SERVERNAH CLOUD DATA PROCESSING AGREEMENT

Atlancis Technologies Limited - Version 1.0 - Effective Date: 24 February 2026 - Last Updated: 24 February 2026

Document Ref	SNH-DPA-001
Version	1.0
Effective Date	24 February 2026
Processor	Atlancis Technologies Limited t/a Servernah, 5th Floor, Top Plaza, Kindaruma Road, Nairobi, Kenya
Controller	The Customer as identified in the applicable Master Services Agreement or Order Form
Primary Legislation	Kenya Data Protection Act 2019; EU GDPR 2016/679; UK GDPR and Data Protection Act 2018
Contact	privacy@servernah.com

This Data Processing Agreement ("DPA") forms part of and is incorporated into the Master Services Agreement, Subscription Agreement, or any other written agreement governing the provision of Servernah Cloud and related services ("Agreement") between Atlancis Technologies Limited trading as Servernah ("Servernah", "Atlancis", "Processor") and the Customer ("Controller"). Defined terms not otherwise defined herein have the meanings given to them in the Agreement.

The parties acknowledge that the Controller is the Data Controller and that Servernah acts solely as a Data Processor in respect of all Personal Data processed under this DPA, except where Servernah is required by law to act as a controller, in which case Servernah shall notify the Controller unless prohibited by law.

In the event of any conflict between this DPA and the main Agreement, this DPA shall prevail with respect to the protection and processing of Personal Data.

1. Purpose and Scope

The purpose of this DPA is to set out the rights, obligations, and responsibilities of the parties with respect to the processing of Personal Data by Servernah on behalf of the Controller in connection with the provision of Servernah's software-as-a-service, cloud infrastructure, artificial intelligence, and managed services.

This DPA is designed to ensure that all Personal Data is processed in accordance with applicable data protection and privacy laws, including:

- The Kenya Data Protection Act 2019 and any regulations issued thereunder
- The EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
- The UK GDPR and Data Protection Act 2018
- Any other data protection or privacy legislation applicable to the processing of Personal Data under the Services

This DPA applies to all processing of Personal Data carried out by Servernah on behalf of the Controller, whether through the Servernah Cloud and AI platform, APIs, support and monitoring activities, or any other service or functionality provided by Servernah under the Agreement.

2. Categories of Data

In the course of providing the Servernah Cloud and related services, Servernah may process the following categories of Personal Data on behalf of the Controller. The specific categories processed will depend on the nature of the Services used and the configuration of the Controller's account.

2.1 Standard Personal Data

Full names, email addresses, country of origin, telephone numbers

- Usernames and account identifiers
- Job titles and employer details
- Business contact information and customer reference numbers

2.2 Financial and Transactional Data

- Payment references and billing records
- Transaction identifiers
- Bank account references (tokenised or masked where applicable)
- Invoicing and settlement data

Servernah does not store full card details. Payment card data is processed exclusively by iPay Africa under PCI-DSS compliant arrangements. Servernah receives only transaction confirmation and reference data.

2.3 Technical and Usage Data

- IP addresses, device identifiers, login and authentication logs
- Session data, system and application logs, audit trails
- Performance and telemetry data

2.4 Customer Content

This includes any data uploaded, stored, transmitted, or processed by the Controller or its users through the Servernah platform, including documents, databases, images, audio or video, structured and unstructured data, and AI inputs and outputs.

2.5 Special Categories of Data

Servernah does not intentionally process special categories of Personal Data (such as health data, biometric data, racial or ethnic origin, or criminal records) unless the Controller chooses to upload such data and has obtained all legally required consents and approvals. Where special category data is processed, it shall be subject to enhanced security and access controls agreed with the Controller in advance.

3. Categories of Data Subjects

Servernah may process Personal Data relating to the following categories of Data Subjects, depending on the Controller's use of the Services:

Category	Examples
CONTROLLER PERSONNEL	Employees, directors, contractors, consultants, temporary staff and agents
CONTROLLER END-USERS	Users authorised by the Controller to access the Servernah platform, including administrators and support users
CONTROLLER CLIENTS AND BUSINESS CONTACTS	Customers, subscribers, account holders, prospects, vendors, suppliers, and partners of the Controller
THIRD PARTIES IN CONTROLLER DATA	Individuals whose data is contained in documents, communications, logs, or records uploaded by the Controller; individuals referenced in AI inputs, datasets, or system records

The Controller is responsible for ensuring that all Data Subjects whose Personal Data is processed through the Servernah platform have been provided with all legally required privacy notices and that any necessary consents or lawful bases for processing have been obtained.

4. Processing Activities

Servernah shall process Personal Data on behalf of the Controller solely for the purpose of providing, maintaining, and improving the Servernah cloud, AI, and managed services in accordance with this DPA, the Agreement, and the Controller's documented instructions.

4.1 Core Processing Activities

- Hosting, storing, and backing up Controller Data
- Ingesting, indexing, analysing, and retrieving data for cloud workloads
- Processing data for application functionality, automation, and analytics
- Managing user access, authentication, and permissions
- Logging, monitoring, and auditing platform activity
- Incident detection, troubleshooting, and technical support
- Data replication and failover for business continuity and disaster recovery
- Performance optimisation, testing, and quality assurance
- Security monitoring, vulnerability detection, and threat response

4.2 AI and Automated Processing

Where Servernah provides artificial intelligence, machine learning, or automated decision-support functionality, processing activities may include pattern recognition, classification, predictive analytics, automated data extraction, tagging and enrichment, and generating outputs based on Controller inputs.

Servernah shall not use Controller Data to train general-purpose AI models for the benefit of other customers without the Controller's explicit written consent.

4.3 Support and Professional Services

Servernah may process Personal Data for customer onboarding and migration, configuration and deployment, ongoing technical support, performance tuning, and incident resolution. Such processing shall be limited to what is strictly necessary to provide the requested services.

4.4 Compliance and Legal Processing

Servernah may process Personal Data to comply with applicable legal obligations, respond to lawful requests from regulators or law enforcement, enforce contractual rights, and detect, prevent, or investigate fraud, security incidents, or abuse.

4.5 Geographic Scope of Processing

All primary processing occurs in Kenya, hosted at iX Africa Limited and Africa Data Centers (ADC) in Nairobi. Processing may also occur in other jurisdictions where Servernah's authorised sub-processors operate, subject to the safeguards set out in Clause 7.

5. Technical and Organisational Measures

Servernah shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including the nature, scope, context, and purposes of processing and the risks of varying likelihood and severity for the rights and freedoms of Data Subjects.

Security Domain	Measures in Place
GOVERNANCE	Formal Information Security Management System (ISMS); documented security policies; defined data protection roles and accountability; regular risk assessments
ACCESS CONTROL	Role-based access control (RBAC); least-privilege access principles; multi-factor authentication (MFA) for administrative access; secure credential management; logging of all privileged activity
ENCRYPTION	AES-256 encryption at rest; TLS 1.3 encryption in transit; secure key management procedures
INFRASTRUCTURE SECURITY	Segmented network architectures; firewalls; intrusion detection and prevention systems (IDS/IPS); DDoS mitigation; continuous infrastructure monitoring
VULNERABILITY MANAGEMENT	Regular vulnerability scanning and penetration testing; timely security patching; tracked remediation of identified weaknesses
DATA SEGREGATION	Customer Data logically separated from other customers through tenant isolation, RBAC, and architectural controls
BACKUP AND CONTINUITY	Regular encrypted backups (Ceph, Veeam, AWS S3); disaster recovery and failover mechanisms; periodic testing of BCP and DRP
INCIDENT RESPONSE	24/7 security monitoring and alerting; documented incident response procedures; breach investigation and containment process
PERSONNEL SECURITY	Staff bound by confidentiality obligations; mandatory security awareness and data protection training; immediate access revocation upon role change or termination
PHYSICAL SECURITY	Controlled physical access at colocation facilities; surveillance, logging, and visitor management; environmental controls and fire suppression

6. Sub-Processors

6.1 Engagement of Sub-Processors

Servernah may engage third-party sub-processors to perform specific processing activities on behalf of the Controller in connection with the Services. Servernah remains fully responsible for the acts and omissions of its sub-processors as if they were Servernah's own.

6.2 Current Sub-Processors

SUB-PROCESSOR	SERVICE	LOCATION	DATA PROCESSED
iPay Africa	Payment processing	Kenya	Payment transaction references; billing confirmation
Microsoft (Microsoft 365)	Business communications	USA / Ireland	Internal email and communications
Odoo ERP	Finance and CRM	Belgium / EU	Billing records and account data
SendGrid (Twilio)	Transactional email delivery	USA	Email address and notification content
Amazon Web Services (S3)	Offsite encrypted backup storage	Kenya / South Africa	Encrypted backup data (opaque; no readable personal data)

SUB-PROCESSOR	SERVICE	LOCATION	DATA PROCESSED
iX Africa Limited	Primary colocation	Kenya	Infrastructure only; no direct personal data access
Africa Data Centers (ADC)	Secondary colocation	USA / Ireland	Infrastructure only; no direct personal data access

Servernah will maintain an up-to-date sub-processor register and make it available to the Controller on request at privacy@servernah.com.

6.3 Sub-Processor Obligations

Each sub-processor is contractually bound to implement appropriate technical and organisational measures to protect Personal Data in accordance with this DPA and applicable data protection law. Sub-processors shall process Personal Data solely on documented instructions from Servernah and, by extension, the Controller.

6.4 New Sub-Processors

Servernah shall provide the Controller with at least 30 days' prior written notice before engaging any new sub-processor. The Controller may object to a new sub-processor on reasonable data protection grounds within 14 days of receiving notice. If no objection is received, the Controller is deemed to have consented to the new sub-processor.

6.5 Liability for Sub-Processors

Servernah shall remain fully liable to the Controller for the performance of any sub-processor's obligations under this DPA. Any breach or failure by a sub-processor shall be deemed a breach by Servernah.

7. International Transfers

Servernah's primary data residency commitment is that all Controller workload data is stored and processed within Kenya. Where limited cross-border data flows arise through sub-processors (as set out in Clause 6.2), Servernah shall ensure the following safeguards are in place:

TRANSFER MECHANISM	DESCRIPTION	WHEN APPLIED
Standard Contractual Clauses (SCCs)	EU Commission-approved contractual obligations binding the recipient to GDPR-equivalent protections	Transfers to Microsoft 365, SendGrid (USA)
Data Processing Agreement	Contractual obligations including processor requirements, security measures, and sub-processing restrictions	All sub-processors
AES-256 Encryption	All data transferred offsite is encrypted at rest and in transit; backup data is processed as opaque encrypted blobs	AWS S3 offsite backup
EU Adequacy Framework	Processing within the EU/EEA is subject to GDPR protections which the EU Commission has found to be adequate	Odoo ERP (Belgium/EU)

Servernah shall notify the Controller of any material changes to the countries in which Personal Data is processed or transferred prior to the commencement of such processing, to allow the Controller to object on reasonable data protection grounds.

Where required by applicable law, Servernah shall assist the Controller in carrying out any Data Protection Impact Assessment (DPIA) or prior consultation with relevant supervisory authorities regarding transfers to third countries.

8. Data Subject Rights

8.1 Support for Controller Requests

Servernah shall, to the extent technically feasible and legally permissible, assist the Controller in responding to requests from Data Subjects to exercise their rights under applicable data protection law, including rights of access, rectification, erasure, restriction of processing, data portability, objection to processing, and withdrawal of consent.

8.2 Controller Responsibility

The Controller shall be responsible for receiving, validating, and determining the appropriate response to Data Subject requests. Servernah shall act only on documented instructions from the Controller and shall use commercially reasonable efforts to respond within timeframes enabling the Controller to comply with statutory deadlines.

8.3 Timeframes

Servernah shall acknowledge Controller instructions regarding Data Subject rights within 5 business days and provide the requested assistance within a timeframe that enables the Controller to comply with its statutory response deadline under the applicable law (21 days under the KDPA 2019; 1 month under the GDPR and UK GDPR).

8.4 Limitations

Servernah may decline to comply directly with a Data Subject request where doing so would violate applicable law, compromise the security or confidentiality of other Data Subjects' Personal Data, or fall outside the scope of the processing activities under this DPA. In such cases, Servernah shall promptly notify the Controller and provide reasonable assistance in formulating an appropriate response.

9. Personal Data Breach Notification

Servernah shall notify the Controller without undue delay, and in any event within 72 hours of becoming aware of a Personal Data Breach affecting Personal Data processed on behalf of the Controller. The notification shall include, to the extent known at the time:

- A description of the nature of the breach, including the categories and approximate number of Data Subjects and records affected
- The likely consequences of the breach
- The measures taken or proposed to address the breach and mitigate its effects
- Contact details of the Servernah representative responsible for managing the breach

9.2 Cooperation

Servernah shall provide reasonable assistance to the Controller in investigating, containing, and remediating the breach, and in fulfilling any notification obligations to Data Protection Authorities or affected Data Subjects under applicable law.

9.3 Documentation

Servernah shall maintain a written record of all Personal Data Breaches, including facts, effects, and remedial actions. This record shall be made available to the Controller upon request.

9.4 Exclusions

Notification is only required for breaches that compromise the confidentiality, integrity, or availability of Personal Data. Security incidents that do not result in unauthorised access, loss, or disclosure of Personal Data shall be logged and addressed according to internal security procedures but do not trigger the notification requirements of this Clause.

9.5 Sub-Processor Breaches

In the event a sub-processor suffers a Personal Data Breach affecting Controller Personal Data, Servernah shall take all necessary steps to ensure the sub-processor notifies Servernah without undue delay, enabling Servernah to fulfil its obligations under this Clause.

10. Retention and Deletion

10.1 Retention

Servernah shall retain Personal Data processed on behalf of the Controller only for as long as necessary to provide the Services, comply with legal obligations, or enforce the terms of the Agreement.

10.2 Deletion on Termination

Upon termination or expiration of the Agreement, or upon the Controller's documented instruction, Servernah shall, at the Controller's election, either delete all Personal Data or return it to the Controller, unless retention is required by applicable law.

10.3 Deletion Procedures

Deletion shall be performed using methods appropriate to the nature of the data and storage medium, including secure deletion from servers and storage devices, removal from active backups, and anonymisation of Personal Data where complete deletion is not technically feasible.

10.4 Backup Data

Temporary retention of Personal Data in encrypted backups is permitted for disaster recovery purposes. Such backup data shall be automatically deleted or rendered irreversibly anonymous within 90 days of the termination of the Agreement or upon deletion or return of the original data, whichever occurs first.

10.5 Documentation

Servernah shall maintain records of data deletion and anonymisation activities and make them available to the Controller on request to demonstrate compliance with this Clause.

10.6 Legal Retention Exceptions

If applicable law requires retention of specific Personal Data beyond the periods stated above, Servernah shall inform the Controller and retain only the minimum necessary data to comply with such obligations, while maintaining security measures consistent with Clause 5.

11. Audit Rights

11.1 Right to Audit

The Controller has the right, upon reasonable notice, to conduct audits or inspections of Servernah's operations, systems, and facilities as they relate to the processing of Personal Data under this DPA. Audits may be conducted directly by the Controller or through a qualified independent auditor.

11.2 Scope

Audits may include review of technical and organisational measures (Clause 5), sub-processor agreements (Clause 6), Personal Data retention and deletion practices (Clause 10), breach notification and incident response processes (Clause 9), and measures to assist with Data Subject rights requests (Clause 8).

11.3 Frequency and Notice

Routine audits may be conducted no more than once per calendar year unless otherwise required by law or regulation. Servernah shall be provided with at least 30 days' prior written notice specifying the scope, objectives, and expected duration of the audit.

11.4 Cooperation

Servernah shall provide reasonable assistance during the audit, including access to relevant documentation, policies, systems, and personnel involved in processing.

11.5 Confidentiality

Any information obtained during the audit shall be treated as strictly confidential by the Controller and appointed auditors and shall not be disclosed except as necessary to demonstrate compliance with applicable data protection law or this DPA.

11.6 Corrective Actions

Servernah shall review audit findings and, where necessary, implement corrective actions to address identified deficiencies. The Controller shall be informed of remediation steps within a reasonable timeframe.

11.7 Costs

Routine audits shall be conducted at the Controller's expense. If a material breach of this DPA is identified, Servernah shall bear the reasonable costs of any additional audit required to verify remediation.

12. AI Processing

12.1 Prohibition on General-Purpose AI Training

Servernah shall not use any Personal Data or Controller Content for the training, development, or improvement of general-purpose AI models or services for the benefit of any third party without the Controller's explicit prior written consent.

12.2 Permitted AI Processing

Servernah may process Controller Data using AI or automated tools solely to provide, maintain, and improve the Services, including generating outputs in response to Controller inputs, automated analysis and enrichment necessary for the functionality of the Service, and pattern recognition or predictive analytics directly related to the Controller's use of the Services.

12.3 Transparency and Control

Servernah shall provide the Controller with clear documentation of AI processing activities affecting Controller Data and the ability to control, configure, or opt out of AI-based processing features where technically feasible.

12.4 Data Protection Measures

All AI processing of Personal Data shall comply with the technical and organisational measures outlined in Clause 5 and shall ensure that outputs do not unintentionally expose or disclose Personal Data to other customers or third parties.

12.5 Ownership of Outputs

Servernah shall not claim ownership of Controller Content or AI-generated outputs derived from Controller Data. All rights in Controller Content and outputs remain with the Controller, subject to the licence granted to Servernah to provide the Services.

12.6 Special Categories of Data

If special categories of Personal Data are processed using AI, Servernah shall ensure that such processing occurs only after the Controller has obtained all legally required consents and approvals from Data Subjects.

13. Liability

13.1 Processor Responsibility

Servernah shall be liable for any breach of its obligations under this DPA, including those relating to compliance with applicable data protection laws, implementation of technical and organisational measures, engagement and oversight of sub-processors, international transfers, support for Data Subject rights, breach notification, retention and deletion, and AI processing activities.

13.2 Extent of Liability

Servernah's liability under this DPA shall be limited to direct damages suffered by the Controller as a result of Servernah's breach of its obligations. Servernah shall not be liable for indirect, incidental, or consequential damages, loss of profits or business opportunities, or damages arising from the Controller's own failure to comply with applicable data protection laws or its obligations under the Agreement.

13.3 Mitigation

Both parties shall take reasonable steps to mitigate any damages arising from a breach of this DPA. Servernah shall use reasonable efforts to remediate any breach and prevent recurrence.

13.4 Sub-Processor Liability

Servernah shall remain fully liable for the acts and omissions of any sub-processor engaged under Clause 6 as if such acts or omissions were carried out by Servernah itself.

13.5 Force Majeure

Servernah shall not be liable for any failure or delay in performing its obligations under this DPA to the extent such failure is caused by events beyond its reasonable control, including natural disasters, acts of government, or network or service outages not caused by Servernah's negligence.

14. Governing Law and Dispute Resolution

14.1 Governing Law

This DPA and any disputes arising out of or in connection with it shall be governed by and construed in accordance with the laws of Kenya, without regard to its conflict of laws principles, unless the parties have expressly agreed otherwise in writing.

14.2 Dispute Resolution

The parties shall use good faith efforts to resolve any dispute arising under this DPA amicably within 30 days of written notice. If a resolution cannot be reached within that period, the dispute shall be submitted to the competent courts of Kenya, unless otherwise agreed by the parties.

14.3 Compliance with Local Laws

Nothing in this DPA shall relieve either party from obligations to comply with applicable data protection, privacy, or other relevant laws of jurisdictions in which Personal Data is processed.

Execution

FOR AND ON BEHALF OF THE PROCESSOR	FOR AND ON BEHALF OF THE CONTROLLER
ATLANCIS TECHNOLOGIES LIMITED T/A SERVERNAH	
Authorised Signatory: Name: Title: Date:	Authorised Signatory: Name: Title: Date: