Access Track (Pty) Ltd
669 Plettenberg Street, Faerie Glen, Pretoria, 0081
Phone: (012) 001 9930 | E-mail: info@accesstrack.co.za
Reg. No: 2013/236447/07 | VAT No: 4570265936

Data Processing Addendum

This addendum is between a responsible party and its operator to fulfil the responsible party's obligation under POPIA to enter into a contract with the operator.

1. INTRODUCTION

1.1. This addendum is between the **responsible party** and **operator.** The responsible party enters into this addendum with the operator to fulfil its data protection legal obligations under the South African Protection of Personal Information Act 4 of 2013 (POPIA). Each party is an organisation incorporated under the laws of the country where it is legally registered and having its registered office and principal business place at the physical address and with the registration or identification number specified in the principal agreement.

2. PURPOSE AND BACKGROUND

2.1. ***Nature of the addendum.*** This addendum supplements the responsible party's principal agreement with the operator. It also clarifies the relationship between the parties under applicable data protection laws.

2.2. ***Recording consensus.*** The parties enter into this written addendum with each other on its terms to manage their relationship, facilitate a productive working dynamic, clearly define their respective rights and responsibilities, avoid misunderstandings or disputes, and ensure a mutually beneficial relationship when it comes to compliance with the applicable data protection laws and responsibility for compliance.

2.3. ***Written agreement required.*** The applicable data protection laws require that responsible party conclude a written agreement with operator with respect to the processing activities of personal information that operator performs on behalf of responsible party. This addendum serves as that written agreement.

2.4. ***Agreement on security measures required.*** The parties must agree on the security measures necessary to safeguard the integrity and confidentiality of personal data in terms of applicable data protection laws.

2.5. ***Drafting approach.*** The parties have drafted this addendum in plain language to be fair and easy to understand. The parties wish to conclude this addendum quickly without unnecessary delay to start adding value to each other as soon as possible. Each party may freely engage the other party to discuss and resolve any issues that may jeopardise the parties wishes in terms of this clause.

3. DEFINITIONS, PARTIES, PRINCIPAL AGREEMENT, AND INTERPRETATION

3.1. ***Definitions***. In this addendum:

applicable data protection laws means the applicable data protection laws, including POPIA together with any national implementing laws, ePrivacy laws, guidance notes from the Information Regulator, and other related laws agreed between the parties in writing;

appropriate technical and organisational measures means, regarding a given goal, the technical and organisational efforts that a reasonable person in the same position would use to achieve that goal as quickly, effectively, and efficiently as possible;

Information Regulator means South Africa's data protection supervisory authority established under POPIA and empowered to monitor and enforce compliance by public and private bodies with the provisions of POPIA and the Promotion of Access to Information Act 2 of 2000 (PAIA);

operator means Access Track (Pty) Ltd, as specified in the principal agreement, being the person who processes personal information for a responsible party without coming under the direct authority of the responsible party, and enters into this addendum with the responsible party;

personal information means any information about a living human being or existing organisation (as applicable data protection laws require), provided that someone is capable of identifying them from that information;

personnel means any director, employee, or another person who works (permanently or temporarily) under either party's supervision; or person who renders services to either party to meet their obligations under this agreement as their agent, consultant, contractor, or another representative;

principal agreement means the agreement between the responsible party and operator under which the operator processes personal information on the responsible party's behalf;

processing means doing anything with or to personal information, including gathering it, disclosing it, or combining it with other information; and

responsible party means the customer, as specified in the principal agreement, the person who determines the purpose ('why') and means ('how') of processing the personal information alone or in conjunction with others, although it is more important that they determine why to process the personal information than how;

responsible party's documented instructions means the principal agreement and any other relevant written documents between the parties, unless the parties agree otherwise in writing;

sub-operator means any sub-operator that the operator engages to process personal information under the principal agreement and this addendum, as those documents permit.

3.2. ***Undefined terms***. Any terms not otherwise defined in this addendum have the meaning the principal agreement or relevant legislation gives to them.

3.3. ***Data protection law terms***. The terms used in this addendum that have meanings ascribed to them in applicable data protection laws. The terms 'data subject', 'processing', 'personal information', 'responsible party' and 'operator' carry the meanings set out under those laws to the extent that this addendum or the principal agreement does not define them.

4. APPLICATION

4.1. ***Applicable processing activities.*** This addendum applies when the operator processes personal information on the responsible party's behalf for the provision of license scanning and information collection equipment and services used by the responsible party for the collection and management of visitor information for the purposes of access control and access authorisation, as set out in the principal agreement. It does not apply to the operator processing on the responsible party's behalf under any other activity not set out in the principal agreement, or any processing that is not on the responsible party's behalf.

4.2. ***Applicable personal information.*** The personal information, data subject categories, and nature and purposes of processing are listed in Annexure 1.

5. REQUIREMENTS

5.1. ***Measure guarantees***. The operator guarantees that it will implement appropriate technical and organisational measures to meet the requirements of applicable data protection laws, and protect data subjects' rights.

5.2. ***Purpose pursuit***. The operator may choose the means it considers necessary to fulfil the purposes for processing listed in Annexure 1 in its discretion, provided that its choices are compatible with this addendum's requirements and the responsible party's documented instructions.

5.3. ***Sub-operator contracts***. The operator must respect the conditions for sub-operator contracts under applicable data protection laws. The operator must enter into a contract or other written agreement with any sub-operator to govern processing by that sub-operator in the same way as the contract or other agreement between responsible party and operator, particularly when it comes to appropriate technical and organisational measures.

6. RESPONSIBLE PARTY AND OPERATOR

6.1. ***Determination by responsible party***. The responsible party will determine the scope, purposes, and manner by which the operator may access or process personal information to the extent that the principal agreement does not adequately describe the operator's data processing activities.

6.2. ***Processing instructions***. The operator will only process the personal information on documented instructions of the responsible party to the extent that this is required for the provision of the services. Should the operator reasonably believe that a specific processing activity, beyond the scope of the responsible party's instructions, is required to comply with a legal obligation to which the operator is subject, the operator will inform the responsible party of such legal obligation and seek explicit authorisation from the responsible party before undertaking such processing. The operator will not process personal information in a manner inconsistent with the responsible party's documented instructions. The operator will notify the responsible party where it believes that a documented instruction is in breach of the applicable data protection laws, provided that such notice does not constitute legal advice to the responsible party.

6.3. ***Responsible party's warranties and responsibilities***. The responsible party warrants that it has all necessary rights to provide the personal information to the operator for the processing to be performed in relation to the services, and that one or more justifiable grounds set forth in the applicable data protection laws support the lawfulness of the processing. The responsible party is responsible for ensuring that all necessary privacy notices are provided to data subjects, that any necessary data subject consent to the processing is obtained, and that a record of any such consent is maintained. Where such consent is revoked, the responsible party must communicate such revocation to the operator.

7. DATA SHARING

7.1. ***Responsibility for secure data transfer***. Where applicable, each party is responsible for securely transferring any data they share with the other party, and each party must take appropriate technical and organisational measures to ensure they transfer data securely to the other party.

8. CONFIDENTIALITY

8.1. ***Treat personal information as confidential***. Without prejudice to any existing contractual arrangements between the parties, the operator will treat all personal information as confidential and will inform its employees, agents or approved sub-operators engaged in processing the personal information of the confidential nature of the personal information. The operator will ensure that all such persons have signed an appropriate confidentiality agreement are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality regarding the personal information.

8.2. ***Survival***. This clause survives the termination of the principal agreement or this addendum.

9. DATA SUBJECT RIGHTS

9.1. ***Responsibility and accountability.*** The responsible party is responsible for and accountable to the data subject for ensuring that it complies with the conditions for lawful processing of personal information.

9.2. ***Applicable data protection law compliance.*** The operator agrees to take all reasonable measures to ensure its compliance with applicable data protection laws in the processing of a data subject's personal information.

9.3. ***Failure to comply.*** If the operator does not comply with applicable data protection laws, it agrees to do everything necessary to comply with those laws as soon as reasonably practicable.

10. SECURITY

10.1. ***Data security***. Taking into account the industry norm, the costs of implementation, the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects, each party will implement appropriate, reasonable technical and organisational measures to ensure a level of security regarding the processing of personal information that is appropriate to the risk. These measures shall include, at a minimum, the security measures agreed upon by the parties in Annexure 2

10.2. ***Security policies***. Each party will maintain and fully implement written security policies that apply to personal information processing. At a minimum, such policies must include:

- internal responsibility for information security management;
- devoting adequate personnel resources to information security;
- carrying out verification checks on permanent staff who will have access to the personal information;
- requiring employees, vendors and others with access to personal information to enter into written

confidentiality agreements; and
- conducting training to make employees and others with access to the personal information aware of information security risks presented by the Processing.

10.3. ***Evidence of compliance***. The operator may use its adherence to an approved code of conduct or security certification standard as an element to show compliance with the requirements set out in the applicable data protection laws.

10.4. ***Improvements to security.*** The parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The operator will therefore evaluate the measures as implemented on an on-going basis in order to maintain compliance with the requirements set out in the applicable data protection laws. Where the responsible party instructs the operator to improve security measures in response to changes in the applicable data protection laws, and such instruction requires an amendment to the principal agreement or this addendum, the parties shall negotiate such amendment in good faith.

11. DATA TRANSFERS

11.1. ***Transferring instructions***. The operator may only transfer personal information to a third country or international organisation on the responsible party's documented instructions unless required to do so by applicable law. The operator must tell the responsible party about the legal requirement before processing the personal information unless the law prohibits them from doing so in the public interest. Annexure 3 provides a list of transfers for which the responsible party grants its authorisation upon the conclusion of this addendum.

12. INFORMATION OBLIGATIONS AND INCIDENT MANAGEMENT

12.1. ***Notification of incident.*** When the operator becomes aware of an incident that has a material impact on the processing of the personal information that is the subject of the principal agreement, it shall promptly notify the responsible party about the incident, shall at all times co-operate with the responsible party, and shall follow the responsible party's instructions with regard to such incidents, in order to enable the responsible party to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident. Notices will contain:

- a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of personal information records concerned;
- the name and contact details of the operator's information officer or another contact point where more information can be obtained;
- a description of the possible consequences of the incident;
- a description of the measures taken or proposed to be taken by the operator to address the incident including, where appropriate, measures to mitigate its possible adverse effects; and
- if known, the identity of the unauthorised person who may have accessed or acquired the personal information.

12.2. ***Incidents.*** In this clause, the term "incident" means:

- a complaint or a request with respect to the exercise of a data subject's rights in terms of the applicable data protection law;
- any unauthorised or accidental access, processing, deletion, loss or any form of unlawful processing of the personal information;
- any breach of security or confidentiality as set out in this addendum leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the personal information, or any indication of such breach having taken or about to take place;
- where, in the opinion of the operator, implementing an instruction received from the responsible party would violate applicable laws to which the responsible party or the operator are subject.

12.3. ***Operator's written procedures.*** The operator will at all times have in place written procedures which enable it to promptly respond to the responsible party about an incident. Where the incident is reasonably likely to require a data breach notification by the responsible party in terms of the applicable data protection law, the operator will implement its written procedures in such a way that it is in a position to notify the responsible party without undue delay after the operator becomes aware of such an incident.

13. CONTRACTING WITH SUB-OPERATORS

13.1. ***Sub-operator restriction***. The operator may not subcontract any of their services related to the processing of the personal information or assign their obligations to a sub-operator without the responsible party's written authorisation.

13.2. ***Sub-operator changes***. The responsible party authorises the operator's use of the sub-operators listed in Annexure 3. The operator will inform the responsible party of the changes of sub-operators and allow the responsible party to object to such changes. If the responsible party raises and provides reasons for such objection timeously, the parties will make a good-faith effort to resolve the responsible party's objection. If the parties cannot resolve the objection, the operator will make commercially reasonable efforts to provide the responsible party with the same level of service described in the principal agreement, without using the sub-operator to process personal information. If the operator's efforts are not successful within a reasonable time, each party may terminate the portion of the service which cannot be provided without the sub-operator, and the operator will be entitled to a pro-rated refund of any applicable service fees.

13.3. ***Operator remains liable***. The operator remains fully liable to the responsible party for any sub-operator's failure to meet their data protection obligations despite the responsible party's authorisation.

13.4. ***Operator's sub-operator obligations.*** The operator will ensure that the sub-operator is bound by data protection obligations compatible with those of the operator under this addendum, will supervise compliance therewith, and will impose on its sub-operators the obligation to implement appropriate technical and organisational measures so that the processing will meet the requirements of the applicable data protection laws.

14. RETURN OR DESTRUCTION OF PERSONAL INFORMATION

14.1. ***Deletion or return obligations.*** Unless otherwise required by law, the operator must, at the responsible party's election, delete, destroy or return all the personal information (including copies) to the responsible party when:

- the principal agreement or this addendum terminates;
- the responsible party gives the operator a written request to do so; or
- the operator has otherwise fulfilled all purposes agreed in the context of the services whereby no further processing is required.

15. ASSISTANCE TO RESPONSIBLE PARTY

15.1. ***Help responsible party respond***. Where reasonably possible, the operator will help the responsible party with appropriate technical and organisational measures to fulfil their obligation to respond to requests by data subjects exercising their rights.

15.2. ***Other help to responsible party***. Considering the nature of the processing and the information available to the operator, the operator will help the responsible party with its obligations regarding the security of processing, and other obligations under applicable data protection laws that are relevant to the data processing described in this addendum, including notifications to a supervisory authority or data subjects.

15.3. ***Make compliance information available***. The operator shall make available to the responsible party all information necessary to demonstrate compliance with the responsible party's obligations and allow for and contribute to audits, including inspections, conducted by the responsible party. The responsible party may contact the operator's information officer using the following contact information:

Phone: 012 001 9930

E-mail: info@accesstrack.co.za

16. DURATION AND TERMINATION

16.1. ***Commencement***. This addendum comes into effect on the effective date of the principal agreement.

16.2. ***Duration***. The operator will process personal information until the principal agreement expires or terminates, unless instructed otherwise by the responsible party, or until such data is returned or destroyed on instruction of the responsible party.

17. GENERAL

17.1. ***Entire contract and conflict.*** This addendum constitutes the entire contract between the parties regarding the matters dealt with in this addendum. In the event of any conflict between the terms of the principal agreement and this addendum, the terms of this addendum will prevail.

17.2. ***Governing law and disputes***. This addendum is governed by the laws of South Africa. Any disputes arising from or in connection with this addendum will be dealt with in the manner and jurisdiction specified in the relevant provisions of the principal agreement.

ANNEXURE 1 – INFORMATION PROCESSED

1. INFORMATION PROCESSED

1.1. The operator provides license scanning and information collection equipment and services that are used for the collection and management of visitor information for purposes of performing access control and access authorisation functions.

2. TYPES OF PERSONAL INFORMATION THAT WILL BE PROCESSED IN THE SCOPE OF DELIVERING THE SERVICE

2.1. Scan of Driving License Card Barcode:

- ID Number, Surname and Initials, Date of Birth, Sex, License Number, Expiry Date, Photo

2.2. Scan of Green South African ID Document Barcode:

- ID Number

2.3. Scan of New South African ID Card Barcode:

- ID Number, Surname and Initials, Date of Birth, Sex, Photo

3. TYPES OF PUBLIC AND OTHER INFORMATION THAT WILL BE PROCESSED IN THE SCOPE OF DELIVERING THE SERVICE

3.1. Scan of Vehicle Registration Disk Barcode:

- License Number, Expiry Date, eNaTiS, Vehicle Make, -Series, -Description and -Colour, Register- and VIN Number, Engine Number.

- Manual Input Fields (as determined by the responsible party):

- Un-verified information obtained verbally and added using texts fields by the operator of the scanning device may include, but not limited to Phone number, number of people inside vehicle, purpose of visit, type of visitor (ex. Courier, Contractor etc.), tenant address, etc.

ANNEXURE 2 – SECURITY MEASURES

1. SECURITY MEASURES

1.1. Details of the security measures deployed are described in the technical specification document, updated from time to time, and available from the operator on request.

2. MINIMUM MEASURES

The operator will:

- Ensure that the personal information can be accessed only by authorized personnel for the purposes set forth in this addendum;
- Take all reasonable measures to prevent unauthorized access to the personal information through the use of appropriate physical and logical (passwords) entry controls, securing areas for information processing, and implementing procedures for monitoring the use of information processing facilities;
- Build in system and audit trails;
- Use secure passwords, network intrusion detection technology, encryption and authentication technology, secure logon procedures and virus protection;
- Account for all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of personal information;
- Ensure pseudonymisation or encryption of personal information, where appropriate;
- Maintain the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Maintain the ability to restore the availability and access to personal information in a timely manner in the event of a physical or technical incident;
- Implement a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of personal information;
- Monitor compliance on an ongoing basis;
- Implement measures to identify vulnerabilities with regard to the processing of personal information in systems used to provide services to the responsible party;
- Provide employee and contractor training to ensure ongoing capabilities to carry out the security measures established in policy.

ANNEXURE 3 – TRANSFER OF INFORMATION

1. TRANSFERS TO OTHER COUNTRIES, OUTSIDE THE REPUBLIC OF SOUTH AFRICA, WITHOUT AN ADEQUATE LEVEL OF PROTECTION FOR WHICH THE RESPONSIBLE PARTY HAS GRANTED ITS AUTHORISATION

Process	Country	Recipient	Recipient Address	Recipient Contact Details
NONE				

2. TRANSFERS TO SUB-OPERATORS FOR WHICH THE RESPONSIBLE PARTY HAS GRANTED ITS AUTHORISATION

Process	Recipient	Recipient Address	Recipient Contact Details
NONE			