



DATA PRIVACY & CLOUD STORAGE CONSENT AGREEMENT

CONNECT ME NOW TECH SOLUTIONS

Document Version 3.0 — Effective 22 July 2026

This Data Privacy & Cloud Storage Consent Agreement ("Agreement") governs the collection, processing, international transfer, and secure storage of personal information provided by the Customer to **Connect Me Now Tech Solutions** ("the Company"). By executing this document or electronically acknowledging its terms, the Customer grants explicit, informed consent for their data to be managed under the strict security protocols and regulatory frameworks outlined below. This consent may be withdrawn at any time in the manner described in Section 8, without affecting the lawfulness of any processing carried out before such withdrawal.

1. CLOUD ARCHITECTURE & AWS DATA STORAGE

To eliminate the inherent vulnerabilities of physical hardware theft, localized server failures, or unencrypted on-premise network breaches, the Company minimizes local machine storage. All Customer personal information, operational profiles, system logs, and transactional data are securely uploaded, hosted, and processed via Amazon Web Services (AWS) cloud infrastructure. Data is geographically hosted within enterprise-grade, highly resilient AWS data center regions, establishing a redundant environment engineered for high availability and absolute threat isolation.

2. AWS RIGOROUS SECURITY STANDARDS

The Company operates under the AWS "Shared Responsibility Model" to deliver enterprise-grade data security. The underlying physical and network infrastructure layers provided by AWS fulfill the world's most stringent international security benchmarks, ensuring that customer infrastructure is structurally shielded against external threats. These standards include:

- **ISO/IEC 27001:** The gold-standard international framework for Information Security Management Systems (ISMS).
- **ISO/IEC 27017 & 27018:** Specific codes of practice governing advanced cloud security controls and the strict protection of Personally Identifiable Information (PII) in public clouds.
- **SOC 1, SOC 2, and SOC 3:** Independent third-party audit reports verifying rigorous, continuous operational controls over information security, availability, and confidentiality.
- **PCI DSS Level 1:** Compliance with the highest global payment card industry security standards for handling transaction-critical and financial information.

3. PURPOSES OF PROCESSING & CATEGORIES OF DATA COLLECTED

The Company collects and processes only the following categories of Customer information: identity and contact details (names, job titles, telephone numbers, email addresses); business information (company name, logo, website, and social media links); profile media voluntarily supplied by the Customer for display on their digital profile (including photographs and promotional material); order and delivery information (products, quantities, finishes, and shipping addresses); and billing and payment records.

This data is processed exclusively for the following purposes: the creation, hosting, and maintenance of the Customer's digital profile; the design and production of physical smart cards; order fulfilment and delivery; billing and payment administration; administration of the two (2) year digital profile license, including renewal notification; the provision of customer and technical support; and compliance with legal obligations. **The Company does not use Customer data for third-party marketing, advertising, or profiling purposes.**

4. DATA PROCESSORS, RECIPIENTS & CROSS-BORDER LEGAL BASIS

In addition to AWS cloud hosting, the Company engages vetted third-party service providers to operate its platform, each processing data strictly for defined service functions: order and form capture (Tally), productivity and electronic mail services (Google), customer relationship management (HubSpot), invoicing and financial administration (Zoho), workflow automation (Zapier), and web, DNS, and email routing infrastructure (Cloudflare). These providers process data on infrastructure located outside Zimbabwe and are bound by their own published security and data processing terms, including encryption of data in transit and at rest. The Company does not sell, rent, or otherwise disclose Customer data to any third party outside of these service functions.

Cross-border transfers of Customer data are conducted on the dual statutory grounds recognized under the Data Protection Act [Chapter 12:07]: (a) the Customer's unambiguous consent granted under this Agreement, and (b) the necessity of such transfers for the performance of the service contract between the Customer and the Company.

5. FULFILMENT OF THE DATA PROTECTION ACT OF ZIMBABWE [CHAPTER 12:07]

As an organization fully aligned with the statutory mandates enforced by the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), the Company ensures that cloud data handling satisfies all local legal obligations:

- **Cross-Border Transfer Compliance (Section 28):** This Agreement serves as the formal statutory disclosure informing the Customer that their data resides on offshore cloud infrastructure. The AWS host environment provides a structural level of privacy and technical protection that matches or exceeds the requirements mandated under Zimbabwean law.
- **Technical Security Measures (Section 19):** In strict compliance with the Act, the Company implements mandatory cryptographic controls including Advanced Encryption Standard (AES-256) for data at rest, Secure Sockets Layer / Transport Layer Security (SSL/TLS) protocols for data in transit, and continuous programmatic logging via AWS CloudTrail to track all data access points.
- **Incident Response Protocols:** The Company maintains real-time structural mechanisms to report any critical infrastructure anomalies to POTRAZ within twenty-four (24) hours, and to the affected Customer within seventy-two (72) hours as legally dictated.

6. UTMOST CONFIDENTIALITY & PRIVACY ASSURANCES

The cornerstone of the Company's operational philosophy is the absolute confidentiality of Customer profiles:

- **Data Minimization:** Ingestion of information is strictly limited to parameters necessary to fulfill digital service execution, platform operations, and system optimization.
- **Zero Unauthorized Access:** Structural access controls prevent remote or physical access to unencrypted customer files by third parties or internal personnel, except where explicitly authorized by the Customer for technical support.

7. DATA RETENTION

Customer data is retained for the duration of the active digital profile license, plus a period of twelve (12) months following its expiry to facilitate license renewal, after which it is securely deleted or irreversibly anonymized. Data may be retained for longer periods only where required by mandatory statutory retention obligations, including tax and accounting laws.

8. DATA SUBJECT RIGHTS

The Customer retains the following rights under Zimbabwean law, exercisable at any time by written request to the Company's official contact channels, and actioned within the periods prescribed by law:

- **Access:** to obtain confirmation of, and access to, the personal data held about them.
- **Rectification:** to have inaccurate or incomplete data corrected or updated.
- **Blocking:** to restrict the processing of their data pending resolution of a dispute or verification.
- **Erasure:** to have their records completely deleted from the cloud infrastructure, subject to mandatory statutory retention laws.
- **Objection:** to object to the processing of their data on legitimate grounds.
- **Withdrawal of Consent:** to withdraw the consent granted under this Agreement at any time, without affecting the lawfulness of processing carried out prior to withdrawal.

The Customer further retains the right to lodge a complaint with the Data Protection Authority, being the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ).

9. CHILDREN'S DATA & AUTOMATED DECISION-MAKING

The Company's products and services are directed at businesses and persons aged eighteen (18) years and above, and the Company does not knowingly collect the personal data of children. Where a data subject is under the age of eighteen (18), processing shall occur only with the consent of a competent person as defined under the Act. The Company does not take any decision producing legal or similarly significant effects concerning a data subject based solely on automated processing of data.

10. CUSTOMER ACKNOWLEDGMENT AND EXPRESS CONSENT

By clicking agree below, the Customer acknowledges that they have read, fully understood, and granted explicit, informed consent to the trans-border flow, processing, and cloud storage of their personal information on securely managed cloud infrastructure under the administration of Connect Me Now Tech Solutions. This consent may be withdrawn at any time by written notice to the Company, without affecting the lawfulness of any processing carried out before such withdrawal. This Agreement is maintained under version control; the version and effective date recorded in the footer of this document form part of the Customer's consent record.