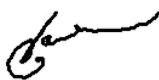



---

**Privacy Policy**


---

# Privacy Policy

Document Classification	Confidential	<input type="checkbox"/>
	Internal	<input checked="" type="checkbox"/>
	Public	<input type="checkbox"/>
Prepared by: Consultant: iOCO	Reviewed by: D Claassen	Approved by: EXCO
Date: 2021/09/10	Date: 2021/09/10	Date: 2021/10/29
N/A		



---

## Privacy Policy

---

### Table of Contents

---

<b>CHANGE CONTROL TABLE .....</b>	<b>3</b>
<b>DOCUMENT STATUS .....</b>	<b>3</b>
<b>VERSIONS.....</b>	<b>3</b>
<b>DISTRIBUTION LIST .....</b>	<b>4</b>
<b>1. DEFINITIONS .....</b>	<b>5</b>
<b>2. INTRODUCTION .....</b>	<b>6</b>
<b>3. PURPOSE .....</b>	<b>6</b>
<b>4. SCOPE .....</b>	<b>6</b>
<b>5. RESPONSIBILITY .....</b>	<b>7</b>
<b>6. ETC POPIA COMPANY AND DATA PROCESSOR OBLIGATION .....</b>	<b>8</b>
<b>7. POLICY .....</b>	<b>8</b>
<b>8. POLICY BREACH .....</b>	<b>12</b>
<b>9. EXCEPTIONS AND VARIATIONS.....</b>	<b>13</b>
<b>10. REFERENCES .....</b>	<b>13</b>
<b>11. RECORDS.....</b>	<b>13</b>

## Privacy Policy

### CHANGE CONTROL TABLE

No.	Revision	Status	Date	Author	Description of the change
1.	00.01	Released	2021/05/27	D Claassen	New
2.	01.00	Released	2021/09/10	D Claassen	Reviewed
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

### DOCUMENT STATUS

No.	Status	Definition / Description
1.	New	New Document
2.	Reviewed	Document reviewed by author and management.
3.	Released	Document checked and released by the Quality Department. This document can only be modified if the version number is updated

### VERSIONS

No.	Versions take place in two stages. Accepted documents receive the next higher integral version number.	
1.	00.01, 00.02 etc.	Not released versions, with the status "processed".
2.	01.00	First released version with the status "released".
3.	01.01, 01.02 etc.	Versions which supplement the version 01.00 and are "processed".
4.	02.00	Second released versions with the status "released".



---

**Privacy Policy**

---

**DISTRIBUTION LIST**

No.	Company	Name & Surname
1.	ETC	ETC EXCO
2.	ETC	All Employees
3.	ER	Employer's Representative
4.		
5.		
6.		
7.		
8.		
9.		
10.		

## Privacy Policy

### 1. DEFINITIONS

<b>Company</b>	Refers to Electronic Toll Collection (Pty) Ltd. (ETC)
<b>Confidential</b>	Information which is confidential by law, marked as confidential, both proprietary and personal in line with Personal Information as defined in the POPIA Act.
<b>CRO</b>	Chief Risk Officer
<b>CV</b>	Curriculum Vitae
<b>Data Protection Laws</b>	Means all applicable law relating to data protection, privacy and security when processing Personal Information under the Agreement. This includes without limitation applicable international and local data protection, privacy, export or data security directives including the Electronic Communications and Transactions Act 25 of 2002, Protection of Personal Information Act 4 of 2013 and the General Data Protection Regulation.
<b>DPIA</b>	Data Protection Impact Assessment
<b>Employee</b>	Any person appointed on a company contract of employment, excluding independent contractors and persons employed by temporary employment services.
<b>EXCO</b>	Executive Committee
<b>GDPR</b>	General Data Protection Regulation
<b>GORT</b>	Gauteng Open Road Tolling
<b>IO</b>	Information Officer
<b>IR</b>	Information Regulator
<b>Internal</b>	Information marked as internal not approved for general circulation outside the Company. Disclosure of such data to anyone outside of the Company requires management authorisation.
<b>Personal Information</b>	Personal data is any data recorded electronically or in hard copy, that if viewed on its own, or collectively with other data, can be used to uniquely identify an individual or a legal entity in line with Personal Information as defined in the POPIA Act
<b>POPIA</b>	Protection of Personal Information Act
<b>Processing</b>	means any operation, or set of operations, performed on Data, by any means, such as by collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction and "Processing" shall have a corresponding meaning.
<b>Public</b>	Data or information that does not fall under any other classification levels and may be broadly distributed without causing damage to the Company, its employees and stakeholders.
<b>RU</b>	Road user
<b>SANRAL</b>	South African National Roads Agency Limited

---

## Privacy Policy

---

### 2. INTRODUCTION

- 2.1. Data protection and privacy through lawful, legitimate and responsible processing and use of personal data is a fundamental human right under the Constitution. This Company Data Privacy Policy (this Policy) outlines the core principals which the Company endeavours to pursue in relation to the processing of personal data. The Principals set out in this Policy ensure that personal data is processed in line with regulatory requirements, industry-wide best practices and our code of conduct. The Protection of Personal Information Act (POPI Act or POPIA) and the General Data Protection Regulation (GDPR) are the primary pieces of legislation that governs how the Company collects and processes personal data.
- 2.2. Consequences of non-compliance
  - 2.2.1. Wilful and deliberate non-compliance with this policy can expose the Company to significant regulatory sanctions, fines, criminal and/or civil liability. The reputational damage arising from such non-compliance will negatively affect the Company's ability to attract and maintain clients.
  - 2.2.2. Employees who fail to comply with this policy may be subject to disciplinary action as Prescribed by the ETC Disciplinary Policy and Code of Conduct, including dismissal and personal liability such as fines and/ or imprisonment under the relevant laws.

### 3. PURPOSE

- 3.1. The purpose of this Policy is to set out the basic principles relating to the processing of personal information. This Policy sets out how the Company process the personal data of its employees, trading partners, suppliers and other third parties.
- 3.2. In addition to the Processing obligation of the Company in respect of the personal data of its employees, trading partners, suppliers and other third parties, it equally has such obligation in respect of Road User (RU) data in respect of the GORT project.

### 4. SCOPE

- 4.1. This policy applies to the Company, in respect of its employees, trading partners, suppliers and other third parties as data subjects and the processing of personal information in Company context.
- 4.2. The Policy also applies to the contractual role and obligations of the Company as Data Processor in commercial agreements with Responsible Parties.
- 4.3. This policy is intended to assist the management and employees of the Company in assessing the legal position applicable to a particular decision, behaviour, conduct, act, or omission.
- 4.4. The Privacy undertaking by the Company towards Registered Road Users is contained in a Privacy Statement on the E-toll Website.

---

## Privacy Policy

---

- 4.5. The collection of unpaid toll fees by the Company is contractually and Legislatively prescribed and various privacy rights of data subjects contained in POPIA opposes the methodology followed for the collection of unpaid toll fees in the GORT context.
- 4.6. To this end the Company has pursued an exemption application for the Information Regulators of certain POPIA prescripts to enable the unhindered collection of unpaid toll debt.

## 5. RESPONSIBILITY

### 5.1. Governance and implementation

- 5.1.1. This policy must be approved by the Company's Executive Committee (EXCO).
- 5.1.2. This policy must be reviewed every two years or when a significant event occurs, taking into account any changes to regulatory requirements and business operations. The review should include assessing opportunities for improvement of all Company policies and approach to managing information security in response to changes to the organisational environment, business circumstances, legal conditions or technical environment.
- 5.1.3. The Information Officer is responsible for the successful implementation of the provisions of this policy.

### 5.2. Roles and responsibilities

Assigning roles and responsibilities are necessary to give effect to the requirements of this policy

#### 5.2.1. Policy Owner

- The Company Policy Owner and Custodian will be the Information Officer and is ultimately accountable for ensuring that the Company and its employees comply with the requirements set out in this process.
- The Policy Custodian is responsible for overseeing all dispensations, waivers and breaches to this process.
- The Policy Custodian is responsible for facilitating the review(s) as set out in the policies or standards.

#### 5.2.2. Board of Directors and the Executive Committee

- The Company Board of Directors and the Executive Committee are ultimately accountable for ensuring that the Company and its employees comply with the requirements set out in this policy; and
- In addition, the EXCO must ensure that The Company complies with all applicable laws, regulations and supervisory requirements.

#### 5.2.3. Business / Function Head

The business or function head is responsible for the following:

- Ensuring this policy is effectively implemented within their business.

---

## Privacy Policy

---

- The Business Head may delegate their responsibility (but not accountability) for implementation of this policy to an appropriate executive within the business.

### 5.2.4. Employees

- All employees within the Company are responsible for complying with this policy.

## 6. ETC POPIA COMPANY AND DATA PROCESSOR OBLIGATION

- 6.1. As recorded under the Scope of the Policy, it applies in respect of the contractual interaction and obligations of contractual commercial projects in which the Company is or may become involved, as well as in respect ETC as a Company its employees, trading partners, suppliers and other third parties as data subjects and the processing of personal information in Company context.
- 6.2. In the context of the contractual commercial agreements where the Company performs the role of Data Processor and applying the POPIA constructs, the instructing party would be the Responsible Party, which determines the purpose and the means for processing personal information.
- 6.3. The Company is the Data Processor, *inter alia* responsible for processing Personal Data in terms of a contract or specific arrangement with the Responsible Party .
- 6.4. The core principles of the Policy apply equally to the Company in its role as Data Processor and to other entities in its role/s as Responsible Party.
- 6.5. The definition of the Data Processor and Responsible party changes depending on the role played by different parties.
- 6.6. In its role as employer, the Company remains the Data Processor of the Personal Data of its employees and subject to the POPIA prescripts
- 6.7. In its contractual relationship with trading partners, suppliers and other third parties where the Company shares Personal Data, the Company may become the Responsible Party to data sub-processors.

## 7. POLICY

### 7.1. Processing of Data

The Company's core principles are based the provisions of POPI and GDPR must ensure that all personal data is:

- 7.1.1. processed lawfully, fairly and in a transparent manner;
- 7.1.2. collected only for specified, clear and legitimate purposes;
- 7.1.3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed;
- 7.1.4. accurate and kept up to date where applicable;
- 7.1.5. not kept in a format which allows identification of a data subject for longer than is necessary for the purposes for which the data is processed;



---

## Privacy Policy

---

- 7.1.6. processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Additionally, the Company must ensure that:
  - 7.1.7. Personal information is not transferred to another country without appropriate safeguards being in place; and
  - 7.1.8. The Company allows people to exercise their rights in relation to their personal data. The Company is responsible for and must be able to demonstrate compliance with all of the above principles.
- 7.2. Lawfulness, Fairness and Transparency
- When collecting and processing personal information for any specific purpose, the Company must always have a lawful basis for doing so. Processing personal information is lawful when at least one of the following circumstances is present:
- 7.2.1. the data subject has given their consent for one or more specific purposes;
  - 7.2.2. the processing is necessary for the performance of a contract to which the data subject is a party;
  - 7.2.3. to comply with Company legal obligations;
  - 7.2.4. to protect the vital interests of the data subject or another person; or
  - 7.2.5. to pursue the Company's legitimate interests where those interests are not outweighed by the interests and rights of the person. The Company must document the above lawful reasons relied upon when processing personal information for each specific purpose.
- 7.3. Consent as a lawful basis for processing
- Consent may not always be the only basis for being able to process data. This will depend on the specified circumstance or scenario. A person's consent must be
- 7.3.1. specific;
  - 7.3.2. informed (explained in plain and accessible language);
  - 7.3.3. unambiguous;
  - 7.3.4. separate and unbundled from any other terms and conditions provided to the data subject;
  - 7.3.5. freely and genuinely given.
- 7.4. Openness
- 7.4.1. A person must be able to withdraw their consent without reservation. Once consent has been given, it will need to be updated where the Company wishes to process the personal data for a new purpose that is not compatible with the original purpose for which they were collected.
  - 7.4.2. Chapter 6 of POPIA and Chapter 3 Section 1 of GDPR requires the Company to ensure that any information provided by the Company to people about how their personal data will be processed is concise, easily accessible, easy to understand and written in plain language. (Privacy Notice).



---

## Privacy Policy

---

- 7.4.3. The Company must demonstrate transparency by providing people with the appropriate Privacy Notices before it collects and processes their personal information and at the appropriate times throughout the processing of their personal information.
- 7.4.4. Where the Company obtains any personal information about a person from a third party (for example, CVs from recruitment or background criminal checks in relation to employee on-boarding) it must check that it was collected by the third party in accordance with this policy's requirements that the sharing of such personal information with the Company was clearly explained to the person.
- 7.5. Data Minimisation
- 7.5.1. The personal information that the Company collects and processes must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.
- 7.5.2. Personal information must only be processed when necessary for the performance of duties and tasks and not for any other purposes.
- 7.5.3. Accessing of personal information where there is no authorisation to do so, or where there is no reason to access, may result in disciplinary action and in certain circumstances, may constitute a criminal offence.
- 7.5.4. When collecting personal information, as required for the performance of duties and tasks, there should not be a request that a person provides more personal information than is strictly necessary for the intended purposes.
- 7.5.5. Where personal information is no longer needed for the specific purposes for which it was collected, such information must be deleted, destroyed and/or anonymised.
- 7.6. Accuracy
- 7.6.1. Personal information that the Company collects and processes must be:
- 7.6.1.1. accurate and, where required and kept up-to-date; and
- 7.6.1.2. corrected and/or deleted, without delay, where an error has been discovered.
- 7.6.2. Where appropriate, any inaccurate or expired records should be deleted or destroyed.
- 7.7. Storage Limitation
- 7.7.1. Unless the Company is contractually or legally obliged to retain personal information must be collected and kept in accordance with the prescripts below:
- 7.7.1.1. The personal information that the Company collects and processes must not be kept in a form that identifies a person for longer than what is necessary in relation to the purposes for which it was collected (this is subject to compliance with any legal, accounting or reporting requirements).

---

## Privacy Policy

---

- 7.7.1.2. Reviews must be conducted of any personal information which has been processed in the performance of duties to assess whether the purposes for which the information was collected has expired.
- 7.7.1.3. If no longer required, reasonable steps must be taken to delete or destroy any personal data that the Company no longer requires.
- 7.7.1.4. All privacy notices and fair processing notices must inform data subjects of the period for which their personal data will be stored or how such period will be determined.

### 7.8. Security of Personal Information

- 7.8.1. The personal information that the Company collects and processes must be secured by appropriate technical and organisational measures against accidental loss, destruction or damage, and against unauthorised or unlawful processing.
- 7.8.2. The Company has developed, implemented and is maintaining appropriate technical and organisational measures for the processing of personal information taking into account the:
  - 7.8.2.1. nature, scope, context and purposes for such processing; and
  - 7.8.2.2. the volume of personal data processed, likelihood and severity of the risks of such processing for the rights of persons.
- 7.8.3. The Company must annually evaluate and test the effectiveness of such measures to ensure that they are adequate and effective. There is a responsibility for ensuring the security of personal information processed throughout the performance of duties.
- 7.8.4. All procedures that The Company have put in place to maintain the security of personal information from collection to destruction must be observed and adhered to.
- 7.8.5. Confidentiality, integrity and availability of personal information must be maintained at all times:
  - 7.8.5.1. Confidentiality means that only people who need to know and are authorised to process any personal information can access it;
  - 7.8.5.2. Integrity means that personal information must be accurate and suitable for the intended purposes;
  - 7.8.5.3. Availability means that those who need to access the personal information for authorised purposes are able to do so.
- 7.8.6. Sharing personal information with third parties is prohibited unless:
  - 7.8.6.1. The Company is legislatively compelled to share such information; and
  - 7.8.6.2. there has been an issuance to the respective person, of a privacy notice, beforehand and where such third party is processing the personal information on the Company's behalf.

### 7.9. Persons' Rights

---

## Privacy Policy

---

- 7.9.1. Chapter 3(5) of POPIA and Chapter 3 of GDPR provides people with a number of rights in relation to their information. These rights include:
- 7.9.1.1. the right to withdraw consent unconditionally;
  - 7.9.1.2. the right to be informed about how the Company collects and processes personal information;
  - 7.9.1.3. the right to receive a copy of the personal information that the Company holds;
  - 7.9.1.4. the right to have inaccurate personal data corrected or incomplete information completed;
  - 7.9.1.5. the right to ask the Company to delete or destroy personal data if the personal data is no longer necessary in relation to the purposes for which it was collected, consent has been withdrawn (where applicable), a person has objected to the processing, the processing was unlawful, the personal information has to be deleted to comply with a legal obligation and/or the personal information was collected from a person under the age of 13 and they have reached the age of 13;
  - 7.9.1.6. the right to restrict processing if there is a reasonable belief that the personal data is inaccurate;
  - 7.9.1.7. the right to receive or ask the Company to transfer personal information to a third party;
  - 7.9.1.8. The right to be notified of a personal data breach; and
  - 7.9.1.9. The right to make a complaint to the CRO or another appropriate supervisory authority.

### 7.10. Data Protection

- 7.10.1. A Data Protection Impact Assessment (DPIA), also known as a Privacy Impact Assessment, is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data. DPIAs are required for processing personal information likely to result in a high risk to the individuals and where new technologies are involved. In practice, the Company requires a DPIA for any projects involving the use of personal data, including new systems, solutions and some research studies. A DPIA must:
- 7.10.1.1. describe the nature, scope, context and purposes of the processing;
  - 7.10.1.2. assess necessity, proportionality and compliance measures;
  - 7.10.1.3. identify and assess risks to individuals; and
  - 7.10.1.4. identify any additional measures to mitigate those risks.

## 8. POLICY BREACH

Employees are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the Information Officer (IO), or nominated member of employees. If

---

## Privacy Policy

---

any breach of this Policy is observed, disciplinary action may be instituted in accordance with ETC's disciplinary procedures.

### 9. EXCEPTIONS AND VARIATIONS

Requests for exceptions to this policy or any sub-policies must be authorised by the IO, or a delegated official. Such requests must be made in writing and must be evaluated based on the case presented to support the specific department.

### 10. REFERENCES

Document Number	Document Description
382-QAS-13-STD-903188	Data Classification Standard
382-QAS-01-PRC-900654	Control of QMS Documents and Records

### 11. RECORDS

Document Number	Document Description
N/A	

All records pertaining to this policy should be retained in accordance with the Company's internal record retention policy.