SERVERNAH CLOUD CROSS-BORDER DATA TRANSFER & INTERNATIONAL DATA TRANSFER POLICY

Atlancis Technologies Limited - Version 2.0 - Effective Date: 24 February 2026 - Last Updated: 24 February 2026

Document Ref	SNH-CBT-001
Version	1.0
Effective Date	24 February 2026
Data Controller	Atlancis Technologies Limited, 5th Floor, Top Plaza, Kindaruma Road, Nairobi, Kenya
Contact	privacy@servernah.com
Primary Jurisdiction	Republic of Kenya
Applicable Law	Kenya Data Protection Act 2019; EU GDPR (where applicable); applicable international frameworks

1. Purpose and Scope

This Cross-Border Data Transfer and International Data Transfer Policy ("Policy") sets out the rules and safeguards Atlancis Technologies Limited ("Atlancis", "Servernah", "we", "us") applies whenever personal data is transferred or made accessible across international borders in connection with the Servernah Cloud platform.

Servernah's core operating principle is data sovereignty: all customer workloads and the personal data processed in delivering Servernah Services are stored and processed within Kenya. This Policy exists to document the limited circumstances in which cross-border data flows do or may occur, the legal bases and safeguards that govern them, and the obligations of Servernah and its customers in those scenarios.

This Policy applies to:

- Personal data of Servernah customers, users, and prospective customers processed by Atlancis in its capacity as Data Controller
- Customer Data processed by Atlancis in its capacity as Data Processor on behalf of enterprise customers under a Data Processing Agreement (DPA)
- Personal data shared with or accessible by Servernah's sub-processors and third-party service providers
- Enterprise customers and their users who may themselves transfer data internationally using Servernah infrastructure

This Policy should be read alongside the Servernah Privacy Policy, Terms of Service, and any applicable Master Service Agreement (MSA) or Data Processing Agreement (DPA).

2. Servernah's Data Residency Position

Core Commitment

All Servernah customer workloads, data, and the personal data Atlancis processes as Data Controller are hosted and processed within Kenya, at our colocation facilities at iX Africa Limited and Africa Data Centers (ADC), both in Nairobi. We do not route, replicate, or store customer data outside Kenya as part of our standard service delivery.

This commitment to Kenyan data residency is a fundamental design principle of the Servernah platform, driven by:

- Compliance with the Kenya Data Protection Act 2019 (KDPA 2019), in particular Section 48 on cross-border transfer restrictions
- Servernah's certification and registration with the Office of the Data Protection Commissioner (ODPC) of Kenya
- The data sovereignty requirements of our enterprise customers in regulated industries including government, healthcare, and financial services
- Our commitment to keeping Kenyan data within Kenyan jurisdiction as a competitive and compliance differentiator

3. When Cross-Border Data Transfers Occur

Despite our data residency commitment, certain limited and unavoidable cross-border data flows do occur. These are documented below with the applicable legal basis and safeguards.

3.1 Third-Party Service Providers (Sub-Processors)

Some of our third-party service providers operate systems in jurisdictions outside Kenya. When Atlancis uses such providers, it may involve limited cross-border processing of personal data. The following table documents these flows:

PROVIDER	COUNTRY	DATA TRANSFERRED	PURPOSE	LEGAL BASIS & SAFEGUARD
Microsoft (Microsoft 365)	USA / EU (Microsoft global)	Email content, business communications	Business email and internal collaboration	Microsoft Data Processing Agreement; EU Standard Contractual Clauses (SCCs); KDPA Section 48 safeguards
SendGrid (Twilio)	USA	Recipient email address, message metadata	Transactional and service email delivery	SendGrid Data Processing Addendum; SCCs; minimal data - no customer content
iPay Africa	Kenya (primary); processor networks may be international	Payment transaction reference, fraud signals	Credit top-up payment processing	iPay DPA; card network compliance (PCI-DSS); no payment card data stored by Atlancis
Odoo ERP	Belgium (Odoo SA) / configurable hosting	Billing records, customer account information	Finance, invoicing, and CRM	Odoo DPA; SCCs where applicable; Atlancis evaluates hosting location for KDPA compliance
GitHub / Code Repositories	USA (Microsoft)	No personal data - infrastructure code only	Platform development and deployment pipelines	No personal data transferred; not subject to KDPA cross-border rules

3.2 Enterprise Customers Using Servernah to Transfer Data Internationally

Enterprise customers who use Servernah infrastructure to process, store, or transmit data that they subsequently transfer internationally are acting as Data Controllers in respect of that transfer. In such cases:

- Atlancis's role is that of Data Processor, and Atlancis has no independent legal basis to restrict or authorise such transfers
- The customer is responsible for ensuring their international transfers comply with KDPA 2019 Section 48, EU GDPR Article 46, or any other applicable data transfer restrictions
- Atlancis will cooperate with customers to provide documentation of its technical and security controls to support the customer's transfer impact assessments or due diligence requirements
- Enterprise customers who require Atlancis to configure Servernah infrastructure specifically to facilitate compliant international transfers should raise this requirement with their Account Manager

4. Legal Framework for Cross-Border Transfers

4.1 Kenya - KDPA 2019 (Primary Governing Law)

The primary legal framework governing Atlancis's cross-border data transfers is the Kenya Data Protection Act 2019. Section 48 of the KDPA 2019 restricts the transfer of personal data outside Kenya unless at least one of the following conditions is met:

Transfer Basis	Description
ADEQUATE PROTECTION	The destination country has been determined by the ODPC to provide adequate data protection - analogous to EU adequacy decisions
APPROPRIATE SAFEGUARDS	The transfer is subject to appropriate safeguards such as contractual clauses, binding corporate rules, or approved codes of conduct
EXPLICIT CONSENT	The data subject has explicitly consented to the proposed transfer after being informed of its risks
CONTRACTUAL NECESSITY	The transfer is necessary for the performance of a contract between the data subject and the controller, or for pre-contractual measures
LEGAL OBLIGATION	The transfer is necessary for compliance with a legal obligation to which the controller is subject

Transfer Basis	Description
VITAL INTERESTS	The transfer is necessary to protect vital interests of the data subject or another person
PUBLIC INTEREST	The transfer is necessary for reasons of substantial public interest

For all Atlancis sub-processor transfers described in Section 3.1, we rely primarily on appropriate safeguards (basis 2) in the form of contractual data processing agreements and, where relevant, EU Standard Contractual Clauses which are recognised as analogous safeguards under the KDPA 2019 framework.

4.2 EU General Data Protection Regulation (GDPR)

Servernah's primary customer base is in Kenya and Africa. However, where Servernah processes the personal data of individuals located in the European Economic Area (EEA) - for example, where a Kenyan company has European employees or customers - the EU GDPR may apply to that processing.

When Does GDPR Apply to Servernah?

The GDPR applies extraterritorially where Atlancis (a) offers services to individuals in the EU/EEA regardless of where processing takes place, or (b) monitors the behavior of individuals in the EU/EEA. If your use of Servernah involves processing personal data of EU/EEA residents, you should ensure your MSA or DPA with Atlancis addresses GDPR compliance requirements, including the inclusion of EU Standard Contractual Clauses.

4.2.1 Transfer Mechanisms Under GDPR (Article 46)

Where GDPR applies to a transfer from the EU/EEA to Servernah infrastructure in Kenya (a third country without EU adequacy status), the following transfer mechanisms are available:

- Standard Contractual Clauses (SCCs): The EU Commission's 2021 SCCs for controller-to-processor transfers can be incorporated into the Atlancis DPA for enterprise customers who require GDPR-compliant transfer mechanisms. Contact cloud@servernah.com to request SCCs.
- Binding Corporate Rules (BCRs): Not currently implemented by Atlancis but may be considered for enterprise engagements at scale.
- Adequacy: Kenya does not currently have an EU adequacy decision. Atlancis monitors developments with the ODPC and the EU Commission in this regard.

4.2.2 Transfer Impact Assessments (TIAs)

Following the Schrems II judgment, organisations transferring personal data from the EU/EEA to third countries using SCCs should conduct a Transfer Impact Assessment (TIA) to evaluate the legal landscape and practical risks in the destination country. Atlancis can provide the following documentation to support customer TIAs:

- Description of technical and organisational security measures (encryption, access controls, audit logging)
- Information on applicable Kenyan law including government access mechanisms
- Our ODPC registration status and compliance posture
- The Servernah Data Processing Agreement and sub-processor list

To request TIA support documentation, contact privacy@servernah.com.

4.3 Other Jurisdictions

Servernah's customer base increasingly spans Africa and beyond. Below is a summary of how we approach data transfer obligations in other relevant jurisdictions:

JURISDICTION	APPLICABLE FRAMEWORK	SERVERNAH'S APPROACH
Kenya (primary)	*KDPA 2019 - Section 48*	All data stored in Kenya by default. Cross-border only as documented in this Policy.
European Union / EEA	*EU GDPR - Chapter V (Articles 44–49)*	SCCs available on request. TIA documentation available. No EU adequacy decision for Kenya at present.
United Kingdom	*UK GDPR / Data Protection Act 2018*	UK International Data Transfer Agreements (IDTAs) available on request where UK personal data is involved.

JURISDICTION	APPLICABLE FRAMEWORK	SERVERNAH'S APPROACH
East African Community (EAC)	*Emerging - various national frameworks*	Atlancis monitors regional developments. KDPA 2019 compliance is our baseline; country-specific requirements assessed on request.
Other African jurisdictions	*POPIA (South Africa); Nigeria NDPR; others*	Assessed on a case-by-case basis for enterprise customers. Contact cloud@servernah.com for a jurisdiction-specific assessment.

5. Safeguards We Apply to All Cross-Border Transfers

Regardless of the destination or legal basis, Atlancis applies the following safeguards to all cross-border transfers involving personal data:

5.1 Contractual Safeguards

- All sub-processors with whom we share personal data are bound by a Data Processing Agreement that requires them to process personal data only on Atlancis's instructions, maintain appropriate security measures, and comply with applicable data protection law
- Sub-processors are prohibited from using personal data for their own purposes or disclosing it to third parties without Atlancis's written authorisation
- Sub-processor agreements include data breach notification obligations (within 24 hours of discovery to Atlancis; Atlancis then notifies the ODPC and affected customers within 72 hours)
- EU Standard Contractual Clauses or equivalent transfer mechanisms are incorporated into sub-processor agreements where required

5.2 Technical Safeguards

- All personal data is encrypted using AES-256 at rest before any transfer outside Kenya
- All data in transit - including to and from sub-processors - is encrypted using TLS 1.3
- Access to personal data by sub-processors is limited to what is strictly necessary for the defined purpose (data minimisation)
- Servernah's infrastructure logs and monitors all data access, including access by sub-processors, through centralised audit logging

5.3 Organisational Safeguards

- Servernah maintains a live sub-processor register (see Section 3.1) that is reviewed at least annually
- Enterprise customers are notified of any new sub-processor engagement at least 14 days in advance, with the right to object
- Atlancis conducts due diligence on all sub-processors before engagement, including reviewing their security certifications and data protection posture
- Staff with access to personal data receive data protection training at least annually

6. Customer Obligations for International Transfers

If you use Servernah infrastructure to store or process personal data and you transfer, export, or otherwise make that data accessible outside Kenya, you are acting as Data Controller in respect of that transfer. You are responsible for:

- Ensuring you have a valid legal basis for the international transfer under the KDPA 2019 and any other applicable law
- Documenting your transfer mechanisms and retaining records as required by applicable law
- Conducting any required Transfer Impact Assessments before exporting data from Servernah
- Ensuring your end customers and data subjects are informed of international transfers in your own privacy notices
- Notifying Atlancis if you require specific infrastructure configuration to support compliant international transfers

Atlancis will provide reasonable cooperation and documentation to support your compliance obligations. To request support, contact privacy@servernah.com.

7. Data Subject Rights in Cross-Border Contexts

Where personal data has been transferred internationally, Servernah remains committed to honouring data subject rights under the KDPA 2019 regardless of where processing ultimately occurs. If you submit a data subject request and your data has been transferred to or processed by a sub-processor in another jurisdiction:

- Atlancis will coordinate with the relevant sub-processor to fulfil your request within the applicable timeframe (21 days under the KDPA 2019)
- You retain the right to lodge a complaint with the ODPC if you believe your rights have not been respected
- In cross-border contexts involving EU/EEA personal data, you may also be entitled to lodge a complaint with the relevant EU supervisory authority

8. Breach Notification in Cross-Border Contexts

In the event of a personal data breach involving data that has been transferred internationally or is processed by a sub-processor outside Kenya:

- The sub-processor must notify Atlancis within 24 hours of discovering the breach
- Atlancis will conduct an initial assessment within 24 hours of receiving the notification
- Atlancis will notify the ODPC within 72 hours of becoming aware of a breach that poses a risk to data subjects, in accordance with Section 43 of the KDPA 2019
- Where EU/EEA personal data is involved, the relevant EU supervisory authority must also be notified within 72 hours under the GDPR
- Affected customers will be notified promptly, with full details of the breach, impact, and remediation steps

9. Sub-Processor Management

9.1 Authorised Sub-Processors

The current list of authorised sub-processors is set out in Section 3.1 of this Policy and in the Servernah Privacy Policy. Enterprise customers may request the full sub-processor register at any time by contacting privacy@servernah.com.

9.2 New Sub-Processors

Atlancis will notify enterprise customers at least 14 days before engaging any new sub-processor that involves cross-border processing of personal data. Customers have the right to object to a new sub-processor within that 14-day period by submitting written notice to cloud@servernah.com. If an objection cannot be resolved, the customer may terminate the affected services in accordance with their MSA.

9.3 Sub-Processor Changes

Atlancis will notify customers of any material change to a sub-processor's processing activities, location, or ownership that may affect the basis for the cross-border transfer.

10. Governing Law and Updates

This Policy is governed by the laws of Kenya. Atlancis monitors developments in international data transfer law; including the ODPC's ongoing guidance under the KDPA 2019, EU adequacy decisions, and evolving frameworks across Africa and will update this Policy accordingly.
Material updates will be communicated to enterprise customers by email and via the Servernah SSP at least 14 days before taking effect. Continued use of Servernah Services after the effective date of any update constitutes acceptance of the revised Policy.

11. Contact

For questions about this Policy, to request Standard Contractual Clauses, TIA documentation, or the full sub-processor register, or to submit a data subject request relating to international processing, please contact:

DATA PROTECTION CONTACT	Atlancis Technologies Limited
EMAIL	privacy@servernah.com
ADDRESS	5th Floor, Top Plaza, Kindaruma Road, Off Ngong Road, Nairobi, Kenya
ODPC	Office of the Data Protection Commissioner — odpc.go.ke
EU SUPERVISORY AUTHORITY	For EU/EEA data subjects: relevant national data protection authority in your country of residence