the personal data / information for the execution of SANRAL's operations and achievement of its goals.

3.6 Access, Correct or update Personal information

3.6.1. SANRAL must take reasonable steps to ensure the accuracy of the personal data / information provided.

3.6.2. To the extent authorised by privacy legislation, SANRAL must provide data subject access to review and amend personal information held by SANRAL. This may be for a reasonable administration fee, via existing communication channels.

3.7 Security of Personal information

3.7.1. SANRAL must take all reasonable steps to ensure that sensitive and personal information is held in a secure environment accessed only by authorised persons for approved business purposes.

3.7.2. SANRAL will maintain sufficient security measures to ensure that the integrity and confidentiality of personal information held and/or processed by it is protected. These responsibilities will include sufficient measure to prevent the loss of, damage to, or unauthorised access to such personal information. In giving effect to these requirements SANRAL ensure the presence of suitable measures to:

3.5.3.1. Identify all reasonably foreseeable internal and external risks to personal information held by SANRAL;

3.5.3.2. Establish and maintain appropriate safeguards against the risks identified above;

3.5.3.3. Regularly review these measures to ensure that they are implemented effectively; and

3.5.3.4. Ensure that these safeguards are consistently reviewed and updated where necessary to keep up to date with the ever-evolving risks associated with the storage and processing of personal information.

3.7.3. SANRAL staff, contractors, third parties are expected to populate and maintain the Identification of Information collected and processed by SANRAL referenced in Table1

3.8 Notifiable Data Breaches

3.8.1. SANRAL recognises the legislative requirements of the reporting of any breaches of personal data / information. As part of storing personal data / information, SANRAL accommodates data security within its ICT framework.

3.8.2. SANRAL will use its resources to the best of its capabilities to prevent any personal information stored in its database(s) being passed to unsolicited third parties. Unfortunately, SANRAL cannot provide a 100% guarantee that personal / sensitive information stored will not be obtained by unsolicited third parties. Examples of data breaches may include (but not limited to)

3.8.2.1. Hacking of a database(s) where contractor or employee sensitive data is stored;

3.8.2.2. Disgruntled employees that have access to such information disclosing information to unsolicited parties;

3.8.2.3. Fake email communications directing payment to an incorrect bank account;

3.8.2.4. Disclosure of login details and passwords to other people; or

3.8.2.5. Printed or soft copy information not being handled, stored or discarded correctly (e.g. resumes and other information dropped in a normal paper waste bin rather being shredded).

3.8.3. In cases where SANRAL has evidence that personal information has been obtained by unsolicited parties, SANRAL will:

3.8.3.1. identify the cause of the breach;

3.8.3.2. limit any further effects of any breach;

3.8.3.3. remedy the breach;

3.8.3.4. inform affected individuals;

3.8.3.5. report any breaches to any relevant statutory authorities as required; and

3.8.3.6. ensure SANRAL enacts any further processes depending on the nature of the breach.

3.8.3.7. Section 2.4 deals with any non-compliance with this policy. SANRAL takes compliance with this policy seriously. Failure to comply puts both data subject and the organisation at risk and will lead to disciplinary action which may result in dismissal.

3.9 Education and Awareness

3.9.1. SANRAL will incorporate the Privacy Policy into its induction pack, provide privacy training to staff dealing with personal data / information, and communicate privacy principles to all staff using awareness programs.

3.10 Privacy Inquiries

3.10.1. Stakeholders may contact the Executive responsible for Information Technology if they wish to:

3.10.1.1. request access to, find out more about or seek amendment of personal data / information held by SANRAL;

3.10.1.2. Such requests for access shall be considered under applicable laws and regulations governing private information such as those referenced under 3.11 and 3.12;

3.10.1.3. inquire generally about privacy rights and obligations;

3.10.1.4. provide suggestions or feedback in respect of SANRAL's handling of personal information; or

3.10.1.5. make a complaint in relation to SANRAL handling of personal information.

3.11 Associated Policies

Reference	Policy
4046032	Information Classification and Handling Policy
4046131	Internal Privacy Policy
2754930	Information Technology Governance Framework
4349160	Global Information Security Policy
5391220	HRP024 - Employee Information Privacy Policy

3.12 Legislative Framework

Policy
The **Protection** of Personal Information **Act** 4 of 2013 ("POPIA")
The **Promotion of Access to Information** Act, 2000
The **General Data Protection Regulation** (EU) 2016/679 (**GDPR**) *widely used as internal best practice and compliance for information stored in the EU

Table 1: Identification of Information collected and processed by SANRAL

Identification of Information collected and processed by SANRAL and Staff, Contractors and Third Parties								
Data collected by Third Party	**Type of information collected. (Sensitive, confidential, Public etc)**	**Reason for data collection?**	**Where do we store this information?**	**Contractual agreement in place?**	**Do you send this data to any other parties?**	**Reason for sending the data to another party**	**Name the parties to which you send the data**	**Updated by**