

## DATA PROTECTION POLICY

### 1. Objective of the policy

- 1.1. This policy describes the Company's guidelines with regards to the regulation, and in harmony with international standards, the processing of personal information by the company in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests.
- 1.2. This policy applies to all personal information, either in electronic or paper format received by the company.

### 2. Purpose of the policy

- 2.1. Elliott Mobility must protect restricted confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. The protection of data in scope is a critical business requirement, yet the flexibility to access data and work effectively is also critical.
- 2.2. It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably protect all data. Its primary objective is user awareness and to avoid accidental loss scenarios.
- 2.3. The purpose of the policy furthers the intention of the Protection of Personal Information Act (POPI) to give effect to the constitutional right to privacy, safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at balancing the right to privacy against other rights, particularly the right of access to information and protecting important interests, including the free flow of information within the republic and across international borders.

### 3. Definitions

- 3.1. For this Policy the following definitions shall apply:

- Agent – means any third party that uses Personal Information provided to it by the company to perform tasks on behalf of and under the instruction of the company.
- Biometrics – means a technique of personal identification that is based on physical, physiological, or behavioral characterization including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition.
- Consent – means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
- Data Subject - means the person to whom personal information relates.
- De-identify – in relation to personal information of a data subject, means to delete any information that identifies the data subject.

- Operator – means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
- Person – means a natural person or a juristic person.
- Personal Information – means information relating to an identifiable, living natural person and where it is applicable, an identifiable existing juristic person including but not limited to:
  - Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, physical age or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person.
  - Information relating to the education or the medical, financial, criminal or employment history of the person.
  - The biometric information of the person.
- Regulator – means the information Regulator established in terms of section 39 of the Protection of Personal Information Act.
- Responsible party – means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

#### **4. Accountability**

- 4.1. The company undertakes to ensure conditions for lawful processing and complies with all the measures that give effect to such conditions at the time of and during the processing itself.

#### **5. Processing limitation**

- 5.1. Personal information shall always be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.
- 5.2. Personal information will only be processed if given the purpose for which it is processed at the time, is adequate, relevant, and not excessive.
- 5.3. Personal information will only be processed if the data subject consents to the processing; if processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; if the processing complies with an obligation imposed by law on the responsible party; if the processing data protects a legitimate interest of the data subject; if processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.
- 5.4. A data subject may object, at any time, to the processing of personal information on reasonable grounds relating to his, her or its situation unless legislation provides for such processing; or for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.
- 5.5. The act of “Live Streaming” or streaming in which audio or video is broadcast live over the Internet, is not acceptable unless we have written approval from the customer.

- 5.6. This excludes Virtual or Video Surveys or any Claims Inspections that take place in the customers home, as this does not fall within the definition of live streaming.
- 5.7. The company undertakes that once an objection to the processing of personal information is received that they will no longer process the personal information.
- 5.8. Personal information shall be collected directly from the data subject except for instances where it would not be applicable, and the information is contained in or derived from a public record or has deliberately been made public by the data subject and the data subject has consented to the collection of the information from another source which would not prejudice a legitimate interest of the data subject. Collection of the information from another source is necessary to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied.

## 6. Purpose specification

- 6.1. The company will obtain personal information that is collected for a specific, explicitly defined, and lawful purpose related to a function or activity by the company. Steps will be taken to ensure that the data subject is aware of the purpose for which the information is collected.
- 6.2. Records of personal information will not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed unless the retention of the record is required by a contract between the parties thereto or the data subject has consented to the retention of the record.
- 6.3. Should the records of personal information be retained for periods over and above those indicated above for purpose of historical, statistical, or research purposes, the company undertakes that the necessary and appropriate measures will be taken to safeguard against the records being used for any other purposes.
- 6.4. The company shall destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the company is no longer authorized to retain the record as indicated above. The destruction or deletion of a record of personal information will be done in a manner that prevents its reconstruction in an intelligible form.

## 7. Further processing limitation

- 7.1. With reference to paragraph 5 above, the company undertakes that any further processing of personal information will be in accordance or compatible with the purpose for which it is collected. In consideration to this, the company will consider:
  - The relationship between the purpose of the intended further processing and the purpose for which the information has been collected.
  - The nature of the information concerned.
  - The consequences of the intended further processing for the data subject.
  - The way the information has been collected and
  - Any contractual rights and obligations between the parties.

7.2. The further processing of personal information is not incompatible with the purpose of collection if:

- the data subject has consented to the further processing of the information.
- the information is used for historical, statistical or research purposes and the responsible party ensures that further processing is carried out solely for such purposes and will not be published in an identifiable form.

## 8. Openness

8.1. When collecting personal information from the data subject the company will take reasonably practicable steps to ensure that the data subject is aware of:

- The information being collected and where the information is not collected from the data subject, the source from which it is collected.
- The name and address of the company.
- The purpose for which the information is being collected.
- Whether or not the supply of the information by the data subject is voluntary.
- The consequences of failure to provide the information.
- The fact that, where applicable, the responsible party intends to transfer the information to a third country or international organization and the level of protection afforded to the information by that third country or international organization.

## 9. Security safeguards on integrity and confidentiality of personal information

9.1. The company will ensure to secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organizational measures to prevent loss of, damage to, or unauthorized destruction of personal information and unlawful access to or processing of personal information.

9.2. To give effect to this objective, the company will take reasonable measures to:

- Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control.
- Establish and maintain appropriate safeguards against the risks identified.
- Regularly verify that the safeguards are effectively implemented.
- And ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

9.3. An operator or anyone processing personal information on behalf of the company must:

- 9.3.1. Process such information only with the knowledge or authorization of the responsible party; and

9.3.2. Treat personal information that comes to their knowledge as confidential and must not disclose it.

9.4. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorized person, the company undertake to notify the:

- Regulator and
- The data subject unless the identity of such data subject cannot be established.

9.5. The notification to the data subject will be in writing and communicated to the data subject in at least one of the following ways:

- Mailed to the data subject's last known physical or postal address.
- Sent by e-mail to the data subject's last known e-mail address.
- As may be directed by the Regulator.


9.6. The notification will provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise.

## 10. Violations

10.1. Any employee who abuses or breaches any of the principles within this policy will be subject to corrective action up to and including termination of the employment contract. If necessary, the company also reserves the right to advise appropriate legal officials of any illegal activities by offenders.

**This policy will be strictly monitored and enforced.**

**We the Board of Elliott Mobility (Pty) Ltd accept and endorse the above Policy.**



**Brad Barker**

8 Feb 2024

**Date**