SELFTRACK

COMPLIANCE MANUAL

FOR THE IMPLEMENTATION OF THE

PROTECTION OF PERSONAL INFORMATION ACT

"POPI"

CONTENTS:

A. INTRODUCTION

The Protection of Personal Information Act (***POPI***) is intended to balance two competing interests. These interests are:

1. Our individual constitutional rights to privacy (which requires our personal information to be protected); and
2. The needs of our society to have access to and to process (work with) our personal information for legitimate purposes, including the purpose of doing business.

This Compliance Manual sets out the framework for Selftrack's compliance with ***POPI***.

Where reference is made to the "processing" of personal information, this will include any activity in which the information is worked with, from the time that the information is collected, up to the time that the information is destroyed, regardless of whether the information is worked with manually, or by automated systems.

B. OUR UNDERTAKINGS TO OUR CUSTOMERS:

1. We undertake to follow ***POPI*** at all relevant times and to process personal information lawfully and reasonably, so as not to infringe unnecessarily on the privacy of our customers.
2. We undertake to process information only for the purpose for which it is intended, to enable us to do our work, as agreed with our customers.
3. We undertake to strictly follow our ***Privacy Policy***, attached hereto marked ***Annexure "A"***, that fully governs the way Selftrack treats and deals with personal information. This Annexure must be read as if specifically incorporated herein.

C. OUR CUSTOMERS' RIGHTS

1. In cases where the customer's consent is required to process their personal information, this consent may be withdrawn.

2. In cases where we process personal information without consent to protect a legitimate interest, to comply with the law or to pursue or protect our legitimate interests, the customer has the right to object to such processing.

3. All customers are entitled to lodge a complaint regarding our application of POPI with the Information Regulator.

D. SECURITY SAFEGUARDS

1. In order to secure the integrity and confidentiality of the personal information in our possession, and to protect it against loss or damage or unauthorised access, we must continue to implement the following security safeguards:

    1.1 Our business premises where records are kept must remain protected by access control, burglar alarms and armed response.

    1.2 Archived files must be securely stored and access to these files need to be restricted and controlled.

    1.3 All the user terminals on our internal computer network and our servers must continue to be protected by passwords.

    1.4 Our email infrastructure must comply with industry standard security safeguards and meet the General Data Protection Regulation (GDPR).

    1.5 Vulnerability assessments must be carried out on our digital infrastructure at least on an annual basis to identify weaknesses in our systems and to ensure we have adequate security in place.

    1.6 We must use an internationally recognised Firewall to protect the data on our local servers, and we must run antivirus protection at least daily to ensure our systems are kept updated with the latest patches.

    1.7 Our staff must be fully acquainted with this ***POPI*** Compliance Manual and thus trained to carry out their duties in compliance with ***POPI***, and this training must be ongoing.

    1.8 It must be a term of the contract with every staff member that they must maintain full confidentiality in respect of all of our customers affairs, including our customers personal information.

1.9 Employment contracts for staff whose duty it is to process a customer's personal information, must include an obligation on the staff member (1) to maintain the Company's security measures, and (2) to notify their manager/supervisor immediately if there are reasonable grounds to believe that the personal information of a customer has been accessed or acquired by any unauthorised person. Such a clause/addendum shall be provided and entered into where relevant with each respective employee.

1.10 The processing of the personal information of our staff members must take place in accordance with the rules contained in the relevant labour legislation.

1.11 The digital work profiles and privileges of staff who have left our employ must be properly terminated.

1.12 The personal information of customers and staff must be destroyed timeously in a manner that de-identifies the person.

2. These security safeguards must be verified on a regular basis to ensure effective implementation, and these safeguards must be continually updated in response to new risks or deficiencies.

E. SECURITY BREACHES

1. Should it appear that the personal information of a customer has been accessed or acquired by an unauthorised person, we must notify the Information Regulator and the relevant customer/s, unless we are no longer able to identify the customer/s. This notification must take place as soon as reasonably possible.

2. Such notification must be given to the Information Regulator first as it is possible that they, or another public body, might require the notification to the customer/s be delayed.

3. The notification to the customer must be communicated in writing in one of the following ways, with a view to ensuring that the notification reaches the customer:

3.1 by mail to the customer's last known physical or postal address;

3.2 by email to the customer's last known email address;

3.3 by publication on our website or in the news media; or

3.4 as directed by the Information Regulator.

4 This notification to the customer must give sufficient information to enable the customer to protect themselves against the potential consequences of the security breach, and must include:

4.1 a description of the possible consequences of the breach;

4.2 details of the measures that we intend to take or have taken to address the breach;

4.3 the recommendation of what the customer could do to mitigate the adverse effects of the breach; and

4.4 if known, the identity of the person who may have accessed, or acquired the personal information.

F. RECORDS REQUESTED BY CUSTOMERS

1. On production of proof of identity, any person is entitled to request that we confirm, free of charge, whether or not we hold any personal information about that person in our records.

2. If we hold such personal information, on request, and upon payment of a fee of R500-00 plus VAT, we shall provide the person with the record, or a description of the personal information, including information about the identity of all third parties or categories of third parties who have or have had access to the information. We shall do this within a reasonable period of time, in a reasonable manner and in an understandable format.

3. A customer requesting such personal information must be advised of their right to request to have any errors in the personal information corrected, which request shall be made on the prescribed application form. See the required *FORM 2* attached hereto marked ***Annexure "B"***.

4. In certain circumstances, we will be obliged to refuse to disclose the record containing the personal information to the customer. In other circumstances, we will have discretion as to whether or not to do so.

5. In all cases where the disclosure of a record will entail the disclosure of information that is additional to the personal information of the person requesting the record, the written consent of the Information Officer (or his/her delegate) will be required, and that person shall make their decision having regard to the provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act.

6. If a request for personal information is made and part of the requested information may, or must be refused, every other part must still be disclosed.

G. THE CORRECTION OF PERSONAL INFORMATION

1. A customer is entitled to require us to correct or delete personal information that we have, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.

2. A customer is also entitled to require us to destroy or delete records of personal information about the customer that we are no longer authorised to retain.

3. Any such request must be made on the prescribed form, *FORM 2*, attached hereto marked ***Annexure "B"***.

4. Upon receipt of such a lawful request, we must comply as soon as reasonably practicable.

5. If a dispute arises regarding the customer's rights to have information corrected, and if the customer so requires, we must attach to the information, in a way that it will always be read with the information, an indication that the correction of the information has been requested but has not been made.

6. We must notify the customer who has made a request for their personal information to be corrected or deleted what action we have taken because of such a request.

H. SPECIAL PERSONAL INFORMATION

1. Special rules apply to the collection and use of information relating to a person's religious or philosophical beliefs, their race or ethnic origin, their trade union membership, their political persuasion, their health or sex life, their biometric information, or their criminal behaviour.

2. We shall not process any of this Special Personal Information without the customer's consent, or where this is necessary for the establishment, exercise, or defense of a right or an obligation in law.

3. Having regard to the nature of our work, it is unlikely that we will ever have to process special personal information, but should it be necessary the guidance of the Information Officer, or their deputy/delegate, must be sought.

I. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

1. We may only process the personal information of a child if we have the consent of the child's parent or legal guardian.

J. INFORMATION OFFICER

1. Our Information Officer is *Erica Masher*, who is our Group Company Secretary and Human Capital Manager, nominated and authorised by our Managing Director in writing. Such authorisation shall be made on the required *FORM*, attached hereto marked ***Annexure "C"***. Our Information Officer's responsibilities include:

    1.1 Ensuring compliance with POPI.

    1.2 Dealing with requests which we receive in terms of POPI.

    1.3 Working with the Information Regulator in relation to investigations.

2. Our Information Officer must designate in writing as many Deputy Information Officers as are necessary to perform the tasks mentioned in

paragraph 1 above. Such designation shall be done by the completion of the prescribed *FORM*, a copy of which is attached hereto marked ***Annexure "D"***.

3. Our Information Officer and our Deputy Information Officers must register themselves with the Information Regulator prior to taking up their duties, see the required *FORMS* attached hereto marked ***Annexure "E"***.

4. In carrying out their duties, our Information Officer must ensure that:

   4.1 this Compliance Manual is implemented;

   4.2 a Personal Information Impact Assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

   4.3 that this Compliance Manual is developed, monitored, maintained, and made available;

   4.4 that internal measures are developed together with adequate systems to process requests for information or access to information;

   4.5 that internal awareness sessions are conducted regarding the provisions of ***POPI***, the Regulations, codes of conduct or information obtained from the Information Regulator; and

   4.6 that copies of this manual are provided to persons at their request, hard copies to be provided upon payment of a fee (as determined by the Information Regulator).

5. Guidance notes on Information Officers have been published by the Information Regulator (on 1 April 2021) and our Information Officer and deputy Information Officers, if and when appointed, must familiarize themselves with the content of these notes.

K. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION

1. In the following circumstances, we will require prior authorisation from the Information Regulator before processing any personal information:

   1.1 In the event that we intend to utilise any unique identifiers of customers (account numbers, file numbers or other numbers or codes

allocated to customers for the purposes of identifying them in our business) for any purpose other than the original intention, or to link the information with information held by others;

1.2 if we are processing information on criminal behaviour or unlawful or objectionable conduct;

1.3 if we are processing information for the purposes of credit reporting (this will be, for example, if reports are made to ITC or TPN).

1.4 if we are transferring special personal information or the personal information of children to a third party in a foreign country, that does not provide adequate protection of that personal information.

2. The Information Regulator must be notified of our intention to process any personal information as set out in paragraph 1 above prior to any processing taking place and we may not commence with such processing until the Information Regulator has decided in our favour. The Information Regulator has 4 weeks to make a decision but may decide that a more detailed investigation is required. In this event the decision must be made in a period as indicated by the Information Regulator, which must not exceed 13 weeks. If the Information Regulator does not make a decision within the stipulated time periods, we can assume that the decision is in our favour and commence processing the information.

L. DIRECT MARKETING

1. We may only carry out direct marketing (using any form of electronic communication) to customers if:

1.1 they were given an opportunity to object to receiving direct marketing material by electronic communication at the time of signing up/on as a customer of Selftrack (refer to Selftrack's Privacy Policy); and

1.2 they did not object then or at any time after receiving any such direct marketing communications from us.

2. We may only approach customers using their personal information, if we have obtained their personal information in the context of providing services associated with Selftrack (Pty) Ltd.

3. We may only carry out direct marketing (using any form of electronic communication) to other people (not a Selftrack customer) if we have received their consent to do so. The prescribed *FORM 4* is attached hereto marked **Annexure "F"**.

4. We may approach a person to ask for their consent to receive direct marketing material only once, and we may not do so if they have previously refused their consent.

5. All direct marketing communications must disclose our identity and contain an address or other contact details to which the customer may send a request that the communications cease.

M. TRANSBORDER INFORMATION FLOWS

1. We may not transfer a customer's personal information to a third party in a foreign country, unless:

   1.1 the customer consents to this, or requests it; or

   1.2 such third party is subject to a law, binding corporate rules or a binding agreement which protects the personal information in a manner like POPI, and such third party is governed by similar rules which prohibit the onward transfer of the personal information to a third party in another country; or

   1.3 the transfer of the personal information is required for the performance of the contract between us and the customer; or

   1.4 the transfer is necessary for the conclusion or performance of a contract for the benefit of the customer entered into between us and the third party; or

   1.5 the transfer of the personal information is for the benefit of the customer, and it is not reasonably possible to obtain their consent and that if it were possible the customer would be likely to give such consent.

N. OFFENCES AND PENALTIES

1. ***POPI*** provides for serious penalties for the contravention of its terms. For minor offences, a guilty party can receive a fine or be imprisoned for up to 12 months. For serious offences, the period of imprisonment rises to a maximum of 10 years. Administrative fines for the company can reach a maximum of R10 million.

2. Breaches of this Compliance Manual will be viewed as a serious disciplinary offence.

3. It is therefore imperative that we comply strictly with the terms of this Compliance Manual and protect our customer's personal information in the same way as if it were our own.

O. SCHEDULE OF ANNEXURES AND FORMS

1. ANNEXURE "A" – Selftrack's Privacy Policy
2. ANNEXURE "B" – Request for Correction
3. ANNEXURE "C" – Authorisation of Information Officer
4. ANNEXURE "D" – Designation of Deputy Information Officers
5. ANNEXURE "E" – Information Officer Registration Form
6. ANNEXURE "F" – Consent for non-Customers

ANNEXURE "A"

SELFTRACK

PRIVACY POLICY

1. INTRODUCTION

1.1. This Privacy Policy governs the manner in which Selftrack (Pty) Ltd, ("Selftrack") treats your personal information collected:

- electronically;
- telephonically;
- when you make use of our website;
- when you apply for and use certain services; and
- from the mobile tracking device in your vehicle, if applicable.

1.2. By submitting your details and/or by using the Selftrack website and/or services we provide and/or by allowing a Selftrack unit to be installed in your vehicle, you accept the terms and conditions of this Privacy Policy and explicitly consent to the collection, use and disclosure of your Personal Information in the manner set out below. If you do not agree with the provisions of this Privacy Policy, or are concerned about any aspect relating to the protection of your Personal Information, please do not continue to use the website and/or allow the mobile tracking device to be installed in your vehicle and/or apply for or use the Selftrack services.

1.3. The Privacy Policy must be read together with Selftrack's terms and conditions of service. To view Selftrack's terms and conditions of service, please visit www.selftrack.co.za. Unless defined elsewhere, terms in this Privacy Policy shall bear the meaning ascribed to them in our terms and conditions of service.

1.4. We respect your privacy and your personal information and for this reason, we take all reasonable measures in accordance with this Privacy Policy, the Protection of Personal Information Act 4 of 2013 ("POPIA") and other relevant legislation, to protect your personal information and to keep it confidential, even when you are no longer our customer.

1.5. This Privacy Policy complies with the principles outlined in POPIA and describes how we handle Personal Information, as defined therein, that we collect from you, from your use of our services, from the mobile tracking device in your vehicle (if applicable), from your use of our website or from third parties involved in our business dealings with you. You agree that we may collect, collate, process and/or store your Personal Information, as defined in POPIA, ("process") for the Purpose as set out in clause 4 below.

1.6. When there are reasonable grounds to believe that your Personal Information has been accessed or acquired by an unauthorised person, we will notify you and the relevant Regulator, unless a public body responsible for detection, prevention or investigation of offences, or the relevant Regulator, informs us that notifying you will impede a criminal investigation, or if there is another legal ground not to inform you. When we notify you that your Personal Information has been accessed or acquired by an unauthorised person, we will provide you with sufficient information to allow you to take protective measures against the potential consequences of the compromise.

2. DEFINITION OF PERSONAL INFORMATION?

2.1. "*Personal information*" as defined in Section 1 of POPIA, means information relating to an identifiable, living, natural person and where it is applicable, an identifiable juristic person, including but not limited to:

2.1.1. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of a person;

2.1.2. any information relating to an identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to a person;

2.1.3. information relating to the education or the medical, financial, criminal or employment history of a person;

2.1.4. the blood type or any other biometric information of a person;

2.1.5. personal opinions, views or preferences of a person;

2.1.6. the views or opinions of another individual about the person;

2.1.7. the name of a 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,

2.1.8. 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; and

2.1.9. 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.

3. COLLECTION OF YOUR PERSONAL INFORMATION

3.1. Whenever you complete an application form, contact us electronically or telephonically, apply for or use the services provided by us, or use our website, we collect your Personal Information.

4. USE OF YOUR PERSONAL INFORMATION

4.1. You agree that we may use the information, including the Personal Information we hold about you, in the following ways:

4.1.1. to identify you;

4.1.2. in order for us to process your instructions or requests;

4.1.3. in order for us to ensure that we provide you with the best possible service at all times;

4.1.4. to collect and analyse your personal information and combine all the information that we have about you to compile a profile of you in order for us to personalise and tailor our services to meet your specific needs;

4.1.5. in aggregate form for purposes of generating statistics and developing strategic and marketing plans;

4.1.6. to allow you to participate in interactive features of our services, when you choose to do so;

4.1.7. to carry out any contracts that may exist between us;

4.1.8. to notify you about changes to our services or introduce you to new services;

4.1.9. once we have collected and analysed your Personal Information, inform you thereof telephonically or send you promotional material or details which we think may be of interest to you. If any of this promotional information relates to products, promotions, news or services of an affiliate party (which may include our business partners and sub-contractors) ("affiliate"), and only if you

indicate that you would like more information, we may inform the affiliate party to contact you directly. You have the option to opt out of receiving any marketing or other material from us or an affiliate at any stage; and

4.1.10. to share certain of your personal (and non-personal) information (such as make and model of your vehicle, frequently travelled areas, traffic information, theft and hi-jacking statistics) with an affiliate.

5. DISCLOSURE OF YOUR PERSONAL INFORMATION

5.1. We will not sell, rent or provide your Personal Information to unauthorised entities or any other third parties (other than as provided herein) for their independent use, without your express consent. If at any stage, after you have given us your consent, you no longer wish for us to use or share your Personal Information with an affiliate, you may withdraw your consent however, your Personal Information may also be shared under the following circumstances:

5.1.1. when required by the laws of the Republic of South Africa and in the public interest. In such instances, we reserve the right to disclose your Personal Information as required in order to comply with our legal obligations or duty, including but not limited to complying with court orders, warrants, subpoenas, service of process requirements, discovery requests or lawful criminal investigations;

5.1.2. under special circumstances where we have reason to believe that such disclosure is necessary to identify, contact or bring legal action against a party who may be breaching our website terms and conditions or may be causing injury to or interference with (either intentionally or unintentionally) our rights or property, other users, or anyone else that could be harmed by such activities.

6. WHO WE COLLECT PERSONAL INFORMATION FROM

6.1. Personal information will be collected directly from you, or our affiliates, except if:

6.1.1. the information is contained in a public record or has deliberately been made public by you;

6.1.2. you have consented to the collection of the information from another source or in accordance with the Selftrack terms and conditions of service;

6.1.3. collection of the information from another source would not prejudice a legitimate interest you may have;

6.1.4. collection of the information from another source is necessary –

- to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
- to enforce a law imposing a pecuniary penalty;
- to enforce legislation concerning the collection of revenue as defined in relevant local legislation;
- for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
- in the legitimate interests of national security.

7. PERSONAL INFORMATION THAT WE COLLECT

7.1. Personal Information collected about you and your dependants or our employees may include:

7.1.1. General identification and contact information:
Your name, address, e-mail address, telephone number, gender, marital status, family status, date of birth, passwords and activity records (such as driving behaviour and location of your vehicle).

7.1.2. Identification numbers issued by government bodies or agencies:
Identity or passport number, VIN number and Registration number of your vehicle.

7.1.3. Financial information and account details:
Bank account number and account details, credit history, credit score and other financial information.

7.1.4. Medical condition and health status (employees only):
Current or former physical or mental or medical condition, health status, injury or disability information, medical procedures performed, personal habits (for example, smoking or consumption of alcohol, prescription information and medical history).

7.1.5. Other sensitive information:
We may obtain information about your criminal record or civil litigation history in the process of preventing, detecting and investigating fraud or in the employment process. We may also obtain sensitive information if you voluntarily provide it to us (for example, if as an employee you express preferences regarding medical treatment based on your religious beliefs).

7.1.6. Telephone recordings:
Recordings of telephone calls to and from our representatives, affiliates and call centres.

7.1.7 Information to investigate crime, including fraud and money laundering:
We will share information with insurers who are investigating an insurance claim or with the SAPS who are investigating a criminal matter, for example.

7.1.8. Information enabling us to provide products and services:
Location and identification of your vehicle (for example, vehicle coordinates and vehicle registration or VIN number).

8. PROTECTION OF YOUR PERSONAL INFORMATION

8.1. We value the information that you choose to provide us with, and we will take reasonable steps to protect your Personal Information from loss, misuse or unauthorised alteration or access. The information we maintain concerning our customers is stored in databases that have built-in safeguards to ensure the privacy and confidentiality of that information. However, the transmission of information via the internet or electronic mail is not completely secure and we cannot guarantee the security of your information transmitted to our website or via electronic mail. Any transmission of your information to our website or via electronic mail is entirely at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

8.2. When you use the services provided by us, you may be given a username and password. You are responsible for maintaining the secrecy and confidentiality of your username and password. Please do not share your password with anyone.

9. UPDATING OF YOUR PERSONAL INFORMATION

9.1. It is your responsibility to ensure that we have your correct Personal Information on our system. If you ever need to update or correct any of your Personal Information held by us, you can contact Selftrack via email or telephonically.

10. CONSUMER PROTECTION ACT ("CPA") AND POPIA

10.1. We subscribe to the CPA and the principles outlined Section 11, in which you have the right to restrict unwanted marketing, which includes your right to refuse to accept, or

require us to discontinue or to pre-emptively block communication about any marketing from us. Moreover, in terms of POPIA, you have the right to object to the processing of your Personal Information, at any time, if the processing is for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications and you have not given your consent. You have the right not to have your Personal Information processed for purposes of direct marketing by means of unsolicited electronic communications from third parties unknown to you, other than Selftrack's duly appointed and authorised third party business partners who may do so on Selftrack's behalf.

11. AMENDMENTS TO THIS PRIVACY POLICY

11.1. We reserve the right, in our sole discretion to amend (including without limitation, by the addition of new terms and conditions) this Privacy Policy from time to time. Any changes to this Privacy Policy will be drawn to your attention on our website. You agree to review the Privacy Policy whenever you visit the Selftrack website for any such amendments. Save as expressly provided to the contrary in this Privacy Policy, the amended version of the Privacy Policy shall supersede and replace all previous versions thereof.

12. YOUR CONSENT

12.1. You consent that we may disclose your Personal Information to Selftrack approved third party business partners and service providers where necessary;

12.2 You agree that Personal Information may be shared under the following circumstances:

12.2.1. with ourselves, our agents, advisers, service providers and suppliers for analysing purposes;

12.2.2. to monitor web traffic: web servers serving the website automatically, collect information about pages you visit. This information is used for internal review, to tailor information to individual visitors and for traffic audits;

12.2.3. for statistics purposes: we may perform statistical analyses in order to measure interest in the various areas of the website (for product development purposes);

12.2.4. to government and law enforcement agencies, where the law requires that we disclose your Personal Information to a party, and where we have reason to believe that a disclosure of Personal Information is necessary to identify, contact or bring legal action against a party who may be in breach of the Privacy

Policy or may be causing injury to or interference with (either intentionally or unintentionally) our rights or property, other users, or anyone else that could be harmed by such activities;

12.2.5. where such consent is necessary in order to give effect to our agreements signed between you and ourselves.

13. YOUR RIGHTS

13.1. You have the right to request that we correct, destroy, or delete any of your Personal Information that we have processed in accordance with this policy. The Personal Information that you may request us to correct, destroy or delete is Personal Information that has been processed that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, obtained unlawfully or that we are no longer authorised to retain.

13.2. You have the right to withdraw your consent for us to process your Personal Information at any time. The withdrawal of your consent can only be made by you on the condition that:

- the withdrawal of your consent does not affect the processing of your Personal Information before the withdrawal of your consent; or
- the withdrawal of your consent does not affect the processing of your Personal Information if the processing is in compliance with an obligation imposed on us by law; or
- the withdrawal of your consent does not affect the processing of your Personal Information where such processing is necessary for the proper performance of a public law duty by a public body; or
- the withdrawal of your consent does not affect the processing of your Personal Information as required to finalise the performance of a contract to which you are a party; or
- the withdrawal of your consent does not affect the processing of your Personal Information as required to protect your legitimate interests or our own legitimate interests or the legitimate interests of a third party to whom the information is supplied.

13.3. You have the right to object to the processing of your Personal Information at any time, on reasonable grounds relating to your particular situation, unless the processing is required by law.

13.4. You can make the objection if the processing of your Personal Information is not necessary for the proper performance of a public law duty by a public body, or if the processing of your Personal information is not necessary to pursue your legitimate

interests, our legitimate interests or the legitimate interests of a third party to which the information is supplied.

13.5. You have the right not to be subjected to a decision which is based solely on the basis of the automated processing of your Personal Information intended to provide a profile of you.

13.6. You have the right to submit a complaint to the Information Regulator regarding an alleged interference with the protection of Personal Information processed in accordance with this policy.

14. HOW DO YOU CONTACT US?

14.1. If you have questions about this Privacy Policy or wish to amend or update any of your Personal Information you may contact us at 0861 909 101.

JANUARY 2021

ANNEXURE "B"

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	DETAILS OF THE DATA SUBJECT
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	Code ( )
Contact number(s):	
Fax number/E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	Code ( )
Contact number(s):	

Fax number/ E-mail address:	
C	INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED
D	REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN. *(Please provide detailed reasons for the request)*

Signed at ..... this ..... day of .....20.....

.....

Signature of data subject/ designated person

ANNEXURE "C"

ANNEXURE C

AUTHORISATION OF INFORMATION OFFICER

(In terms of the Promotion of Access to Information Act, 2000)

I, the undersigned

PIETER HENDRIK COETZEE

Managing Director of SELFTRACK (PTY) LTD

Hereby authorise ***ERICA NOELLE MASHER*** as an Information Officer of **SELFTRACK (PTY) LTD** and authorise you to exercised any of the powers, duties and responsibilities conferred or imposed on me by the Protection of Personal Information Act, 2013 and the Promotion of Access to Information Act, 2000.

Please be advised that I reserve my right to exercise any of the powers, duties and responsibilities conferred herein, as well as the right to amend and/or withdraw any of those powers, duties, and responsibilities.

PH COETZEE (MD OF SELFTRACK)

By my signature herein below, I hereby accept the authorisation as an Information Officer.

ERICA NOELLE MASHER

Designation: Human Capital Manager & Group Company Secretary

Date: 7 June 2021

ANNEXURE 'D'

DESIGNATION AND DELEGATION OF AUTHORITY TO THE DEPUTY INFORMATION OFFICER

(*In terms of section 56 of the Protection of Personal Information Act, 2013 (POPIA) and Section 17(1) of the Promotion of Access to Information Act, 2000(PAIA)*

I, the undersigned,

_____

(Name of the Information Officer)

hereby designate.....
(**name of the person being designated**) as a Deputy Information Officer of .....
(**name of the body or responsible party**)

Furthermore, I hereby delegate to you the following powers, duties and responsibilities, as conferred or imposed on me by POPIA and PAIA-

a)

Please be advised that I reserve the right to exercise any of the powers, duties and responsibilities conferred herein, as well as the right to amend and/or withdraw any of those powers, duties and responsibilities.

_____

Information Officer

By my signature herein below, I hereby accept the delegation and designation as the Deputy Information Officer

_____

(Name of the designate)

Date: .....

ANNEXURE 'E'

INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

INFORMATION OFFICER'S REGISTRATION FORM

NOTE: ***The personal information submitted herein shall be solely used for your registration with the Information Regulator ("Regulator").***

All the information submitted herein shall be used for the purpose stated above, as mandated by law. This information may be disclosed to the public. The Regulator undertakes to ensure that appropriate security control measures are implemented to protect all the information to be submitted in this document.

PART A INFORMATION OFFICER	
Full Name of Information Officer	
Designation	
Postal Address	
Physical Address	
Cellphone Number	
Landline Number	
Fax Number	
Direct Email Address	
General Email Address	

PART B DEPUTY INFORMATION OFFICER			
Personal details of designated or delegated Deputy Information Officer(s)	Name	Name	Name
	Direct Landline	Direct Landline	Direct Landline
	Cellphone Number	Cellphone Number	Cellphone Number
	Email Address	Email Address	Email Address
Postal Address			
Physical Address			
Fax Number			
General Email Address			

PART C BODY / RESPONSIBLE PARTY				
Type of Body	Public Body		Private Body	
Full Name of the Body (Registered Name)				
Trading Name				
Registration No, if any				

Postal Address	
Physical Address	
Landline Number	
Fax Number	
Email Address	
Website	

PART D
DECLARATION

I declare that the information contained herein is true, correct and accurate.

SIGNED and **DATED** at _____on this the_____day of _____**202_**

_____

INFORMATION OFFICER

ANNEXURE 'F'

FORM 4

APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING IN TERMS OF SECTION 69(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 6]

TO: _____

_____

_____

_____

(Name of data subject)

FROM: _____

_____

_____

_____

Contact number(s): _____

Fax number: _____

E-mail address: _____

(Name, address and contact details of responsible party)

Full names and designation of person signing on behalf of responsible party:

_____

.....

Signature of designated person

Date: _____

PART B

I, _____*(full names of data subject)* hereby:

☐ Give my consent.

To receive direct marketing of goods or services to be marketed by means of electronic communication.

SPECIFY GOODS or SERVICES:

SPECIFY METHOD OF COMMUNICATION: FAX:
E - MAIL:
SMS:
OTHERS – SPECIFY:

Signed at ..... this ..... day of .....20.....

.....
Signature of data subject