

LEGAL DOCUMENT

Data Processing Agreement

*Processing of personal data under the Cyber and Data Protection
Act [Chapter 12:07]*

REFERENCE	CH-LEG-003
-----------	------------

VERSION	1.0
---------	-----

EFFECTIVE DATE	27 October 2026
----------------	-----------------

ISSUED BY	Credible Brands (Credible Host)
-----------	---------------------------------

CONTACT	support@credible.host · +263 772 519 128
---------	---

This document is published at credible.host/legal. The online version is the official version.

DOCUMENT CONTROL

Document	Data Processing Agreement
Reference	CH-LEG-003
Version	1.0
Effective date	27 October 2026
Issued by	Credible Brands (trading as Credible Host), Harare, Zimbabwe
Official version	The version published at credible.host/legal prevails over any printed or downloaded copy.

This agreement sets out how Credible Brands processes personal data on behalf of its customers when providing hosting, domain, email and related services, as required by the Cyber and Data Protection Act [Chapter 12:07]. It forms part of our Terms of Service.

CONTENTS

1.	Parties	2
2.	Definitions	2
3.	Scope and roles	3
4.	Customer obligations	3
5.	Credible Brands' obligations	3
6.	Sub-processors	4
7.	Location and international transfers	4
8.	Personal Data Breaches	5
9.	Data subject requests	5
10.	Information and audits	6
11.	Return and deletion	6
12.	General	6
	Annex A: Details of processing	8
	Annex B: Sub-processors	9
	Annex C: Security measures	10
	Signatures	11

1. Parties

This Data Processing Agreement (the **Agreement**) is made between:

- 1.1 **The Customer**, being the person or entity named in the client account or order to which this Agreement applies (the **Data Controller**); and
- 1.2 **Credible Brands**, trading as Credible Host, a company registered in Zimbabwe with its principal place of business in Harare, Zimbabwe (the **Data Processor**),

together the **Parties** and each a **Party**.

Background. The Parties have entered into an agreement under which Credible Brands provides the Customer with the Services described in Annex A (the **Service Agreement**, comprising the Credible Host Terms of Service, the order and any service level agreement). In providing the Services, Credible Brands will process personal data on the Customer's behalf. Section 18(5) of the Cyber and Data Protection Act requires a data controller to enter into a written contract with its data processor. The Parties therefore agree as follows.

2. Definitions

In this Agreement, unless the context requires otherwise:

Term	Meaning
Act	The Cyber and Data Protection Act [Chapter 12:07] (Act No. 5 of 2021) and any regulations made under it, as amended.
Authority	The Data Protection Authority under the Act, being the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ).
Customer Personal Data	Personal data that the Customer, its users or its website visitors store on, or transmit through, the Services, and which Credible Brands processes on the Customer's behalf.
Data subject	An identified or identifiable natural person to whom Customer Personal Data relates.
Personal data	Any information relating to a data subject, as defined in the Act.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.
Processing	Any operation performed on personal data, including collection, storage, retrieval, use, disclosure, backup and deletion.
Services	The hosting, domain, email, VPS, backup and related services described in Annex A.
Sub-processor	Any third party engaged by Credible Brands to process Customer Personal Data.

This Agreement covers Customer Personal Data only. Personal data that Credible Brands collects about the Customer itself (for example account, billing and domain registration

contact details) is processed by Credible Brands as a data controller under its Privacy Policy.

3. Scope and roles

- 3.1 The Customer is the data controller and Credible Brands is the data processor of Customer Personal Data.
- 3.2 Credible Brands shall process Customer Personal Data only on the Customer's documented instructions, as required by section 17 of the Act. The Service Agreement, this Agreement and the Customer's use and configuration of the Services constitute those instructions.
- 3.3 Credible Brands may process Customer Personal Data otherwise only where required by law. In that case it shall inform the Customer before processing, unless the law prohibits it.
- 3.4 The subject matter, nature, purpose, duration and categories of data and data subjects are set out in Annex A.
- 3.5 This Agreement applies for as long as Credible Brands processes Customer Personal Data in providing the Services, including during the return and deletion period in clause 11.

4. Customer obligations

The Customer shall:

- 4.1 ensure that all Customer Personal Data is collected and processed lawfully, and that it has a lawful basis (including any consent required) for Credible Brands to process it;
- 4.2 provide its own privacy notice to its data subjects, and handle their requests to exercise their rights under the Act;
- 4.3 ensure its instructions to Credible Brands comply with the Act;
- 4.4 be responsible for the security of everything within its own control, including passwords, user accounts, website software, plugins and themes it installs, and the content it uploads;
- 4.5 where required, register with or obtain a licence from the Authority as a data controller; and
- 4.6 on request, provide Credible Brands with reasonable assistance needed for it to meet its obligations under this Agreement.

5. Credible Brands' obligations

Credible Brands shall:

- 5.1 **Security.** Implement and maintain the technical and organisational measures in Annex C, appropriate to the nature of the data and the level of risk, and keep them operating continuously, as required by section 18 of the Act.

- 5.2 **Purpose limitation.** Not use Customer Personal Data for any purpose other than providing the Services and performing this Agreement. Credible Brands shall not sell Customer Personal Data or use it for its own marketing.
- 5.3 **No access to content.** Not access the content of the Customer's websites, files, databases or mailboxes, except where the Customer requests it (for example in a support ticket), where needed to keep the Services secure (for example automated malware and spam scanning), or where required by law.
- 5.4 **Confidentiality.** Keep Customer Personal Data confidential during and after the term of this Agreement, and ensure that staff and contractors who have access to it are bound by written confidentiality obligations and are trained in data protection.
- 5.5 **No disclosure.** Not disclose or make Customer Personal Data available to any third party, except to authorised Sub-processors under clause 6 or where required by law.
- 5.6 **Unlawful instructions.** Promptly inform the Customer if, in its opinion, an instruction from the Customer breaches the Act.
- 5.7 **Assistance.** Taking into account the nature of the processing and the information available to it, reasonably assist the Customer with its obligations on security, breach notification, data protection impact assessments and consultation with the Authority.
- 5.8 **Records.** Keep a record of the categories of processing it carries out on behalf of the Customer.
- 5.9 **Suspicious activity.** Respond within 8 business hours to any report from the Customer of suspicious activity affecting its account or Services.

6. Sub-processors

- 6.1 The Customer gives general authorisation for Credible Brands to engage the Sub-processors referred to in Annex B.
- 6.2 Credible Brands shall give the Customer at least 30 days' notice, by email or through the client area, before adding or replacing a Sub-processor.
- 6.3 The Customer may object on reasonable data protection grounds within that 30-day period. If the Parties cannot resolve the objection, the Customer may terminate the affected Services and receive a pro-rata refund of any prepaid fees for them.
- 6.4 Credible Brands shall impose on each Sub-processor, by written contract, data protection obligations no less protective than those in this Agreement.
- 6.5 Credible Brands remains responsible to the Customer for the performance of each Sub-processor's obligations.

7. Location and international transfers

- 7.1 Credible Brands operates servers in **Zimbabwe, South Africa** and the **United Kingdom**. The location of the Customer's Services is shown in its order or client area, and Customer Personal Data is stored in that location and in the backup location described in Annex A.

- 7.2 Credible Brands shall not move the Customer's Services to a different country without notifying the Customer in advance, except temporarily where needed to restore the Services after a failure.
- 7.3 Where Customer Personal Data is stored or processed outside Zimbabwe, Credible Brands shall transfer it only where an adequate level of protection is ensured in the recipient country, or where an exception in section 29 of the Act applies, as required by section 28 of the Act.
- 7.4 The Parties record that South Africa (Protection of Personal Information Act, 2013) and the United Kingdom (UK GDPR and Data Protection Act 2018) have comprehensive data protection laws. Credible Brands shall also bind its Sub-processors in those countries to written data protection terms.
- 7.5 The Customer is responsible for choosing a Service location appropriate to its own legal obligations, including any restriction the Authority places on transferring particular categories of data.

8. Personal Data Breaches

Credible Brands shall notify the Customer without undue delay, and in any event **within 12 hours**, after becoming aware of a Personal Data Breach. This gives the Customer time to meet its own duty under section 19 of the Act to notify the Authority within 24 hours.

- 8.2 The notice shall be sent to the Customer's account email address and shall describe, as far as then known: (a) the nature of the breach, including the categories and approximate number of data subjects and records concerned; (b) the likely consequences of the breach; (c) the measures taken or proposed to contain it and reduce its effects; and (d) a contact person at Credible Brands for further information.
- 8.3 Where information is not available at first, Credible Brands shall provide it in stages as it becomes available.
- 8.4 Credible Brands shall take reasonable steps to contain and investigate the breach, and shall cooperate with the Customer and the Authority.
- 8.5 Credible Brands shall not notify the Customer's data subjects directly unless the Customer instructs it to or the law requires it.
- 8.6 Notice of a breach is not an admission of fault or liability by Credible Brands.

9. Data subject requests

- 9.1 If Credible Brands receives a request from a data subject relating to Customer Personal Data, it shall forward the request to the Customer within 5 business days and shall not respond to it directly, unless authorised by the Customer.
- 9.2 Taking into account the nature of the processing, Credible Brands shall provide reasonable assistance to help the Customer respond to requests to access, correct, delete or object to the processing of personal data.

- 9.3 In most cases the Customer can carry out these actions itself through the control panel and client area. Where Credible Brands' assistance goes beyond that, it may charge its standard support rates, agreed in advance.

10. Information and audits

- 10.1 On written request, Credible Brands shall provide the Customer with the information reasonably necessary to demonstrate compliance with this Agreement, such as a written summary of its security measures or completed security questionnaires.
- 10.2 Where that information is not sufficient, or where the Authority requires it, the Customer may carry out an audit, by itself or through an independent auditor bound by confidentiality, on at least 30 days' written notice.
- 10.3 Audits shall take place during business hours, no more than once in any 12-month period (unless following a Personal Data Breach or required by the Authority), and without access to other customers' data or to infrastructure in a way that could affect its security.
- 10.4 Each Party bears its own costs of an audit.

11. Return and deletion

- 11.1 During the term of the Services, the Customer can download or export Customer Personal Data at any time using the control panel and backup tools. Credible Brands keeps backups of Customer Personal Data only where the Customer subscribes to a backup plan.
- 11.2 When the Services end, the Customer has **14 days** to export its data, unless the Services were terminated for non-payment or abuse under the Service Agreement.
- 11.3 After that period, Credible Brands shall delete Customer Personal Data from its active systems. Copies in backups shall be overwritten in the normal backup cycle, and in any event within **30 days**.
- 11.4 Credible Brands may keep Customer Personal Data longer only where required by law. In that case this Agreement continues to apply to that data until it is deleted.
- 11.5 On request, Credible Brands shall confirm deletion in writing.

12. General

- 12.1 **Liability.** Each Party's liability under this Agreement is subject to the limitations of liability in the Service Agreement, except to the extent the Act does not allow liability to be limited.
- 12.2 **Precedence.** If this Agreement conflicts with the Service Agreement in relation to the processing of Customer Personal Data, this Agreement prevails.
- 12.3 **Changes in law.** Credible Brands may update this Agreement to comply with changes to the Act or guidance from the Authority, by giving the Customer at least 30 days' notice. Any other amendment must be agreed in writing by both Parties.

- 12.4 **Term.** This Agreement takes effect when the Customer accepts the Service Agreement or signs this Agreement, and ends when Credible Brands no longer processes any Customer Personal Data. Clauses 5.4 (confidentiality) and 11 (return and deletion) survive termination.
- 12.5 **Severability.** If any provision is found invalid, the rest of this Agreement remains in force.
- 12.6 **Governing law.** This Agreement is governed by the laws of the Republic of Zimbabwe.
- 12.7 **Disputes.** The Parties shall first try to resolve any dispute through good-faith negotiation. Disputes not resolved within 30 days shall be referred to the courts of Zimbabwe. This does not prevent either Party from complaining to the Authority.
- 12.8 **Notices.** Notices to Credible Brands under this Agreement shall be sent to its Data Protection Officer at dpo@crediblebrands.co.zw. Notices to the Customer shall be sent to the email address on its client account.

ANNEX A: DETAILS OF PROCESSING

Item	Details
Services	Shared and reseller web hosting, WordPress and Windows (ASP.NET) hosting, VPS hosting, business email hosting, domain DNS hosting, website backups, and any related services ordered by the Customer.
Purpose of processing	Providing the Services under the Service Agreement: hosting, storing, transmitting and backing up the Customer's websites, databases, files and email.
Nature of processing	Storage, hosting, transmission, backup, restoration, security scanning (malware and spam), monitoring of server performance, and deletion.
Categories of data subjects	The Customer's staff and representatives; the Customer's clients and their representatives; the Customer's suppliers and other partners and their representatives; visitors to and users of the Customer's websites and applications; senders and recipients of email to and from the Customer's mailboxes; and any other persons whose personal data the Customer stores on the Services.
Categories of personal data	Names; email addresses; telephone numbers; postal addresses; photographs and other images; account usernames and passwords stored in the Customer's applications; IP addresses and website access logs; email content and attachments; and any other personal data the Customer chooses to store on the Services.
Special categories of data	Not expected. If the Customer stores sensitive data (such as health, financial, biometric or children's data), it is responsible for assessing whether the Services' security measures are adequate and for any additional safeguards required.
Frequency	Continuous, for the duration of the Services.
Duration and retention	For the term of the Services, plus the 14-day export period and up to 30 days for backups to be overwritten (clause 11).
Storage and backup location	The data centre location shown in the Customer's order or client area: Zimbabwe, South Africa or the United Kingdom. Details of where backups of a particular service are kept are available on request.

ANNEX B: SUB-PROCESSORS

A list of Credible Brands' authorised Sub-processors is available on request from dpo@crediblebrands.co.zw.

ANNEX C: SECURITY MEASURES

Credible Brands maintains the following technical and organisational measures, which it may update from time to time provided the overall level of protection is not reduced.

Area	Measures
Access control	Administrative access limited to authorised staff on a need-to-know basis; individual accounts; strong passwords and two-factor authentication on control panels and administrative systems; access removed promptly when staff leave.
Account isolation	Each hosting account isolated from others (CloudLinux LVE / CageFS on shared servers); resource limits to contain abuse.
Encryption	TLS/HTTPS for the website, client area and control panels; free SSL certificates available for Customer websites; passwords stored hashed.
Network and server security	Firewalls; intrusion and brute-force protection; malware scanning and web application protection (Imunify360); regular operating system and software security updates.
Backups and availability	Automated backups for Services covered by a Credible Host backup plan, with the ability to restore data; self-service backup tools in the control panel for all hosting accounts; monitoring of server availability and performance; redundant power and connectivity at data centres.
Physical security	Servers housed in professionally operated data centres with controlled physical access, CCTV, fire suppression and environmental controls.
Logging and monitoring	Security and access logs retained for up to 90 days to detect and investigate incidents.
People	Confidentiality obligations for all staff and contractors; data protection training; a designated Data Protection Officer.
Incident response	Documented process for detecting, containing, investigating and notifying Personal Data Breaches within the times in clause 8.
Secure deletion	Deletion of Customer Personal Data at the end of the Services and secure disposal of storage media in line with clause 11.

Signatures

Customers who accept the Credible Host Terms of Service online accept this Agreement as part of them, without needing to sign it. Where a signed copy is required, the Parties sign below.

For the Data Controller (Customer)

For the Data Processor (Credible Brands)

Organisation

Credible Brands (Credible Host)

Organisation

Full name

Full name

Title

Title

Signature

Signature

Date

Date

— END OF DOCUMENT —