## THIRD PARTY SUPPLIER MINIMUM LEGISLATIVE OBLIGATIONS

As a registered business entity in the Republic of South Africa and a third-party service provider to SA Taxi Holdings (Pty) Ltd (and any entity the financial results of which are, or are required to be, partially or wholly consolidated in SA Taxi Holdings (Pty) Ltd's annual financial statements from time to time in accordance with SA Taxi Holdings (Pty) Ltd's accounting principles) ("SA Taxi Group"), you are obliged to adhere to certain legislative and regulatory requirements. As a result, you must take cognisance of and adhere to the below minimum legislative obligations –

1. **Protection of Personal Information Act 4 of 2013 ("POPIA")**

   All entities are obliged to comply with Chapter 3 of POPIA which sets out the lawful conditions for the processing of personal information. The SA Taxi Group, as a responsible party, must ensure that all its third-party service providers who gain possession of personal information, as an operator, must adhere to the lawful conditions for the processing thereof. The SA Taxi Group has developed the below minimum standards which seek to ensure that the operators are in position to comply the lawful conditions.

| Minimum Standards | Service provider obligation |
|---|---|
| 1) Registered Information Officer and published Privacy Policy | The service provider must have a POPIA Information Officer registered with the Information Regulator (failing which the CEO is deemed the Information Officer) and have a published Privacy Policy on its website. |
| 2) Data Collection, Storage and Use | The service provider must be able to demonstrate documentary evidence that its data storage is secure by indicating a "Backup" policy, offsite storage or utilization of an industry recognized backup solution. |
| 3) Data Security | The service provider needs to demonstrate appropriate data security principles covering organisational information security and access control policies. |
| 4) Cyber Security Practice, Risk Assessment & | The service provider must assess and document the appropriate security levels by considering the risks of |

| Minimum Standards | Service provider obligation |
|---|---|
| Compliance Monitoring | processing personal identifiable information which should include but is not limited to the following:<br>1) accidental or unlawful destruction<br>2) loss<br>3) alteration or unauthorised change to personal identifiable information<br>4) misuse of personal identifiable information<br>5) Unauthorised disclosure of personal identifiable information<br>6) Unauthorised access to personal identifiable information transmitted, stored, or otherwise processed<br><br>Maintain a record of processing activities in relation to the personal information the service provider is responsible for processing as well as the record of associated risks.<br>The service provider must ensure that personal identifiable information is processed solely in accordance with SA Taxi's contractual agreement.<br>The service provider shall conduct regular compliance monitoring checks to confirm data protection and information security controls. |
| 5) Cyber–Security Management practices | The service provider must be able to demonstrate its basic information security practices in place in relation to data processed. This should consist of the following:<br>1) Controlled access (physical & logical) based on need to know for all accounts /access to premises including person(s) with administrative privileges. Regular review & ongoing monitoring of access.<br>2) Appropriate information security controls (confidentiality, availability & integrity) for hardware and software assets |

| Minimum Standards | Service provider obligation |
|---|---|
| | 3) Information Security safeguards for data in transit (email & system interfaces), in use (web-based protection) and at rest (storage). For example, encryption of devices, transport layer security (TLS), anonymisation of data where appropriate.<br>4) Secure configuration of hardware and software for endpoints, data centres (on-premises, cloud & hybrid), network devices, routers, and switches (including wireless access control)<br>5) Continuous vulnerability management, review of information technology environment and security posture (Continuous Risk & threat analysis)<br>6) Maintenance, monitoring and analysis of audit trails and system logs (Threat Management & Incident Identification)<br>7) Incident response and management policy & response plan(s) (tested at least annually), which include business continuity, disaster recovery and cyber response.<br>8) Secure Application Development (SDLC) & Change Management Processes<br>9) Security awareness & Training program |
| 6) Cyber Insurance | The service provider must show that it has the appropriate cyber insurance cover in place for the processing of any personal identifiable information in the event of the loss of any personal identifiable Information and subsequent claims related thereto. |

## 2. Anti-Bribery and Corruption Legislation ("ABC Laws")

The SA Taxi Group is committed to ethical business practices and is committed to complying with applicable Anti-bribery and Corruption laws. The SA Taxi Group is also committed to continuously conducting its business with integrity and with proper regard for ethical business practices and therefore has a zero-tolerance approach to acts of bribery and corruption by business partners, employees, vendors and all third parties that it engages with. ABC laws refer

to applicable laws that govern bribery and corruption in a jurisdiction. All business entities which operate within South Africa are obliged to adhere to the Prevention and Combating of Corrupt Activities Act, 2004 ("PRECCA"). Other ABC laws may be applicable to the activities of the SA Taxi Group, its employees and its business partners depending on the nature of the business activities involved, and ABC laws should be understood as including any other applicable national or international regulatory enactment of similar import to PRECCA (i.e. the Prevention of Organised Crime Act 121 of 1998) that may have a bearing on the activities of the SA Taxi Group.

As a third-party service provider to the SA Taxi Group you are to ensure that no conflict of interest arises between your business and business interests and your obligations to SA Taxi. You are required to notify the SA Taxi Group immediately (in any event, not later than 24 hours after becoming aware of a potential conflict of interest having arisen) after becoming aware that a potential conflict of interest has arisen.

## 3. Constitution of the Republic of South Africa, 1996 ("The Constitution")

Chapter 2 of The Constitution contains the Bill of Rights which enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality and freedom. Respect for human rights is a fundamental value for the SA Taxi Group, and we strive to protect and promote human rights in accordance with the UN Guiding Principles on Business and Human Rights in our relationships with our employees, suppliers, funders and customers.
The United Nations Global Compact's Ten Principles are -.

Principle 1 - Businesses should support, respect and protect internationally proclaimed human rights;

Principle 2 – Businesses must ensure that they are not complicit in human rights abuses;

Principle 3 - Business should uphold freedom of association and effective recognition of the right to collective bargaining;

Principle 4 – Businesses must eliminate all forms of forced and compulsory labour;

Principle 5 – Businesses must ensure the effective abolition of child labour in their operations; and

Principle 6 – Businesses must eliminate discrimination in respect of employment and occupation.