

Data Processing Addendum

VERSION: 20260920

This Data Processing Addendum (the “DPA”) sets out the terms on which eCommerceAfrica Processes Personal Information on behalf of Customer.

This DPA is an Addendum to, and forms part of, the eCommerceAfrica Master Services Agreement (the “MSA”), and forms part of the Agreement as that term is defined in the MSA.

Capitalised terms used in this DPA have the meaning given to them in the MSA. Where a term is defined both in Clause 1 (Defined Terms) and in the MSA, and that term relates to the Processing of Personal Information or to the Parties’ respective roles under Data Protection Laws, the definition in Clause 1 prevails. Where a capitalised term used in this DPA is not defined in the MSA, the definition set out in Clause 1 applies.

1. Defined Terms

“**Business Hours**” means the hours between 08:00 and 17:00 (GMT+2), Monday to Friday, excluding public holidays in South Africa.

“**Data Protection Laws**” means any law relating to data protection, privacy and security applicable to a Party in connection with the processing of Personal Information under the MSA including but not limited to (each as amended or replaced from time to time) (a) POPI Act, and (b) any applicable laws relevant to eCommerceAfrica or the Customer (where applicable and as recipient of eCommerceAfrica Services provided by eCommerceAfrica) relating to data protection.

“**Personal Information**” means personal information as defined in the POPI Act that is provided to eCommerceAfrica by, or on behalf of, the Customer in connection with the eCommerceAfrica Services, including any professional services performed by eCommerceAfrica on the Customer’s own systems, or by any other means. Personal Information includes, but is not limited to, the following:

- i) 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 the person.
- ii) information relating to the education or the medical, financial, criminal or employment history of the person.
- iii) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person.
- iv) the biometric information of the person.
- v) the personal opinions, views or preferences of the person.



- vi) 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.
- vii) the views or opinions of another individual about the person; and
- viii) 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.

Lower case terms: The following lower-case terms used but not defined in this DPA, such as “**data subject**”, “**information regulator**”, “**operator**”, “**responsible party**” and “**processing**” will have the same meaning as set forth in Section 1 of POPI Act, or where not specifically defined under Data Protection Laws, the same meaning as analogous terms in those Data Protection Laws.

2. Agreement

- 2.1. eCommerceAfrica agree that they will comply with the POPI Act regulations and process all the information and/or Personal Information in respect of the eCommerceAfrica Services being rendered in accordance with the said regulation and only for the purpose of providing the eCommerceAfrica Services set out in the MSA.
- 2.2. Both Parties agree and acknowledge that all information provided, whether personal or otherwise, may be used and processed by eCommerceAfrica.
- 2.3. The Customer owns the Customer Data and all intellectual property rights in it.
- 2.4. eCommerceAfrica acknowledges that in providing the eCommerceAfrica Services to the Customer that eCommerceAfrica may be exposed to the Customer Data.
- 2.5. eCommerceAfrica will use its best endeavours and take all reasonable precautions to ensure that any information provided, is only used for the purposes it has been provided.
- 2.6. The Parties specifically record that all Customer Data provided by the Customer to eCommerceAfrica or to which eCommerceAfrica may be exposed in the performance of its obligations in terms of this Agreement, shall constitute Confidential Information and as such, eCommerceAfrica shall comply with all the provisions of this Agreement in relation to same.
- 2.7. eCommerceAfrica hereby warrants in favour of the Customer, that it shall, at all times, strictly comply with all applicable legislation and with all the provisions and requirements of the Customer's Data Protection Policies and Procedures as may be updated from time to time as notified to eCommerceAfrica in writing.
- 2.8. eCommerceAfrica hereby warrants and undertakes that it shall not, at any time copy, compile, collect, collate, process, mine, store, transfer, alter, delete, interfere with or in any other manner use the Customer for any purpose other than with the express prior



written consent of the Customer, and to the extent necessary to provide the eCommerceAfrica Services to the Customer.

- 2.9. All data, including Customer Data, provided by the Customer, or accessed (or accessible) by eCommerceAfrica, shall be used by eCommerceAfrica only in connection with the provision of the eCommerceAfrica Services and shall not be commercially exploited by eCommerceAfrica in any manner whatsoever.
- 2.10. eCommerceAfrica further warrants that it shall ensure that all its systems which it uses to provide the eCommerceAfrica Services, including all systems onto which the Customer Data is copied, compiled, collected, collated, processed, mined, stored, transmitted, altered, or deleted, or otherwise used as part of providing the eCommerceAfrica Services, shall at all times be of a minimum standard required by law for the protection, control and use of Personal Information.
- 2.11. eCommerceAfrica has procured written undertakings from all its staff that those staff members who have access to Confidential Information are bound by confidentiality undertakings no less onerous than those contained in the MSA.
- 2.12. eCommerceAfrica may retain Confidential Information to the extent required by, and for the duration of, any eCommerceAfrica Services performed for the Customer in terms of agreements between the Parties, provided that the Customer has not waived performance of such eCommerceAfrica Services and subject to the right of the Customer to recover the Confidential Information at any time on the terms agreed herein.

3. Applicable Law

- 3.1. eCommerceAfrica may be required to process Personal Information on behalf of the Customer under any applicable Data Protection Laws.
- 3.2. Unless expressly stated otherwise, in the event of any conflict between the main body of this DPA and Data Protection Laws, the applicable Data Protection Laws will prevail.

4. Duration and Termination

- 4.1. This DPA will commence on the earlier of (i) the date on which the MSA becomes binding on the Parties and (ii) the date on which eCommerceAfrica first Processes Personal Information on behalf of Customer, and will remain in force so long as the MSA remains in effect or eCommerceAfrica retains any Personal Information related to the MSA in its possession or control.
- 4.2. eCommerceAfrica will process Personal Information until the date of expiration or termination of the MSA, unless instructed otherwise by the Customer in writing, or until such Personal Information is returned or destroyed on the written instructions of the



Customer or to the extent that eCommerceAfrica is required to retain such Personal Information to comply with applicable laws.

5. Personal Information Types and Processing Purposes

- 5.1. The Customer and eCommerceAfrica acknowledge that the Customer is the responsible party and eCommerceAfrica is the operator of Personal Information.
- 5.2. The details of the processing operations, in particular the categories of Personal Information and the purposes of processing for which the Personal Information is processed on behalf of the responsible party concerning the eCommerceAfrica Services described in the MSA, are specified in Clause 17.
- 5.3. The Customer remains responsible for its compliance obligations under applicable Data Protection Laws, including providing any required notices, obtaining any required consents, and for the processing instructions it gives to eCommerceAfrica.

6. eCommerceAfrica Obligations

- 6.1. **Customer knowledge, authorisation and documented instructions.** When eCommerceAfrica acts as the operator of Personal Information, it will only process the Personal Information with the Customer's knowledge, authorisation, and on the Customer's documented instructions as identified in Clause 17, and to the extent that this is required to fulfil the eCommerceAfrica Services as per the MSA. eCommerceAfrica will not process the Personal Information for any other purpose or in a way that does not comply with this DPA or applicable Data Protection Laws.
- 6.2. **Processing beyond instructions.** Should eCommerceAfrica reasonably believe that a specific processing activity beyond the scope of the Customer's instructions is required to comply with a legal obligation to which eCommerceAfrica is subject, eCommerceAfrica must inform the Customer of that legal obligation and seek written authorisation from the Customer before undertaking such processing. eCommerceAfrica will not process the Personal Information in a manner inconsistent with the Customer's documented instructions.
- 6.3. **Independent responsible party.** To the extent eCommerceAfrica uses or otherwise processes Personal Information in connection with eCommerceAfrica's legitimate business operations, eCommerceAfrica will be an independent responsible party for such use, will process Personal Information in accordance with this DPA, and will be responsible for complying with all applicable laws and responsible party obligations.
- 6.4. **Compliance.** eCommerceAfrica will reasonably assist the Customer in complying with the Customer's obligations under applicable Data Protection Laws, considering:
 - 6.4.1. the nature of eCommerceAfrica's processing,



- 6.4.2. the information made available to eCommerceAfrica, including in relation to data subject rights,
- 6.4.3. data protection impact assessments and
- 6.4.4. reporting to and consulting with information regulator.

6.5. **Notification.** eCommerceAfrica will immediately notify the Customer if, in its opinion, any instruction infringes applicable Data Protection Laws. This notification will neither constitute a general obligation on the part of eCommerceAfrica to monitor or interpret the laws applicable to the Customer, nor constitute legal advice to the Customer.

6.6. **Disclosure.** eCommerceAfrica will not disclose Personal Information except: (a) as the Customer directs in writing, (b) as described in this DPA or (c) as eCommerceAfrica will use reasonable endeavours to notify the Customer and attempt to redirect the public authority to request the Personal Information directly from the Customer.

7. Contracting with Sub-Operators

7.1. **Register of sub-operators.** eCommerceAfrica maintains a register of the sub-operators it engages that process the Customer's Personal Information, stating for each the category of service provided and the country in which processing takes place. eCommerceAfrica will provide the register to the Customer within 5 (five) business days of written request, and will give the Customer 30 (thirty) days' prior written notice before adding a sub-operator to the register. eCommerceAfrica will ensure that each sub-operator added to the register is bound by obligations no less protective than those imposed on eCommerceAfrica under this DPA.

7.2. **General authorisation.** The Customer provides its general authorisation to eCommerceAfrica's engagement with sub-operators, to provide some of eCommerceAfrica Services e.g. hosting eCommerceAfrica Services, on its behalf.

7.3. **Changes.** eCommerceAfrica will notify the Customer in writing of any intended changes to the agreed outsourced eCommerceAfrica Services.

7.4. **Performance.** eCommerceAfrica is responsible for its sub-operator's compliance in relation to eCommerceAfrica's obligations in this DPA.

8. Customer Obligations

8.1. **Data Subject requests.** If eCommerceAfrica receives a request from the Customer's data subject to exercise one or more of its rights under applicable Data Protection Laws, in connection with a Service for which eCommerceAfrica is an operator, eCommerceAfrica will redirect the data subject to make its request directly to the Customer. The Customer will be responsible for responding to any such request. eCommerceAfrica will comply with reasonable requests by the Customer to assist with the Customer's response to such a



data subject request. The Customer will be responsible for reasonable costs eCommerceAfrica incurs in providing this assistance.

- 8.2. **The Customer requests.** eCommerceAfrica must promptly comply with any Customer request (a) requiring eCommerceAfrica to amend, transfer, delete or otherwise process the Personal Information, or to stop, mitigate or remedy any unauthorised processing, (b) relating to the Customer's obligations regarding the security of processing and (c) the Customer's obligations in terms of applicable Data Protection Laws, considering the nature of the processing and the information available to eCommerceAfrica.
- 8.3. **Warranty.** The Customer warrants that: (a) it has all necessary rights to provide the Personal Information to eCommerceAfrica for the processing to be performed in relation to the eCommerceAfrica Services, and (b) eCommerceAfrica's expected use of the Personal Information for the eCommerceAfrica Services as specifically instructed by the Customer, will comply with all applicable Data Protection Laws.
- 8.4. **Privacy notices.** To the extent required by applicable Data Protection Laws, the Customer is responsible for ensuring that all necessary privacy notices are provided to data subjects, and unless another legal basis set forth in applicable Data Protection Laws supports the lawfulness of the processing, any necessary data subject consents to the processing are obtained and a record of such consents is maintained. Should such consent be revoked by a data subject, the Customer is responsible for communicating the fact of such revocation to eCommerceAfrica, and eCommerceAfrica remains responsible for implementing the Customer's instruction with respect to the processing of that Personal Information.

9. Security

- 9.1. **TOMs.** eCommerceAfrica will implement appropriate and reasonable Technical and Organisational Measures (herein after referred to as "**TOMs**") to ensure the security of the Personal Information in terms of applicable Data Protection Laws, including the security measures set out in Clause 18. This includes protecting the Personal Information against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the Personal Information.
- 9.2. **Access to Personal Information.** eCommerceAfrica will grant access to the Personal Information undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring the MSA . eCommerceAfrica will ensure that persons authorised to process the Personal Information received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.



10. Audits

- 10.1. **Certifications.** eCommerceAfrica will maintain any certifications that it is contractually obligated to maintain and comply with as expressly stated in the MSA. eCommerceAfrica will re-certify against those certifications as reasonably required.
- 10.2. **Provision of evidence.** At the Customer's written request, eCommerceAfrica will provide the Customer with evidence of those certifications relating to the processing of Personal Information, including applicable certifications or audit reports of its computing environment and physical data centres that it uses in processing Personal Information to provide the eCommerceAfrica Services so that the Customer can reasonably verify the data centres compliance with its obligations under this DPA.
- 10.3. **Compliance with TOMs.** eCommerceAfrica may also rely on those certifications to demonstrate compliance with the requirements set out in Clause 9.1.
- 10.4. **Confidential information.** Any evidence provided by eCommerceAfrica is confidential information and is subject to nondisclosure and distribution limitations of eCommerceAfrica and/or any eCommerceAfrica sub-operator.
- 10.5. **The Customer Audits.** The Customer may carry out audits of eCommerceAfrica's premises and operations as these relate to the Personal Information of the Customer if:
- 10.5.1. eCommerceAfrica has not provided the evidence requested under Clause 10.2 within 10 (ten) business days of the Customer's written request;
 - 10.5.2. an audit is formally required by the information regulator; or
 - 10.5.3. applicable Data Protection Laws provide the Customer with a direct audit right (and as long as the Customer only conducts an audit twice in any twelve-month period unless mandatory applicable Data Protection Laws require more frequent audits); or
 - 10.5.4. eCommerceAfrica has notified a Security Incident under Clause 11.1 affecting the Customer's Personal Information; or
 - 10.5.5. the Customer has notified eCommerceAfrica in writing, identifying the specific facts relied on and the provision of this DPA to which they relate, and eCommerceAfrica has not, within 10 (ten) business days of that notice, either remedied the matter or provided the Customer with evidence that the matter did not occur.
- 10.6. **Audit limits.** Each audit under Clause 10.5 is subject to the following, except where mandatory Data Protection Laws or a data protection authority of competent jurisdiction requires otherwise:
- 10.6.1. the Customer may conduct no more than 2 (two) audits in any 12 (twelve) month period;
 - 10.6.2. each audit is limited to 3 (three) business days on site;
 - 10.6.3. each audit is limited to the eCommerceAfrica Service, environment and Personal Information to which the ground relied on under Clause 10.5 relates, and does not extend to any environment or system controlled or operated by the Customer; and



10.6.4. no audit extends to the data, systems, Personal Information or Confidential Information of any other eCommerceAfrica customer, or to shared or multi-tenant infrastructure except to the extent that infrastructure processes the Customer's Personal Information.

10.7. **Response to notified facts.** Where the Customer notifies eCommerceAfrica under Clause 10.5.5, eCommerceAfrica will within 5 (five) business days of that notice: (a) provide the Customer with a written response addressing each fact identified in the notice; and (b) make available to the Customer remotely the logs, records and other evidence within eCommerceAfrica's control relating to those facts, excluding the data, systems, Personal Information and Confidential Information of any other eCommerceAfrica customer. Evidence provided under this Clause 10.7 is subject to Clause 10.4.

10.8. **Audit process.** Each audit is subject to the following:

10.8.1. the audit may be carried out by the Customer or by a third party appointed by the Customer, provided that the third party is not a competitor of eCommerceAfrica and has first entered into a confidentiality agreement with eCommerceAfrica;

10.8.2. the Customer must give eCommerceAfrica not less than 30 (thirty) days' written notice of an audit, except that where the ground relied on is Clause 10.5.2, 10.5.4 or 10.5.5, the Customer must give not less than 5 (five) business days' written notice;

10.8.3. audits are conducted during Business Hours, and eCommerceAfrica's personnel may accompany the Customer's auditors at all times;

10.8.4. eCommerceAfrica will co-operate with the audit and grant the Customer's auditors access to the premises, systems and devices involved in the processing of the Customer's Personal Information;

10.8.5. the Parties will use current certifications and audit reports provided under Clause 10.2 to avoid repeat audits of the same subject matter; and

10.8.6. the Customer bears the costs of each audit, except that eCommerceAfrica bears those costs where the audit identifies a failure by eCommerceAfrica to comply with Clause 9 (Security), Clause 11 (Incident Management) or Clause 18 (Technical and Organisational Measures). eCommerceAfrica will remedy any failure identified by an audit at its own cost within 30 (thirty) days, or within such shorter period as applicable Data Protection Laws require.

11. Incident Management

11.1. **Security incidents.** If eCommerceAfrica becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Information or the Customer's Confidential Information while processed by eCommerceAfrica (each a "**Security Incident**"), eCommerceAfrica will promptly and without undue delay:

11.1.1. notify the Customer of the Security Incident.



11.1.2. investigate the Security Incident and provide the Customer with sufficient information about the Security Incident, including whether the Security Incident involves Personal Information of the Customer.

11.1.3. take reasonable steps to mitigate the effects and minimise any damage resulting from the Security Incident.

11.2. **Security incident notification.** Notification(s) of Security Incidents will take place in accordance with Clause 11.1. Where the Security Incident involves Personal Information of the Customer, eCommerceAfrica will make reasonable efforts to enable the Customer to perform a thorough investigation into the Security Incident, formulate a correct response, and take suitable further steps in respect of the Security Incident. eCommerceAfrica will make reasonable efforts to assist the Customer in fulfilling the Customer's obligation under Section 22 of POPI Act or other applicable Data Protection Laws to notify the relevant data protection authority and data subjects about such Security Incident. eCommerceAfrica's notification of or response to a Security Incident under this clause is not an acknowledgement by eCommerceAfrica of any fault or liability for the Security Incident.

11.3. **Other incidents.** eCommerceAfrica will notify the Customer promptly if eCommerceAfrica becomes aware of:

11.3.1. a complaint or a request concerning the exercise of a data subject's rights under any applicable Data Protection Laws about Personal Information eCommerceAfrica processes on behalf of the Customer and its data subjects; or

11.3.2. an investigation into or seizure of the Personal Information of the Customer by government officials, or a specific indication that such an investigation or seizure is imminent; or where, in the opinion of eCommerceAfrica, implementing an instruction received from the Customer about the processing of Personal Information would violate applicable laws to which the Customer or eCommerceAfrica are subject.

11.4. **The Customer notifications.** Any notifications made to the Customer under Clause 11 will be addressed to the Customer as per the MSA.

12. Cross Border Transfers of Personal Information

12.1. **General.** The Customer's Personal Information is hosted in the Amazon Web Services Ireland region. eCommerceAfrica may in addition process the Customer's Personal Information through the sub-operators disclosed under Clause 7.1, in the countries stated in that register, and will give the Customer 30 (thirty) days' prior written notice before processing the Customer's Personal Information in a country not stated in it. eCommerceAfrica will process the Customer's Personal Information only in a country in respect of which the requirements of Clause 12.2 are met, and no such change will reduce the level of protection applicable to the Customer's Personal Information.

12.2. **Adequate safeguards.** eCommerceAfrica will identify in Clause 17 the transfer mechanism that provides an appropriate level of protection to the third party who receives the Personal Information either by way of a law, binding corporate rules or binding agreement under Section 72(1)(a) of POPI Act.



13. Return or Destruction of Personal Information

- 13.1. **eCommerceAfrica-managed Customer deletion.** For certain eCommerceAfrica Services, eCommerceAfrica is responsible for installing, hosting, and processing Personal Information. Here only eCommerceAfrica can access, extract and delete Personal Information stored in that Service. Where the particular Service does not support access, retention or extraction by software provided by the Customer, eCommerceAfrica will notify the Customer of that limitation and the parties will agree reasonable alternative measures, such as isolation or anonymisation of the affected Personal Information. eCommerceAfrica's liability in respect of deletion under this Clause 13 is subject to Clause 14.
- 13.2. **Delete or return.** Where the MSA requires eCommerceAfrica to retain Personal Information, eCommerceAfrica will delete that Personal Information within the period agreed to in the MSA, unless eCommerceAfrica is permitted or required by applicable law to retain such Personal Information. Where the retention of Personal Information has not been addressed in the MSA, eCommerceAfrica will either delete, destroy, or return all Personal Information to the Customer and destroy or return any existing copies when eCommerceAfrica has finished providing eCommerceAfrica Services:
- 13.2.1. related to the processing.
 - 13.2.2. when this DPA terminates.
 - 13.2.3. The Customer requests eCommerceAfrica to do so in writing; or
 - 13.2.4. eCommerceAfrica has otherwise fulfilled all purposes agreed in the context of the eCommerceAfrica Services related to the processing activities where the Customer does not require eCommerceAfrica to do any further processing.
- 13.3. **Certificate of destruction.** eCommerceAfrica will provide the Customer with a destruction certificate at the Customer's request. Where the deletion or return of the Personal Information is not technically feasible, or where backups and/or archived copies have been made of the Personal Information, eCommerceAfrica will retain such Personal Information in compliance with applicable Data Protection Laws, will isolate it from any further processing, and will delete it as soon as deletion becomes technically feasible or, in the case of backups and archived copies, on expiry of the applicable backup or archival cycle.
- 13.4. **Third parties.** On termination of this DPA, eCommerceAfrica will notify all sub-operators supporting its processing and make sure that they either destroy the Personal Information or return the Personal Information to the Customer, at the discretion of the Customer.

14. Liability and Warranty



- 14.1. Any limitation of liability in the MSA will apply to this DPA, other than to the extent such limitation is not permitted by applicable law (including in respect of liability to data subjects under the POPI Act).

15. Notice

- 15.1. Any notice or other communication given to a Party under or in connection with this DPA must be in writing and sent either (a) by a nationally recognised courier, to that Party at the address set out in the MSA or, where no address is set out there, at that Party's registered office; or (b) by electronic email. Where notice is given to eCommerceAfrica, a copy must also be sent to compliance@ecommerceafrica.com.
- 15.2. Contact information of eCommerceAfrica's information officer:

Email: compliance@ecommerceafrica.com

16. Miscellaneous

- 16.1. **Conflict of terms.** The Agreement terms remain in full force and effect except as modified in this DPA. Insofar as eCommerceAfrica will be processing Personal Information subject to applicable Data Protection Laws on behalf of the Customer in the course of the performance of the Agreement, the terms of this DPA will apply. If the terms of this DPA conflict with the terms of the Agreement, the terms of this DPA will take precedence over the terms of the Agreement, save that no provision of this DPA limits, varies or disapplies the provisions of the MSA governing third-party claims and limitation of liability unless it expressly states that it overrides those provisions.
- 16.2. **Governing law.** This DPA is governed by South African law.
- 16.3. Jurisdiction:
- 16.3.1. In respect of any action, claim or matter arising under or in connection with this DPA, the Parties irrevocably submit to the exclusive jurisdiction of the courts of the Republic of South Africa; and
- 16.3.2. either Party may apply to any court of competent jurisdiction for urgent interim or injunctive relief.
- 16.4. **Counterparts:** This DPA may be executed in any number of counterparts, each of which will constitute an original, but which will together constitute one agreement. Where one or both of the Parties chooses to execute this DPA by electronic signature, each electronic signature will have the same validity and legal effect as the use of a signature affixed by hand and is made to authenticate this DPA and evidence the intention of that Party to be bound by this DPA.



17. Particulars of Processing

17.1. **Categories of data subjects whose Personal Information is processed:**

17.1.1. eCommerceAfrica acknowledges that, depending on the Customer's use of the eCommerceAfrica Services, eCommerceAfrica may process the Personal Information of any of the following types of data subjects:

- (a) The Customer employees, contractors, temporary workers, agents and representatives
- (b) The Customer's customers
- (c) The Customer's suppliers
- (d) Applicant and/or candidate information
- (e) Categories of Personal Information

17.1.2. eCommerceAfrica acknowledges that, depending on the Customer's use of the eCommerceAfrica Services, the types of Personal Information processed by eCommerceAfrica may include, but are not limited to the following:

- (a) Basic Personal Information (for example first name, last name, email address and work address).
- (b) Bank account information.
- (c) Contact information (for example work email and phone number).
- (d) Professional or employment-related information (for example, employer name and job title).
- (e) Location information (for example, geo-location network data).

17.2. **Duration and object of processing:**

17.2.1. The duration of processing will be for the duration of the MSA between the Customer and eCommerceAfrica.

17.2.2. The objective of the data processing is the provision of eCommerceAfrica Services.

17.2.3. Personal Information may be processed on a continuous basis in order to provide the eCommerceAfrica Services under the MSA.

17.3. **Nature of the processing.** The Personal Information processed will be subject to the following basic processing activities, each of which will be carried out only in accordance with this DPA and the MSA:

17.3.1. Receiving information, including collection, accessing, retrieval, recording, and data entry.

17.3.2. Holding information, including storage, organisation and structuring.

17.3.3. Using information, including analysing, consultation, testing, automated decision making and profiling.

17.3.4. Updating information, including correcting, adaptation, alteration, alignment and combination.

17.3.5. Protecting information, including restricting, encrypting, and security testing.

17.3.6. Sharing information, including disclosure, dissemination, allowing access or otherwise making available.

17.3.7. Returning information to the Customer or data subject.



17.3.8. Erasing information, including destruction and deletion.

17.4. **Purpose(s) of the processing and further processing.** The purposes of processing Personal Information are for eCommerceAfrica to provide the eCommerceAfrica Services under the MSA, including technical support, administration and configuration activities performed at Customer's request or under an applicable Service Schedule.

17.5. **The retention period.** See Clause 13 of this DPA.

17.6. **Data transfers to sub-operators.** In accordance with this DPA, eCommerceAfrica may engage sub-operators to provide eCommerceAfrica Services on eCommerceAfrica's behalf. Any such sub-operators will be permitted to obtain Personal Information only to provide the eCommerceAfrica Services, eCommerceAfrica has engaged them to provide, and they are prohibited from using Personal Information for any other purpose.

17.7. **Transfer mechanism.** For the purposes of Clause 12.2, eCommerceAfrica relies on Section 72(1)(a) of the POPI Act. Each recipient of Personal Information outside the Republic of South Africa is subject to a law, binding corporate rules or a binding written agreement that upholds principles for reasonable processing substantially similar to the conditions for lawful processing under the POPI Act, and that includes provisions relating to onward transfers substantially similar to Section 72.

18. Technical and Organisational Measures

18.1. eCommerceAfrica shall implement, maintain, and monitor information security controls that contains appropriate technical and organisational measures (ensuring a level of security appropriate to the risk presented by the processing) to protect Personal Information against Security Breach and against all other unauthorised forms of processing.

18.2. These information security controls shall include the following technical and organisational measures:

18.2.1. Implement strong authentication mechanisms, such as multi-factor authentication.

18.2.2. Enforce least privilege access to systems and data.

18.2.3. Encrypt sensitive data at rest and in transit.

18.2.4. Use strong encryption algorithms and manage keys securely.

18.2.5. Deploy network firewalls to control incoming and outgoing traffic.

18.2.6. Install and maintain antivirus and anti-malware software.

18.2.7. Regularly update and patch operating systems, applications, and firmware.

18.2.8. Automate patch management processes where possible.

18.2.9. Separate critical systems and sensitive data from other network segments.

18.2.10. Implement virtual local area networks (VLANs) and subnetting.

18.2.11. Implement regular data backup processes.

18.2.12. Test data recovery procedures periodically.

18.2.13. Set up alerts for suspicious activities and potential breaches.



- 18.2.14. Enable logging for all critical systems and applications.
 - 18.2.15. Use a Security Information and Event Management (SIEM) system to centralise and analyse logs.
 - 18.2.16. Implement secure coding practices.
 - 18.2.17. Conduct regular code reviews and security testing for applications.
 - 18.2.18. Apply security best practices for cloud environments.
 - 18.2.19. Ensure proper configuration and management of cloud services.
 - 18.2.20. Assess and monitor the security practices of third-party vendors, where applicable.
 - 18.2.21. Include security requirements in vendor contracts, where applicable.
 - 18.2.22. Implement Identity and Access Management (IAM) solutions to manage user identities and access.
 - 18.2.23. Regularly review and update access rights.
 - 18.2.24. Ensure information security controls are communicated and enforced throughout the organisation.
- 18.3. eCommerceAfrica shall ensure that any person processing Personal Information on the operator's behalf will do so in compliance with this clause.

